UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

FACULTAD DE INGENIERIA

**PROGRAMA ACADÉMICO DE INGENIERÍA DE REDES Y
COMUNICACIONES**

**Diseño de un Sistema de Gestión de Seguridad de la Información basado en la
norma ISO/IEC 27001:2013 para la Municipalidad Distrital de El Agustino**

TESIS

Para optar el título profesional de Ingeniero de Redes y Comunicaciones

AUTOR

Monteza Mera, Lisbet Odelly (0000-0001-5841-5493)

ASESOR

Flores Solís, Fernando Rolyn (0000-0002-6105-3371)

Lima, 26 de febrero de 2019

DEDICATORIA

A Dios, a mis padres, hermanas, sobrinas y sobrinos por su amor y apoyo. A Rolando por su amistad incondicional.

RESUMEN

Este proyecto describe el diseño del Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para proteger los activos de información asociados al proceso de recaudación y fiscalización tributaria de la Municipalidad Distrital de El Agustino. Tal como sugiere la norma ISO 27001 se siguió el ciclo de Deming o PDCA y consta de las siguientes etapas: en la primera se realizó el diagnóstico inicial de la entidad con respecto a la norma ISO/IEC 27001:2013; en la segunda se estableció el contexto de la organización, definiendo los procesos, el alcance, la política de seguridad y el comité de seguridad de la información; en la tercera se siguió la metodología de análisis y gestión de riesgo bajo la norma ISO/IEC 31000 donde se identificó, clasificó y valoró los activos de información, se identificaron las amenazas y vulnerabilidades, se realizó el cálculo del impacto y del riesgo para luego realizar el plan de tratamiento de riesgos identificando los controles de la norma ISO/IEC 27002:2013; en la cuarta etapa se elaboró la Declaración de Aplicabilidad y finalmente se elaboró el documento del Manual del SGSI. Dentro de este marco el trabajo nos permitió concluir en la importancia de protección de los activos de información garantizando la confidencialidad, integridad y disponibilidad de estos.

Palabras clave: Sistema de Gestión de Seguridad de la Información; ISO/IEC 27001:2013; Gestión de Riesgos; Plan de tratamiento de riesgos.

Design of an Information Security Management System based on the ISO/IEC 27001:2013
standard for the District Municipality of El Agustino

ABSTRACT

This project describes the design of the Information Security Management System based on ISO / IEC 27001: 2013 to protect the information assets associated with the tax collection and control process of the District Municipality of El Agustino. As the ISO 27001 standard suggests, the Deming or PDCA cycle was followed and consists of the following stages: in the first one the initial diagnosis of the entity was made with respect to the ISO / IEC 27001: 2013 standard; in the second, the context of the organization was established, defining the processes, scope, security policy and information security committee; in the third, the risk analysis and management methodology was followed under the ISO / IEC 31000 standard where information assets were identified, classified and valued, threats and vulnerabilities were identified, impact and risk calculation was performed and then carry out the risk treatment plan identifying the controls of ISO / IEC 27002: 2013; in the fourth stage the Declaration of Applicability was prepared and finally the document of the ISMS Manual was prepared. Within this framework, the work allowed us to conclude on the importance of protection of information assets, guaranteeing their confidentiality, integrity and availability.

Keywords: Information Security Management System; ISO/ IEC 27001: 2013; Risk management; Risk treatment plan

TABLA DE CONTENIDOS

1	ASPECTOS INTRODUCTORIOS	1
1.1	ORGANIZACIÓN OBJETIVO	1
1.2	CAMPO DE ACCIÓN DE LA ORGANIZACIÓN OBJETIVO	2
1.3	SITUACIÓN PROBLEMÁTICA Y PROBLEMAS A RESOLVER EN EL CAMPO DE ACCIÓN .	3
1.3.1	Situación problemática	3
1.3.2	Problemas a resolver.....	4
1.4	OBJETIVOS DEL PROYECTO GENERAL Y ESPECÍFICOS	4
1.4.1	Objetivo general	4
1.4.2	Objetivos específicos	4
1.5	INDICADORES O MECANISMOS DEL LOGRO DE LOS OBJETIVOS	5
1.6	JUSTIFICACIÓN DEL PROYECTO	5
1.7	ESTADO DEL ARTE	6
1.7.1	Introducción.....	6
1.7.2	Casos de aplicación en el entorno del sector público	6
1.7.3	Seguridad de la información vs Seguridad informática.....	9
1.7.4	Ciberseguridad.....	12
1.7.5	Normas y regulaciones de seguridad de la información en el Perú.....	13
1.7.6	Modelos de seguridad de la información.....	15
1.7.7	Metodologías de gestión de riesgos.....	25
1.7.8	Soluciones de productos comerciales	50
1.7.9	Conclusiones del estado del arte.....	54
2	MARCO TEÓRICO	56
2.1	TÉRMINOS BÁSICOS	56
2.1.1	Municipalidad.....	56
2.1.2	Activo	57
2.1.3	Información	57
2.1.4	Activo de información	58
2.1.5	Seguridad.....	59
2.1.6	Seguridad de la Información	59
2.1.7	Amenazas.....	61

2.1.8	Vulnerabilidades	62
2.1.9	Riesgo	63
2.1.10	Impacto	63
2.1.11	Control	63
2.1.12	Políticas de seguridad de la información	63
2.2	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	64
2.2.1	Definición	64
2.2.2	Ciclo de mejora continua	65
2.3	GESTIÓN DE RIESGOS	68
2.3.1	Análisis de riesgo	68
2.4	ISO/IEC 27001:2013	75
2.5	ISO/IEC 27002:2013	79
2.6	ISO 31000	82
2.7	ANÁLISIS DE BRECHAS - GAP	87
2.7.1	Modelo de madurez	87
3	DEFINICIÓN DEL PROBLEMA	90
3.1	INTRODUCCIÓN	90
3.2	DEFINICIÓN DEL PROBLEMA	95
3.2.1	Análisis del problema	95
3.2.2	Causas del problema	99
3.3	IMPACTO DEL PROBLEMA EN LA MUNICIPALIDAD	99
3.4	ANÁLISIS DEL ESTADO INICIAL DE LA MDEA	101
3.4.1	Nivel de madurez por cláusulas de la norma ISO/IEC 27001:2013	101
3.4.2	Nivel de madurez por dominios de la norma ISO/IEC 27001:013	105
3.5	INTERESADOS	108
3.6	TOMA DE REQUERIMIENTOS	109
3.7	ESTRUCTURA DE DESGLOSE DE TRABAJO	110
3.7.1	Vista jerárquica	110
3.7.2	Mapa de procesos - EDT	111
4	DISEÑO DE LA SOLUCIÓN	113
4.1	ETAPA 1: INICIO DEL PROYECTO	113
4.1.1	Compromiso de la alta dirección	113

4.1.2	Acta de constitución del proyecto	114
4.1.3	Cronograma del proyecto	114
4.1.4	Presupuesto del proyecto	116
4.2	ETAPA 2: PLANIFICACIÓN DEL PROYECTO.....	116
4.2.1	Contexto de la entidad	116
4.2.2	Alcance del SGSI	130
4.2.3	Política de seguridad de la información	131
4.2.4	Objetivos de Seguridad de la Información	133
4.2.5	Estructura organizacional del SGSI.....	133
4.2.6	Metodología de gestión de riesgos	138
4.2.7	Plan de tratamiento del riesgo – PTR	153
4.2.8	Declaración de aplicabilidad – SOA	154
4.2.9	Programa de capacitación y concientización.....	154
4.3	ETAPA 3: EJECUCIÓN DEL PROYECTO.....	155
4.3.1	Manual del SGSI	155
5	PRUEBAS, RESULTADOS Y VALIDACIÓN	156
5.1	ETAPA 4: EVALUACIÓN DEL PROYECTO	156
5.1.1	Método de trabajo para la validación de las pruebas.....	156
5.1.2	Objetivo específico 1	157
5.1.3	Objetivo específico 2	176
5.1.4	Objetivo específico 3	180
5.1.5	Objetivo específico 4	183
5.2	ETAPA 5: CIERRE DEL PROYECTO	186
6	CONCLUSIONES.....	187
7	RECOMENDACIONES	188
8	REFERENCIAS	189
9	GLOSARIO.....	195
10	SIGLARIO	198
11	ANEXOS	199

ÍNDICE DE TABLAS

Tabla 1. Indicadores o mecanismos del logro de los objetivos	5
Tabla 2. Seguridad de la información vs seguridad informática	10
Tabla 3. Normas publicadas de la serie ISO/IEC 27000	17
Tabla 4. Nombres de familia e Identificadores de controles NIST	20
Tabla 5. Niveles de Madurez usados por O-ISM3.	24
Tabla 6. Actualizaciones OCTAVE	31
Tabla 7. Procesos y actividades de la fase 1 - OCTAVE - S.....	34
Tabla 8. Procesos y actividades de la fase 2 - OCTAVE - S.....	35
Tabla 9. Procesos y actividades de la fase 3 - OCTAVE - S.....	35
Tabla 10. Ejemplo del balance control vs productividad en una política de seguridad	64
Tabla 11. Actividades por cada fase del Modelo PDCA	66
Tabla 12. Ejemplo de escala de valores de los activos	69
Tabla 13. Probabilidad que una amenaza se materialice	72
Tabla 14. Impacto que una amenaza se materialice	72
Tabla 15. Matriz del análisis de riesgo	73
Tabla 16. Ejemplo de criterios para el tratamiento de riesgos.....	74
Tabla 17. Áreas de control del Anexo A	78
Tabla 18. Incidentes reportados del año 2018	99
Tabla 19. Evolución mensual de ingresos del año 2018 de la MDEA	100
Tabla 20. Ingresos del Periodo 2015 - 2018 de la MDEA	100
Tabla 21. Criterios para evaluar los requisitos de la norma ISO/IEC 27001:2013	102
Tabla 22. Resultado por cláusula.....	102
Tabla 23. Criterios para evaluar los controles de la norma ISO/IEC 27001:2013	105
Tabla 24. Resultado por dominios.....	106
Tabla 25. Interesados del SGSI	108
Tabla 26. Requerimientos de las partes interesadas	109
Tabla 27. Presupuesto del proyecto	116
Tabla 28. Contexto externo de la MDEA	117
Tabla 29. Matriz FODA de la MDEA	120
Tabla 30. Requisitos de las partes interesadas.....	129
Tabla 31. Categorías de activos de información.....	140
Tabla 32. Clasificación de los activos de la información	141

Tabla 33. Frecuencia de uso de los activos de información	142
Tabla 34. Campos de identificación del inventario de activos de información.....	142
Tabla 35. Criterios para la valoración de activos de información	143
Tabla 36. Preguntas para determinar la criticidad del activo de información	143
Tabla 37. Nivel de criticidad de los activos de información	144
Tabla 38. Catálogo de vulnerabilidades	145
Tabla 39. Catálogo de amenazas	147
Tabla 40. Catálogo de amenazas de tipo humano	148
Tabla 41. Probabilidad de ocurrencia del riesgo	149
Tabla 42. Impacto del riesgo	150
Tabla 43. Cálculo del riesgo	151
Tabla 44. Criterios de valoración de la magnitud del riesgo	151
Tabla 45. Criterios de aceptación del riesgo.....	152
Tabla 46. Opciones de tratamiento de riesgo	153
Tabla 47. Costo aproximado para el PTR.....	153
Tabla 48. Tiempo aproximado para el PTR	154
Tabla 49. Campos de identificación de la Declaración de Aplicabilidad.....	154
Tabla 50. Indicadores de logro y métricas del objetivo 1.....	157
Tabla 51. Encuesta aplicada a la pregunta 1	161
Tabla 52. Encuesta aplicada a la pregunta 2.....	162
Tabla 53. Encuesta aplicada a la pregunta 3.....	163
Tabla 54. Encuesta aplicada a la pregunta 4.....	164
Tabla 55. Encuesta aplicada a la pregunta 5.....	165
Tabla 56. Encuesta aplicada a la pregunta 6.....	166
Tabla 57. Encuesta aplicada a la pregunta 7.....	167
Tabla 58. Encuesta aplicada a la pregunta 8.....	168
Tabla 59. Encuesta aplicada a la pregunta 9.....	169
Tabla 60. Encuesta aplicada a la pregunta 10.....	170
Tabla 61. Encuesta aplicada a la pregunta 11	171
Tabla 62. Encuesta aplicada a la pregunta 12.....	172
Tabla 63. Encuesta aplicada a la pregunta 13.....	173
Tabla 64. Encuesta aplicada a la pregunta 14.....	174
Tabla 65. Encuesta aplicada a la pregunta 15.....	175

Tabla 66. Indicadores de logro y métricas del objetivo 2.....	176
Tabla 67. Indicadores de logro y métricas del objetivo 3.....	180
Tabla 68. Indicadores de logro y métricas del objetivo 4.....	183
Tabla 69. Controles aplicables de seguridad de la información	185
Tabla 70. Plan de concientización	315
Tabla 71. Plan de capacitación	320

ÍNDICE DE FIGURAS

<i>Figura 1.</i> Aspectos de la Seguridad de la información vs Seguridad informática	11
<i>Figura 2.</i> Seguridad de la información vs Seguridad informática	11
<i>Figura 3.</i> Familia de normas ISO/IEC 27000	15
<i>Figura 4.</i> Estructura de documentación de NIST	18
<i>Figura 5.</i> Marco de Gestión de Riesgos NIST	19
<i>Figura 6.</i> Historia de COBIT	21
<i>Figura 7.</i> Modelo ISM3	23
<i>Figura 8.</i> Proceso de Metodología Magerit.....	27
<i>Figura 9.</i> Perspectiva general de Mehari.....	29
<i>Figura 10.</i> Etapas de CRAMM	31
<i>Figura 11.</i> Tres Aspectos de equilibrio de OCTAVE	32
<i>Figura 12.</i> Fases del Proceso OCTAVE	33
<i>Figura 13.</i> Fases y pasos de OCTAVE Allegro	36
<i>Figura 14.</i> Proceso de análisis de riesgos de NIST 800-30.....	38
<i>Figura 15.</i> Procesos de gestión de riesgos de seguridad de la información	40
<i>Figura 16.</i> Procesos de gestión de riesgos según ISO 31000.....	41
<i>Figura 17.</i> Elementos de COSO I	43
<i>Figura 18.</i> Elementos de COSO ERM.	44
<i>Figura 19.</i> Vinculación del riesgo con los objetivos y la estrategia.....	44
<i>Figura 20.</i> Ejemplos de riesgos de fraude	45
<i>Figura 21.</i> Ciclo de fases de EBIOS	46
<i>Figura 22.</i> Marco RISK IT.....	48
<i>Figura 23.</i> Los siete pasos de la metodología CORAS.....	49
<i>Figura 24.</i> Logo de ePULPO	52
<i>Figura 25.</i> Módulos de Inmuno Suite	53
<i>Figura 26.</i> Componentes del servicio de implementación autónoma ISO 27001.....	54
<i>Figura 27.</i> Concepto de Información	57
<i>Figura 28.</i> Propiedades de los activos de información	59
<i>Figura 29.</i> Base de la seguridad de la información	60
<i>Figura 30.</i> Ciclo PDCA.....	66
<i>Figura 31.</i> Ciclo PDCA en ISO/IEC 27001:2013	67
<i>Figura 32.</i> Fases que componen el análisis de riesgo	68

<i>Figura 33. Tipos de amenazas.....</i>	<i>70</i>
<i>Figura 34. Priorización de riesgos</i>	<i>73</i>
<i>Figura 35. Origen y evolución de la norma ISO/IEC 27001</i>	<i>75</i>
<i>Figura 36. Cláusulas de la Norma ISO/IEC 27001:2013.....</i>	<i>76</i>
<i>Figura 37. Cláusulas de la ISO/IEC 27002:2013.....</i>	<i>80</i>
<i>Figura 38. Principios, marco de referencia y proceso de la ISO 31000.....</i>	<i>83</i>
<i>Figura 39. Proceso de la gestión de riesgo de la ISO 31000.....</i>	<i>85</i>
<i>Figura 40. Niveles de madurez CMMI</i>	<i>88</i>
<i>Figura 41. Perspectiva global sobre delitos económicos y fraude</i>	<i>90</i>
<i>Figura 42. Encuesta global de seguridad.</i>	<i>91</i>
<i>Figura 43. ¿La función de seguridad de la información cumple con las necesidades de la organización?.....</i>	<i>91</i>
<i>Figura 44. Tipos de delito más cometido.....</i>	<i>92</i>
<i>Figura 45. Vulnerabilidades con mayor exposición a los riesgos.....</i>	<i>93</i>
<i>Figura 46. Impacto de los delitos económico en las organizaciones.</i>	<i>94</i>
<i>Figura 47. Beneficios de la Seguridad de Información.....</i>	<i>95</i>
<i>Figura 48. Oficina administrativa de rentas</i>	<i>96</i>
<i>Figura 49. Mayores fuentes de riesgo para la seguridad de datos</i>	<i>97</i>
<i>Figura 50. Oficina de TI.....</i>	<i>97</i>
<i>Figura 51. Oficina de rentas.....</i>	<i>98</i>
<i>Figura 52. Gabinete del área de TI.....</i>	<i>98</i>
<i>Figura 53. Análisis de brechas de las cláusulas</i>	<i>103</i>
<i>Figura 54. Grado de cumplimiento de la norma ISO/IEC 27001:2013</i>	<i>104</i>
<i>Figura 55. Nivel de madurez con respecto a la norma ISO/IEC 27001:2013.....</i>	<i>104</i>
<i>Figura 56. Análisis de brecha por dominio</i>	<i>107</i>
<i>Figura 57. Grado de cumplimiento de los dominios de la norma ISO/IEC 27001:2013..</i>	<i>107</i>
<i>Figura 58. Nivel de madurez con respecto a los dominios de la norma ISO/IEC 27001:2013</i>	<i>108</i>
<i>Figura 59. EDT.</i>	<i>112</i>
<i>Figura 60. Cronograma</i>	<i>115</i>
<i>Figura 61. Frontis de la MDEA</i>	<i>118</i>
<i>Figura 62. Organigrama de la Municipalidad Distrital de El Agustino</i>	<i>119</i>
<i>Figura 63. Mapa de procesos de la MDEA.....</i>	<i>121</i>

<i>Figura 64. Subproceso: Determinar obligaciones tributarias.....</i>	122
<i>Figura 65. Subproceso: Verificar cumplimiento de obligaciones tributarias</i>	123
<i>Figura 66. Subproceso: Cobranza de obligaciones tributarias.....</i>	124
<i>Figura 67. Subproceso: Ejecutar incremento o disminución de valores tributarios</i>	125
<i>Figura 68. Subproceso: Emitir las notificaciones de pago de tributos.....</i>	126
<i>Figura 69. Alcance del SGSI</i>	131
<i>Figura 70. Política del SGSI</i>	132
<i>Figura 71. Estructura organizacional del SGSI.....</i>	134
<i>Figura 72. Modelo de gestión de riesgos bajo la ISO 31000:2018.....</i>	138
<i>Figura 73. Apetito del riesgo para el tratamiento de riesgos</i>	152
<i>Figura 74. Flujo de trabajo para la validación de las pruebas.....</i>	156
<i>Figura 75. Cláusulas vs Nivel de madurez</i>	159
<i>Figura 76. Dominios vs Nivel de madurez</i>	160
<i>Figura 77. Frecuencia de respuesta de la pregunta 1</i>	161
<i>Figura 78. Frecuencia de respuesta de la pregunta 2</i>	162
<i>Figura 79. Frecuencia de respuesta de la pregunta 3</i>	163
<i>Figura 80. Frecuencia de respuesta de la pregunta 4</i>	164
<i>Figura 81. Frecuencia de respuesta de la pregunta 5</i>	165
<i>Figura 82. Frecuencia de respuesta de la pregunta 6</i>	166
<i>Figura 83. Frecuencia de respuesta de la pregunta 7</i>	167
<i>Figura 84. Frecuencia de respuesta de la pregunta 8</i>	168
<i>Figura 85. Frecuencia de respuesta de la pregunta 9</i>	169
<i>Figura 86. Frecuencia de respuesta de la pregunta 10</i>	170
<i>Figura 87. Frecuencia de respuesta de la pregunta 11</i>	171
<i>Figura 88. Frecuencia de respuesta de la pregunta 12</i>	172
<i>Figura 89. Frecuencia de respuesta de la pregunta 13</i>	173
<i>Figura 90. Frecuencia de respuesta de la pregunta 14</i>	174
<i>Figura 91. Frecuencia de respuesta de la pregunta 15</i>	175
<i>Figura 92. Cantidad vs Estado del activo</i>	178
<i>Figura 93. Cantidad vs Riesgos críticos.....</i>	181
<i>Figura 94. Porcentaje de controles aplicables.....</i>	185

INTRODUCCIÓN

Hoy en día, casi todas las organizaciones públicas o privadas dependen de alguna manera de la tecnología de la información como una herramienta primordial para el logro de sus objetivos de negocio; es casi imposible pensar en organizaciones y/o empresas que no soporten sus procesos de negocio en la información, para convertirlas en productos y servicios.

“La información es un activo que, al igual que otros activos del negocio, es esencial para la organización, y por lo tanto debe ser protegido de forma adecuada” (ISO/IEC 17799:2005). Entonces, dado el alto valor e importancia que la información tiene para cualquier organización, es predecible suponer que se deban enfrentar con una amplia gama de amenazas y vulnerabilidades, que puedan poner en riesgo dicha información.

Es así que, debido a la inseguridad que afecta la información en cualquiera de sus medios, surjan marcos de referencia, normas, mejores prácticas y controles, que ayuden a las organizaciones a garantizar la seguridad de la información. Tal es el caso del estándar ISO/IEC 27001:2013, norma reconocida y certificable que especifica los requisitos para implementar, operar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) para cualquier empresa sea cual sea su tamaño, actividad o volumen de negocio.

Un Sistema de Gestión de Seguridad de la Información es una herramienta de gestión que va a permitir conocer, gestionar y minimizar los posibles riesgos que atentan contra la seguridad de la información de la organización; de una forma documentada, sistemática, estructurada, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías, siendo su objetivo primordial el resguardo de la confidencialidad, integridad y disponibilidad de los activos de información.

En el Perú, contamos con la Norma Técnica Peruana NTP-ISO/IEC 27001:2014, que mediante Resolución Ministerial N°004-2016-PCM, aprobó el uso obligatorio en todas las entidades integrantes del Sistema Nacional de Informática. Sin embargo, por desconocimiento de estos temas por parte de los organismos públicos, no han tomado las medidas necesarias para su implementación.

Esto es lo que motivo mi interés en el tema, ya que la Municipalidad Distrital de El Agustino (MDEA), a pesar de ser integrante del Sistema Nacional de Informática, no cuenta con un

SGSI que le permita manejar una correcta gestión de seguridad de la información y cumplir con la normativa vigente. Es así que, la municipalidad tendrá la oportunidad de cumplir con las exigencias que el Estado solicite y, además, contar con una herramienta que le ayude a proteger sus activos de información en cada uno de sus procesos.

El objetivo de la tesis es diseñar un Sistema de Gestión de Seguridad de la Información para proteger adecuadamente los activos de información asociados al proceso de recaudación y fiscalización tributaria del área de rentas de la Municipalidad Distrital de El Agustino.

Para llevar a cabo nuestro estudio, la tesis se ha estructurado en 5 capítulos. En el capítulo 1 “Aspectos introductorios” se describe el panorama de los aspectos generales de la investigación como son la identificación del problema, formulación del problema, los objetivos, la justificación y el estado del arte. En el capítulo 2 “Marco teórico” se efectúan algunas precisiones teóricas conceptuales tanto de seguridad de la información, gestión de riesgos, la norma internacional ISO/IEC 27001:2013 y otras definiciones de términos básicos que permiten comprender mejor el tema. En el capítulo 3 “Definición del problema” se sustenta el problema identificado con datos concretos y describiendo el alcance e impacto en la municipalidad, además de realizar un análisis GAP o de brechas para conocer el estado inicial de la entidad. En el capítulo 4 “Diseño de la solución” se elabora las especificaciones del diseño del Sistema de Gestión de Seguridad de la Información de acuerdo con los requerimientos exigidos por la norma ISO/IEC 27001:2013, se identifican y valoran los activos de información, se realiza el análisis y evaluación de la gestión de riesgos bajo el estándar ISO/IEC 31000, plan de tratamiento de riesgos y el manual del SGSI. Finalmente, en el capítulo 5 “Pruebas, resultados y validación” se valida de manera rigurosa el cumplimiento de los objetivos específicos de acuerdo a los indicadores de logros y las métricas planteadas.

1 ASPECTOS INTRODUCTORIOS

1.1 Organización Objetivo

El proyecto se llevará a cabo en la Municipalidad Distrital de El Agustino a la que llamaremos en adelante MDEA, que según el Reglamento de Organización y Reglamento – ROF (2019), “es un órgano de gobierno promotor del desarrollo local, que tiene su domicilio fiscal en la Av. Riva Agüero N° 1358 del distrito de El Agustino. Fue creado mediante la Ley N° 15353, el 06 de enero de 1965” (p. 4).

También, el ROF (2019) indica que, “...tiene personería jurídica de derecho público con autonomía política, económica y administrativa en los asuntos de su competencia, de conformidad con la Ley N° 27972, Ley Orgánica de las Municipalidades” (p. 5).

“La Municipalidad Distrital de El Agustino tiene como objetivo planificar, ejecutar y promover el desarrollo social y económico del distrito, proporcionando al vecino el ambiente adecuado para la satisfacción de sus necesidades de salubridad, abastecimiento, educación, recreación, turismo, seguridad y comunicaciones; así como, apoyar en las acciones de participación organizada de los vecinos en el desarrollo de acciones comunales” (ROF, 2019, p. 5).

Dentro de su información institucional tenemos:

Visión: Ser una institución líder, moderna, innovadora y que gestione eficientemente los recursos con la finalidad de lograr el desarrollo del distrito y brindar una mejor calidad de vida para la población.

Misión: Prestar servicios públicos de calidad y de manera responsable para satisfacer las necesidades colectivas de los ciudadanos y promover la participación de los mismos para el progreso del distrito.

Objetivos estratégicos:

La Municipalidad Distrital de El Agustino tiene los siguientes objetivos estratégicos:

- Reducir los índices de inseguridad ciudadana en el distrito de El Agustino.
- Promover la gestión ambiental en el distrito de El Agustino
- Promover la competitividad económica en el distrito de El Agustino.

- Proteger a la población y sus medios de vida frente a los peligros de origen natural y antrópicos.
- Promover el desarrollo urbano territorial ordenado y sostenible en el distrito de El Agustino.
- Promover el desarrollo humano y hábitos saludables en el distrito de El Agustino.
- Incrementar los recursos financieros de la Municipalidad Distrital de El Agustino.
- Modernizar la gestión con tecnologías de información y comunicación con la participación de la población.
- Fortalecer el liderazgo de la municipalidad basada en una gestión de procesos y resultados.
- Fortalecer la gestión institucional de la Municipalidad Distrital de El Agustino.

1.2 Campo de acción de la organización objetivo

El campo de acción será en el proceso de Recaudación y Fiscalización Tributaria, el cual es soportado por las áreas de Rentas y Tecnologías de la Información, este proceso cuenta con los siguientes subprocesos:

- Determinar las obligaciones tributarias.
- Verificar cumplimiento de obligaciones tributarias.
- Cobranza de obligaciones tributarias.
- Ejecutar incremento o disminución de valores tributarios.
- Emitir las notificaciones de pago de tributos.

La municipalidad cuenta con dos áreas, donde se lleva a cabo la actividad principal, y son:

Área de Rentas. – Según el Artículo 46 del Reglamento de Organizaciones y Funciones Municipales – ROF (2019) “se encarga de administrar y operar los servicios administrativos tributarios municipales y no tributarios pecuniarios en el ámbito de su competencia, administra, dirige, ejecuta y controla las acciones de cobranza ordinaria de la deuda tributaria y se encarga de los procesos de recaudación de los ingresos de la municipalidad” (p. 22).

Es así que, es un órgano de línea de la municipalidad, responsable de la captación de los ingresos de la municipalidad por conceptos de tributos y otras rentas municipales, con sujeción a la ley de tributación municipal, código tributario y otras normas aplicables. Depende jerárquicamente de la Gerencia Municipal.

Área de Tecnologías de Información. – Según el Artículo 39, “Se encarga de brindar soporte técnico en materia de hardware y software, la provisión de servicios de internet e intranet, así como el manejo de las redes informáticas de los locales de la municipalidad” (ROF, 2019, p. 17). Además, de implementar un plan de contingencia de informática en todos los niveles.

1.3 Situación problemática y problemas a resolver en el campo de acción

1.3.1 Situación problemática

La Municipalidad Distrital de El Agustino es un órgano del sector público que tiene como objetivo promover toda clase de actividades y prestar servicios públicos que contribuyan a satisfacer las necesidades y aspiraciones de la comunidad, en el ámbito de su competencia de acuerdo a lo dispuesto en la Ley Orgánica del Régimen Municipal.

La entidad para cumplir con sus objetivos recurre a la utilización de infraestructura tecnológica, sistemas de información, infraestructura física, recursos financieros y recursos humanos, mediante el cual genera y procesa información de manera digital y física, los cuales son protegidos mediante controles físicos, técnicos y administrativos. Sin embargo, se ha observado que dichos controles implementados no han sido suficientes para garantizar y mantener los principios básicos de la seguridad de la información.

Un hecho palpable fue el robo o desaparición de cuatro computadoras del área de logística, evento reportado por los trabajadores del municipio el día 17 de octubre de 2018. El robo se habría dado en la madrugada y los ladrones se habrían fugado por la salida del Parque Triangular. Estas computadoras tenían información de los últimos movimientos de compras directas que ejecuto la municipalidad durante los últimos meses (Prensa El Agustino, 2018).

También, en una entrevista con el subgerente de la Unidad de Planeamiento, Gestión de Procesos y Tecnología de Información el Ingeniero Roger Arturo Chuctaya Yauri, nos menciona algunos incidentes de seguridad ocurridos en el municipio referente a los servicios de red, y mal manejo y uso de la información como:

- Pérdida de información valiosa de las áreas de contabilidad y asesoría jurídica, debido a un desperfecto técnico en el servidor, imposibilitando que estuvieran disponibles y recuperando solo el 90% de dicha información.
- Robo o fuga de información (física y digital) por parte de empleados o exempleados sobre los predios, comercios o negocios de los contribuyentes del distrito, para ser mal usados en fraudes y extorsiones.

- Fallo en las comunicaciones, relacionado con la vejez del cableado de red y los defectos de la mala instalación de la red LAN.
- Falta de un procedimiento formal para llevarse a cabo las copias (el respaldo) de seguridad de los servidores y equipos, además, de no contar con un inventario de la información crítica que necesita ser respaldada. Muchas veces son realizadas sin tener en cuenta la periodicidad con las que se deberían hacer.
- No existe una programación de mantenimiento de los equipos informáticos, muchas veces solo se realiza cuando el equipo falló. Adicionalmente, algunos equipos están ubicados en lugares no seguros.
- La entidad cuenta con una red LAN simple que no cumple las especificaciones de cableado estructurado, por ello frecuentemente los equipos pierden comunicación con el servidor.
- No se tiene la cantidad suficiente de licencias vigentes de sistema operativo y ofimática para los equipos de cómputo.
- No existe un compromiso expreso por parte de las autoridades sobre la protección de la información.

1.3.2 Problemas a resolver

Falta de un modelo que permita gestionar la seguridad de la información que comprometen la confidencialidad, integridad y disponibilidad de la información de la Municipalidad Distrital de El Agustino.

1.4 Objetivos del proyecto general y específicos

1.4.1 Objetivo general

Diseñar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para proteger adecuadamente los activos de información asociados al proceso de recaudación y fiscalización tributaria de la Municipalidad Distrital de El Agustino.

1.4.2 Objetivos específicos

OE1. Determinar el estado actual de cumplimiento de la MDEA con respecto a los requisitos de la norma ISO/IEC 27001:2013.

OE2. Identificar los activos críticos de información del proceso de recaudación y fiscalización tributaria de la MDEA.

OE3. Identificar los riesgos de los activos críticos de información.

OE4. Determinar los controles para el plan de tratamiento de riesgo de la seguridad de la información.

1.5 Indicadores o mecanismos del logro de los objetivos

Para medir los objetivos específicos se tendrán los indicadores de logro que se muestran en la tabla 1.

Tabla 1

Indicadores o mecanismos del logro de los objetivos

Objetivo Específico	Indicador de logro	Métrica
OE1	Informe del análisis de brechas de la MDEA	Porcentaje de cumplimiento de las cláusulas de la norma ISO/IEC 27001:2013 Porcentaje de cumplimiento de los dominios de la norma ISO/IEC 27002:2013
OE2	Inventario de activos de la información.	Porcentaje de activos críticos de información.
OE3	Matriz de gestión riesgos	Porcentaje de riesgos críticos de los activos de información
OE4	Declaración de aplicabilidad (SOA)	Porcentaje de controles aplicables

Nota: Elaboración propia

1.6 Justificación del proyecto

Como ya mencionamos, la información es un activo esencial para la organización y por lo tanto deber ser protegida de manera adecuada. Es por ello que se justifica la realización de un Sistema de Gestión de Seguridad de la Información que permitirá proteger adecuadamente los activos de la información asociados al proceso de recaudación y fiscalización tributaria reduciendo el riesgo de que sus procesos se van afectados por la ocurrencia de eventos que comprometan su seguridad.

Por otra parte, la implementación de un SGSI es un paso importante que conseguirá dar cumplimiento a la Resolución Ministerial 004-2016-PCM que declara el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 Tecnología de la Información.

Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición, en todas las entidades integrantes del Sistema Nacional de Informática (con fecha de publicación 14 de enero del 2016 en el Diario Oficial El Peruano) con la finalidad de cooperar con la infraestructura de gobierno electrónico, por considerar a la seguridad de la información un componente crucial para dicho objetivo.

Finalmente, lograr la certificación ISO/IEC 27001:2013, cambiará la imagen institucional de la municipalidad, tendrá un elemento diferenciador respecto a otras municipalidades aumentando la confianza de los ciudadanos y contribuyentes.

1.7 Estado del arte

1.7.1 Introducción

El objetivo del proyecto, como ya se mencionó, es diseñar un Sistema de Gestión de Seguridad de la Información para una entidad pública. Por ello se decidió realizar la búsqueda de casos de éxito de diseño e implementación de este sistema en municipalidades distritales y provinciales, tanto a nivel nacional como internacional, tratando de encontrar cuales son aquellas buenas prácticas que podemos tomar de referencia a nuestra realidad.

De las investigaciones realizadas no se ha encontrado trabajos de investigación similares en el ámbito local, pero si a nivel nacional e internacional, comprobando que, si existen investigaciones relacionadas al diseño de un SGSI, motivo por el cual son base para el desarrollo del proyecto de tesis planteado.

Además, se ha realizado un estudio de los conceptos relacionados con la gestión de seguridad de la información, los marcos legales y productos comerciales que ayudan a proteger los activos de información de las organizaciones y que serán de utilidad para el desarrollo del tema a tratar.

1.7.2 Casos de aplicación en el entorno del sector público

1.7.2.1 Casos a nivel nacional

Tarrillo y Correa (2015), en la ciudad de Lambayeque se presentaron su tesis denominada “Metodología para un Sistema de Gestión de Seguridad de la Información basado en la Norma Técnica Peruana NTP – 17799 en la Administración de la Municipalidad Distrital de Lambayeque Setiembre 2013 – febrero 2014”. Investigación que tuvo como objetivo proponer una metodología y para esto lo dividieron en 3 fases: a) fase de diagnóstico de la situación actual de la municipalidad de Lambayeque en relación a la seguridad de la

información; b) evaluación de factibilidad técnica, económica y financiera de la propuesta; c) y, por último, la propuesta de metodología para un sistema de seguridad de la información basado en la NTP 17799. Metodología que permitió determinar los objetivos, procesos y procedimientos para el establecimiento de políticas de seguridad, así como un conjunto de controles de seguridad que ayudaran a gestionar los riesgos de seguridad de la información que maneja el organismo de estudio, mejorando de esta forma la gestión de incidentes de seguridad que se detectan y generando resultados de concordancia con los objetivos y políticas requeridas para optimizar la plataforma de la municipalidad.

De la Cruz (2016), en la ciudad de Piura se presentó la tesis titulada “Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016”. Investigación de tipo descriptiva y cuantitativa que permitió recoger información y evaluar el estado actual de la seguridad de la información de la municipalidad, además de determinar la factibilidad técnica, económica y operativa de la propuesta. Obteniendo como resultados que el 72.37% de los empleados municipales opinan que, SI se encuentran expuestos a riesgos y amenazas, el 100% de los encuestados opinan que SI existe factibilidad técnica, económica y operativa de la propuesta y el 100% de los empleados opinan que NO existen controles pertinentes en cuanto a la seguridad de la información. Concluyendo finalmente, que la Municipalidad Provincial de Paita carece de políticas y controles eficientes en cuanto a la protección de los activos de la información (los servidores públicos y/o contratistas, la creación de información, los procesos, las tecnologías de información incluido el hardware y el software y las instalaciones), demostrando que es necesario y beneficioso el diseño e instalación de la propuesta de políticas basadas en buenas prácticas, para la gestión de la seguridad de la información en la municipalidad.

Ccesa (2017), en la ciudad de Ayacucho presento su tesis titulada “Diseño de un Sistema de Gestión de Seguridad de la Información bajo la NTP ISI/IEC 27001:2014 para la Municipalidad Provincial de Huamanga, 2016”. Investigación que propone el diseño de un SGSI para cumplir con lo que el estado peruano exige a las entidades públicas integrantes del sistema nacional de informática, la implementación de la NTP ISO/IEC 27001:2014; y que, por desconocimiento, falta de presupuesto y falta de personal especializado no se cumple con el cronograma de implementación establecido por el estado. En la investigación se realizó primero el diagnóstico inicial de la entidad con respecto a la NTP ISO/IEC 27001:2014, en segundo lugar, se estudió a la organización y su contexto, identificando el

proceso crítico, se definió la política de seguridad, el alcance y se identificó al comité de seguridad de la información de la organización; en tercer lugar, siguiendo la metodología de análisis y gestión de riesgos, se identificó y valoró los activos de información, se identificó las amenazas, se realizó el cálculo del impacto y del riesgo, se identificaron las medidas de control necesarias para mitigar los riesgos a un nivel aceptable; y finalmente, se elaboró un documento denominado declaración de aplicabilidad que contiene la justificación de qué controles del Anexo A de la NTP ISO/IEC 27001:2014 pueden ser implementados en la municipalidad.

Dávila (2018), en la ciudad de Chimbote presento su tesis titulada “Evaluación de un Sistema de Gestión de Seguridad de la Información basado en la Norma ISO 27001:2013, en la Municipalidad Distrital de José Crespo y Castillo – Aucayacu; 2018”. Investigación de nivel cuantitativo, de diseño no experimental de tipo descriptiva. Donde se realizó una recolección de datos con la técnica de encuesta, obteniendo como resultados: que el 85.5% de los encuestados indican que no cuentan con un SGSI y el mismo porcentaje indican la necesidad de implementar el SGSI.

Castillo (2016), en la ciudad de Huaraz presento su tesis titulada “Sistema de Gestión de Seguridad de la Información en la Municipalidad Distrital de Pira aplicando la Norma ISO/IEC 27001:2013”. Investigación que propone un SGSI debido a que las medidas de control para satisfacer los requisitos mínimos en seguridad han sido afectivas solo parcialmente. Se desarrolló el SGSI basado en la fase de planeación de la norma ISO/IEC 27001:2013 y en los controles. Se empleó MAGERIT versión 3.0 como metodología de Análisis de Gestión del Riesgo, que se aplica a los sistemas de información de toda la Municipalidad Distrital de Pira. Finalmente, dando recomendaciones con respecto al correcto uso y administración de los activos, a la seguridad de la información y los cambios que se requieren para lograr los mejores resultados en los sistemas de seguridad de la información en la municipalidad.

1.7.2.2 Casos a nivel internacional

Angarita y Bautista (2014), en la ciudad de Bucaramanga presento su tesis titulada “Diseño de un Sistema de Gestión de la Seguridad de la Información ISO 27001 para la alcaldía de Floridablanca y Plan de acción para su implementación según la guía PMBOK”. Investigación que propone un diseño de un SGSI fundamentado en los principales procesos de la entidad, y que posteriormente realiza el proceso de gestión del proyecto basado en la

guía PMBOK, lo que permitirá tener a la entidad un mejor control sobre sus principales activos de información y lograr el mejoramiento continuo de los controles implementados.

Landeta y Quille (2016), presentaron su tesis titulada “Análisis y diseño de un Sistema de Gestión de Seguridad de la Información en base a las normas ISO 27001 y 27002 para la Superintendencia de Control del Poder de Mercado”. Investigación que presenta a la norma como una guía para lograr analizar, definir y diseñar estándares que pueden ser aplicados posteriormente dentro de la entidad, para tener un proceso adecuado en el manejo de posibles riesgos que atenten contra la seguridad de la información. El resultado finalmente fue, la propuesta con lineamientos y buenas prácticas de seguridad de acuerdo a las necesidades de la entidad.

1.7.3 Seguridad de la información vs Seguridad informática

Entender a fondo la seguridad de la información es vital en el paradigma en el cual nos encontramos, ya que la sociedad se inclina cada día más a compartir datos y almacenarlos digitalmente. Es por eso que, también necesario indicar que la seguridad de la información es un término distinto a seguridad informática, aunque no hay duda que ambos términos se encuentran entrelazados de alguna manera.

Seguridad de la información

Una definición importante que se debe tener claro en este proyecto es el concepto de seguridad de la información. Es así que “es el conjunto de procesos y actividades que permiten mantener libre de peligros y daños por accidente o ataque a los activos de información que forman parte de una organización” (Tupia, 2010, p.21).

La seguridad de la información, se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos más importantes para las empresas. Es la disciplina que nos habla de los riesgos, de las amenazas, de las buenas prácticas y esquemas normativos, que exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información.

Seguridad informática

También, conocido como Seguridad de Tecnologías de la Información, es el área de la informática que consiste en asegurar que los recursos del sistema de información (material

informático o programas) de una organización, sean utilizados de manera correcta. (CSI, 2016). Es decir, se describe como la distinción táctica y operacional de la seguridad.

Esta disciplina se encarga de la implementación técnica de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, atención de incidentes, entre otros elementos, que establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo.

A continuación, se muestra la tabla 2, donde se plantea las diferencias entre ambas perspectivas:

Tabla 2
Seguridad de la información vs seguridad informática

Seguridad de la información	Seguridad informática
Es una función estratégica de negocio.	Es una función técnica.
Instaura las políticas de seguridad y elementos de control en materia de seguridad de la información.	Incorpora y trata a los sistemas de información y telecomunicaciones.
Se encarga de los aspectos físico, lógico y legal de la seguridad de información dentro de la empresa.	Asegura que los sistemas carezcan de riesgos perniciosos.
Busca garantizar la disponibilidad, integridad, confidencialidad, autenticidad, auditabilidad y no repudio de la información.	Garantiza que los sistemas y sus activos de información asociados se empleen para lo que fueron concebidos.

Nota: Tupia, 2010, p. 21

Finalmente, podemos resumir todo lo mencionado en las figuras 1 y 2, que muestran que la seguridad de la información va mas allá ocupandose de los riesgos, normativas, procesos, impulsados por la alta dirección. Mientras que la seguridad informática ve soluciones tácticas.

Figura 1. Aspectos de la Seguridad de la información vs Seguridad informática
Adaptado de <https://www.slideshare.net/seguridad-de-la-informacion>

Figura 2. Seguridad de la información vs Seguridad informática
Adaptado de <https://www.slideshare.net/seguridad-de-la-informacion>

1.7.4 Ciberseguridad

La ciberseguridad o seguridad en internet hace referencia al conjunto de técnicas o procedimientos que velan por la seguridad de los usuarios que comparten información entre sistemas computacionales.

ISACA define la ciberseguridad como la “protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados”

Otro concepto a tener en cuenta es que “la ciberseguridad es el arte de evitar y proteger de ataques maliciosos todo tipo de dispositivos electrónicos desde ordenadores, servidores, redes informáticas a teléfonos móviles e impresoras para impedir que estos aparatos sean atacados y así asegurar los datos personales que contengan” (Cernadas, 2018).

Las amenazas a las que se enfrenta la ciberseguridad son infinitas, pero hay amenazas comunes o habituales en la red, que son:

Ciberguerra. - Se trata de un ataque cuya finalidad por norma general es política. En este contexto, los ciberdelincuentes intentan recopilar el mayor número de información posible y datos relevantes que pueden comprometer, en un futuro, a un partido político o un gobierno.

Ciberdelincuencia. - El ciberdelincuencia es una de las amenazas más comunes y la que más se suele producir en todo tipo de países. A través de ella, los hackers acceden a sistemas informáticos protegidos e intentan obtener ganancias financieras. También se realiza a nivel de usuario, tomando el control de dispositivos concretos y solicitando cantidades económicas a cambio de su liberación entre otras posibilidades.

Ciberespionaje. - Este tipo de ataque informático pone el foco, sobre todo, en la información que guarden las empresas. Pero también pueden tener como objetivo recabar datos personales sobre un individuo en particular o una organización en concreto.

Ciberterrorismo. - Se trata de un concepto más complejo que los anteriores y también más peligroso. Su objetivo es fomentar un estado de terror y pánico entre una población concreta, amenazando su estabilidad y modo de vida. Por ejemplo, si uno de estos ataques lograra inutilizar los sistemas informáticos que utiliza un país, el daño sería tremendo.

1.7.5 Normas y regulaciones de seguridad de la información en el Perú

1.7.5.1 Ley de protección de datos personales

El 3 de julio del 2011 se promulgo la Ley N° 29733 – Ley de Protección de Datos Personales (LPDP) – su aplicación fue aprobada el 22 de marzo del 2013 y entro en vigencia el 8 mayo del mismo año. Esta ley nace como respuesta a la necesidad de contar con un documento que regule la manera en la que se hace uso de la información personal en los procesos de negocio de todas las organizaciones que realicen operaciones en el Perú. Tiene por objetivo garantizar el derecho fundamental a la protección de los datos personales, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconoce.

Consta de seis títulos y cuarenta artículos que describen las disposiciones generales, los principios rectores, el tratamiento de datos personales, los derechos del titular de datos personales, el registro nacional de protección de datos personales, y por último las infracciones y sanciones ante actos contrarios a lo dispuesto en la ley (Congreso de la República, 2013)

La ley considera como dato personal a cualquier información que permita identificar a una persona, ya sea directa o indirectamente como el nombre, apellidos, fecha de nacimiento, dirección de domicilio, dirección de correo electrónico, número de teléfono, número de RUC, número de la placa del vehículo, la huella digital, el ADN, una imagen, el número del seguro social, etc. Además, dentro de esta categoría están los “datos sensibles” que están constituidos por los datos biométricos, datos de origen racial y étnico, los ingresos económicos, convicciones políticas y religiosas, información relacionada a la salud o a la vida sexual (APDP, 2013)

Es muy cierto que estos datos son siempre necesarios al momento de acceder o solicitar algún servicio, pero como señala la ley el titular de los datos tiene los siguientes derechos:

- Acceso: solicitar la información que la organización posee sobre él, de cómo sus datos fueron recopilados, y a solicitud de quién se realizó la recopilación.
- Rectificación: solicitar que sus datos se modifiquen por ser inexactos, incompletos, erróneos o falsos.

- Cancelación: solicitar la supresión o cancelación de sus datos personales cuando estos hayan dejado de ser necesarios o no sean pertinentes para la finalidad que fueron recopilados.
- Oposición: tiene la posibilidad de oponerse al tratamiento de sus datos personales.

Es así que la presente ley tiene por objeto garantizar el derecho fundamental de protección de datos personales, previsto en la Constitución Política del Perú en el artículo 2 inciso 6 – Derecho a la Autodeterminación Informativa, que indica: “Toda persona tiene derecho a que los servicios informativos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar”

La Autoridad Nacional de Protección de Datos Personales (APDP) es el ente regulador de esta ley, cuya función es la de cumplir y hacer cumplir la normatividad vigente en materia de protección de datos personales. Sus funciones son administrativas, orientadoras, normativas, resolutivas, fiscalizadoras y sancionadoras.

1.7.5.2 NTP ISO/IEC 27001:2014

En el Perú se cuenta con la Norma Técnica Peruana, norma alineada a la norma internacional ISO/IEC 27001. Así tenemos la NTP ISO/IEC 27001:2014 Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requisitos. Esta proporciona los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información dentro del contexto de la organización.

Esta Norma Técnica Peruana es una herramienta que ha elaborado el Instituto Nacional de Calidad (INACAL), para salvaguardar la información de las organizaciones. INACAL promueve que instituciones públicas y privadas apliquen este estándar de calidad.

Su estructura es como sigue:

0. Introducción
1. Objeto y campo de aplicación
2. Referencias normativas
3. Términos y definiciones
4. Contexto de la organización
5. Liderazgo
6. Planificación

7. Soporte
8. Operación
9. Evaluación
10. Mejora
11. Anexo A – Lista de controles

1.7.5.3 Ley de delitos informáticos

Ley N° 30096, que entró en vigencia el 23 de octubre de 2013. Esta ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

1.7.6 Modelos de seguridad de la información

1.7.6.1 Serie 27000

La International Organization for Standardization (ISO) e International Electrotechnical Commission (IEC), desarrollaron la familia de normas ISO/IEC 27000, donde se proporcionan los lineamientos y normativas para la gestión de la seguridad de la información en cualquier tipo de organización sea pública o privada, grande o pequeña. A continuación, en la figura 3, se muestran cómo están relacionadas esta serie de normas y se detallan las mismas, dado que algunas nos servirán para realizar los procesos del presente proyecto.

Figura 3. Familia de normas ISO/IEC 27000
Adaptado de Olivan, 2017.

- ISO/IEC 27001

Information Security Management Systems – Requirements. Es el estándar principal de la familia 27000, brinda los requerimientos para el desarrollo y operación de un SGSI incluyendo una lista de controles para el manejo y mitigación de los riesgos asociados a los activos de información.

- ISO/IEC 27002

Code of Practice for Information Security Controls. Este estándar brinda la guía de implementación de la lista de las mejores prácticas y los objetivos de control presentados como anexo en la ISO/IEC 27001, con el objetivo de facilitar la elección de controles para asegurar la seguridad de los activos de información.

- ISO/IEC 27003

Information Security Management System Implementation Guidance. Este estándar es una guía para el diseño e implementación de un SGSI de acuerdo con la ISO/IEC 27001. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI.

- ISO/IEC 27004

Information Technology – Security Techniques – Information Security Management – Measurement. “Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001” (López & Ruiz, 2012, pp. 3). Esta norma incluye la política, la gestión de riesgos de seguridad, objetivos de control, controles, procesos y procedimientos, además de apoyar el proceso de revisión, lo que ayuda a determinar si alguno de los procesos o controles del SGSI deben ser cambiados o mejorados. Recordar que ninguna medida de control puede garantizar una seguridad total, pero la aplicación de este enfoque constituye un programa de medición de seguridad de la información.

- ISO/IEC 27005

Information Security Risk Management. Estándar que describe la gestión de riesgos de seguridad de la información. Norma no certificable.

- ISO/IEC 27006

Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems. Este estándar se complementa con el ISO/IEC 17021 y brinda los requerimientos necesarios para la acreditación de la certificación de una organización que certifique los SGSI según la ISO/IEC 27001.

- ISO/IEC 27007

Information technology - Security Techniques - Guidelines for Information Security Management Systems Auditing. Es una guía de auditoria de un SGSI, como complemento a lo especificado en la ISO 19011.

- ISO/IEC 27008

Information Technology - Security techniques -- guidelines for the assessment of information security controls. Es una guía de auditoria de los controles seleccionados en el marco de implementación de un SGSI.

A continuación, en la tabla 3 se muestra las normas que han sido publicadas de la familia 27000.

Tabla 3
Normas publicadas de la serie ISO/IEC 27000

Identificación	Título
UNIT-ISO/IEC 27000:2014	Visión general y vocabulario
UNIT-ISO/IEC 27001:2013	Sistema de Gestión de la Seguridad de la Información - Requisitos
UNIT-ISO/IEC 27002:2013	Código de buenas prácticas para la Gestión de Seguridad de la Información
UNIT-ISO/IEC 27003:2010	Directrices para la Implementación de un Sistema de Gestión de Seguridad de la Información
UNIT-ISO/IEC 27004:2009	Gestión de la Seguridad de la Información - Medición
UNIT-ISO/IEC 27005:2018	Gestión del Riesgo de Seguridad de la Información
UNIT-ISO/IEC 27006:2011	Requisitos para los Organismos que realizan Auditorías y Certificaciones de Sistemas de Gestión de Seguridad de la Información

UNIT-ISO/IEC 27007:2011	Directrices para Auditar Sistemas de Gestión de Seguridad de la Información
UNIT-ISO/IEC 27008:2011	Directrices para los Auditores sobre Controles de Seguridad de la Información

Nota: Elaboración propia

1.7.6.2 NIST: Serie 800

Del acrónimo en inglés *National Institute of Standards and Technology*, fundado en 1990, es un organismo federal no regulador que forma parte de la Administración de Tecnología del Departamento de Comercio de los EE.UU.

La misión del NIST consiste en elaborar y promover patrones de medición, normas y tecnología con el fin de incrementar la productividad, facilitar el comercio y mejorar la calidad de vida. Es una serie de documentos de interés general sobre seguridad de la información, de descarga gratuita y contiene más de ciento treinta documentos. Su estructura es como se muestra en la figura 4.

Figura 4. Estructura de documentación de NIST
Adaptado de El blog ISO 27001 e ISO 22301

Para realizar la evaluación de los riesgos, la serie 800 tiene un conjunto de documentos que han sido creados utilizando la metodología de riesgo en seis pasos, tal como se muestra en la figura 5.

Figura 5. Marco de Gestión de Riesgos NIST
Adaptado de NIST, 2013.

- Paso 1: Categorizar. – Se debe dar prioridad a los sistemas de información que se basan en la evaluación del impacto. Detalle en SP 800–60.
- Paso 2: Seleccionar. – Se definen los controles que se deben de aplicar en base a la evaluación del impacto y las bases de SP 800–53, como documento de referencia.
- Paso 3: Poner en práctica. – Se deben implementar los controles y la elaborar los documentos de acuerdo a lo indicado en el SP 800–160.
- Paso 4: Evaluar. – La confirmación de que los controles se implementan de forma correcta, operar según lo previsto y producir los resultados deseados. Detalle en SP 800–53.
- Paso 5: Autorizar. – La aceptación del escenario de riesgo, y la autorización para la operación de los sistemas de información y utilización. Detalle en SP 800–37.
- Paso 6: Monitorear. – Se verifica la efectividad y el cumplimiento de los controles dictados. Detalle en SP 800–137.

En el documento NST 800-53 se muestra una visión global del catálogo de control de seguridad de todos los controles de seguridad NIST. Este catálogo consta de dos capas:

- NIST Capa 1: Familia
Contiene 18 familias, que se pueden apreciar en la tabla 4.
- NIST Capa 2: Controles de seguridad
El catálogo tiene 240 controles de seguridad. Cada control de seguridad tiene información básica: familia, nombre, control y orientación complementaria.

Tabla 4
Nombres de familia e Identificadores de controles NIST

ID	Familia
AC	Control de acceso
AT	Conciencia y entrenamiento
AU	Auditoria y rendición de cuentas
CA	Evaluación e seguridad y autorización
CM	Gestión de configuración
CP	Planificación de contingencias
IA	Identificación y autenticación
IR	Respuesta al incidente
MA	Mantenimiento
MP	Protección de medios
PE	Protección física y ambiental
PL	Planificación
PS	Seguridad personal
RA	Evaluación de riesgos
SA	Adquisición de sistemas y servicios
SC	Sistema y protección de comunicaciones
SI	Integridad del sistemas y la información
PM	Gestión de programas

Nota: Traducido de NIST 800-53, 2013.

1.7.6.3 COBIT

Del acrónimo en inglés *Control Objectives for Information and Related Technology*. Es un marco de trabajo de buenas prácticas creado por la Information Systems Audit and Control Association (ISACA) y el IT Governance Institute (ITGI).

COBIT es una metodología mundialmente aceptada para el control adecuado de proyectos de TI, se utiliza para planear, implementar, controlar y evaluar el gobierno sobre las TIC, añadiendo objetivos de control, directivas, medidas de rendimiento y resultados, factores críticos de éxito y modelos de madurez.

Según su alcance, y tal como se muestra en la figura 6, COBIT ha evolucionado desde su primera publicación.

Figura 6. Historia de COBIT

Adaptada de COBIT Introduction - Spanish, ISACA.ppt

Como menciona Sánchez (2015) en su blog de auditoría informática, la historia de COBIT es como sigue:

- En 1996, se publica la primera edición de COBIT. Esta incluía la colección y análisis de fuentes internacionales reconocidas y fue realizada por equipos en Europa, Estados Unidos y Australia.

- En 1998, se publica la segunda edición de COBIT; el principal cambio fue la adición de las guías de gestión.
- En 2000, se publica la tercera edición COBIT; y en el 2003, la versión en línea ya se encontraba disponible en el sitio de ISACA. Fue posterior al 2003 que el marco de referencia de COBIT fue revisado y mejorado para soportar el incremento del control gerencial, introducir el manejo del desempeño y mayor desarrollo del Gobierno de TI.
- En 2005, se publica la cuarta edición COBIT y en mayo de 2007, se liberó la versión 4.1.
- En 2012, se publica la quinta edición COBIT. En esta edición se consolidan e integran los marcos de referencia de COBIT 4.1, Val IT 2.0 y Risk IT. Integrado principalmente del Modelo de Negocios para la Seguridad de la Información (BMIS, Business Model for Information Security) y el Marco de Referencia para el Aseguramiento de la Tecnología de la Información (ITAF, Information Technology Assurance Framework).

1.7.6.4 O-ISM3

Del acrónimo en inglés *Open Information Security Management Maturity Model*, su primera versión nació en el año 2004, desarrollado por el español Vicente Aceituno y publicado por The Open Group, líder en el desarrollo de certificaciones y estándares de TI abiertos y neutrales para el proveedor.

“Es un estándar para la creación del Sistema de Gestión de la Seguridad de la Información que se alinea a la misión empresarial” (Medina, 2015, p. 9).

Es así que, este estándar, como lo indica Cardoso (2014), proporciona:

- Un enfoque por niveles (genérico, estratégico, táctico y operacional), donde en cada nivel se implementan diferentes procesos de seguridad, los cuales pueden interrelacionarse con otros procesos de otros niveles.
- Herramienta para la creación de un SGSI alineados con la misión de la empresa y el cumplimiento de las necesidades.
- Permite a las organizaciones priorizar y optimizar su inversión en seguridad de la información.

- Permite la mejora continua del SGSI estableciendo metas de seguridad y midiendo el desempeño mediante la aplicación de métricas.
- Es un estándar compatible con la implementación de ISO 27001, Cobit, ITIL e ISO 9001 (p. 12).

1.7.6.4.1 Modelo ISM3

El modelo ISM3 es adaptable a cualquier tipo de organización, ya que su metodología se basa en convertir los objetivos del negocio a nivel de seguridad, en especificaciones técnicas de seguridad.

Figura 7. Modelo ISM3
Adaptado de "O-ISM3"

Tal como se puede apreciar en la figura 7, el modelo ISM3 define cinco categorías de objetivos de seguridad, que a continuación pasamos a explicar:

1. **Prioridad.** - Disponibilidad para el negocio. Ejemplos: copias de seguridad e identificación de puntos únicos de falla, canales de comunicación e interfaces.
2. **Durabilidad.** – Integridad de la información. Ejemplos: políticas de mantenimiento planificado y destrucción de la información.
3. **Calidad de la información.** – También se refiere a la integridad de la información.
4. **Control de acceso.** – Se refiere a la identificación y gestión de los usuarios autorizados.

5. Seguridad técnica. – Infraestructura del centro de datos. Ejemplos: firewalls, antivirus, parches de seguridad, actualizaciones, etc.

Además, O-ISM3 también se basa en cinco niveles de madurez estructurados de la siguiente forma, como se muestra en la tabla 5.

Tabla 5
Niveles de Madurez usados por O-ISM3.

Nivel de Madurez	Descripción
Nivel 0 O-ISM3	Nivel no recomendable, ello debido a su alcance en la reducción de amenazas técnicas sobre el alcance de seguridad de la información previamente definido.
Nivel 1 O-ISM3	Este nivel resulta en una reducción significativa de riesgos de amenazas técnicas, con una mínima inversión en procesos de seguridad de la información. Se recomienda este nivel para organizaciones con bajos objetivos en seguridad de la información en entornos de bajo nivel.
Nivel 2 O-ISM3	Este nivel resulta en una mayor reducción de riesgos de amenazas técnicas para una moderada inversión en procesos de seguridad de la información. Se recomienda este nivel para organizaciones con objetivos normales de seguridad de la información en entornos normales de riesgo.
Nivel 3 O-ISM3	Este nivel resulta en una mayor reducción del riesgo de amenazas técnicas para una alta inversión en procesos de seguridad de la información. Se recomienda este nivel para organizaciones con objetivos altos en seguridad de la información en entornos de alto riesgo.
Nivel 4 O-ISM3	Este nivel resulta en una mayor reducción del riesgo de las amenazas técnicas e internas para una alta inversión en procesos de seguridad de la información. Se recomienda este nivel para organizaciones afectadas por requisitos específicos, tales como: servicios públicos, instituciones y organizaciones financieras, que compartan o mantengan información sensible, con objetivos altos en seguridad de la información en entornos de normal o alto riesgo.

Nota: Adaptado de Torres, 2018.

1.7.7 Metodologías de gestión de riesgos

1.7.7.1 MAGERIT

Es el acrónimo de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas, elaborada por el Consejo Superior de Administración Electrónica (CSAE) del gobierno de España, como respuesta a la percepción de que la Administración, y en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

Actualmente, Magerit se encuentra en la versión 3.0 publicada en el año 2012, pero ha pasado tiempo desde la publicación de su primera versión en el año 1997, con un enfoque hacia los riesgos fundamentales en materia de sistemas de información; y su segunda versión publicada en el año 2005, con el fin de realizar una revisión constructiva con respecto a los riesgos de las organizaciones, implicando cuestiones más profundas sobre la gestión de riesgos. Y la última versión, que busca una nueva adaptación, ya no teniendo solo en cuenta la experiencia práctica sino, además la evolución de las normas internacionales ISO.

En su libro I de la publicación de Magerit versión 3, persigue los siguientes objetivos:

1. Concientizar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de información y comunicaciones (TIC).
3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.
4. Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

Según el estudio, lo interesante de esta metodología, es que presenta una guía completa y paso a paso de cómo llevar a cabo el análisis de riesgo. Está dividida en tres libros:

Libro I: Método. – Donde se describe la estructura que debe tener el modelo de gestión de riesgos.

Libro II: Catálogo de elementos. – El cual es una especie de inventario que puede utilizar la empresa para enfocar el análisis de riesgo (Gutiérrez, 2013). Es así que contiene: tipos de

activos, dimensiones de valoración, criterios de valoración, amenazas y controles que se deben tener en cuenta.

Libro III: Guía de técnicas. – Donde se describen algunas técnicas utilizadas en análisis y gestión de riesgos. Se considera técnica a un conjunto de heurísticos y procedimientos que ayudan a alcanzar los objetivos propuestos (Magerit – libro 3, p. 4). Las técnicas que recoge son:

- Análisis mediante tablas
- Análisis algorítmico
- Árboles de ataque
- Técnicas generales
- Análisis costo – beneficio
- Diagramas de flujos de datos
- Diagramas de procesos
- Técnicas gráficas
- Planificación de proyectos
- Sesiones de trabajo: entrevistas, reuniones y presentaciones
- Valoración Delphi

El método de análisis de riesgo de Magerit, indica los pasos a seguir para determinar y evaluar de forma adecuada los riesgos, amenazas y salvaguardas que pueden tener y ejecutar una organización. Algunos de los pasos son:

- Establecer los activos relevantes para la organización, su interrelación y su valor.
- Definir a qué amenazas están expuestos los activos.
- Determinar las salvaguardas dispuestas y cuan eficaces son frente al riesgo.
- Estimar el impacto o daño sobre el activo derivado de la materialización de la amenaza.
- Estimar el riesgo y el impacto ponderado con la tasa de ocurrencia de la amenaza.

En la figura 8, se puede apreciar el proceso de la metodología Magerit y los elementos de análisis de riesgos.

Figura 8. Proceso de Metodología Magerit
Adaptado del Blog Sbd Security by Default por Ramos, A, 2013.

Finalmente, podemos decir que Magerit fue creada con el fin de cumplir con objetivos como conocer el estado de seguridad de los sistemas de información y la implementación de medidas de seguridad, garantizar que no haya elementos que queden fuera del análisis para que haya una profundidad adecuada en el mismo, mitigar vulnerabilidades y asegurar el desarrollo del sistema en todas las fases de desarrollo (Abril, Pulido & Bohada, 2013, p.40).

1.7.7.2 MEHARI

Del acrónimo en inglés *Method for Harmonized Analysis of Risk*, - Método Armonizado de Análisis de Riesgos. Esta metodología fue propuesta y desarrollada por CLUSIF (Club De La Sécurité De L'information Francais) en el año 1996, es de acceso público y para todo tipo de organizaciones.

Es una metodología utilizada para apoyar a los responsables de la seguridad informática de una empresa mediante un análisis riguroso de los principales factores de riesgo, evaluando cuantitativamente, de acuerdo con la situación de la organización, donde se requiere el análisis; acopla los objetivos estratégicos

existentes con los nuevos métodos de funcionamiento de la empresa mediante una política de seguridad y mantenimiento de los riesgos a un nivel convenido. Mehari propone un módulo para analizar los intereses implicados por la seguridad y un método de análisis de riesgos con herramientas de apoyo. (Alemán & Rodríguez, 2014, p. 5).

Mehari, tiene como primer objetivo proporcionar un método para la evaluación y gestión de riesgos, específicamente en el dominio de la seguridad de la información, conforme a los requisitos de la ISO/IEC 27005:2008, brindando un conjunto de herramientas y elementos necesarios para su implementación (CLUSIF, 2010).

Otros objetivos adicionales son:

- Permitir un análisis directo e individual de situaciones de riesgos descritas en los escenarios.
- Proporcionar un completo conjunto de herramientas específicamente diseñadas para la gestión de la seguridad a corto, mediano y largo plazo, adaptables a diferentes niveles de madurez y tipos de acciones consideradas.

Al respecto del análisis o evaluación de riesgos, Mehari proporciona un enfoque estructurado, basándose en unos simples principios. Una situación de riesgo se puede caracterizar por:

- Factores estructurales (u organizacionales), los cuales no dependen de medidas de seguridad, sino de la actividad principal de la organización, su entorno y su contexto.
- Factores de reducción de riesgo, que son una función directa de las medidas de seguridad implementadas.

Mehari permite la evaluación cualitativa y cuantitativa de esos factores. Además, que integra herramientas (criterios de evaluación, fórmulas, etc.) y bases de datos de conocimiento que son un esencial complemento al marco mínimo propuesto por la ISO/IEC 27005.

Por otra parte, las evaluaciones de seguridad, permite evaluar el nivel de calidad de los mecanismos y soluciones encaminadas a la reducción del riesgo. Abarca los siguientes puntos:

- Revisión de vulnerabilidades, un elemento de análisis de riesgos.
- Planes de seguridad basados en la revisión de vulnerabilidades.

- Apoyo de las bases de conocimiento en la creación de un marco de referencia de seguridad.
- Dominios cubiertos por el módulo de evaluación de vulnerabilidades.
- Descripción general del módulo de evaluación.

Finalmente, el análisis de amenazas, que significa que la comprensión de las amenazas al negocio es fundamental, y que el análisis del contexto de seguridad merece un nivel prioritario y un método riguroso de evaluación. Trata los siguientes puntos:

- Análisis de las amenazas, la base para un análisis de riesgos.
- El análisis de las amenazas de seguridad: la piedra angular de cualquier plan estratégico de acción.
- Clasificación: un elemento esencial para las políticas de seguridad. Las empresas que gestionan la seguridad a través de un conjunto de reglas se encuentran obligadas a diferenciar entre las propias reglas y entre las acciones que se tienen que implementar en función de la sensibilidad de la información procesada (CLUSIF, 2010, p. 9).
- Análisis de las amenazas de seguridad: fundamento de la planificación de la información.

Desde una perspectiva general, en la figura 9, se puede observar las fases de Mehari:

Figura 9. Perspectiva general de Mehari
Adaptado de Santonja, 2019.

1.7.7.3 CRAMM

Del acrónimo en inglés *CCTA Risk Analysis and Management Method*. Es una metodología de análisis de riesgos, desarrollada por el Central Communication and Telecommunication Agency (CCTA) del gobierno del Reino Unido, utilizada, por lo general en Europa y dirigida a grandes industrias, entre otras, organizaciones gubernamentales (Aleman & Rodríguez, 2014, p.6). Su versión inicial es de 1987 y su versión vigente la 5.2.

Además, CRAMM

... permite identificar, medir y reducir al mínimo los ataques a los que están expuestas las organizaciones día a día y es definida como una metodología que aplica los conceptos de manera formal, estructurada y disciplinada protegiendo los principios de seguridad de la información de un sistema y de sus activos” (Abril et al, 2013, p. 43).

Cabe resaltar que CRAMM realiza un análisis de riesgos cualitativo y cuantitativo por lo que se conoce como una metodología mixta, se apoya en una herramienta de gestión, lo que permite a las organizaciones tener una visión clara y priorizada de las amenazas a las que está expuesta y pueden afectar los recursos y la continuidad del negocio (Abril et al, 2013, p. 43).

Los elementos que se deben tener en cuenta para realizar un adecuado análisis de riesgos, para obtener un mejor resultado y asegurar la continuidad de negocios, son: activos, vulnerabilidades, riesgos, amenazas, contramedidas, implementación y auditoría

CRAMM se divide en tres etapas, que se muestran en la figura 10.

- Etapa 1: Establecimiento de los objetivos de seguridad. - Recoge la definición global de los objetivos de seguridad.
 - Definición del alcance
 - Identificación y evaluación de los activos físicos y software implicados.
 - Determinación del valor de los datos en cuanto al impacto en el negocio y la identificación.
- Etapa 2: Análisis de riesgos. – Se identifican:
 - Amenazas que afectan al sistema.
 - Vulnerabilidades que explotan dichas amenazas.
 - Cálculo de los riesgos de materialización de las mismas.

- Etapa 3: Identificación y selección los salvaguardas. – Se identifican y seleccionan los controles de seguridad aplicadas en la entidad obteniendo el riesgo residual. CRAMM consta de 31 amenazas genéricas, 8 impactos y 3000 contramedidas.

Figura 10. Etapas de CRAMM
Adaptado de Santonja, 2019.

1.7.7.4 OCTAVE

Del acrónimo en inglés *Operationally Critical Threat, Asset, and Vulnerability Evaluation*, fue publicada por el Software Engineering Institute (SEI) en la Universidad Carnegie Mellon en 1999.

En la tabla 6 podemos apreciar que, desde su aparición, han surgido una serie de actualizaciones y cambios sobre esta metodología.

Tabla 6
Actualizaciones OCTAVE

Fecha	Título de publicación
Setiembre 1999	OCTAVE Framework, versión 1.0
Setiembre 2001	OCTAVE Framework, versión 2.0
Diciembre 2001	OCTAVE Criteria, versión 2.0
Setiembre 2003	OCTAVE - S v0.9

Marzo 2005	OCTAVE - S v1.0
Junio 2007	Introducción de OCTAVE Allegro v1.0

Nota: Adaptado de Santonja, 2019

“OCTAVE, describe un conjunto de criterios para desarrollar métodos que se adhieran a guías específicas de evaluación y administración de riesgos” (Alemán & Rodríguez, 2014, p. 3).

OCTAVE está dirigida al riesgo organizacional y se centra en cuestiones estratégicas relacionadas con la práctica. Se trata de una evaluación flexible que puede adaptarse a la mayoría de las organizaciones (Alberts, Dorofee, Stevens & Woody, 2003, p. 3).

Al aplicar OCTAVE, se equilibran tres aspectos claves que son: riesgo operacional, tecnología y prácticas de seguridad, tal como se aprecia en la figura 11.

Figura 11. Tres Aspectos de equilibrio de OCTAVE
Adaptado de Alberts, Dorofee, Stevens & Woody, 2003

OCTAVE, está destinada a ayudar a las organizaciones en:

- Desarrollar criterios de evaluación de riesgos cualitativos que describan el riesgo operacional y la tolerancia al mismo.
- Identificar los activos que son importantes para el desarrollo de función de la organización.
- Identificar vulnerabilidades y amenazas a esos activos.

- Determinar y evaluar las posibles consecuencias para la organización si se materializan alguna de las amenazas identificadas.

Hasta la fecha OCTAVE tiene 3 métodos:

1.7.7.4.1 Método OCTAVE

Que ha sido definida para grandes organizaciones de trescientos o más empleados (Abril et al, 2013, p. 43). Se basa en dos aspectos: el riesgo operacional y las prácticas de seguridad. Mediante su uso, una organización toma decisiones de protección de la información basadas en riesgos a la confidencialidad, integridad y disponibilidad de los activos relacionados con la información crítica. Todos los aspectos del riesgo (activos, amenazas, vulnerabilidades e impacto organizacional) se tienen en cuenta en la toma de decisiones, que a la organización le permite combinar una estrategia de protección en base a prácticas con sus riesgos de seguridad.

Este método comprende tres fases, que se muestran en la figura 12 y que también se describen a continuación:

Figura 12. Fases del Proceso OCTAVE

Adaptado de <http://seguridades7a.blogspot.com/p/octave.html>

Fase 1: Visión organizativa. - Crear perfiles de amenazas basados en activos, se identifican los activos importantes que están destinados al tratamiento de la información y la estrategia de protección actual sobre esos activos, se documenta los requisitos de seguridad e identifica las amenazas.

Fase 2: Visión tecnológica. - Identificar vulnerabilidades de infraestructura, se realiza la evaluación de la infraestructura para complementar el análisis de amenazas hecho en la fase 1.

Fase 3: Estrategia y desarrollo del plan. - Desarrollar estrategias y planes de seguridad, se identifican los riesgos para los activos críticos de la organización y se decide qué hacer con ellos.

1.7.7.4.2 Método OCTAVE - S

Que se enfoca para pequeñas empresas, por ejemplo, PYMES con veinte a ochenta empleados. Dirigido por un pequeño grupo interdisciplinario de una organización que recopila y analiza información, quienes producen una estrategia de protección y planes de mitigación basados en los riesgos de seguridad operacional únicos de la organización.

OCTAVE – S se basa en tres fases descritas en OCTAVE, aunque el número y la secuencia de actividades difieren de los utilizados en el método OCTAVE.

Fase 1: Crear perfiles de amenazas basados en activos. A continuación, en la tabla 7, se muestra los procesos y actividades.

Tabla 7

Procesos y actividades de la fase 1 - OCTAVE - S

Fase	Proceso	Actividad
Fase 1: Generación de perfiles de amenazas basados en activos, evaluación organizacional	Proceso S1: Identificar la información organizacional	S1.1 Establecer criterios de evaluación de impacto
		S1.2 Identificar los activos organizacionales
		S1.3 Evaluar las prácticas de seguridad organizacional
	Proceso S2: Crear perfiles de amenazas	S2.1 Seleccionar activos críticos
		S2.2 Identificar requisitos de seguridad para activos críticos
		S2.3 Identificar amenazas a activos críticos
		S2.4 Analizar procesos relacionados con la tecnología

Nota: Adaptado de Alberts, Dorofee, Stevens & Woody, 2005.

Fase 2: Identificar vulnerabilidades de infraestructura. A continuación, en la tabla 8, se muestra los procesos y actividades.

Tabla 8
Procesos y actividades de la fase 2 - OCTAVE - S

Fase	Proceso	Actividad
Fase 2: Identificar vulnerabilidades de infraestructura	Proceso S3: Examinar la infraestructura de computación en relación con activos críticos.	S3.1 Examinar rutas de acceso
		S3.2 Analizar procesos relacionados con la tecnología

Nota: Adaptado de Alberts, Dorofee, Stevens & Woody, 2005.

Fase 3: Desarrollar estrategias y planes de seguridad. A continuación, en la tabla 9, se muestra los procesos y actividades.

Tabla 9
Procesos y actividades de la fase 3 - OCTAVE - S

Fase	Proceso	Actividad
Fase 3: Desarrollar estrategias y planes de seguridad	Proceso S4: Identificar y analizar los riesgos	S4.1 Evaluar los impactos de las amenazas
		S4.2 Establecer criterios de evaluación de probabilidad
		S4.3 Evaluar las probabilidades de las amenazas
	Proceso S5: Desarrollar la estrategia de protección y planes de mitigación	S5.1 Seleccionar los activos críticos
		S5.2 Seleccionar enfoques de mitigación
		S5.3 Desarrollar planes de mitigación de riesgos
		S5.4 Identificar cambios en la estrategia de protección
		S5.5 Identificar los siguientes pasos

Nota: Adaptado de Alberts, Dorofee, Stevens & Woody, 2005.

1.7.7.4.3 Método OCTAVE ALLEGRO

Este método está diseñado para permitir una evaluación amplia del entorno de riesgo operacional de una organización con el objetivo de producir resultados más sólidos sin la necesidad de un amplio conocimiento de la evaluación de riesgos.

OCTAVE Allegro puede realizarse en un entorno de colaboración, y está respaldado por guías, hojas de trabajo y cuestionarios. Sin embargo, también es adecuado para el uso de personas que desean realizar una evaluación de riesgos sin una participación organizacional extensa, experiencia o aportes (Caralli, Stevens, Young & Wilson, 2007, p. 4).

Tal como se muestra en la figura 13, OCTAVE Allegro consta de ocho pasos que se organizan en cuatro fases.

Fase 1: Establecer impulsores, la organización desarrolla criterios de medición de riesgo coherentes con los impulsores organizativos.

Fase 2: Perfiles de activos, se perfilan los activos de información que se determinan críticos. Establece límites claros para el activo, se identifica los requisitos de seguridad e identifica los lugares donde se almacena, transporta y procesa el activo.

Fase 3: Identificar amenazas, se identifican en el contexto de las ubicaciones donde se almacena, transporta y procesa el activo.

Fase 4: Identificar y mitigar riesgos, se identifican y analizan los riesgos de los activos de información y se inicia el desarrollo de los enfoques de mitigación (Caralli et al, 2007, p. 5).

Figura 13. Fases y pasos de OCTAVE Allegro
Adaptado de Alberts, Dorofee, Stevens & Woody, 2005.

1.7.7.5 NIST SP 800-30

SP 800-30 - Guía de gestión de riesgos de los sistemas de tecnología de la información. “Es una guía que propone un conjunto de recomendaciones y actividades para una adecuada gestión de riesgos como parte de la gestión de la seguridad de la información” (Alemán & Rodríguez, 2014, p. 77). No obstante, esto no basta, ya que se necesita el apoyo de toda la organización para que los objetivos y alcance de la gestión de riesgos finalice con éxito.

En la figura 14 se puede apreciar la metodología NIST SP 800-30 para el análisis de riesgo, que está compuesta por nueve pasos y son:

- Paso 1: Caracterización del sistema.
- Paso 2: Identificación de amenazas.
- Paso 3: Identificación de vulnerabilidades.
- Paso 4: Análisis de controles.
- Paso 5: Determinación de probabilidades.
- Paso 6: Análisis de impacto.
- Paso 7: Determinación del riesgo.
- Paso 8: Recomendación de controles.
- Paso 9: Documentación de resultados.

Figura 14. Proceso de análisis de riesgos de NIST 800-30
Adaptado de <http://seguridades7a.blogspot.com/p/nist-sp-800-30.html>

Finalmente se puede decir que NIST SP 800-30 se destaca por la gestión de riesgos en proyectos de TI y alcanza niveles satisfactorios en hardware, software, base de datos, redes y telecomunicaciones, ya que su estructura establece los tres criterios más comunes de seguridad, confidencialidad, integridad y disponibilidad, que son la base para realizar el análisis y valorar la materialización de amenazas e impactos sobre los elementos de TI. Pero también, al ser una metodología tan robusta, se convierte en una limitante para su aplicación

en pequeñas empresas con altas limitaciones de recursos humanos (Alemán & Rodríguez, 2014, p. 78).

1.7.7.6 ISO 27005

Es una norma ISO Internacional que no especifica ningún método de análisis de riesgo concreto, sino que, contiene recomendaciones y directrices generales para la gestión de riesgos de seguridad de la información. Depende de la organización definir su enfoque para la gestión de riesgos, dependiendo, por ejemplo, del alcance de un SGSI, el contexto de la gestión de riesgos o el sector industrial.

Esta norma se basa en el método de identificación de riesgos de activos, amenazas y vulnerabilidades que ya no es requerido por ISO/IEC 27001 (ISO/IEC 27005:2018). Sin embargo, respalda los conceptos generales especificados en ISO/IEC 27001 y está diseñada para ayudar en la implementación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

Su primera edición fue publicada el 15 de junio de 2008. Su segunda edición fue publicada el 1 de junio de 2011. Y la tercera edición fue publicada en julio de 2018 con actualizaciones respecto a los requisitos de la norma ISO/IEC 27001:2013.

Como ya mencionamos, no proporciona una metodología concreta de análisis de riesgos, sino que describe a través de su clausulado el proceso recomendado de análisis incluyendo las fases que lo conforman:

- Establecimiento del contexto (Cláusula 7)
- Evaluación de riesgos (Cláusula 8)
- Tratamiento de riesgo (Cláusula 9)
- Aceptación del riesgo (Cláusula 10)
- Comunicación de riesgos (Cláusula 11)
- Seguimiento y revisión de riesgos (Cláusula 12)

Esta norma abarca las mejores prácticas en seguridad de la información, describiendo un conjunto de objetivos de control de seguridad en su contenido.

En la figura 15, se puede apreciar las fases con las que cuenta esta norma, tales como el establecimiento del contexto, identificación del riesgo, estimación del riesgo, evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo y revisión y monitoreo del riesgo.

Figura 15. Procesos de gestión de riesgos de seguridad de la información
Adaptado de ISO/IEC 27005:2018.

1.7.7.7 ISO 31000

Esta norma es una herramienta que establece una serie de principios para la implementación de un Sistema de Gestión de Riesgos en las empresas (ISOTools, 2018, p. 8). Se puede aplicar a cualquier tipo de organización independiente de su tamaño, razón social, mercado, fuente de capital, espectro comercial o forma de financiación.

La norma parte del hecho de que todas las empresas, en mayor o menor medida, llevan a cabo prácticas para la gestión de los riesgos. La diferencia radica en la coordinación y alineamiento de dichas prácticas.

La norma ISO 31000 tiene un enfoque de procesos. Por lo tanto, la implementación de un Sistema de Gestión de Riesgos debe seguir una serie de pasos para que sea eficaz y cumpla con los objetivos trazados al inicio. Los pasos básicos se muestran en la figura 16.

Figura 16. Procesos de gestión de riesgos según ISO 31000
Adaptado de ISOTools, 2018.

1.7.7.8 COSO

Del acrónimo en inglés *Committee of Sponsoring Organizations of the Treadway Commission* - Comisión de Estados Unidos para hacer frente a la información financiera fraudulenta. Es una comisión voluntaria constituida por representantes de cinco organizaciones del sector privado EEUU, para proporcionar liderazgo intelectual frente a tres temas interrelacionados la gestión del riesgo empresarial (ERM), el control interno, y la disuasión del fraude. Las organizaciones son:

- La Asociación Americana de Contabilidad (AAA).
- El Instituto Americano de Contadores Públicos Certificados (AICPA).
- Ejecutivos de Finanzas Internacional (FEI)
- El Instituto de Auditores Internos (IIA)
- La Asociación Nacional de Contadores (ahora Instituto de Contadores Administrativos (AMI)).

Desde su fundación en el año 1985 en EEUU, promovida por las malas prácticas empresariales y los años de crisis anteriores, COSO estudia los factores que pueden dar lugar a información financiera fraudulenta y elabora textos y recomendaciones para todo tipo de organizaciones y entidades reguladoras como el SEC (Agencia Federal de Supervisión de Mercados Financieros) y otros.

COSO tiene como misión “... proporcionar liderazgo intelectual a través del desarrollo de marcos generales y orientaciones sobre la Gestión del Riesgo, Control Interno y Disuasión del Fraude, diseñado para mejorar el desempeño organizacional y reducir el alcance del fraude en las organizaciones.” (COSO, 2004)

1.7.7.8.1 COSO I – Marco Integrado de Control Interno

El resultado de la comisión fue la creación del Marco Integrado de Control Interno (COSO I) publicado en 1992, después modificado en el año 1994 y finalmente en el año 2013. A la fecha se considera el punto de referencia al momento de implementar un sistema de control interno en las compañías.

COSO cree que el control interno tiene que ser un proceso integrado con el negocio que ayude a lograr los resultados que se esperan en materia de rentabilidad y rendimiento.

Es así que, COSO (2013) define el control interno del modelo COSO de la siguiente manera:

“Es un proceso realizado por el consejo, la dirección y otro personal de la entidad, diseñado para proporcionar aseguramiento razonable con respecto al logro de los objetivos relacionados a las operaciones, la fiabilidad de la información financiera y el cumplimiento”.

De este concepto inferimos que el control interno es:

- Orientado al logro de los objetivos.
- Es un proceso continuo e iterativo.
- Depende de todo el personal de la organización.
- Brinda aseguramiento razonable.

- Se adapta a la organización

Los elementos del control interno constan de tres categorías de objetivos y cinco componentes, tal como se muestran en la figura 17.

Figura 17. Elementos de COSO I
Adaptado de Deloitte, 2015

1.7.7.8.2 COSO II – ERM

COSO publicó a partir del año 2004 el conocido COSO ERM (Enterprise Risk Management). Aquí se amplió el concepto de control interno y se dio mayor importancia a la cultura de riesgo en las organizaciones.

El modelo COSO define la ERM, como:

La gestión de riesgos empresariales es un proceso realizado por el Consejo de Administración, la gerencia y otro personal de la entidad, aplicado en la definición de estrategias y en toda la empresa, diseñado para identificar eventos potenciales que podrían afectar a la entidad y gestionar riesgos para que se encuentren dentro de su deseo de arriesgarse, para proporcionar aseguramiento razonable en relación con la consecución de los objetivos de la entidad (COSO, 2004).

COSO ERM está integrado por ocho componentes, que se muestran en la figura 18.

Figura 18. Elementos de COSO ERM.
Adaptado de Deloitte, 2015.

La evaluación del riesgo lo realiza de la siguiente manera:

1. Especifica objetivos para la identificación y valoración de los riesgos relacionados a dichos objetivos.

Es así que un programa de administración integral de riesgos brinda un proceso para la identificación, valoración y respuesta de riesgos que impactan el cumplimiento de los objetivos e iniciativas estratégicas de la compañía.

Figura 19. Vinculación del riesgo con los objetivos y la estrategia
Adaptada de Galaz, 2015.

2. Analiza los riesgos para determinar cómo deben de administrarse.

Para este paso se realiza lo siguiente:

- Identificación de riesgos.
 - Evaluación de riesgos: Inherente y residual.
 - Mantener el equilibrio: Riesgo vs recompensa. Es necesario priorizar la atención en riesgos a los objetivos estratégicos.
 - Enfocarse en el costo total del riesgo. Es decir, el costo total del riesgo debe ser calculado y considerarse en la priorización de las opciones de respuesta al riesgo.
3. Considera la posibilidad de fraude en la evaluación de riesgos. Existen diversos factores de riesgo que pueden propiciar el fraude en las organizaciones, como por ejemplo las que se muestran en la figura 20.

Figura 20. Ejemplos de riesgos de fraude
Adaptado de Galaz, 2015

4. Indica y evalúa cambios que pueden impactar significativamente la gestión de riesgos.

Para este paso se realiza lo siguiente:

- Monitoreo de alertas tempranas, atención en las métricas correctas.
- Evaluar el riesgo con un nuevo giro. Esta nueva visión del riesgo implica considerar impacto vs vulnerabilidad vs velocidad de aparición, dejando en un segundo plano la probabilidad.

1.7.7.9 EBIOS

Del acrónimo francés *Expression des Besoins et Identification des Objectifs de Sécurité*; que quiere decir, expresión de las necesidades e identificación de los objetivos de seguridad.

“Es una metodología francesa de análisis y gestión de riesgos de seguridad de sistemas de información que comprende un conjunto de guías y herramientas de código libre, enfocada a gestores del riesgo de TI” (Alemán & Rodríguez, 2014, p. 78).

Fue fundada en el año 1995 por ANSSI y regularmente actualizada. La ANSSI y EBIOS Club desarrolló la versión 2010 del método EBIOS para tener en cuenta la retroalimentación y los cambios normativos y regulatorios (Ccesa, 2017, p.30).

Es un juego de guías más una herramienta de código libre gratuita, enfocada a gestores del riesgo de TI. Tal como se puede apreciar en la figura 21, esta metodología se desarrolla mediante cinco fases:

Fase 1: Estudio del contexto

Fase 2: Estudio de los eventos peligrosos / las necesidades de seguridad

Fase 3: Estudio de los escenarios de amenazas

Fase 4: Estudio de los riesgos

Fase 5: Estudio de las medidas de seguridad

Figura 21. Ciclo de fases de EBIOS
Adaptado de <http://ingsistemas.ufps.edu.co>

Finalmente, podemos indicar que es una herramienta completa que permite evaluar y abordar los riesgos relacionados con la seguridad informática promoviendo una eficaz comunicación dentro de la organización y entre sus socios, dando cumplimiento a los últimos estándares de la ISO27001, 27005 y 31000.

1.7.7.10 RISK IT

Este marco de referencia para la gestión de riesgos fue publicado en el año 2009 por ISACA, diseñado y creado como un recurso educativo para los oficiales de información, la alta dirección y administración de TI. Se basa en los principios de gestión de los riesgos organizacionales (ERM), las normas y marcos como COSO ERM y ASN/NZS 4360, y provee información de cómo aplicar estos principios a las TI. Además, se complementa con COBIT, que proporciona un marco integral para el control y gestión de las organizaciones de soluciones y servicios de TI.

ISACA (2009), define al RISK IT como un marco de referencia para la gestión de riesgos basado en el valor y beneficios que la organización obtiene a través de las iniciativas de TI. Principalmente se centra en la consecución de objetivos de la organización y en la gestión de los riesgos que causan la no obtención de valor y sus beneficios, y de igual manera analiza el riesgo de no aprovechar las iniciativas y ventajas de TI.

De esta definición es que RISK IT se diferencia de los otros modelos de gestión, ya que los otros modelos priorizan eliminar los riesgos, mientras que RISK IT ve la posibilidad de tomar riesgos que pueden traer beneficios a la organización, teniendo en cuenta que haya un adecuado balance entre el riesgo y el valor para tomar ventaja de TI.

Tal como se puede apreciar en la figura 22, RISK IT está compuesto por tres dominios que incluyen: Gobierno de riesgos, Evaluación de riesgos y Respuesta al riesgo, cada uno con tres procesos, que permite ser una herramienta excelente para ofrecer y mantener valor en las empresas.

Figura 22. Marco RISK IT
Adaptado de ISACA, 2009

1. Gobierno de riesgos

Asegura que las prácticas de gestión de riesgos de TI estén implementadas en la organización, permitiendo asegurar un retorno óptimo ajustado a los riesgos. Tiene los siguientes procesos:

- Establecer y mantener una visión común del riesgo.
- Integrar con ERM.
- Tomar conciencia de las decisiones de riesgos en la organización.

2. Evaluación de Riesgos

Asegurar que las oportunidades y riesgos asociados a TI sean identificados, analizados y presentados en términos comerciales. Tiene los siguientes procesos:

- Recopilar información.
- Analizar los riesgos.
- Mantener un perfil de riesgos.

3. Respuesta ante riesgos

Asegurar que los problemas, oportunidades y eventos relacionados con los riesgos TI sean tratados de forma costo/efectiva y estén alineados con las prioridades del negocio. Tiene los siguientes procesos:

- Articular los riesgos.
- Gestionar el riesgo.
- Reaccionar a eventos de riesgos.

1.7.7.11 CORAS

Del acrónimo en inglés *Consultative Objective Risk Analysis System* “es un proyecto desarrollado desde el año 2001 por SINTEF, un grupo de investigadores noruego financiado por organizaciones del sector público y privado, cuya misión es proporcionar un marco de trabajo encaminado a sistemas en los que la seguridad es crítica” (Aleman & Rodríguez, 2014, p. 78).

Su aplicación permite la detección de fallas de seguridad, inconsistencias, redundancia y el descubrimiento de vulnerabilidades de seguridad, exploradas en siete pasos, tal como se muestra en la figura 23.

Figura 23. Los siete pasos de la metodología CORAS.
Adaptado de <http://seguridades7a.blogspot.com/p/coras.html>

- Paso 1: *Introducción*. - Reunión inicial para presentar los objetivos y el alcance del análisis y obtener información inicial.
- Paso 2: *Análisis de alto nivel*. – Entrevistas para verificar la comprensión de la información obtenida y la documentación analizada. Además, se identifican amenazas, vulnerabilidades e incidentes.
- Paso 3: *Aprobación*. – Descripción detallada de los objetivos, alcance y consideraciones, para su aprobación por parte del destinatario del análisis de riesgos.
- Paso 4: *Identificación de riesgos*. – Identificación detallada de amenazas, vulnerabilidades e incidentes.
- Paso 5: *Estimación del riesgo*. – Estimación de probabilidades e impactos de los incidentes identificados en el paso anterior.
- Paso 6: *Evaluación del riesgo*. – Emisión del informe de riesgos, para su ajuste fino y correcciones.
- Paso 7: *Tratamiento del riesgo*. – Identificación de los controles necesarios y realización del análisis costo – beneficio.

Por otra parte, esta metodología suministra un método basado en modelos, acompañado específicamente de los siguientes componentes:

- Una metodología de análisis de riesgos basados en la elaboración de modelos.
- Un lenguaje gráfico basado en UML (Unified Modelling Language).
- Un editor gráfico para soportar la elaboración de modelos (Microsoft Visio).
- Una biblioteca de casos reutilizables.
- Una herramienta de gestión de casos (gestión y reutilización de casos).
- Representación textual basada en XML (eXtensible Mark-up Language).
- Un formato estándar de informe para facilitar la comunicación de distintas partes en el proceso de análisis de riesgos.

1.7.8 Soluciones de productos comerciales

Se logrado identificar las siguientes herramientas de software que automatizan la operación de un SGSI.

1.7.8.1 ISOTools: Software ISO

Es una plataforma que provee agilidad y mejora de los procesos. Adaptable a cualquier tipo de organización independientemente del tamaño o el sector al que pertenezca. Esta solución

está en un entorno web con el objetivo de dar cumplimiento a los requisitos de las normas ISO. Facilita a las organizaciones la implementación, mantenimiento y mejora continua de los sistemas de gestión ISO como Sistemas de Calidad (ISO 9001), Medio Ambiente (ISO 14001), Seguridad y Salud en el Trabajo (OHSAS 18001) y Seguridad de la Información (ISO 27001).

Los sectores que atiende son los siguientes: Aeroespacial, Alimentación, Automotriz, Colegios, Construcción, Energía, Finanzas, Hidrocarburos, Industria, Minería, Salud, Sector público, Servicios y Transporte.

1.7.8.2 ePULPO

Es una plataforma GRC (Governance, Risk and Compliance Management) para la gestión integral de los procesos de TI y de la seguridad de la información.

“Es una plataforma GRC desarrollada por Ingenia que permite a la organización estar alineada con la actividad TI y relacionarlas con los objetivos del negocio” (García, 2019).

Permitir realizar de una forma eficaz la gestión de riesgos integrada con la solución de la herramienta PILAR. Además, también nos va a permitir un mantenimiento del día a día del cumplimiento que se requiere.

García (2019) menciona que esta herramienta va a permitir realizar una gestión multinorma, es decir facilita el seguimiento y cumplimiento de normativas y estándares establecidos, tales como RGPD (Reglamento General de Protección de Datos), SGSI basado en la norma ISO 27001 o la gestión de servicios basada en ITIL e ISO 20000. Es una plataforma configurable, porque es versátil y puede adaptarse a la necesidad de la organización.

Tiene las siguientes funcionalidades:

- Inventario y gestión de activos
- Gestión de incidentes y peticiones (establecer acuerdos de servicio, tickets).
- Análisis y gestión de riesgos. Integrada con la herramienta PILAR.
- Gestión documental.
- Gestión de planes de acción. A raíz de un análisis GAP o un análisis de riesgo surgen unas acciones a realizar.
- Gestión para el Reglamento General de Protección de Datos.
- Generación de informes.

- Cuadros de mandos, métricas e indicadores.
- Formación

Figura 24. Logo de ePULPO

Adaptado de: <https://www.ingenia.es/pe/productos/epulpo/>

1.7.8.3 EAR PILAR

Las herramientas EAR (Entorno de Análisis de Riesgos) soportan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología MAGERIT y está desarrollada y financiada parcialmente por el CCN (Centro Criptológico Nacional).

PILAR dispone de una biblioteca estándar de propósito general, y es capaz de realizar calificaciones de seguridad respecto de normas ampliamente conocidas como son:

- ISO/IEC 27002 (2005, 2013) - Código de buenas prácticas para la Gestión de la Seguridad de la Información.
- ENS - Esquema Nacional de Seguridad.

Existen diversas variantes:

PILAR: versión íntegra de la herramienta. Se analizan los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Y para el tratamiento del riesgo se propone:

- salvaguardas (o contramedidas)
- normas de seguridad
- procedimientos de seguridad

PILAR Basic: versión sencilla para Pymes y Administración Local. Para tratar el riesgo se proponen salvaguardas (o contramedidas), analizándose el riesgo residual a lo largo de diversas etapas de tratamiento.

μPILAR: versión de PILAR reducida a su mínima expresión, destinada a la realización de análisis de riesgos muy rápidos. Al igual que las anteriores se analizan los riesgos en varias dimensiones y se trata el riesgo proponiendo controles y analizando el riesgo residual.

RMAT (Risk Management Additional Tools) Personalización de herramientas.

- EVL - Perfiles de protección.
- TSV - Perfiles de amenazas.
- KB - Protecciones adicionales: Detallando protecciones adicionales sobre ciertos tipos de activos. Se puede llegar a dar instrucciones al administrador del activo.

Estas herramientas permiten preparar y mantener personalizaciones, que se incorporan dinámicamente a la biblioteca, extendiéndola para adaptarse a un determinado contexto.

1.7.8.4 Inmuno Suite

Es una Suite de Automatización del Sistema de Gestión de Seguridad de la Información conforme a ISO 27001, producido por M&T; que ha sido diseñada por expertos en SGSI y para cumplir exclusivamente con ISO 27001. Cuenta con un módulo de gestión de riesgos complejo y un módulo de operación del SGSI, como se puede apreciar en la figura 25.

Figura 25. Módulos de Inmuno Suite

Adaptado de <https://es.scribd.com/document/248099173/Inmuno-Suite>

Contiene seis herramientas que son las siguientes y se pueden apreciar en la figura 26

1. Una guía de implementación, la cual indica paso a paso las actividades y tareas que se deber realizar a fin de llevar a cabo la implementación de manera autónoma.
2. Automatiza y cumple los requisitos de la norma ISO 27001.
3. Entrenamiento en el uso de Inmuno Suite.
4. Conjunto de plantillas SGSI a partir de las cuales se diseña el SGSI de acuerdo al contexto de la organización, con estas plantillas se arma el “core” del SGSI.
5. Una bolsa de hora de asesoría para atender las principales consultas que tengan los clientes durante el proceso de implementación del SGSI.
6. Una herramienta de soporte técnico en la nube, la cual permite acceder en cualquier momento.

Figura 26. Componentes del servicio de implementación autónoma ISO 27001.
Adoptado de <http://www.americasistemas.com.pe/que-significa-el-sia-27001/>

1.7.9 Conclusiones del estado del arte

Después de haber presentado el estado del arte describiendo formas, metodologías, regulaciones y plataformas existentes para resolver el problema, se concluye que existen productos que resuelven de manera técnica algunos incidentes o necesidades específicas de seguridad de la información. Sin embargo, no se han encontrado formas exactas de resolver

la inseguridad de la información, ya que depende del contexto y del ámbito en el que se desempeña la empresa, además, una organización siempre estará expuesta a diversos factores de riesgo que altere sus procesos de negocio. Si se desea que la organización controle, monitoree, proteja y conserve su información de manera centralizada y sistemática, es necesario adoptar un modelo de gestión de seguridad de la información que vaya más allá de la seguridad informática, es decir que involucre los procesos, personas y tecnología de información. Y es precisamente por ello que se ha decidido por establecer un diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013.

2 MARCO TEÓRICO

En este capítulo se presentarán los principales conceptos necesarios para el entendimiento del desarrollo del proyecto, así como para el diseño del Sistema de Gestión de la Seguridad de la Información para la Municipalidad Distrital de El Agustino. Con esta información proporcionada se podrá dar inicio a la elaboración del diseño del SGSI basado en la norma ISO/IEC 27001:2013.

2.1 Términos básicos

2.1.1 Municipalidad

2.1.1.1 Concepto

Es la institución del estado, con personería jurídica, facultada para ejercer el gobierno de un distrito o provincia, promoviendo la satisfacción de las necesidades de la población y el desarrollo de su ámbito (Municipioaldia.com)

Las Municipalidades o Gobiernos Locales son instituciones que forman parte de la estructura orgánica del Estado. Su principal característica es la cercana relación que mantiene con la comunidad de su jurisdicción. A través de los municipios, la ciudadanía expone los problemas localizados en el desarrollo de su vida cotidiana, canalizando propuestas de solución a favor de la integración de los vecinos para una mejor convivencia en armonía. (Municipioaldia.com).

2.1.1.2 Ley organiza de municipalidades

Es la Ley 27972, que establece las competencias y funciones de los gobiernos locales, su organización y los servicios que presta.

2.1.1.3 Misión

La misión de las municipalidades está contenida en la Ley Orgánica de Municipalidades, que establecen que su finalidad está definida en tres elementos:

- **Ser una instancia de representación.** Son los ciudadanos y ciudadanas, quienes democráticamente deciden otorgar un mandato para que tanto alcaldes como regidores asuman su representación en la conducción del gobierno local, dicho mandato, está sujeto a un conjunto de reglas, que, si no son cumplidas pueden generar el retiro de la confianza ciudadana y por tanto el resquebrajamiento de la legitimidad para ejercer dicha representación. En ese sentido, cobra importancia el vínculo de ida y vuelta que debe existir entre las autoridades municipales y la población, de tal manera que se permita a la población estar informada, intervenir en los asuntos de la gestión y, a las

autoridades municipales ejercer el mandato para el cual fueron elegidas, con eficiencia y transparencia. (Municipioaldia.com)

- **Ser una instancia promotora del desarrollo integral sostenible.** La municipalidad, en tanto, órgano de gobierno local es la entidad llamada y facultada para liderar la gestión del desarrollo integral de su ámbito, ya sea distrital o provincial. Entendiendo por desarrollo integral sostenible un proceso de mejora de la calidad de vida de la población, en donde la persona, especialmente aquella en condiciones de pobreza y exclusión, se convierta en el centro de atención de todos los esfuerzos siempre y cuando ello no comprometa la calidad de vida de las poblaciones futuras.
- **Ser una instancia prestadora de servicios públicos.** Entendidos como aquellos servicios brindados por la municipalidad, que permitan a los ciudadanos, individual o colectivamente ser atendidos en determinadas necesidades que tengan carácter de interés público y sirvan al bienestar de todos.

2.1.2 Activo

“Cualquier cosa que tenga valor para la organización” (ISO/IEC 17799:2005).

2.1.3 Información

Según Wikipedia, es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. En este sentido, permite que el hombre adquiera conocimiento necesario para la toma de decisiones en su vida cotidiana. En la figura 27, se puede apreciar gráficamente el concepto mencionado de lo que es información.

Figura 27. Concepto de Información
Adaptado de: www.ISO27001.es

La información independientemente de su forma en que se guarde o se transmita, ya sea impresa, digital, hablada es considerada como un activo dentro de las organizaciones y que por lo tanto se debe proteger. La información será de utilidad para las organizaciones en la medida que esta facilite la toma de decisiones y como lo menciona Gómez (2011) debe cumplir algunos requisitos tales como: exactitud, completitud, economicidad, confianza, relevancia, nivel de detalle, oportunidad y verificabilidad.

2.1.4 Activo de información

De la definición de la ISO/IEC 17799:2005 Código para práctica de la gestión de la seguridad de la información, un activo de información es “algo a lo que una organización directamente le asignan un valor y, por lo tanto, la organización debe proteger”.

Otra definición importante de activo de información es “aquel bien o servicio tangible o intangible, que genera, procesa o almacena información al cual una organización directamente le atribuye valor y por tanto requiere una adecuada protección y cuidado” (Seminario, 2015).

Los activos de información según INTECO (2010) pueden dividirse en diferentes grupos según su naturaleza y estos son:

- Servicios.
- Datos e información.
- Aplicaciones de software.
- Equipos informáticos.
- Personal.
- Redes de comunicaciones.
- Soportes de información.
- Equipamiento auxiliar.
- Instalaciones.
- Imagen y reputación.

Además, los activos de información también cuentan con ciertas propiedades que se pueden observar en la figura 28.

Figura 28. Propiedades de los activos de información
Adaptado de Seminario, 2015

2.1.5 Seguridad

Se entiende como:

“La ausencia de riesgos en determinados entornos, sean estos humanos o empresariales. La seguridad dentro de una empresa será la capacidad que tienen esta para minimizar los efectos negativos provocados por los riesgos presentes en su entorno, brindando así, un cierto nivel de confianza a los miembros de la comunidad organizacional” (Tupia, 2010, p. 20).

2.1.6 Seguridad de la Información

“Es el conjunto de procesos y actividades que permiten mantener libre de peligros y daños por accidente o ataques a los activos de información que forman parte de una organización” (Tupia, 2010, p. 21).

Otra importante definición “es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y

maximizar el retorno de las inversiones y las oportunidades comerciales” (Aliaga, 2013, p. 12).

Estas definiciones nos conllevan a entender que la seguridad de la información va más allá, ocupándose de los riesgos, beneficios, buen uso, procesos y actividades involucradas con la información y los activos involucrados a ella.

En la figura 29. se muestra los tres elementos claves que son la base en la que se establece la seguridad de la información y, por lo tanto, se tiene que preservar y proteger.

Figura 29. Base de la seguridad de la información
Adaptado de www.rekursostic.educacion.es

Confidencialidad

“Propiedad de que la información no está disponible o divulgada a individuos, entidades o procesos no autorizados” (ISO/IEC 13335-1:2004). Es decir, que la información sea mostrada, manipulada o difundida por aquellas personas que tengan derecho a conocerla, es garantía de que la información llegue solo a las personas autorizadas.

Integridad

“Propiedad de salvaguardar la exactitud y totalidad de los activos” (ISO/IEC 13335-1:2004). La información deber ser protegida contra modificaciones no autorizadas. Esta propiedad es la garantía de que los datos sean correctos y de la completitud de la información (Tupia, 2010, p.20).

Disponibilidad

“Propiedad de estar accesible y utilizable bajo demanda de una entidad autorizada” (ISO/IEC 13335-1:2004). Esta propiedad se refiere a que la información se puede utilizar cuando se la

necesite; es garantía de que los servicios ofrecidos por el negocio, puedan operar y ser usados cuando sea preciso.

Además, dependiendo de las necesidades del negocio, las propiedades a tener en cuenta también son:

Autenticidad

Esta referido a las operaciones de negocio y los intercambios de información entre distintas ubicaciones. Es decir, la garantía de que, quien se hace responsable por una información, transacción o prestación de servicio ante una contraparte, sea quien dice ser. (Tupia, 2010, p. 20).

No repudio

Propiedad que permite que la información sea validada a través de algún mecanismo que compruebe su integridad y contenido, declarándola como genuina.

Auditabilidad

Propiedad que permite garantizar que en todo momento es posible identificar el origen (autor) de la transacción u operación, la fecha de realización y los medios empleados para la misma.

2.1.7 Amenazas

La ISO/IEC 27000:2014 lo define como “causa potencial de un incidente no deseado, que puede provocar daños a un sistema u organización” (p. 11).

Son todas las actividades, eventos o circunstancias que pueden afectar el buen uso de un activo de información dañándolo y no permitiendo que brinde soporte a algún proceso, perjudicando directamente la consecución de los objetivos de negocio (Tupia, 2010, p. 48).

Las amenazas pueden ser:

- Naturales o ambientales: ocasionados por fenómenos de la naturaleza, de carácter ambiental o telúrico.
- Accidentales.
- Técnicas: entre las que pueden destacar
 - Fallas físicas premeditadas: por ejemplo, la colocación de explosivos, robos.

- Fallas no tangibles premeditadas: por ejemplo, fraudes, hacking, espionaje industrial.
- Producidos por el hombre que pueden contener componentes técnicos. Proviene del personal descontento tanto interno como externo a la organización, así como de los denominados ignorantes accidentales quienes, por desconocimiento en el manejo de activos de información actúan como fuentes de amenaza.

2.1.8 Vulnerabilidades

“La vulnerabilidad es el grado de susceptibilidad de un activo a verse afectado por una amenaza” (Tupia, 2010, p. 48).

Las vulnerabilidades se pueden clasificar en las siguientes categorías:

- Seguridad de los recursos humanos (falta de entrenamiento en seguridad, carencia de toma de conciencia en seguridad, falta de mecanismos de monitoreo, falta de políticas para el uso correcto de las telecomunicaciones, no eliminar los accesos al término del contrato de trabajo, carencia de procedimiento que asegure la entrega de activos al término del contrato de trabajo, empleados desmotivados).
- Control de acceso (segregación inapropiada de redes, falta de política sobre escritorio y pantalla limpia, falta de protección al equipo de comunicación móvil, política incorrecta para control de acceso, password sin modificarse).
- Seguridad física y ambiental (control de acceso físico inadecuado a oficinas, salones y edificios, ubicación en áreas sujetas a inundaciones, almacenes desprotegidos, carencia de programas para sustituir equipos, mal cuidado de equipos, susceptibilidad de equipos a variaciones de voltaje).
- Gestión de operaciones y comunicación (complicadas interfaces para usuarios, control de cambio inadecuado, gestión de red inadecuada, carencia de mecanismos que aseguren el envío y recepción de mensajes, carencia de tareas segregadas, carencia de control de copiado, falta de protección en redes públicas de conexión).
- Mantenimiento, desarrollo y adquisición de sistemas de información (protección inapropiada de llaves criptográficas, políticas incompletas para el uso de criptografía, carencia de validación de datos procesados, carencia de ensayos de software, documentación pobre de software, mala selección de ensayos de datos).

2.1.9 Riesgo

“El riesgo es la probabilidad de que una amenaza se materialice explotando una vulnerabilidad sobre el activo, provocando un impacto negativo sobre él” (Tupia, 2010, p. 49).

2.1.10 Impacto

“Es la consecuencia de la materialización de una amenaza sobre un activo aprovechando una vulnerabilidad” (INCIBE, 2016, p. 5).

Se relaciona con la severidad de las consecuencias en caso de que ocurra o se materialice un riesgo, estas consecuencias suelen traducirse en pérdidas económicas, confianza, oportunidades de negocio, etc.

2.1.11 Control

“Medida que modifica el riesgo” (ISO/IEC 27000:2014).

Existen varias formas de establecer controles sobre riesgos organizacionales, los cuales son:

- Disuasivos: su presencia disuade de la comisión de acciones en contra de alguna política o procedimiento establecido y considerado correcto. Ejemplo: cámaras de vigilancia.
- Preventivos: detectan problemas antes que ocurran por medio de monitoreo constante. Ejemplo: políticas de contratación.
- Detectivos: detectan y reportan los problemas suscitados por errores u omisiones, en el momento en que éstos ocurren. Ejemplo: uso de antivirus.
- Correctivos: minimizan el impacto de una amenaza ya consumada. Ejemplo: planes de contingencia.

2.1.12 Políticas de seguridad de la información

Se podría definir como que:

“Son los estándares coherentes de seguridad a nivel de gerencia, usuarios y personal técnico que salvaguardan los activos de información manteniendo un balance adecuado entre el proceso de controlar (costo y esfuerzo para establecer y monitorear controles) y la productividad (los controles no deben complicar la labor de los usuarios de TI). Son documentos de alto nivel que revelan la filosofía corporativa y el pensamiento estratégico de la organización” (Alexander, 2007, p. 45).

A continuación, en la tabla 10, se puede apreciar un ejemplo de este balance:

Tabla 10

Ejemplo del balance control vs productividad en una política de seguridad

Política	Objetivo de control	Control	Forma de aplicación
Cambio de contraseña de acceso a aplicación / red / correo	Solicitar el cambio de la contraseña de acceso a todos los usuarios por periodos de tiempo.	Evitar intromisiones y suplantaciones de identidades.	. Diariamente . Cada 3 meses

Nota: Elaboración propia

2.2 Sistema de Gestión de Seguridad de la Información

2.2.1 Definición

Conocido como SGSI o ISMS – Information Security Management System. “Es un conjunto de procesos que permiten establecer, implementar, mantener y mejorar de manera continua la seguridad de la información, tomando como base para ello los riesgos a los que se enfrenta la organización” (Gómez & Fernández, 2015, p. 11).

La enciclopedia de seguridad informática lo define como “... aquella parte del sistema general de gestión que comprende la política, la estructura organizativa, los recursos necesarios, los procedimientos y los procesos necesarios para implementar la gestión de seguridad de la información en una organización” (Gómez, 2011, p. 52).

Es decir, un SGSI es una forma sistemática de administrar la información sensible de una organización para que permanezca segura, y su implementación supone el establecimiento de procesos formales y una clara definición de responsabilidades en base a una serie de políticas, planes y procedimientos que tienen que constar como información documentada.

Fundamentalmente se distinguen dos tipos de procesos:

1. Procesos de gestión. Controlan el funcionamiento del propio sistema de gestión y su mejora continua.
2. Procesos de seguridad. Se centran en los aspectos relativos a la propia seguridad de la información.

Es importante que el sistema de gestión de seguridad de la información sea parte de y esté integrado con los procesos de la organización y la estructura de gestión general y que la

seguridad de la información se considere en el diseño de procesos, sistemas y controles de la información.

2.2.2 Ciclo de mejora continua

El diseño del SGSI sigue un enfoque basado en procesos que utiliza el ciclo de mejora continua o ciclo de Deming, también conocido como modelo PHVA (PDCA en inglés, Plan – Do – Check – Act).

La norma ISO/IEC 27001 en su versión 2013 no considera el ciclo PDCA como marco obligatorio para la gestión de la mejora continua del SGSI, pero en su apartado 10.2 de la norma ISO/IEC 27001:2013 menciona que la organización debe mejorar continuamente la conveniencia, adecuación y efectividad del Sistema de Gestión de Seguridad de la Información. Es decir, el ciclo PDCA está implícito en la propia estructura de la norma.

El modelo PDCA consta de un conjunto de fases que permiten establecer un modelo comparable a lo largo del tiempo

- **Planificar (Plan)**

En esta fase se planifica la implantación del SGSI. Se determina el contexto de la organización, se definen los objetivos y las políticas que permitirán alcanzarlos.

- **Hacer (Do)**

En esta fase se implementa y se pone en funcionamiento el SGSI. Se ponen en práctica las políticas y los controles que, de acuerdo al análisis de riesgos, se han seleccionado para cumplirlas. Para ello debe disponerse de procedimientos en los que se identifique claramente quién debe hacer qué tareas, asegurando la capacitación necesaria para ello.

- **Verificar (Check)**

En esta fase se realiza la monitorización y revisión del SGSI. Se controla que los procesos se ejecutan de la manera prevista y que además permiten alcanzar los objetivos de la manera más eficiente.

- **Actuar (Act)**

En esta fase se mantiene y mejora el SGSI, definiendo y ejecutando las acciones correctivas necesarias para rectificar los fallos detectados en la anterior fase (Gómez et al., 2015)

En la figura 30, se puede apreciar las fases del ciclo PDCA, además, de como un sistema de gestión utiliza como entrada los requisitos y las expectativas de las partes interesadas, y como se producen, con las acciones y procesos necesarios, los resultados de seguridad de la información que cumplan con los requisitos y expectativas.

Figura 30. Ciclo PDCA

Adaptado del <http://www.ofisegconsulting.com/iso27000.htm>

Para una implementación exitosa de un SGSI, es necesario hacer un mapeo detallado de las actividades de cada fase del modelo PDCA, además de los entregables exigidos por la norma ISO/IEC 27001:2013, en la tabla 11 se especifica las principales actividades que indica la norma en las fases del ciclo de Deming. Además, también en la figura 31 se muestran los procesos del modelo PDCA en la norma ISO/IEC 27001:2013.

Tabla 11

Actividades por cada fase del Modelo PDCA

Ciclo PDCA	Actividades
Planificar (Plan) (Establecer el SGSI)	<ul style="list-style-type: none"> – Definición del alcance y límites del SGSI. – Definir la Política del SGSI. – Realizar el análisis y evaluación de riesgos. – Establecer las operaciones para el tratamiento de riesgos. – Definir las políticas y procedimientos de seguridad y del SGSI. – Obtener la aprobación y autorización de la dirección para implementar el SGSI. – Establecer el SOA (Declaración de Aplicabilidad).

Ciclo PDCA	Actividades
Ejecutar (Do) (Implementar y operar el SGSI)	<ul style="list-style-type: none"> – Formular e implementar el Plan de Tratamiento de Riesgos. – Implementar las políticas y procedimientos SGSI. – Programas de capacitación y toma de conciencia. – Gestionar la operación del SGSI. – Gestionar los recursos para el SGSI.
Verificar (Check) (Monitorear y revisar el SGSI)	<ul style="list-style-type: none"> – Ejecutar procedimientos de monitoreo y revisión del SGSI. – Revisiones regulares de la eficacia del SGSI. – Medir la eficacia de los controles. – Revisar las evaluaciones de riesgos realizadas. – Realizar auditorías internas del SGSI. – Realizar una revisión por la dirección del SGSI. – Registrar las acciones e incidentes de seguridad.
Actuar (Act) (Mantener y mejorar el SGSI)	<ul style="list-style-type: none"> – Implementar las mejoras identificadas en el SGSI. – Tomar las acciones preventivas y correctivas apropiadas. – Actualizar los controles de seguridad. – Comunicar las acciones y mejoras a todas las partes involucradas.

Nota: Adaptado del Curso de Seguridad de la Información por Seminario, 2015.

Figura 31. Ciclo PDCA en ISO/IEC 27001:2013

Adaptado del Taller de transición de la norma ISO/IEC 27001:2005 a la ISO/IEC 27001:2013, por la ONGEI.

2.3 Gestión de riesgos

La gestión de riesgos es una pieza clave dentro de la implementación de un Sistema de Gestión de Seguridad de la Información.

La gestión de riesgos es un proceso que busca establecer un equilibrio entre lo que la empresa “quiere ganar” frente a lo que “está dispuesta a sufrir”: ganancias enfrentadas a las vulnerabilidades y pérdidas que pueda por efecto de las amenazas a sus recursos más críticos. En este caso específico, los recursos de información (Tupia, 2010, p.50).

Es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo.

2.3.1 Análisis de riesgo

Es el primer paso en la gestión de riesgo, que tiene como propósito determinar los componentes de un sistema que requiere protección, sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo.

Cabe mencionar que las fases o etapas que componen un análisis de riesgo dependen de la metodología seleccionada, sin embargo, vamos a utilizar las fases más comunes de la mayoría de las metodologías para el análisis de riesgo. Estas fases se pueden apreciar en la figura 32.

Figura 32. Fases que componen el análisis de riesgo
Adaptado de INCIBE, 2017.

Fase 1: Definir el alcance

El alcance está constituido por los parámetros globales de rendimiento que se espera cumplir dentro de la gestión de riesgo, considerando los factores internos y externos en los que está inmersa la organización, así como un marco de referencia sobre el cual se basa la gestión de riesgo y que sea aplicable a sus características de negocio (presupuestos y capacidades de personal) (Tupia, 2010, p. 56).

Para la elección del marco más adecuado y del alcance del proceso de gestión de riesgo, es necesario entender el entorno de la organización, los factores externos e internos que la afectan, así como las regulaciones pertinentes aplicables a ella. Se debe conocer igualmente, la forma en que los riesgos han sido identificados y controlados hasta el momento (Tupia, 2010, p. 56).

Fase 2: Identificación de activos

Una vez definido el alcance, es necesario identificar los activos más importantes que guardan relación con el departamento, proceso, o sistema objeto del estudio. Este debe hacerse a un nivel de detalle que proporcione información suficiente para la evaluación de riesgos.

La ISO 27005 divide los activos en dos grandes categorías:

1. Los principales activos consisten en procesos de negocio y activos de información. Estos son los principales activos que tienen la mayor importancia para tener en cuenta en el análisis de riesgos.
2. Los activos de apoyo incluyen el hardware, software, redes informáticas, el personal, los sitios y las estructuras organizativas.

A los activos se les tiene que asignar valores para realizar un mejor análisis de riesgo, y puede ser de acuerdo a la escala que se muestra en la tabla 12.

Tabla 12
Ejemplo de escala de valores de los activos

Escala	Valor de los activos
Insignificante	0
Baja	1
Mediana	2
Alta	3

Escala	Valor de los activos
Muy alta	4

Nota: Elaboración propia

Fase 3: Identificación de amenazas

Habiendo identificado los principales activos, ahora hay que identificar las amenazas a las que están expuestos.

Las amenazas se clasifican según su naturaleza y son de seis tipos, tal como se aprecia en la figura 33.

1. Amenazas naturales (inundaciones, tsunamis o maremotos, tornados, huracanes, sismos, tormentas, incendios forestales).
2. Amenazas a instalaciones (fuego, explosión, caída de energía, daño de agua, pérdida de acceso, fallas mecánicas).
3. Amenazas humanas (huelgas, epidemias, materiales peligrosos, problemas de transporte, pérdida de personal clave).
4. Amenazas tecnológicas (virus, hacking, pérdida de datos, fallas de hardware, fallas de software, fallas en la red, fallas en las líneas telefónicas).
5. Amenazas operacionales (crisis financieras, pérdida de suplidores, fallas en equipos, aspectos regulatorios, mala publicidad).
6. Amenazas sociales (motines, protestas, sabotaje, vandalismo, bombas, violencia laboral, terrorismo).

Figura 33. Tipos de amenazas
Adoptado de Alexander, 2007.

Para valorar las amenazas en su justa medida hay que tener en cuenta cual sería el impacto en caso de que ocurrieran y a cuál o cuáles son los parámetros de seguridad que afectaría, si a la confidencialidad, la integridad o la disponibilidad.

Fase 4: Identificación de vulnerabilidades

La siguiente fase consiste en estudiar las características de los activos para identificar puntos débiles o vulnerabilidades. Hay que tener en cuenta que la presencia de una vulnerabilidad por sí misma no causa daño. Para que se produzca este daño debe existir una amenaza que pueda explotarla.

La evaluación de la vulnerabilidad puede ser complicada por una percepción errónea de que las debilidades o deficiencias siempre se asocian con características negativas. Muchas vulnerabilidades en realidad son características negativas como el caso de un sistema de información donde los “parches” no se actualizan. (PECB, 2016, p. 82).

Las vulnerabilidades pueden ser intrínsecas o extrínsecas. Las vulnerabilidades intrínsecas están relacionadas con las características intrínsecas de los activos. Las vulnerabilidades extrínsecas están relacionadas con las características de las circunstancias específicas del activo. Por ejemplo, un servidor que no tiene capacidad para procesar los datos es una víctima de la vulnerabilidad intrínseca y si este servidor está en un sótano en una zona inundable, se somete a una vulnerabilidad extrínseca (PECB, 2016, p. 82).

Las vulnerabilidades se pueden clasificar en:

- Seguridad de los recursos humanos.
- Control de acceso.
- Seguridad física y ambiental.
- Gestión de operaciones y comunicación.
- Mantenimiento, desarrollo y adquisición de sistemas de información.

Fase 5: Evaluación del riesgo

En esta fase disponemos de los siguientes elementos: Inventario de activos, conjunto de amenazas a los que está expuesto cada activo, conjunto de vulnerabilidades asociados a cada activo y el conjunto de medidas implantadas.

Con esta información se puede calcular el riesgo. Para cada par activo-amenaza, se estimará la probabilidad de que la amenaza se materialice y el impacto sobre el negocio que esto produciría. El cálculo del riesgo se puede realizar usando criterios cuantitativos como cualitativos. A continuación, se muestra la tabla 13 sobre la probabilidad de que una amenaza se materialice.

Tabla 13
Probabilidad que una amenaza se materialice

Nivel	Escala Cualitativa	Probabilidad
1	Muy baja	Una vez cada 10 años
2	Baja	Una vez cada 5 años
3	Media	Una vez al año
4	Alta	Una vez al mes
5	Muy alta	Una vez por semana

Nota: Elaboración propia

Luego, pasamos al cálculo del impacto, que puede realizarse con la tabla 14.

Tabla 14
Impacto que una amenaza se materialice

Escala cuantitativa	Escala cualitativa	Impacto
4	Crítico	Afecta irreversiblemente la operatividad, competitividad, rentabilidad o imagen de la organización.
3	Serio	Afecta seriamente la operatividad, competitividad, rentabilidad o imagen de la organización.
2	Medio	Afecta considerablemente la operatividad, competitividad, rentabilidad o imagen de la organización.
1	Mínimo	No afecta considerablemente la operatividad, competitividad, rentabilidad o imagen de la organización.

Nota: Adaptado de Torres, 2018.

Cálculo del riesgo

Dependiendo si se ha optado por un análisis cuantitativo o cualitativo, se calculará el riesgo multiplicando los factores de probabilidad e impacto. Y se obtendrá la matriz que se muestra en la tabla 15.

$$\text{Riesgo} = \text{Probabilidad} \times \text{Impacto}$$

Tabla 15
Matriz del análisis de riesgo

		Impacto			
		Critico (4)	Serio (3)	Medio (2)	Mínimo (1)
Probabilidad	Muy baja (1)	4	3	2	1
	Baja (2)	8	6	4	2
	Media (3)	12	9	6	3
	Alta (4)	16	12	8	4
	Muy alta (5)	20	15	10	5

Nota: Elaboración propia

Priorización del riesgo

Una vez establecida de manera jerárquica el inventario de los escenarios posibles incidentes u amenazas, es necesario definir criterios para una clasificación simple de los riesgos para su priorización (PECB, 2016, p. 96).

En la figura 34, se puede apreciar que el riesgo cero no existe, pero es posible definir un umbral por debajo del cual es aceptable no hacer nada para reducir el riesgo. En el otro extremo de la escala, hay un umbral más allá del cual es riesgo inaceptable, entonces se debe hacer todo lo posible para eliminar su fuente, o reducir los riesgos de forma fiable (PECB, 2016, p. 96).

Figura 34. Priorización de riesgos
Adaptado de PECB, 2016.

Fase 6: Tratamiento del riesgo

Una vez calculado el riesgo, debemos tratar aquellos riesgos que superen un límite que se haya establecido. Por ejemplo, se tratarán aquellos riesgos cuyo valor sea superior a “4” o superior a “Medio” en caso que se haya hecho el cálculo en términos cualitativos.

Se selecciona la opción de tratamiento adecuada (evitar, reducir, transferir o aceptar) para cada uno de los riesgos de la lista. Para elegir las opciones, o una combinación de ellas, se considera no sólo la valoración obtenida para cada riesgo sino también el costo del tratamiento. En la tabla 16 se puede apreciar un ejemplo de las opciones de tratamiento de riesgo bajo el criterio del costo – beneficio.

Tabla 16

Ejemplo de criterios para el tratamiento de riesgos

Costo - Beneficio	Tratamiento
El costo del tratamiento es muy superior a los beneficios.	Evitar el riesgo , por ejemplo, dejando de realizar esa actividad
El costo del tratamiento es adecuado a los beneficios.	Reducir o mitigar el riesgo , seleccionando e implementando los controles o medidas adecuadas que hagan que se reduzca la probabilidad o el impacto.
El costo del tratamiento por terceros es más beneficioso que el tratamiento directo	Transferir el riesgo , por ejemplo, contratando un seguro o subcontratando el servicio.
El nivel de riesgo está muy alejado del nivel de tolerancia	Retener o aceptar el riesgo , sin implementar controles adicionales. Monitorizando para confirmar que no se incrementa.

Nota: Adaptado de INCIBE, 2015.

El resultado de esta fase se concreta en el Plan de Tratamiento de Riesgo (PRT), es decir, la selección y justificación de una o varias opciones para cada riesgo identificado. A este plan se añadirá una relación de riesgos residuales, es decir, aquellos que aún siguen existiendo a pesar de las medidas tomadas.

2.4 ISO/IEC 27001:2013

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y la International Electrotechnical Commission (IEC).

“Es una norma que ha sido preparada para brindar los requisitos para establecer, implementar, mantener y mejorar de manera continua un Sistema de Gestión de Seguridad de la Información (SGSI)” (ISO 27001:2013).

Se deriva de la norma británica BS 7799-2 publicada en 1998, luego revisada en el año 2002 donde se determinó que se incorpore el ciclo de Deming (Plan – Do – Check - Act) para su publicación en el año 2005. La última revisión de esta norma fue publicada en año 2013 y donde su nombre completo oficial es ISO/IEC 27001:2013 Tecnología de la información - Técnicas de seguridad –Sistema de gestión de Seguridad de la información -Requisitos.

En la figura 35, se puede apreciar la historia de la norma.

Figura 35. Origen y evolución de la norma ISO/IEC 27001

Adaptado de <https://www.pmg-ssi.com/2013/08/la-nch-iso-27001-origen-y-evolucion/>

La ISO/IEC 27001 puede ser implementada en cualquier tipo de organización con o sin fines de lucro, pública o privada, grande o pequeña. Además, que permite que una empresa sea certificada, lo que significa que una entidad certificadora independiente acredita que la seguridad de la información ha sido implementada en esta empresa cumpliendo los requisitos de la norma ISO/IEC 27001.

La ISO/IEC 27001:2013 consta de diez cláusulas más el Anexo A, de las cuales las primeras tres son introductorias y presentan el contexto de la norma; y los otros siete, muestran los requisitos para la implementación del SGSI, tal como se puede apreciar en la figura 36.

Figura 36. Cláusulas de la Norma ISO/IEC 27001:2013
Adaptado de ISO/IEC 27001

A continuación, detallamos cada una de las cláusulas:

Cláusula 1: Alcance y campo de aplicación

Indica la finalidad de la norma y el uso de la misma dentro de cualquier tipo de organización.

Cláusula 2: Referencias normativas

Indica que la norma tiene como referencia a la ISO/IEC 27000.

Cláusula 3: Términos y definiciones

Se aplican los términos y definiciones proporcionados en la ISO/IEC 27000.

Cláusula 4: Contexto de la organización

Esta es una de las fases de la planificación del ciclo PDCA y define los requerimientos para comprender la organización en su contexto. Además, comprender las necesidades y expectativas de las partes interesadas y determinar el alcance del Sistema de Gestión de la Seguridad de la Información.

Cláusula 5: Liderazgo

Define las responsabilidades de la alta dirección con respecto al Sistema de Gestión de Seguridad de la Información, demostrando liderazgo y compromiso, estableciendo políticas apropiadas y asignando roles organizacionales.

Cláusula 6: Planificación

Define las acciones para abordar los riesgos. Es decir, se realiza la valoración, análisis y evaluación de los riesgos de la seguridad de la información. También, se realiza el plan de tratamiento de riesgo a los elementos identificados, la declaración de aplicabilidad y se definen los objetivos de seguridad.

Cláusula 7: Apoyo

La organización debe determinar y proporcionar los recursos necesarios para la correcta operación del sistema de gestión. Así también, determinar las competencias necesarias de las personas que trabajan y procurar que el personal tome conciencia de la importancia de las políticas establecidas. Finalmente, toda la información necesaria para esta norma debe estar correctamente documentada.

Cláusula 8: Operación

En este punto la organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información y para implementar las acciones definidas en la planificación. Así también, la organización deber realizar evaluaciones de riesgo en intervalos planificados y el tratamiento de riesgos de seguridad de la información.

Cláusula 9: Evaluación de desempeño

Se define los requerimientos para monitoreo, medición, análisis y evaluación del Sistema de Gestión de Seguridad de la Información a través de los resultados de auditoria interna y por la revisión por parte de la dirección.

Cláusula 10: Mejora

Se define el tratamiento de las no conformidades, acciones correctivas y mejora continua.

Anexo A

Es la serie de objetivos de control de seguridad para la implementación ISO/IEC 27001:2013 y consta de:

- 14 áreas de control: temas principales que cubren la mayoría de los aspectos de seguridad de la información.
- 34 objetivos de control.
- 114 controles: controles aplicables a ser implementados en el Sistema de Gestión de Seguridad de la Información.

En la tabla 17, se puede apreciar las áreas de control con su correspondiente cantidad de controles.

Tabla 17
Áreas de control del Anexo A

Número de Anexo	Área de control	Cantidad de controles
A5	Políticas de seguridad de la información	2
A6	Organización de la seguridad de la información	7
A7	Seguridad de los recursos humanos	6
A8	Gestión de activos	10
A9	Control de acceso	14
A10	Criptografía	2
A11	Seguridad física y ambiental	15
A12	Seguridad de las operaciones	14
A13	Seguridad de las comunicaciones	7
A14	Adquisición, desarrollo y mantenimiento de sistemas	13
A15	Relaciones con los proveedores	5
A16	Gestión de incidentes de seguridad de la información	7
A17	Aspectos de seguridad de la información en la gestión de continuidad de negocio	4
A18	Cumplimiento	8
Número total de controles		114

Nota: Elaboración propia

Finalmente, con respecto a la norma ISO/IEC 27001: 2013, mencionaremos que el proceso de auditoria consta de dos fases, tal como lo indica Gómez (2015):

- Fase 1. El equipo auditor confirma el alcance de la certificación y se asegura de que el nivel de implantación es suficiente para pasar a la fase 2. Para ello se revisa la documentación del sistema de gestión, se recopila información sobre el alcance del sistema, procesos, ubicaciones y aspectos legales, se identifican los aspectos clave del desempeño de procesos, objetivos y funcionamiento del SGSI y se evalúan las auditorías internas y la revisión por la dirección.
- Fase 2. El equipo auditor comprueba que el SGSI descrito en la documentación se encuentra efectivamente implantado. En caso de detectarse alguna no conformidad, se dispondrá de un plazo para subsanarla o presentar un plan de acciones correctoras, cuya implantación será verificada en posteriores auditorías.

2.5 ISO/IEC 27002:2013

Es una norma que establece un catálogo de buenas prácticas que determina una serie de objetivos de control y controles que se integran dentro de todos los requisitos de la norma ISO 27001 en relación con el tratamiento de riesgos. (ISOTools, 2016).

Esta norma fue publicada por la Organización Internacional de Normalización (ISO) y Comisión Electrotécnica Internacional (IEC) como ISO/IEC 17799, pero que tiene su origen en el British Standard BS 7799-1 publicada en el año 1995. Ya en el año 2002 la publicaron como ISO/IEC 17799:2000 y luego de un periodo de revisión y actualización se publicó en el año 2005 la ISO/IEC 17799:2005 hasta el año 2007, donde se cambió el nombre a ISO/IEC 27002:2005, y actualmente estamos con la última versión ISO/IEC 27002:2013.

Como ya mencionamos esta norma está diseñada para que las organizaciones lo utilicen como referencia en la selección de controles dentro del proceso de implementación de un SGSI en base a la ISO 27001, o como un documento guía para las organizaciones que implementan controles de seguridad de la información comúnmente aceptados. Es importante también mencionar que esta norma es para todos los tipos y tamaños de organizaciones, incluyendo al sector público y privado, comercial y sin fines de lucro.

La ISO/IEC 27002:2013 consta de 14 cláusulas de control de seguridad, que a su vez tienen un total de 35 objetivos de control y 114 controles. Estas se pueden observar en la figura 37 y que a continuación pasamos a describir.

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD. 5.1 Directrices de la Dirección en seguridad de la información. 5.1.1 Conjunto de políticas para la seguridad de la información. 5.1.2 Revisión de las políticas para la seguridad de la información. 6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN. 6.1 Organización interna. 6.1.1 Asignación de responsabilidades para la seguridad de la información. 6.1.2 Segregación de tareas. 6.1.3 Contacto con las autoridades. 6.1.4 Contacto con grupos de interés especial. 6.1.5 Seguridad de la información en la gestión de proyectos. 6.2 Dispositivos para movilidad y teletrabajo. 6.2.1 Política de uso de dispositivos para movilidad. 6.2.2 Teletrabajo. 7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS. 7.1 Antes de la contratación. 7.1.1 Investigación de antecedentes. 7.1.2 Términos y condiciones de contratación. 7.2 Durante la contratación. 7.2.1 Responsabilidades de gestión. 7.2.2 Conciliación, educación y capacitación en seguridad de la información. 7.2.3 Proceso disciplinario. 7.3 Cese o cambio de puesto de trabajo. 7.3.1 Cese o cambio de puesto de trabajo. 8. GESTIÓN DE ACTIVOS. 8.1 Responsabilidad sobre los activos. 8.1.1 Inventario de activos. 8.1.2 Propiedad de los activos. 8.1.3 Uso aceptable de los activos. 8.1.4 Devolución de activos. 8.2 Clasificación de la información. 8.2.1 Directrices de clasificación. 8.2.2 Etiquetado y manipulación de la información. 8.2.3 Manipulación de activos. 8.3 Manejo de los soportes de almacenamiento. 8.3.1 Gestión de soportes extraíbles. 8.3.2 Eliminación de soportes. 8.3.3 Soportes físicos en tránsito. 9. CONTROL DE ACCESOS. 9.1 Requisitos de negocio para el control de accesos. 9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados. 9.2 Gestión de acceso de usuario. 9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.5 Revisión de los derechos de acceso de los usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso. 9.3 Responsabilidades del usuario. 9.3.1 Uso de información confidencial para la autenticación. 9.4 Control de acceso a sistemas y aplicaciones. 9.4.1 Restricción de acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario. 9.4.4 Uso de herramientas de administración de sistemas. 9.4.5 Control de acceso al código fuente de los programas.	10. CIFRADO. 10.1 Controles criptográficos. 10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves. 11. SEGURIDAD FÍSICA Y AMBIENTAL. 11.1 Áreas seguras. 11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.4 Protección contra las amenazas externas y ambientales. 11.1.5 El trabajo en áreas seguras. 11.1.6 Áreas de acceso público, carga y descarga. 11.2 Seguridad de los equipos. 11.2.1 Emplazamiento y protección de equipos. 11.2.2 Instalaciones de suministro. 11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos. 11.2.5 Salida de activos fuera de las dependencias de la empresa. 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento. 11.2.8 Equipo informático de usuario desistado. 11.2.9 Política de puesto de trabajo desapejado y bloqueo de pantalla. 12. SEGURIDAD EN LA OPERATIVA. 12.1 Responsabilidades y procedimientos de operación. 12.1.1 Documentación de procedimientos de operación. 12.1.2 Gestión de cambios. 12.1.3 Gestión de capacidades. 12.1.4 Separación de entornos de desarrollo, prueba y producción. 12.2 Protección contra código malicioso. 12.2.1 Controles contra el código malicioso. 12.3 Copias de seguridad. 12.3.1 Copias de seguridad de la información. 12.4 Registro de actividad y supervisión. 12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes. 12.5 Control del software en explotación. 12.5.1 Instalación del software en sistemas en producción. 12.6 Gestión de la vulnerabilidad técnica. 12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software. 12.7 Consideraciones de las auditorías de los sistemas de información. 12.7.1 Controles de auditoría de los sistemas de información. 13. SEGURIDAD EN LAS TELECOMUNICACIONES. 13.1 Gestión de la seguridad en las redes. 13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.1.3 Segregación de redes. 13.2 Intercambio de información con partes externas. 13.2.1 Políticas y procedimientos de intercambio de información. 13.2.2 Acuerdos de intercambio de información. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.	14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN. 14.1 Requisitos de seguridad de los sistemas de información. 14.1.1 Análisis y especificación de requisitos de seguridad. 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas. 14.1.3 Protección de las transacciones por redes telemáticas. 14.2 Seguridad en los procesos de desarrollo y soporte. 14.2.1 Política de desarrollo seguro de software. 14.2.2 Procedimientos de control de cambios en los sistemas. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. 14.2.4 Restricciones a los cambios en los paquetes de software. 14.2.5 Uso de principios de ingeniería en protección de sistemas. 14.2.6 Seguridad en entornos de desarrollo. 14.2.7 Externalización del desarrollo de software. 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9 Pruebas de aceptación. 14.3 Datos de prueba. 14.3.1 Protección de los datos utilizados en pruebas. 15. RELACIONES CON SUMINISTRADORES. 15.1 Seguridad de la información en las relaciones con suministradores. 15.1.1 Política de seguridad de la información para suministradores. 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores. 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones. 15.2 Gestión de la prestación del servicio por suministradores. 15.2.1 Supervisión y revisión de los servicios prestados por terceros. 15.2.2 Gestión de cambios en los servicios prestados por terceros. 16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN. 16.1 Gestión de incidentes de seguridad de la información y mejoras. 16.1.1 Responsabilidades y procedimientos. 16.1.2 Notificación de los eventos de seguridad de la información. 16.1.3 Notificación de puntos débiles de la seguridad. 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones. 16.1.5 Respuesta a los incidentes de seguridad. 16.1.6 Aprendizaje de los incidentes de seguridad de la información. 16.1.7 Recopilación de evidencias. 17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO. 17.1 Continuidad de la seguridad de la información. 17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 17.2 Redundancias. 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información. 18. CUMPLIMIENTO. 18.1 Cumplimiento de los requisitos legales y contractuales. 18.1.1 Identificación de la legislación aplicable. 18.1.2 Derechos de propiedad intelectual (DPI). 18.1.3 Protección de los registros de la organización. 18.1.4 Protección de datos y privacidad de la información personal. 18.1.5 Regulación de los controles criptográficos. 18.2 Revisiones de la seguridad de la información. 18.2.1 Revisión independiente de la seguridad de la información. 18.2.2 Cumplimiento de las políticas y normas de seguridad. 18.2.3 Comprobación del cumplimiento.
---	---	---

Figura 37. Cláusulas de la ISO/IEC 27002:2013
Adaptado de <http://www.iso27000.es/iso27000.html>

Cláusula 5 – Políticas de Seguridad

Se refiere a la necesidad de definir, publicar y revisar los diferentes tipos de políticas requeridas para la gestión de la seguridad de la información.

Cláusula 6 – Organización de la seguridad de la información

Se refiere a la necesidad definir y asignar las funciones y responsabilidades necesarias para los procesos y actividades de gestión de la seguridad de la información.

Cláusula 7 – Seguridad de los recursos humanos

Se refiere a los controles necesarios para los procesos relacionados con la contratación del personal, su trabajo durante el empleo y después de la finalización del contrato.

Cláusula 8 – Gestión de activos

Se refiere a las responsabilidades requeridas que se definen y asignan para los procesos y procedimientos de gestión de activos.

Cláusula 9 – Control de accesos

Se refiere a los requisitos para controlar el acceso a los activos de información y las instalaciones de procesamiento de información.

Cláusula 10 – Cifrado

Se refiere a las políticas sobre los controles criptográficos para la protección de la información para garantizar el uso adecuado y eficaz de la criptografía con el fin de proteger la confidencialidad, autenticidad, integridad, no repudio y autenticación de la información.

Cláusula 11 – Seguridad física y ambiental

Se refiere a la necesidad de prevenir el acceso físico no autorizado, los daños y las interferencias a las instalaciones de información y procesamiento de información de la organización.

Cláusula 12 – Seguridad de las operaciones

Se refiere a la capacidad de la organización para asegurar que las operaciones sean correctas y seguras.

Cláusula 13 – Seguridad de las comunicaciones

Se refiere a la capacidad de la organización para garantizar la protección de la información en sistemas y aplicaciones en redes y sus instalaciones de procesamiento de información y apoyo.

Cláusula 14 – Adquisición de sistemas, desarrollo y mantenimiento

Se refiere a los controles para la identificación, análisis y especificación de los requisitos de seguridad de la información, la seguridad de los servicios de aplicación en los procesos de desarrollo y soporte.

Cláusula 15 – Relaciones con los proveedores

Se refiere a los controles en relación con los proveedores, incluyendo las políticas y procedimientos de seguridad de la información.

Cláusula 16 – Gestión de incidencias que afectan la seguridad de la información

Se refiere a los controles de responsabilidades y procedimientos, información de informes y debilidades de seguridad, evaluación y decisión sobre eventos de seguridad de la información.

Cláusula 17 – Aspectos de seguridad de la información para la gestión de la continuidad del negocio

Se refiere a la capacidad de la organización para contrarrestar las interrupciones de las operaciones normales, incluyendo la disponibilidad de instalaciones de procesamiento de información, verificar, revisar y evaluar la continuidad de la seguridad de la información.

Cláusula 18 – Conformidad

Se refiere a la capacidad de la organización para cumplir con los requisitos reglamentarios, estatutarios, contractuales y de seguridad.

2.6 ISO 31000

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO), que proporciona directrices para gestionar el riesgo al que se enfrentan las organizaciones. La aplicación de estas directrices puede adaptarse a cualquier organización y a su contexto, (ISO 31000:2018).

En la figura 38, se aprecia que la norma está estructurada por tres componentes que son:

- Los principios para la gestión del riesgo.
- El marco de referencia
- El proceso de gestión de riesgo.

Estos componentes podrían existir previamente en toda o parte de la organización, sin embargo, podría ser necesario adaptarlos o mejorarlos para que la gestión de riesgo sea eficiente, eficaz y coherente.

Figura 38. Principios, marco de referencia y proceso de la ISO 31000
Adaptado de ISO 3100:2018

Principios

El propósito de la gestión del riesgo *es la creación y la protección del valor*. Por lo tanto, los principios proporcionan orientación sobre las características de una gestión de riesgo eficaz y eficiente, comunicando valor y explicando su intención y propósito. Son ocho los principios, que a continuación se detallan:

1. Integrada. - La gestión del riesgo es parte integral de todas las actividades de la organización.
2. Estructurada y exhaustiva. - Este principio contribuye a la gestión del riesgo a que los resultados sean coherentes y comparables.
3. Adaptada. - La gestión del riesgo se debe alinear con el contexto externo e interno y los objetivos de la organización.

4. Inclusiva. - Una buena gestión del riesgo incluye la participación apropiada y oportuna de las partes interesadas permitiendo que se consideren su conocimiento, puntos de vista y percepciones.
5. Dinámica. - Los riesgos pueden aparecer, cambiar o desaparecer con los cambios de los contextos externo e interno de la organización. La gestión del riesgo anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna.
6. Mejor información disponible. - Las entradas a la gestión del riesgo se basan en información histórica y actualizada, así como en expectativas futuras.
7. Factores humanos y culturales. - En la gestión del riesgo influyen considerablemente el comportamiento humano y la cultura en todos los niveles y etapas.
8. Mejora continua. - La gestión del riesgo mejora continuamente mediante aprendizaje y experiencia.

Marco de referencia

El marco de referencia implica integrar, diseñar, implementar, valorar y mejorar la gestión de riesgo a lo largo de toda la organización, y por otro lado la alta dirección debe demostrar su liderazgo y compromiso con el sistema de gestión de riesgo, y para ello deberá:

- Implementar todo el marco de referencia.
- Definir y publicar una política de gestión de riesgos.
- Asignar recursos para la gestión de riesgos.
- Comunicar los beneficios de la gestión de riesgos.
- Asignar roles, responsabilidades y autoridades.
- Rendir cuentas por gestionar el riesgo.

La integración de la gestión de riesgo depende de la comprensión de las estructuras y el contexto de la organización, es por ello que todos tienen la responsabilidad de gestionarlo. La organización debe analizar y comprender sus contextos externos e internos cuando diseñe el marco de referencia para gestionar el riesgo. La implementación del marco de referencia debe implementar valorando su eficacia, haciendo seguimiento y mejorando continuamente su idoneidad, adecuación y eficacia (Equipo Lteam, 2019).

Proceso

El proceso de la gestión del riesgo implica la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registro e informe del riesgo. La comunicación y consulta de las partes externas e internas deberán llevarse a cabo en todas las partes del proceso, ellas deberán comprender el riesgo y las bases con que se toman las decisiones.

En la figura 39, se muestra todo el proceso de gestión de riesgo, que a continuación pasamos a explicar.

Figura 39. Proceso de la gestión de riesgo de la ISO 31000
Adaptado de ISO 31000:2018

Alcance, contexto y criterios

El propósito del establecimiento del alcance, contexto y criterios es adoptar el proceso de la gestión del riesgo, para permitir una evaluación del riesgo eficaz y un tratamiento apropiado del riesgo. El alcance, contexto y criterios implica definir el alcance del proceso, y comprender los contextos externo e interno.

Evaluación del riesgo

Es el proceso global de identificación, análisis y valoración del riesgo.

1. Identificación del riesgo, en esta fase se debe atender lo siguiente:
 - Fuentes de riesgos tangibles e intangibles.
 - Causas y eventos.
 - Oportunidades.
 - Fortalezas y debilidades.
 - Contexto interno y externo.
 - Indicadores generales de riesgo.
 - Activos y recursos de la organización.
 - Dificultades de acceso a la información y calidad de la misma.
2. Análisis de los riesgos, en esta fase se debe atender los siguientes factores:
 - Probabilidad de los eventos.
 - Naturaleza y magnitud de las consecuencias.
 - La complejidad.
 - Factores relacionados con el tiempo.
 - Eficacia de los controles existentes.
3. Valoración del riesgo, en esta fase se deben comparar los resultados del análisis, con los criterios del riesgo y decidir:
 - No hacer nada.
 - Opciones nuevas de tratamiento de riesgo.
 - Análisis adicional.
 - Mantener los controles existentes.
 - Reconsiderar los objetivos.

Tratamiento de riesgo

- Formular opciones para el tratamiento de riesgo.
- Seleccionar la opción más adecuada, esta requiere considerar el costo, el esfuerzo y las consecuencias de la implementación. Las opciones de tratamiento de riesgo son:
 - ✓ Eliminar el riesgo
 - ✓ Asumir el riesgo
 - ✓ Disminuir la probabilidad de ocurrencia
 - ✓ Disminuir el impacto negativo
 - ✓ Compartir el riesgo

✓ Retener el riesgo

- Planificar e implementar el tratamiento de riesgo.
- Evaluar la efectividad de las acciones implementadas.
- Calificar el riesgo residual aceptable o no aceptable.
- Tratamiento para el riesgo residual no aceptable.

2.7 Análisis de Brechas - GAP

“El análisis de brecha es una técnica para determinar los pasos para pasar del estado actual a un estado futuro deseado” (PECB, 2016, p. 144).

Un análisis de brechas se lleva a cabo en tres etapas:

1. Determinar el estado actual: a fin de identificar, en la organización, los procesos y controles de seguridad vigentes con sus características.
2. Identificación de objetivos: por comparación con otras organizaciones (o de otras divisiones de la organización) determinar el grado de madurez necesario para cada control de seguridad.
3. Análisis de brechas: el análisis de la disparidad es identificar las diferencias que puedan existir entre los controles de seguridad en la actualidad y a los requisitos de la norma ISO/IEC 27001. Esto permite a la empresa determinar cuáles son los procesos actuales que necesitan mejoras.

2.7.1 Modelo de madurez

“Un Modelo de Madurez es una medición estructurada del desempeño organizacional que permite identificar vacíos o debilidades para así establecer procesos de mejora continua” (Holguín & Lema, 2019, pp. 3). Además, también nos indica que un modelo de madurez es un esquema con niveles jerárquicos, que permiten a una organización comprender su situación actual y orientarla a la consecución de un nivel más elevado lo cual requiere la implementación de mejores prácticas o rutas de mejora.

Hay varios modelos de para medir la madurez como COBIT, ITIL, CMMI, etc. Para este proyecto, dentro de los modelos destaca el CMMI, ya que tiene como fortaleza la priorización de los esfuerzos iniciales como soporte para la transición evolutiva. En la figura 40, se aprecia el modelo con sus respectivos niveles de madurez.

Figura 40. Niveles de madurez CMMI

Adaptado de <http://rupandcmmi.blogspot.com/p/niveles-de-madurez.html>

Inicial (1): Los procesos son generalmente ad-hoc y caóticos. La organización no proporciona un entorno estable para dar soporte a los procesos. A menudo se producen productos y servicios que funcionan, sin embargo, exceden sus presupuestos y no cumplen sus calendarios.

Administrado (2): Los proyectos de la organización han asegurado que los procesos se planifican y realizan de acuerdo a políticas. Los procesos se realizan y gestionan de acuerdo a sus planes documentados

Definido (3): Los procesos son bien caracterizados y se describen en estándares, procedimientos, herramientas y métodos. Los procesos estándar de la organización se usan para establecer la consistencia en la organización. Un proceso definido establece claramente el propósito, entradas, actividades, roles, medidas, etapas de verificación, salidas y criterios de salida.

Administrado cuantitativamente (4): La organización y los proyectos establecen objetivos cuantitativos en cuanto al rendimiento de calidad. Los objetivos cuantitativos los utilizan como criterios de gestión de los procesos. El rendimiento de calidad y del proceso se comprende en términos estadísticos y se gestionan durante la vida del proceso.

Optimizado (5): Se centra en mejorar continuamente el rendimiento de sus procesos mediante mejoras incrementales de proceso y tecnológicas. La organización se interesa en tratar causas comunes de variación del proceso y cambia el proceso para mejorar el rendimiento y alcanzar sus objetivos cuantitativos de mejora.

3 DEFINICIÓN DEL PROBLEMA

3.1 Introducción

Hoy en día, la sociedad digital cada vez más compleja y a medida que se incrementa nuestra dependencia de los datos y la interconectividad, es necesario estar preparado y desarrollar resiliencia a los diversos ataques cibernéticos a los que están expuestas las organizaciones, quienes tienen muchos errores en cuestión de seguridad, tanto a nivel técnico como de procedimientos.

En los últimos años, los delitos económicos y el fraude tienen mayor visibilidad y no existe compañía invulnerable, independientemente de su tamaño, no hay sector que se haya salvado de recibir estos ataques. De acuerdo a la encuesta global sobre delitos económicos y fraude 2018 de la PwC (PricewaterhouseCooper) el 49% de los entrevistados comentó que su empresa sufrió fraude en los últimos dos años y para el caso del Perú el 55%, tal como se puede apreciar en la figura 41.

Figura 41. Perspectiva global sobre delitos económicos y fraude
Adaptado de la encuesta global sobre delitos económicos y fraude 2018 de PwC.

Aunque si bien, ya las empresas parecen estar reaccionando y ser conscientes de los peligros que conlleva un ataque, la mayoría todavía no se encuentra preparada para defenderse o lidiar con ello. En la figura 42 se aprecia que según los resultados de la encuesta global de seguridad de la información 2018 por PwC de Argentina, a nivel mundial el 44% del total de encuestados no posee una estrategia general de seguridad de la información y a nivel de América del Sur el 48%. Con respecto al programa de capacitación y concientización al personal, también tiene un porcentaje alto, un 48% indica no contar con un programa de

capacitación de seguridad para sus empleados; y finalmente el 54% carece de un plan contingencia ante un incidente.

Figura 42. Encuesta global de seguridad.

Adaptado de los resultados de la encuesta global de seguridad de la información 2018 de PwC.

Si bien es cierto que en general el 92% de las organizaciones se preocupan por la función de seguridad de la información, en áreas claves, se nos viene la pregunta: ¿la función de seguridad de la información cumple con las necesidades de la organización?, a lo que la encuesta global de seguridad de la información 2018-19 de EY Latam, responde que solo el 8% de las organizaciones tienen funciones de seguridad de la información que satisfacen totalmente sus necesidades y un 59% cumple parcialmente, pero con planes de mejorar, tal como se puede apreciar en la figura 43.

Figura 43. ¿La función de seguridad de la información cumple con las necesidades de la organización?

Adaptado de Encuesta Global de la Información 2018-19 de EY Latam

En estos días, el ataque a los activos de las empresas es cada vez más constante, ya que de lo anteriormente mencionado la función de la seguridad de información cumple parcialmente su función para los que poseen una estrategia de seguridad. Así se revela en la encuesta global realizada por PwC sobre delitos económicos y fraude 2018, la apropiación ilícita de los activos lidera los tipos de fraude cometidos con un 45% a nivel mundial y en el Perú con un 60%, a esto le sigue también el cibercrimen con un 31% a nivel mundial y un 16% en el Perú, tal como se puede apreciar en la figura 44.

Figura 44. Tipos de delito más cometido
Adaptado de Encuesta global sobre delitos económicos y fraude 2018 de PwC

Como ya se ha mencionado también, un activo es cualquier cosa que tenga valor para la organización y por lo tanto tiene que ser protegido de amenazas y vulnerabilidades, y según la encuesta global de seguridad de la información 2018-19 de EY Latam las vulnerabilidades que presentan más riesgo a la organización son: los empleados descuidados o inconscientes con un 34%, los controles de seguridad obsoletos con un 26% y el acceso no autorizado con un 13% y otros más que también se pueden apreciar en la figura 45.

Figura 45. Vulnerabilidades con mayor exposición a los riesgos
Adaptado de la encuesta global de seguridad de la información 2018-19 de EY Latam.

El daño que todas las acciones mencionadas anteriormente ocasionan a una organización se reduce en pérdidas económicas. Según el estudio que presentó el integrador de seguridad de informática Digiware (2016); Brasil, México y Colombia países de América Latina se vieron afectados por ataques informáticos con pérdidas de 184.000 millones de dólares. El Perú no es ajeno a estas estadísticas ya que aumento de 3.600 millones a 4.000 millones de dólares respecto al año anterior. Además, la encuesta global sobre delitos económicos y fraude 2018 de PwC, en la figura 46 muestra el promedio que la organización considera haber perdido a través de un delito informático a nivel mundial y el Perú.

Figura 46. Impacto de los delitos económico en las organizaciones.
Adaptado de la encuesta global de seguridad de la información 2018 de PwC.

Finalmente, en base a lo presentado y analizando los resultados de las encuestas, pareciera que muchas empresas no saben o no cuentan con los recursos necesarios para lidiar con los riesgos, amenazas y vulnerabilidades. Por eso; es necesario presentar, tal como se muestra en la figura 47, el estudio donde se menciona que la adopción de un sistema de seguridad de la información trae muchos beneficios a la organización. Lo más destacado es que las empresas identificaron y priorizaron sus riesgos a los que estaban expuestos, y más allá de solo la evaluación de los riesgos, pudieron hacer frente a los incidentes de seguridad más rápido ya que cuentan con controles precisos. Además, que permite que los datos sensibles estén resguardados en forma segura, existe una comprensión de las brechas de seguridad y hay una mejor comunicación de los incidentes.

Figura 47. Beneficios de la Seguridad de Información.

Adaptado de los resultados de la encuesta global de la seguridad de la información 2016 de PwC.

3.2 Definición del problema

3.2.1 Análisis del problema

Como se mencionó en el capítulo 1, el problema principal de la Municipalidad Distrital de El Agustino es la falta de un modelo de gestión de seguridad de la información que permita gestionar la seguridad de la información que compromete la confidencialidad, integridad y disponibilidad de la información, para tal caso se identificaron situaciones específicas que dan evidencia del problema y que generaría riesgo a la municipalidad.

Los problemas que se identificaron en la MDEA son:

- Pérdidas de información confidencial tanto en forma física como digital de los contribuyentes y/o ciudadanos, como también propia de las áreas de la institución. Ya sea por robo por parte de empleados, exempleados o personas ajenas que ingresan a las instalaciones de la municipalidad, tal como se puede apreciar en la figura 48, los archivos con documentos se encuentran expuestos a cualquier extracción. Es así que, como ya mencionamos el descuido del personal o la falta de conciencia en seguridad de la información es lo que genera más riesgo a una organización.

Otra ubicación de la información es en los servidores, que actualmente no cuentan con niveles de acceso restringido y sin ninguna jerarquización o clasificación del tipo de información. Además, que actualmente tampoco cuentan con un sistema de respaldo de la información.

Otra pérdida de información se da debido a desperfectos técnicos en los servidores, que no cuentan con soporte técnico y mantenimiento correctivo afectando en gran medida la confidencialidad, integridad y disponibilidad de la información de la municipalidad.

Figura 48. Oficina administrativa de rentas
Elaboración propia

- Ausencia de un inventario de activos de información relacionados al proceso de recaudación y fiscalización tributaria de la municipalidad. Impidiendo así, realizar un análisis de riesgo que permita identificar las amenazas y vulnerabilidades a los que están expuestos los activos de información.
- Falta de conocimientos de seguridad de la información por falta de capacitación y concientización que involucre a la alta dirección en nuestro caso al alcalde y a todo el personal que labora en la institución, ya que es uno de los mayores problemas en las organizaciones. Según la encuesta realizada por Cisco sobre seguridad a empleados españoles, el 48% no tienen conciencia sobre las amenazas de seguridad más conocidas, convirtiéndose en una creciente fuente de riesgos. Es decir, el propio comportamiento del empleado es uno de los mayores riesgos de seguridad, dado que esperan que los mecanismos de seguridad implementados por la municipalidad se ocupen de todo y no son conscientes del verdadero peligro de las amenazas y sin asumir ninguna responsabilidad personal para proteger la información corporativa. En la figura 49 se aprecia la encuesta.

Figura 49. Mayores fuentes de riesgo para la seguridad de datos
Adaptado de la encuesta de Cisco a 1000 empleados de empresas españolas.

- Inadecuada red LAN, que no cumple con las especificaciones técnicas de cableado estructurado, lo que conlleva a que los equipos pierdan constantemente comunicación con el servidor, conexión a internet deficiente, mucho desorden con el cableado, excesos de dispositivo conectados, etc. Lo mismo sucede en el centro de datos, donde se encuentran los servidores y equipos de comunicación totalmente desordenados y propensos a sufrir cualquier daño físico. Eso se puede evidenciar en las figuras 50, 51 y 52.

Figura 50. Oficina de TI
Elaboración propia

Figura 51. Oficina de rentas
Elaboración propia

Figura 52. Gabinete del área de TI
Elaboración propia

Como consecuencia de lo indicado con la red LAN, en la tabla 18 se muestra los incidentes registrados correspondiente al año 2018.

Tabla 18
Incidentes reportados del año 2018

Nº	Incidencias	Total
1	Deterioro de conectores RJ45	9
2	Cableado de red expuesto	26
3	Rosetas expuestas	13
4	Daño de cable de red por roedores	7
5	Interrupción de conectividad de la red	56

Nota: Reporte de soporte de la subgerencia de TI

3.2.2 Causas del problema

Lo que origina los problemas mencionados en la municipalidad son:

- No existe una clasificación de la información dentro de los activos de información, clasificada como: privada, confidencial y pública.
- Falta de un inventario de activos de información que estén involucrados en el proceso de recaudación y fiscalización tributaria.
- Falta de identificación de los procesos críticos de la municipalidad, que son la base para una clasificación de los impactos operacionales.
- Falta de controles de acceso a los sistemas críticos de la municipalidad, como al sistema de cobranzas, caja, fiscalización, etc.
- No existe un Sistema de Gestión de Seguridad de la Información donde se consigne las políticas, procedimientos y estándares relacionados con la protección de los activos de la información de la municipalidad.
- Falta de personal con las competencias necesarias para asumir las responsabilidades de la seguridad de la información.

3.3 Impacto del problema en la municipalidad

El proyecto tiene como punto el proceso de recaudación y fiscalización tributaria, el cual es soportada por las áreas de rentas y tecnologías de la información. Es así, que el impacto que generan los problemas anteriormente comentados en la MDEA, serían:

- Impacto en la continuidad del servicio, dado que no contar con la base de datos de los contribuyentes, de los predios, el sistema de caja o tesorería, no se podría realizar el

pago y/o cobro de los arbitrios, ocasionando el no ingreso de dinero a la municipalidad, y la molestia de los ciudadanos contribuyentes.

- Impacto en la productividad del servicio, ya que al no contar con el sistema de caja para el cobro de los arbitrios el área estaría inoperativa trayendo como consecuencia una gestión inadecuada con los contribuyentes, generando caos, colas, insatisfacción, etc.
- Impacto el económico por pérdidas en el ingreso de dinero mediante la recaudación de impuestos prediales y arbitrios. Podemos apreciar en la evolución mensual y anual de ingresos del año 2018 de la MDEA en las tablas 19 y 20 respectivamente, y sacando cálculos matemáticos son miles de soles que no ingresarían a las arcas de la municipalidad por horas o días fallas del sistema.

Tabla 19

Evolución mensual de ingresos del año 2018 de la MDEA

Concepto / Mes	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Setiembre	Octubre	Noviembre
Impuesto Predial	366,905	2,027,410	1,019,407	909,899	1,583,493	465,756	658,635	1,255,829	691,589	269,833	1,018,197
Arbitrios	160,207	1,552,984	414,682	531,252	282,503	463,563	239,699	377,976	206,361	410,008	95,858

Nota: Adaptado del Acta de transferencia 2018 – MDEA

Tabla 20

Ingresos del Periodo 2015 - 2018 de la MDEA

CONCEPTO / AÑOS	2015	2016	2017	2018
1: IMPUESTOS Y CONTRIBUCIONES OBLIGATORIAS	12,050,631	12,501,497	12,985,916	11,377,608
3: VENTA DE BIENES Y SERVICIOS Y DERECHOS ADMINISTRATIVOS	7,770,627	7,722,610	7,413,024	6,938,187
4: DONACIONES Y TRANSFERENCIAS	5,495,898	6,389,936	5,830,451	16,705,753
5: OTROS INGRESOS	330,654	596,179	455,220	294,839
8. ENDEUDAMIENTO	0	0	6,159,345	1,837,928
9: SALDOS DE BALANCE	635,606	530,881	2,007,976	4,054,890
TOTALES	26,283,416	27,741,103	34,851,932	41,209,205

Nota: Adaptado del Acta de transferencia 2018 – MDEA

- Impacto legal y penal por pérdidas de información confidencial. Ya que como indica la Ley 29733 – Ley de Protección de Datos Personales, es de uso obligatorio en las instituciones públicas y privadas que hacen uso de información personal en los procesos de negocio. Ya que las infracciones a esta ley pueden generar sanciones económicas y procesos legales engorrosos, todo por no resguardar debidamente la información que tienen en su poder.

3.4 Análisis del estado inicial de la MDEA

La seguridad de la información es un componente crítico dentro de la estrategia de gobierno por lo que se recomienda realizar un análisis GAP (análisis de brecha) para conocer el estado de madurez de la seguridad de la información de la municipalidad antes de iniciar el diseño del Sistema de Gestión de Seguridad de la Información. Este diagnóstico se basa teniendo en cuenta las cláusulas y dominios del anexo A de la norma ISO/IEC 27001:2013.

Los pasos que se realizaron para llegar a este análisis GAP son:

Paso 1: Elaboración de cuestionarios, aquí se realizaron las siguientes actividades:

1. Revisión de la norma ISO/IEC 27001:2013.
2. Elaboración de preguntas por cláusula y dominio.
3. Definición de niveles y criterios de madurez.

Paso 2: Entrevistas e inspecciones en la municipalidad, se realizaron las siguientes actividades:

1. Entendimiento de la estructura organizacional.
2. Revisión de los perfiles e identificación de los procesos.
3. Ejecución de las entrevistas al personal interesado e inspecciones en la entidad.

Paso 3: Consolidación de resultados, se realizaron las siguientes actividades:

1. Clasificación del nivel de madurez de las cláusulas.
2. Clasificación del nivel de madurez de los dominios
3. Revisión de calificaciones.

Paso 4: Análisis de los resultados, se realizaron las siguientes actividades:

1. Cálculo del promedio por cláusula.
2. Cálculo del promedio por dominio.
3. Elaboración de gráficas de madurez y brecha.

3.4.1 Nivel de madurez por cláusulas de la norma ISO/IEC 27001:2013

Para determinar el nivel de madurez con respecto a los requisitos de la norma, se ha definido un modelo de madurez de cinco niveles, que se detallan en la tabla 21.

Tabla 21

Criterios para evaluar los requisitos de la norma ISO/IEC 27001:2013

Estado	Valor	Significado
No diseñado	1	Las actividades/métodos demuestran que no se tiene el requisito y/o no se ha bosquejado su implementación.
Parcialmente diseñado	2	Las actividades/métodos demuestran que se tiene el requisito definido, pero éste no es del todo conforme con el requisito de la norma ISO/IEC 27001:2013.
Diseñado	3	Los métodos son conformes con el requisito de la norma ISO/IEC 27001:2013, pero sin evidencias de aplicación.
Parcialmente implementado	4	Las actividades/métodos son conformes con los requisitos de la norma ISO/IEC 27001:2013, pero con pocas evidencias de aplicación.
Completamente implementado	5	Las actividades/métodos son conformes con el requisito de la norma ISO/IEC 27001:2013 y se encuentra con evidencias de aplicación permanentes.

Nota: Adaptado de Ccesa, 2017.

La tabla con las cláusulas de la norma ISO/IEC 27001:2013 su respectivo grado de madurez, se puede apreciar en el anexo 2 - Análisis de brechas.

En la tabla 22 se muestra los resultados de la evaluación realizada a la municipalidad sobre los requisitos de la norma ISO/IEC 27001:2013, donde se aprecia que del total del 100% esta solo obtuvo un 4% de cumplimiento, lo que determina que la entidad se encuentra en un nivel “no diseñado” de cumplimiento de la norma.

Tabla 22

Resultado por cláusula

N°	Cláusulas	Estado inicial	Brecha	Estado esperado	Nivel
4	Contexto de la organización	0%	100%	100%	No diseñado
5	Liderazgo	7%	93%	100%	No diseñado
6	Planificación	0%	100%	100%	No diseñado

N°	Cláusulas	Estado inicial	Brecha	Estado esperado	Nivel
7	Soporte	11%	89%	100%	No diseñado
8	Operación	8%	92%	100%	No diseñado
9	Evaluación del desempeño	0%	100%	100%	No diseñado
10	Mejoras	0%	100%	100%	No diseñado
Promedio		4%			No diseñado

Elaboración propia

Analizando la figura 53 y 54 se evidencia la gran brecha porcentual de cumplimiento que existe con las cláusulas de la norma, ya que las cláusulas Liderazgo, Soporte y Operación presentan solo 7%, 11% y 8% respectivamente y las demás cláusulas en 0%. Es así que todas las cláusulas están por debajo de un nivel optimizado, teniendo un 4% de promedio de las cláusulas.

Figura 53. Análisis de brechas de las cláusulas
Elaboración propia

Figura 54. Grado de cumplimiento de la norma ISO/IEC 27001:2013

Elaboración propia

De la figura 55, se aprecia que el 88% de los requisitos está en un estado “No diseñado” y solo un 12% en un estado “Parcialmente diseñado”.

Finalmente, del resultado anterior podemos concluir que la municipalidad se encuentra en un nivel de madurez “No diseñado” y que el diseño e implementación del Sistema de Gestión de Seguridad de la Información implicará un mayor esfuerzo y dependerá del compromiso y disponibilidad del personal de la entidad.

Figura 55. Nivel de madurez con respecto a la norma ISO/IEC 27001:2013

Elaboración propia

3.4.2 Nivel de madurez por dominios de la norma ISO/IEC 27001:013

Para determinar el grado de cumplimiento de los controles de la norma ISO/IEC 27001:2013, se definió una escala de seis niveles, que se detallan en la tabla 23.

Tabla 23

Criterios para evaluar los controles de la norma ISO/IEC 27001:2013

Estado	Valor	Cumplimiento
Sin control	0	No se lleva a cabo el control de seguridad en los sistemas de información.
Control inicial	1	Los controles existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.
Control repetible	2	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.
Control definido	3	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.
Control gestionado	4	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.
Control optimizado	5	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.

Nota: Elaboración propia

Continuando con el análisis de brechas para los dominios, se realizó una tabla con los 14 dominios y 114 controles de la norma ISO/IEC 27001:2013 sus respectivas preguntas y grado de madurez, que pueden ser revisadas en el anexo 3 - Análisis GAP de dominios de la norma ISO/IEC 27001:2013.

Luego, en la tabla 24, se muestra el grado actual de implementación y cumplimiento de los controles de la norma por parte de la entidad.

Tabla 24
Resultado por dominios

N°	Dominio	Estado inicial	Brecha	Estado esperado	Nivel
A.5	Políticas de seguridad de la información	0%	100%	100%	Sin control
A.6	Organización de la seguridad de la información	14%	86%	100%	Control inicial
A.7	Seguridad en los recursos humanos	17%	83%	100%	Control inicial
A.8	Gestión de activos	16%	84%	100%	Control inicial
A.9	Control de acceso	20%	80%	100%	Control inicial
A.10	Criptografía	0%	100%	100%	Sin control
A.11	Seguridad física y ambiental	12%	88%	100%	Control inicial
A.12	Seguridad de las operaciones	9%	91%	100%	Control inicial
A.13	Seguridad de las comunicaciones	11%	89%	100%	Control inicial
A.14	Adquisición, desarrollo y mantenimiento de sistemas	11%	89%	100%	Control inicial
A.15	Relaciones con los proveedores	4%	96%	100%	Control inicial
A.16	Gestión de incidentes de seguridad de la información	12%	88%	100%	Control inicial
A.17	Aspectos de seguridad de la información en la gestión de continuidad del negocio	0%	100%	100%	Sin control
A.18	Cumplimiento	13%	87%	100%	Control inicial
Promedio de dominios		10%			Control inicial

Nota: Elaboración propia

Analizando la figura 56, se puede observar que el dominio con mayor nivel de madurez es el A.9 Control de acceso (Control inicial) con un 20%, seguido de A.7 Seguridad de los recursos humanos (Control inicial) con un 17%, A.8 Gestión de activos (Control inicial) con un 16%, siendo que los demás dominios se encuentran por debajo de un 15% correspondiente también a un nivel de “control inicial”.

Figura 56. Análisis de brecha por dominio
Elaboración propia

A continuación, se presenta la figura 57 de tipo radar donde también se puede apreciar la gran brecha existente con relación a los 14 dominios y 114 controles de la norma ISO/IEC 27001:2013 que fueron analizados en la entidad.

Figura 57. Grado de cumplimiento de los dominios de la norma ISO/IEC 27001:2013
Elaboración propia

Finalmente, tal como se aprecia en la figura 58, podemos concluir que la municipalidad referente al cumplimiento de los dominios se encuentra en un nivel de madurez 1 “Control inicial”, ya que el promedio es de 10%. Además, el 61% no tienen controles y solo el 21% tiene un control inicial. Por lo que se requiere de una intervención inmediata dado que el objetivo es proteger adecuadamente los activos de información de la entidad.

Figura 58. Nivel de madurez con respecto a los dominios de la norma ISO/IEC 27001:2013
Elaboración propia

3.5 Interesados

Los interesados en el presente proyecto, se muestran en la tabla 25:

Tabla 25
Interesados del SGSI

Interesado	Organización a la que pertenece	Cargo	Categoría de interesado	Nivel de interés (Bajo, Medio, Alto)	Nivel de influencia (Bajo, Medio, Alto)
Mg. Víctor Modesto Salcedo Ríos	MDEA	Alcalde	Patrocinador	Alto	Alto
Ing. Roger Arturo Chuctaya Yauri	MDEA	Subgerente de planeamiento, gestión de procesos y	Cliente final	Alto	Alto

Interesado	Organización a la que pertenece	Cargo	Categoría de interesado	Nivel de interés (Bajo, Medio, Alto)	Nivel de influencia (Bajo, Medio, Alto)
		tecnología de información			
Ing. Roñan Luis Ambicho Meza	MDEA	Gerente de rentas	Cliente final	Alto	Alto
Bach. Ricardo Torero Llanos	MDEA	Subgerente de recaudación y fiscalización tributaria	Cliente final	Medio	Alto
Personal	MDEA	Empleados	Usuario	Medio	Medio
Vecinos	MDEA	Contribuyentes	Usuario	Bajo	Bajo
Lisbet Monteza Mera	Empresa consultora	Consultor	Proveedor y director de proyecto	Alto	Alto

Nota: Elaboración propia

3.6 Toma de requerimientos

En base a las reuniones y entrevistas con los interesados se elaboró la tabla 26, donde se detalla que es lo que el cliente espera del proyecto.

Tabla 26

Requerimientos de las partes interesadas

Requerimiento	Descripción	Interesado	Prioridad
Situación actual de la Municipalidad Distrital de El Agustino	La municipalidad desea conocer el estado actual referente a la seguridad de la información de la entidad.	– Subgerente de planeamiento, gestión de procesos y tecnología de información	Alta
Inventario de activos de información	La municipalidad desea contar con un inventario de activos de información para conocer cuáles son los que necesitan ser protegidos de potenciales riesgos	– Subgerente de planeamiento, gestión de procesos y tecnología de información.	Alta

Requerimiento	Descripción	Interesado	Prioridad
Disminuir los riesgos de seguridad de la información	La municipalidad desea reducir los riesgos y optimizar el desempeño de los procesos de recaudación y fiscalización tributaria.	<ul style="list-style-type: none"> – Gerente de rentas. – Subgerente de recaudación y fiscalización tributaria. 	Alta
Disminuir los incidentes de seguridad de la información	La municipalidad desea tener un plan para tratar los riesgos existentes.	<ul style="list-style-type: none"> – Subgerente de planeamiento, gestión de procesos y tecnología de información. – Gerente de rentas. 	Alta
Diseño del SGSI	La municipalidad desea cumplir con la Resolución Ministerial 004-2016-PCM.	<ul style="list-style-type: none"> – Alcalde 	Alta

Nota: Elaboración propia

3.7 Estructura de desglose de trabajo

3.7.1 Vista jerárquica

Diseño de un SGSI basado en la norma ISO/IEC 27001:2013 para la Municipalidad Distrital de El Agustino.

1. Inicio

- 1.1. Acta de constitución del proyecto
- 1.2. Cronograma
- 1.3. Análisis del estado actual de la municipalidad – Análisis de brechas

2. Planificación

- 2.1. Contexto Organizacional
- 2.2. Alcance del SGSI
- 2.3. Política de seguridad de la información
- 2.4. Estructura organizacional del SGSI
- 2.5. Metodología de gestión de riesgos
- 2.6. Plan de tratamiento de riesgos – PTR
- 2.7. Declaración de aplicabilidad – SOA
- 2.8. Programa de capacitación y concientización

- 3. Ejecución
 - 3.1. Manual del SGSI
 - 4. Validación y pruebas
 - 4.1. Plan de pruebas
 - 4.2. Ejecución de las pruebas
 - 4.3. Resultado de las pruebas
 - 4.4. Plan de mejoras del diseño del SGSI
 - 5. Cierre
 - 5.1. Acta de cierre y entrega del proyecto
- 3.7.2 Mapa de procesos - EDT
- Se muestra en la figura 59.

Figura 59. EDT.
Elaboración propia

4 DISEÑO DE LA SOLUCIÓN

Este capítulo corresponde al diseño del Sistema de Gestión de Seguridad de la Información de acuerdo a los requerimientos tomados y justificando los criterios de elección. Para lo cual, primero se realizó el alcance del SGSI (con enfoque en procesos), la política de seguridad de la información. Luego se realizó el análisis y gestión de riesgos bajo la metodología de la norma ISO 31000:2018; el plan de tratamiento del riesgo y se redactó la Declaración de aplicabilidad. Para finalizar, se realizó el manual del SGSI con la documentación requerida por la norma ISO/IEC 27001:2013 para la Municipalidad Distrital de El Agustino.

4.1 Etapa 1: Inicio del proyecto

El 12 de agosto de 2019 se dio inicio al proyecto del diseño del Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para proteger adecuadamente los activos de información asociados al proceso de Recaudación y Fiscalización Tributaria de la Municipalidad Distrital de El Agustino, para lo cual se obtuvo el compromiso de la alta dirección y se elaboró y aprobó el acta de constitución del proyecto.

4.1.1 Compromiso de la alta dirección

Es un compromiso que la alta dirección ha asumido desde el primer momento en que se planteó realizar el diseño del Sistema de Gestión de Seguridad de la Información, siempre contemplado desde el punto de vista del alcance del SGSI, dado que tiene asignado las siguientes tareas fundamentales:

- Autorizar el diseño del SGSI.
- Formular y aprobar la política del SGSI y las políticas específicas de seguridad de la información.
- Establecer roles y responsabilidades de seguridad de la información. Estos serán asignados de acuerdo a la estructura organizacional de SGSI.
- Asignar los recursos necesarios para llevar a cabo el SGSI. Es responsabilidad de la dirección garantizar recursos para:
 - El diseño del SGSI, que es el alcance que tiene el presente proyecto.
 - Identificar todos los requerimientos necesarios para cumplir con la legislación vigente. En este caso, la Resolución Ministerial N°004-2016-PCM que declara el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 y la Ley N° 29733 “Ley de Protección de Datos Personales”.

- Realizar todas las revisiones cuando sea preciso.
- Mejorar la eficacia del SGSI.
- Formación y concientización en seguridad de la información. Son elementos básicos para lograr el éxito del SGSI, es por ello que la alta dirección debe asegurar que todo el personal de la municipalidad tiene sus responsabilidades asignadas y definidas en el SGSI, por lo que deberá:
 - Determinar las competencias necesarias que debe tener cada persona de la municipalidad en función de las tareas a desempeñar.
 - Satisfacer las necesidades de seguridad de la información en la municipalidad por medio de planes de formación.
 - Evaluar la eficacia de las acciones realizadas en cuestión de seguridad de la información.
 - Mantener todos los registros de estudios, formación, habilidades, experiencia y cualificación del personal en cuestión de seguridad de la información.
- Decidir los criterios y niveles de aceptación del riesgo.

4.1.2 Acta de constitución del proyecto

Se elaboró el acta de constitución del proyecto para establecer la relación de colaboración que existe entre la Municipalidad Distrital de El Agustino y el ejecutor del proyecto, donde se especificó la información general, la descripción del proyecto, los objetivos y el alcance, y que fue presentado a la entidad para su aprobación. (Ver anexo 1 – Acta de constitución del proyecto).

4.1.3 Cronograma del proyecto

A continuación, en la figura 60 se muestra el cronograma para el proyecto.

Figura 60. Cronograma
Elaboración propia

4.1.4 Presupuesto del proyecto

En este paso se desarrolla una estimación aproximada de los recursos económicos necesarios para completar las actividades del proyecto. En la tabla 27 se presenta el monto del costo de inversión para el diseño del Sistema de Gestión de Seguridad de la Información, cabe mencionar que el financiamiento será con recursos propios por parte de la tesista.

Tabla 27
Presupuesto del proyecto

Ítem	Cantidad	Precio unitario	Total
Bienes			
Laptop	1	2000	2000
Impresora	1	350	350
Papel bond	3	20	60
Servicios			
Internet	7	60	420
Transporte	–	–	300
Costo total			3130

Nota: Elaboración propia

4.2 Etapa 2: Planificación del proyecto

4.2.1 Contexto de la entidad

El capítulo 4 de la norma ISO/IEC 27001:2013, referente al contexto de la organización, indica la importancia de determinar los aspectos externos e internos. Así como también comprender las necesidades y expectativas de las partes interesadas a fin de determinar el alcance del Sistema de Gestión de Seguridad de la Información.

4.2.1.1 Contexto externo

Es importante el entendimiento del contexto externo para asegurar que los objetivos e inquietudes de las partes interesadas externas se toman en cuenta cuando se diseña el SGSI. La herramienta de análisis PEST (Factores Políticos – Económicos – Sociales – Tecnológicos), nos ha facilitado en la investigación a identificar los factores generales que influenciaran en el desarrollo del diseño del SGSI de la Municipalidad Distrital de El Agustino, tal como se muestra en la tabla 28.

Tabla 28
Contexto externo de la MDEA

Factores	Descripción
Políticos – legales	<ul style="list-style-type: none"> ▪ Interés del estado peruano por la seguridad de la información en todas las entidades públicas. ▪ Marco legal sobre seguridad de la información. ▪ Estandarización de procesos y sistemas de gestión.
Económicos	<ul style="list-style-type: none"> ▪ Bajo presupuesto por parte del estado. ▪ Costo elevado de consultores en SGSI.
Socio – culturales	<ul style="list-style-type: none"> ▪ Preocupación de la sociedad por la seguridad de la información. ▪ Mas hogares con acceso a internet y dispuestos a realizar trámites y transacciones en línea.
Tecnológicos	<ul style="list-style-type: none"> ▪ Aparición de nuevas tecnologías de información que son adaptados por el estado. ▪ Tendido de fibra óptica para mejorar la velocidad de acceso a la información.

Nota: Elaboración propia

4.2.1.2 Contexto interno

El Sistema de Gestión de Seguridad de la Información debe ser alineada a la cultura, estructura organizacional, procesos y la estrategia de la organización, razón por la cual se ha analizado a la municipalidad en los siguientes puntos.

4.2.1.2.1 Naturaleza de la entidad

La Municipalidad Distrital de El Agustino es un órgano de gobierno promotor del desarrollo local, que tiene su domicilio fiscal en la Av. Riva Agüero N° 1358 del distrito de El Agustino. Fue creado mediante la Ley N° 15353, el 06 de enero de 1965.

Tiene personería jurídica de derecho público con autonomía política, económica y administrativa en los asuntos de su competencia, de conformidad con la Ley N° 27972 - Ley Orgánica de las Municipalidades.

En la figura 61 se puede apreciar el frontis del local con el que cuenta la municipalidad para realizar sus trabajos administrativos de acuerdo a su competencia.

Figura 61. Frontis de la MDEA
Adaptado del diario La República

4.2.1.2.2 Finalidad

La Municipalidad Distrital de El Agustino, representa al vecindario, promueve la adecuada prestación de los servicios públicos locales, y el desarrollo integral, sostenible y armónico de su circunscripción. (ROF, 2019, p. 2).

4.2.1.2.3 Misión

“Prestar servicios públicos de calidad y de manera responsable para satisfacer las necesidades colectivas de los ciudadanos y promover la participación de los mismos para el progreso del distrito”

4.2.1.2.4 Visión

“Ser una institución líder, moderna, innovadora y que gestione eficientemente los recursos con la finalidad de lograr el desarrollo del distrito y brindar una mejor calidad de vida para la población”

4.2.1.2.5 Objetivos estratégicos

La Municipalidad Distrital de El Agustino tiene los siguientes objetivos estratégicos:

- Reducir los índices de inseguridad ciudadana en el distrito de El Agustino.
- Promover la gestión ambiental en el distrito de El Agustino
- Promover la competitividad económica en el distrito de El Agustino.

- Proteger a la población y sus medios de vida frente a los peligros de origen natural y antrópicos.
- Promover el desarrollo urbano territorial ordenado y sostenible en el distrito de El Agustino.
- Promover el desarrollo humano y hábitos saludables en el distrito de El Agustino.
- Incrementar los recursos financieros de la municipalidad distrital de El Agustino.
- Modernizar la gestión con tecnologías de información y comunicación con la participación de la población.
- Fortalecer el liderazgo de la municipalidad basada en una gestión de procesos y resultados.
- Fortalecer la gestión institucional de la municipalidad distrital de El Agustino.

4.2.1.2.6 Estructura orgánica

Figura 62. Organigrama de la Municipalidad Distrital de El Agustino
Adaptado de MOF, 2019.

4.2.1.2.7 Matriz FODA

Para precisar el estado actual en el que se encuentra la Municipalidad Distrital de El Agustino se realizó el análisis FODA (Fortalezas, Oportunidades, Debilidades, Amenazas), que se muestra en la tabla 29.

Tabla 29.

Matriz FODA de la MDEA

Fortalezas	Oportunidades
<ul style="list-style-type: none"> - Apoyo de la alta dirección. - Buenas relaciones de la subgerencia de planeamiento, gestión de procesos y tecnologías de la información (encargada de la seguridad de la información) con los órganos de gobierno de la MDEA. - Comunicación con la Secretaria de Gobierno Digital (SEGDI). 	<ul style="list-style-type: none"> - Apoyo del estado a través de la Secretaria de Gobierno Digital en temas de seguridad de la información. - Acceso a nuevas tecnologías por el crecimiento económico del país. - Existencia de información especializada, normativa y buenas prácticas para el desarrollo de la seguridad de la información.
Debilidades	Amenazas
<ul style="list-style-type: none"> - Infraestructura tecnológica limitada. - Falta de personal dedicado a la seguridad de la información. - Falta de aplicación de metodologías y buenas prácticas en la gestión de seguridad de la información. - Falta de programas de capacitación para el personal de la municipalidad en temas de seguridad. - Controles insuficientes en seguridad informática y seguridad de la información. - Falta de políticas bien definidas. 	<ul style="list-style-type: none"> - Falta de presupuesto. - Posibilidad creciente de ataques informáticos. - No contar con un plan de capacitación para el personal de TI que limite el desarrollo técnico y de gestión. - Acceso físico no autorizado al área de sistemas. - Fuga de información o pérdida.

Nota: Elaboración propia

4.2.1.2.8 Procesos institucionales

Después de haber analizado a la Municipalidad Distrital de El Agustino y sus áreas funcionales, se procedió a identificar los procesos de la entidad y diseñar el mapa de procesos. En la figura 63, se puede observar que la municipalidad cuenta con un sistema de gestión institucional con 14 procesos, clasificados en estratégicos, misionales y de soporte, los cuales gestionados articuladamente garantizan la planeación y administración de la entidad.

Figura 63. Mapa de procesos de la MDEA
Elaboración propia

Es así que, la gestión de recaudación y fiscalización tributaria es un proceso operacional u misional que es soportado por el proceso de gestión de infraestructura tecnológica, que a continuación pasamos a describir.

Proceso de recaudación y fiscalización tributaria

Este proceso se encarga de administrar las cobranzas ordinarias de los diferentes tributos municipales, así como fiscalizar y controlar la veracidad de la información tributaria declarada por los contribuyentes. Este proceso consta de los siguientes subprocesos:

- Determinar las obligaciones tributarias

En este proceso se determina el valor total del predio de acuerdo a la Ley y reglamento municipal vigente, donde se realiza el cálculo según las características del predio.

- Verificar cumplimiento de obligaciones tributarias

En este proceso se verifica los contribuyentes deudores, con la finalidad de notificar el detalle de su estado de cuenta, a fin de que pueda cumplir con sus obligaciones tributarias.

- Cobranza de obligaciones tributarias

En este proceso se efectúa el cobro al contribuyente (nuevo o antiguo), cumpliendo con sus obligaciones tributarias.

- Ejecutar incremento o disminución de valores tributarios

En este proceso se actualizan los valores tributarios a partir de la declaración jurada que emite el contribuyente o partiendo del personal de la municipalidad (inspector de rentas) sobre la actualización o modificación de un predio del contribuyente.

- Emitir las notificaciones de pago de tributos

En este proceso se da a conocer a los contribuyentes morosos a través de las notificaciones (OP, RM y RD) para que realicen el pago de sus obligaciones tributarias de acuerdo a tasas vigentes.

A continuación, pasamos a mostrar cada uno de los diagramas de los subprocesos:

Figura 64. Subproceso: Determinar obligaciones tributarias
Elaboración propia

Figura 65. Subproceso: Verificar cumplimiento de obligaciones tributarias
Elaboración propia

Figura 66. Subproceso: Cobranza de obligaciones tributarias
Elaboración propia

Figura 67. Subproceso: Ejecutar incremento o disminución de valores tributarios
Elaboración propia

Figura 68. Subproceso: Emitir las notificaciones de pago de tributos
Elaboración propia

Proceso de gestión de infraestructura tecnológica

Proceso que tiene como objetivo planear, organizar y ejecutar el diseño e implementación, y mantenimiento de la infraestructura tecnológica de la Municipalidad Distrital de El Agustino, promoviendo el uso de los recursos tecnológicos para así garantizar los niveles adecuados de confidencialidad, integridad y disponibilidad de los sistemas de información, de los datos y de las comunicaciones de la entidad. Su alcance inicia en la elaboración del Plan Operativo Institucional (POI), estableciendo para ello planes de contingencia y mejora continua a ser ejecutadas para alcanzar los objetivos y metas institucionales.

A continuación, pasamos a mencionar los subprocesos de la gestión de infraestructura tecnológica de la municipalidad.

- Gestión de soporte técnico
- Gestión de la seguridad de la información
- Gestión del inventario de equipos de cómputo
- Gestión de soporte técnico
- Gestión de la página web y servicios en línea.

4.2.1.2.9 Infraestructura tecnológica

La Municipalidad Distrital de El Agustino tiene una red de área local (LAN), formada por aproximadamente 90 estaciones de trabajo y 3 servidores (1 servidor de aplicación, 1 servidor de base de datos y 1 servidor de dominios). En los servidores se centraliza toda la información para el funcionamiento de los diferentes sistemas y los accesos a la red de la entidad (cuentas de red, etc.). También, cuenta con una página web y correo corporativo para cada trabajador.

Se cuenta con 1 líneas de internet, además cuenta con un firewall para controlar el acceso a la red. El área de tecnologías de información está a un nivel de subgerencia con el nombre de Planeamiento, Gestión de Procesos y Tecnologías de la Información.

La entidad tiene un servicio de “Pago en línea” alojada en su página web, donde el ciudadano puede realizar el pago de sus arbitrios municipales, impuestos prediales, impuesto vehicular, etc.

4.2.1.3 Partes interesadas

De acuerdo a la norma ISO/IEC 27001:2013 requisito 4.2 Comprender las necesidades y expectativas de las partes interesadas, se ha determinado las partes interesadas internas y externas que son pertinentes para el diseño del Sistema de Gestión de Seguridad de la Información, identificando los requisitos de cada uno de ellos.

4.2.1.3.1 Partes interesadas internas

- **Órganos de gobierno**
Conformado por el consejo municipal y alcaldía. Deben demostrar liderazgo y compromiso con la seguridad de la información, asegurando la integración de los requisitos del SGSI en los procesos de la municipalidad y garantizando la disponibilidad de los recursos necesarios para su diseño e implementación.
- **Órganos de la alta dirección**
Conformado por la Gerencia Municipal. Debe demostrar liderazgo y compromiso respecto al SGSI, asegurando que los objetivos que se establecen son compatibles con la planeación estratégica de la municipalidad y estableciendo la política de seguridad de la información.
- **Subgerencia de Planeamiento, gestión de procesos y tecnologías de la información**
Es el responsable de la seguridad de la información y continuidad tecnológica de la municipalidad.
- **Jefe de recursos humanos**
Responsable de la seguridad de la información antes, durante y después de la contratación de los funcionarios y empleados.
- **Empleados de la entidad**
Responsables de velar por la seguridad de los activos de la información, cumplir con las normas y políticas de seguridad de la municipalidad. También, tienen la responsabilidad del tratamiento de los datos personales de los titulares vinculados con la entidad.

4.2.1.3.2 Partes interesadas externas

- **Secretaría de Gobierno Digital (SeGDí)**
“La Secretaría de Gobierno Digital es el órgano de línea, con autoridad técnico normativa a nivel nacional, responsable de formular y proponer políticas nacionales y sectoriales, planes nacionales, normas, lineamientos y estrategias en materia de Informática y Gobierno Electrónico” (Gobierno Digital, par.1).

Entre sus funciones tiene de aprobar las normas y estándares para promover el desarrollo e implementación de la seguridad de la información, infraestructura de datos espaciales, datos abiertos, interoperabilidad, portales del Estado, entre otros, de las entidades públicas del Estado. Además, de brindar asistencia técnica a las entidades de la administración pública para la implementación de proyectos de tecnologías de la información en las materias de su competencia.

- Contraloría General de la República

“La Contraloría General de la República es la máxima autoridad del Sistema Nacional de Control. Supervisa, vigila y verifica la correcta aplicación de las políticas públicas y el uso de los recursos y bienes del Estado. Para realizar con eficiencia sus funciones, cuenta con autonomía administrativa, funcional, económica y financiera” (La Contraloría General de la República del Perú, parr.1)

- La comunidad

Corresponde a los contribuyentes y grupos externos que se ven impactados por las actividades que desarrolla la municipalidad

4.2.1.3.3 Requisitos de las partes interesadas

De acuerdo a las entrevistas y consultas con las partes interesadas, en la tabla 30 se muestra los requisitos de seguridad de la información.

Tabla 30

Requisitos de las partes interesadas

Partes interesadas		Requisitos	
Internas			
Órganos de gobierno		<ul style="list-style-type: none">- Cumplimiento de las leyes y normatividad vigente en temas de seguridad de la información.- Demostrar liderazgo y compromiso con la seguridad de la información.	
Órganos de Alta Dirección		<ul style="list-style-type: none">- Supervisar los proyectos y actividades de la subgerencia de planeamiento, gestión de procesos y tecnologías de la información.- Demostrar liderazgo y compromiso con la seguridad de la información.	

Subgerencia de planeamiento, gestión de procesos y tecnologías de la información	<ul style="list-style-type: none"> - Levantamiento de las no conformidades. - Capacitar a los trabajadores en temas de seguridad de la información.
Responsable de Recursos Humanos	<ul style="list-style-type: none"> - Verificar la seguridad de la información antes, durante y después de la vinculación de los trabajadores a la entidad.
Trabajadores	<ul style="list-style-type: none"> - Conocer las normas y políticas en temas de seguridad de la información. - Velar por los activos de información. - Protección de su información personal - Disponibilidad de los servicios de la municipalidad. - Capacitación en temas de seguridad de la información.
Externas	
Gobierno	<ul style="list-style-type: none"> - Cumplimiento del marco legal y normativo de la seguridad de la información. - Alcanzar los objetivos de la política de estado y planes de gobierno 2016-2021
Contraloría General de la República	<ul style="list-style-type: none"> - Cumplimiento de la normatividad de control interno de las entidades del estado relacionado a las tecnologías de información y comunidades: apartado 3.10 de la resolución de contraloría general N° 320-2016-CG.
Comunidad	<ul style="list-style-type: none"> - Seguridad de sus datos sensibles
Proveedores	<ul style="list-style-type: none"> - Acuerdos contractuales claros en temas de seguridad de la información.

Nota: Elaboración propia

4.2.2 Alcance del SGSI

En el requisito 4.3, como indica la norma ISO/IEC 27001:2013, luego de analizar el contexto de la municipalidad y comprender las necesidades y expectativas de las partes interesadas, las interfaces y dependencias entre los procesos operacionales y de soporte de la

municipalidad, la entidad determina el siguiente alcance para el diseño del Sistema de Gestión de Seguridad de la Información, como se muestra en la figura 69.

Figura 69. Alcance del SGSI
Elaboración propia

4.2.3 Política de seguridad de la información

Habiéndose establecido el alcance del SGSI, y de acuerdo a lo indicado en el requisito 5.2 de la norma ISO/IEC 27001:2013, se establece la política de seguridad de la información, que es de vital importancia dado que se especifica los lineamientos generales de seguridad que deben ser cumplidos por la municipalidad. Además, de los objetivos que se pretende alcanzar en relación a la seguridad de la información en el ámbito definido en el alcance.

Es así que, para asegurar su cumplimiento debe ser aprobado por la alta dirección (alcalde), quien tiene la obligación de comunicarla a la municipalidad, indicando la importancia que tiene para lograr alcanzar los objetivos trazados en la política.

En la figura 70, se muestra la política de alto nivel del Sistema de Gestión de Seguridad de la Información que se definió:

POLÍTICA DEL SGSI

La Municipalidad Distrital de El Agustino (MDEA) en cumplimiento con su misión, visión y valores, comprometido con la mejora de sus procesos y generando valor económico, social y ambiental para el desarrollo del distrito, establece el diseño e implementación del Sistema de Gestión de Seguridad de la Información (SGSI) y se compromete a:

- *Proteger los activos de información frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información.*
- *Proporcionar los recursos necesarios para asegurar la implementación de las medidas de control necesarias para evitar que los riesgos de la seguridad de la información se materialicen.*
- *Mejorar el nivel de conciencia de seguridad de la información en los funcionarios, colaboradores, y contribuyentes de los servicios de la entidad.*
- *Mejorar continuamente la eficacia del SGSI a fin de minimizar constantemente los riesgos de seguridad de la información.*
- *Cumplir con los requisitos legales y regulatorios que afectan a la entidad respecto a la seguridad de la información.*

Aplicabilidad de la política del SGSI

Esta política aplica a toda la entidad, sus trabajadores, proveedores, terceros y demás partes interesadas.

Figura 70. Política del SGSI
Elaboración propia

Además de esto una política de seguridad de la información debe contener una estructura adecuada para ser presentada a la alta gerencia, esta se puede revisar en el anexo 4 - Política de Seguridad de la Información.

4.2.4 Objetivos de Seguridad de la Información

Los objetivos del Sistema de Gestión de Seguridad de la Información son:

- Asegurar la confidencialidad, integridad y disponibilidad de la información de la Municipalidad Distrital de El Agustino.
- Asegurar que los actuales y futuros procesos cumplan con la legislación vigente en materia de seguridad de la información.
- Minimizar los riesgos de seguridad de la información a un nivel aceptable para la entidad.
- Evaluar la efectividad del Sistema de Gestión de Seguridad de la Información y llevar a cabo una mejora continua.

4.2.5 Estructura organizacional del SGSI

Según el requisito 5.3 de la norma ISO/IEC 27001:2013, roles organizacionales, responsabilidades y autoridades, la alta dirección debe asegurar que las responsabilidades y las autoridades para los roles pertinentes a la seguridad de la información sean asignados y comunicados. Para ello será necesario conformar un Comité de Gestión de Seguridad de la Información, tal como lo indica las Resoluciones Ministeriales N° 004-2016-PCM y N°166-2017-PCM en su artículo 5 “Del Comité de Gestión de Seguridad de la Información” en donde la propia entidad designará un comité de gestión de seguridad de la información estableciendo las funciones que desempeñará. (Anexo 13 – Resoluciones Ministeriales)

En la figura 71, se muestra la estructura organizacional del SGSI y las personas que van a conformarla, quienes tendrán el compromiso de velar por el cumplimiento del Sistema de Gestión de Seguridad de la Información.

Figura 71. Estructura organizacional del SGSI.

Adaptado del Curso de Seguridad de la Información por Seminario, 2015.

4.2.5.1 Roles y responsabilidades

4.2.5.1.1 CGSI – Comité de gestión de seguridad de la información

Tiene los siguientes roles y responsabilidades:

- Revisar y aprobar las políticas específicas de seguridad de la información.
- Proveer los recursos necesarios para la seguridad de la información.
- Asignar los roles específicos y responsabilidades en materia de seguridad dentro de la entidad.
- Iniciar planes y programas para lograr y mantener la concientización de la seguridad de la información.
- Velar por el cumplimiento de programas de seguridad, normas y leyes vigentes.

Los integrantes del CGSI son:

- Alcalde
 - Aprobar la política de seguridad de la información.
 - Conocer y difundir la política de seguridad de la información a todos los empleados de la municipalidad.
 - Iniciar una cultura de seguridad de la información en la municipalidad.
- Gerente municipal
 - Proponer al alcalde y consejo municipal la política de seguridad de la información para la municipalidad.
 - Hacer cumplir la política de seguridad de la información dentro de la municipalidad.
 - Controlar el avance del Sistema de Gestión de Seguridad de la Información dentro de la municipalidad.
- Gerente de planificación y presupuesto
 - Gestionar los recursos necesarios para la implementación, ejecución y mantenimiento del Sistema de Gestión de Seguridad de la Información.
- Subgerente de planeamiento, gestión de procesos y tecnologías de información
 - Informar al gerente municipal acerca del Sistema de Gestión de Seguridad de la Información.
 - Garantizar la disponibilidad y operatividad de los sistemas de información, equipos informáticos y de comunicaciones.
 - Establecer los mecanismos adecuados para la gestión de riesgos y seguridad de la información.
 - Asegurar la existencia de metodologías para el tratamiento de riesgos.
 - Asegurar la existencia de documentos exigidos por la norma ISO/IEC 27001:2013.
 - Asegurar el cumplimiento de las políticas específicas de seguridad de la información para la adquisición, diseño, desarrollo, operación y mantenimiento de la infraestructura tecnológica de la municipalidad.
 - Delegar las funciones, roles y responsabilidades de seguridad a los empleados a su cargo para la gestión de la infraestructura tecnológica de la municipalidad.
 - Aprobar la implementación de los controles y medidas de seguridad.
- Gerente de asesoría jurídica
 - Conocer e interpretar las leyes vigentes sobre la seguridad de la información.
 - Evaluar el cumplimiento de las leyes vigentes en temas de seguridad de la información en la municipalidad.

4.2.5.1.2 GISI – Comité interdisciplinario de seguridad de la información

Los integrantes de este grupo son el gerente de rentas y el subgerente de recaudación y fiscalización tributaria.

Tiene los siguientes roles y funciones:

- Asegurar que las actividades de seguridad sean ejecutadas en cumplimiento con la política de seguridad de la información.
- Aprobar las principales iniciativas para incrementar la seguridad de la información.
- Permitir que el personal exprese sus inquietudes sobre asuntos de seguridad.
- Aprobar metodologías y procesos de seguridad de la información.
- Promover la difusión y apoyo a la seguridad de la información dentro de la municipalidad.

4.2.5.1.3 OSI – Oficial de seguridad de la información

- Diseñar y coordinar la implementación de las políticas, normas y procedimientos de seguridad de la información.
- Identificar los riesgos y amenazas a los que están expuestos los activos de información de la municipalidad.
- Establecer un cronograma de revisión de vulnerabilidades y coordinar planes de mitigación.
- Supervisar el cumplimiento de los controles de seguridad de la información.
- Desarrollar programas de capacitación y concientización sobre seguridad de la información al personal de la municipalidad.
- Controlar la documentación del SGSI.
- Organizar la realización de las auditorías internas y externas del SGSI.
- Supervisar permanentemente las diferentes áreas de la municipalidad referente a la seguridad de la información.
- Elaborar y actualizar el plan de seguridad de la información.
- Liderar los proyectos de mejora del SGSI.

4.2.5.1.4 Propietario, custodio y usuario de los activos de información

Tiene los siguientes roles y funciones:

- Propietario

- Conocer, identificar y clasificar aquellos activos de información de los cuales son dueños.
- Determinar los criterios y niveles de acceso a los activos de información de su propiedad.
- Asegurar que los activos de información que tienen son manejados y administrados correctamente.
- Reportar al oficial de seguridad de la información sobre cualquier vulnerabilidad detectada que afecte sus activos de información.
- Verificar que los controles de seguridad aplicados sean consistentes con la clasificación realizada.
- En coordinación con el oficial de seguridad de la información, revisar y evaluar los resultados de la implementación de los controles aplicados a los activos de su propiedad.
- Custodio
 - Dar acceso a los usuarios de acuerdo con las especificaciones establecidas por los propietarios.
 - Administrar los accesos a los activos de información.
 - Cumplir las políticas, procedimientos y controles implementados para la protección de los activos asignados para su custodia.
 - Administrar los procedimientos de backup, recuperación y restauración de información.
 - Comunicar al propietario del activo de información las amenazas y vulnerabilidades que encuentre durante el desarrollo de sus actividades.
- Usuario
 - Cumplimiento de las políticas y directivas de seguridad de la información.
 - Mantener la confidencialidad de las contraseñas para el acceso a aplicaciones, sistemas de información y recursos informáticos.
 - Utilizar la información de la municipalidad solo para el cumplimiento de sus funciones y/o fines de la entidad.
 - Reportar incidentes y debilidades de seguridad de la información

4.2.6 Metodología de gestión de riesgos

La norma ISO/IEC 27001:2013 define como obligatoria la gestión del riesgo, los requisitos 6.1.1, 6.1.2 y 6.1.3 especifican cómo se deben evaluar y tratar los riesgos; además, los requisitos 8.1, 8.2 y 8.3 disponen mantener los resultados de esas actividades.

Para este proyecto se utilizará la metodología de la norma ISO 31000, que indica que la evaluación del riesgo es el proceso global de identificación, análisis y valorización del riesgo. Esta evaluación se tiene que llevar a cabo de manera sistemática, iterativa y colaborativa, en base al conocimiento y los puntos de vista de las partes interesadas. En la figura 72, se puede apreciar la metodología de gestión de riesgos bajo la norma ISO 31000:2018 con sus respectivos números de cláusulas a cumplir en el proyecto, que permitirá evaluar las amenazas y vulnerabilidades de seguridad que afectan la confidencialidad, integridad y disponibilidad de los activos de información.

Figura 72. Modelo de gestión de riesgos bajo la ISO 31000:2018
Adaptado de ISO 31000:2018

4.2.6.1 Alcance, contexto y criterios

Esta fase es la base fundamental de la norma ISO 31000:2018, donde se definen los parámetros básicos externos e internos para la gestión del riesgo. Se ha conocido el estado

actual de la Municipalidad Distrital de El Agustino y se han definido los criterios necesarios para la gestión del riesgo de este proyecto:

- Contexto de la entidad (Capítulo 4.2.1).
- Necesidades y expectativas de las partes interesadas para conocer sus requisitos sobre la seguridad de la información (Capítulo 4.2.1.3).
- Análisis de brechas del estado inicial de la municipalidad con respecto a la seguridad de la información (Anexo 2– Análisis de brechas de la MDEA).
- Declaración del alcance del Sistema de Gestión de Seguridad de la Información especificando el proceso crítico a proteger en este diseño (Capítulo 4.2.2).

4.2.6.2 Identificación del riesgo

El propósito de la identificación del riesgo es encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a la municipalidad lograr sus objetivos.

Para poder identificar los riesgos es necesario elaborar un inventario de activos de información de los procesos dentro del alcance del SGSI, para luego ser valorados en base a los criterios de seguridad de la información.

Para obtener el inventario se siguen las siguientes actividades:

1. Identificación de activos
2. Clasificación de activos
3. Valoración de activos
4. Identificación de amenazas y vulnerabilidades

4.2.6.2.1 Identificación de activos

Esta actividad tiene como objetivo determinar los activos de información que intervienen en el proceso de recaudación y fiscalización tributaria, y que de verse afectados originen un efecto negativo en la continuidad del negocio. Para ello se necesita realizar los siguientes pasos:

- Conocer el proceso y las áreas involucradas, en base a la declaración del alcance del SGSI.
- Identificar al personal que participa en el proceso de recaudación y fiscalización tributaria, y entrevistarlos a fin de que definan que activos son críticos para ellos y la municipalidad.

- Registrar los activos identificados en el inventario de activos, así como los riesgos identificados en la matriz de riesgos.

Para lograr la realización de esta actividad en el proyecto se utilizó el diagrama tortuga, una herramienta que nos resultó muy útil para la identificación de todos los activos que intervienen en el proceso mencionado. Diagrama que pueden visualizarlo en el anexo 13 – Diagrama Tortuga.

4.2.6.2.2 Clasificación de activos

En esta actividad se ha clasificado a los activos de información con los siguientes atributos:

- Categoría de activo: Define el tipo al cual pertenece el activo (Ver tabla 31)
- Clasificación: Se refiere al nivel de accesibilidad del activo (Ver tabla 32)
- Frecuencia de uso: Repetición con que se usa el activo (Ver tabla 33)

Tabla 31

Categorías de activos de información

Id	Categoría	Descripción
D	Dato	Todos aquellos datos (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyan en la entidad. Ejemplos: base de datos, archivos electrónicos, datos de configuración, documentos y registros de papel.
SW	Software	Todos los programas que se utilizan para la gestión de la información. Ejemplos: software base, sistemas operativos, utilitarios, programas, etc.
HW	Hardware	Todos los medios físicos destinados a soportar directa o indirectamente los servicios que presta la entidad. Ejemplos: Servidores, PCs, laptops, storage, impresoras, etc.
RC	Red de comunicación	Todos los equipos de telecomunicaciones para conectar físicamente los elementos de un sistema de información y administrarlos. Ejemplos: Switches, routers, firewalls, access point, sistemas de telefonía, red LAN, Red WAN, Red VPN, etc.
S	Servicios	Son los servicios internos o externos que a la municipalidad le proveen o suministran. Ejemplos: Página web, correo electrónico, internet, línea dedicada, infraestructura de clave pública, etc.

Id	Categoría	Descripción
P	Personal	Se encuentra tanto la plantilla propia de la municipalidad, como el personal subcontratado, los clientes, usuarios y, en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la entidad.
I	Instalaciones	Lugares en los que se alojan los sistemas de información y comunicaciones. Ejemplos: Oficinas, datacenter, sedes, salas, almacenes, etc.
SI	Soporte de información	Dispositivos físicos que permiten almacenar información de forma permanente o durante largos periodos de tiempo. Ejemplos: Cintas de backups, DVDs, etc.
EA	Equipamiento auxiliar	En este tipo entrarían a formar parte todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos. Ejemplos: Aire acondicionado, UPS, grupo electrógeno, alarmas, detectores de humo, extintores de fuego, etc.
IR	Imagen - Reputación	La imagen de la municipalidad frente al público, clientes, personas, otras organizaciones, mostrando identidad y competencia que se diferencia de otras.

Nota: Elaboración propia

Tabla 32

Clasificación de los activos de la información

Id	Clasificación	Descripción
C	Confidencial	Es la información que debe mantenerse en la más estricta reserva. Está sujeta al cumplimiento de requisitos legales y/o contractuales. Información accesible solo por la dirección o personal concreto. Ejemplos: Información de los contribuyentes, información del personal, información económica – financiera, etc.
I	Interna	Es aquella información inherente a las operaciones de un proceso o área de negocio específica. Información accesible solo al personal de la municipalidad o un área en particular. Ejemplos: Procesos operativos, políticas específicas, manuales técnicos y de usuario, formatos, registros, procedimientos, instructivos, etc.
P	Pública	Información cuyo contenido puede ser conocido y distribuido sin ninguna restricción. Ejemplo: Publicaciones en la página web.

Nota: Elaboración propia

Tabla 33

Frecuencia de uso de los activos de información

Id	Frecuencia	Descripción
A	Alta	Información utilizada en forma diaria o semanal.
M	Media	Información utilizada en forma mensual o semestral.
B	Baja	Información utilizada en forma anual.

Nota: Elaboración propia

En base a los criterios mencionados, se elaboró el inventario de activos de información que permitió clasificar los activos de información (Ver anexo 5 – Inventario de activos de información). Dicho inventario cuenta con los siguientes campos de identificación que se muestra en la tabla 34.

Tabla 34

Campos de identificación del inventario de activos de información

Campo	Descripción
Nº	Número de activos.
Nombre	Nombre del activo de información
Descripción	Descripción breve del activo de información
ID Categoría	ID de la categoría a la cual pertenece el activo de información.
Ubicación	Ubicación física o lógica del activo de información
Proceso	Proceso donde se encuentra el activo de información
Responsabilidad	Responsabilidad del activo de información (Usuario - Custodio - Propietario)
Clasificación	Tipo de accesibilidad del activo de información.
Frecuencia de uso	Repetición con que se usa el activo de información

Nota: Elaboración propia

4.2.6.2.3 Valorización de activos

Luego de haber identificado los activos de información, se procede a valorar su grado de importancia y criticidad para la municipalidad. Para ello, se valoriza la afectación o pérdida que le puede generar a la entidad en los aspectos financiero, legal y de imagen, dado que al materializarse una amenaza sobre el activo afecte su confidencialidad, integridad y disponibilidad. Es así, que en la tabla 35 se muestran los criterios de la respectiva valoración:

Tabla 35

Criterios para la valoración de activos de información

Aspectos	Descripción	Criterio de calificación	Valor
Financiero (F)	Pérdidas económicas	No genera pérdidas económicas	1
		Pérdidas económicas mínimas	2
		Pérdidas económicas graves	3
		Pérdidas económicas elevadas	4
		Pérdidas económicas excepcionalmente elevadas	5
Legal (L)	Incumplimiento de leyes y normas	No tiene incumplimiento frente a las leyes y normas.	1
		Genera incumplimiento mínimo o leve de una ley o norma.	2
		Genera incumplimiento moderado de una ley o norma.	3
		Genera incumplimiento grave de una ley o norma.	4
		Genera incumplimiento excepcionalmente grave de una ley o norma.	5
Imagen (I)	Afectación de la imagen de la municipalidad	Conocido solo de manera interna dentro de la municipalidad, pero no de interés público.	1
		Atención de algunas partes interesadas a nivel local.	2
		Mediana atención de las partes interesadas a nivel local y regional.	3
		Alta atención de las partes interesadas a nivel local, regional y nacional.	4
		Conocido a nivel nacional e internacional	5

Nota: Adaptado de Ccesa, 2017

Luego, se establecieron preguntas para determinar la criticidad del activo de información en las tres dimensiones que persigue la ISO/IEC 27001. En la tabla 36, se aprecian las preguntas:

Tabla 36

Preguntas para determinar la criticidad del activo de información

Dimensión	Aspecto	Pregunta
Confidencialidad	Financiero	¿Su divulgación no autorizada puede relevar información sensible de la municipalidad requerida para la toma de decisiones estratégicas y financieras causando pérdidas económicas?

Dimensión	Aspecto	Pregunta
	Legal	¿Su divulgación no autorizada puede afectar el cumplimiento de leyes o normas impartidas por entes de control o generar demandas de terceros?
	Imagen	¿Su divulgación no autorizada puede afectar la imagen de la entidad?
Integridad	Financiero	¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar pérdidas económicas para la municipalidad?
	Legal	¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar sanciones de entes de control?
	Imagen	¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede afectar la imagen de la entidad?
Disponibilidad	Financiero	¿Si el activo o la información que se gestiona a través de él no están disponibles puede generar pérdidas económicas para la municipalidad?
	Legal	¿Si el activo o la información que se gestiona a través de él no están disponibles puede generar sanciones legales de entes de control o demandas de terceros?
	Imagen	¿Si el activo o la información que se gestiona a través de él no están disponibles puede afectar la imagen de la municipalidad?

Nota: Adaptado de Ccesa, 2017.

Finalmente, para determinar la criticidad de los activos de información, se utiliza los criterios de evaluación de la tabla 37. La tabla completa de la valoración de activos se puede revisar en el anexo 6 – Valoración de activos.

Es así que los activos que se encuentran en un nivel de criticidad “medio” y “alto” pasaran a la siguiente etapa del análisis del riesgo.

Tabla 37

Nivel de criticidad de los activos de información

Criterio de evaluación	Valor	Criticidad
Cuando la destrucción, modificación, relevamiento o interrupción del activo de información afecta seriamente la	$3 < VF \leq 5$	Alto

Criterio de evaluación	Valor	Criticidad
confidencialidad, integridad y disponibilidad de la información de la MDEA.		
Cuando la destrucción, modificación, relevamiento o interrupción del activo de información afecta parcialmente la confidencialidad, integridad y disponibilidad de la información de la MDEA.	VF = 3	Medio
Cuando la destrucción, modificación, relevamiento o interrupción del activo de información afecta mínimamente la confidencialidad, integridad y disponibilidad de la información de la MDEA.	$0 < VF < 3$	Bajo

Nota: Elaboración propia

4.2.6.2.4 Identificación de vulnerabilidades y amenazas

Esta actividad tiene como objetivo identificar las vulnerabilidades y amenazas que se filtran contra cada uno de los activos valorizados de la actividad anterior.

Una vulnerabilidad es cualquier cosa que pueda desembocar en un problema de seguridad y una amenaza es la acción específica que aprovecha una vulnerabilidad para crear un problema de seguridad. Entre ellas hay una estrecha relación: sin vulnerabilidad no hay amenaza y sin amenaza no hay vulnerabilidad.

Para ello se ha tomado como referencia el catálogo de amenazas y vulnerabilidades que presenta la norma ISO/IEC 27005, que podrían detonar en los activos de información de la municipalidad. En la tabla 38 se presenta el catálogo de vulnerabilidades.

Tabla 38

Catálogo de vulnerabilidades

Tipo	Vulnerabilidades
Software	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo.
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado.
	Falta de documentación.
	Gestión deficiente de las contraseñas.
	Descarga y uso no controlados de software.
	Falta de copias de respaldo.
	Falta de parches al sistema operativo.

Tipo	Vulnerabilidades
	Falta de una política de gestión de cambios.
	Falta de mantenimiento a la base de datos.
	Falta de bitácoras de acceso al sistema.
	Interfase de usuario complicadas.
	Falta de mecanismos de identificación y autenticación como la autenticación de usuario.
Hardware	Falta de mantenimiento preventivo.
	Falta de control de cambio con configuración eficiente.
	Falta de control para el uso de impresoras.
	Falta de un cronograma de reemplazo periódico.
	Almacenamiento de cintas de backup sin protección.
	S susceptibilidad a las variaciones de tensión eléctrica.
Red	Juntas malas de cableado.
	Arquitectura de red insegura.
	Conexiones no protegidas de la red pública.
	Líneas de comunicación no protegidas.
Personal	Falta de entrenamiento en seguridad.
	Uso incorrecto de software y hardware.
	Falta de conciencia acerca de la seguridad.
	Trabajo no supervisado del personal de limpieza.
Instalaciones	Uso inadecuado o descuidado del control de acceso físico a las instalaciones de la entidad.
	Falta de protección física de las puertas de la entidad.
Entidad	Falta de procedimiento formal para el registro y retiro del registro de usuario.
	Falta de proceso formal para la revisión(supervisión) de los derechos de acceso.
	Falta o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes.
	Falta de procedimiento de monitoreo de los recursos de procesamiento información.
	Falta de procedimientos de identificación y evaluación de riesgos.
	Falta de procedimiento formal para la autorización de la información disponible al público.
	Falta de planes de continuidad.
	Falta de políticas sobre el uso del correo electrónico.
	Falta de procedimientos para la introducción del software en los sistemas operativos.
	Falta de registros en las bitácoras*(logs) de administrador y operario.
	Falta de procedimientos para el manejo de información clasificada.

Tipo	Vulnerabilidades
	Falta de responsabilidades en la seguridad de la información en la descripción de los cargos.
	Falta o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados.
	Falta de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información.
	Falta de política formal sobre la utilización de computadores portátiles.
	Falta de control de los activos que se encuentran fuera de las instalaciones.
	Falta o insuficiencia de política sobre limpieza de escritorio y de pantalla.
	Falta de autorización al acceso a las instalaciones de procesamiento de la información.

Nota: Adaptado de ISO/IEC 27005

La tabla 39, muestra una lista de amenazas, estas pueden ser deliberadas (D), accidentales (A) o naturales (N). Una amenaza puede tener su origen dentro o fuera de la entidad.

Tabla 39.

Catálogo de amenazas

Tipo	Amenaza	Origen
Daño Físico	Fuego	A, D, N
	Daños por agua	A, D, N
	Contaminación del medio ambiente	A, D, N
	Destrucción de los equipos o medios de comunicación	A, D, N
	Polvo, corrosión, congelación	A, D, N
Eventos naturales	Fenómeno sísmico	N
	Inundación	N
Pérdida de servicios esenciales	Fallo del sistema de suministro de aire acondicionado o de agua	A, D
	Pérdida del suministro de energía	A, D, N
	Falla de equipos de telecomunicaciones	A, D
Compromiso de información	Interceptación de señales	D
	Espionaje remoto	D
	Escucha ilegal	D
	Robo de multimedia o documentos	D
	Robo de equipos	D
	Recuperación de multimedia reciclados o desechados	D
	Divulgación	A, D
	Datos procedentes de fuentes no confiables	A, D
	Manipulación de hardware	D

Tipo	Amenaza	Origen
	Manipulación de software	A, D
	Detección de posición	D
Fallas técnicas	Fallo de equipo	A
	Mal funcionamiento de equipo	A
	Saturación del sistema de información	A, D
	Mal funcionamiento de software	A
	Incumplimiento de mantenimiento del sistema de información	A, D
Acciones no autorizadas	Uso de equipo sin autorización	D
	Uso de software falsificado o copiado	A, D
	Datos corruptos	D
	Tratamiento ilegal de datos	D
Compromiso de funciones	Error en el uso	A
	Abuso de los derechos	A, D
	Falsificación de derechos	D
	Incumplimiento de la disponibilidad de personal	A, D, N

Nota: Adaptado de ISO/IEC 27005

Adicionalmente, es muy importante prestar atención a las fuentes de amenazas humanas; es así que, estas se listan en la tabla 40.

Tabla 40

Catálogo de amenazas de tipo humano

Origen de la amenaza	Amenaza
Hacker, cracker	Hacking
	Ingeniería social
	Intrusión, accesos forzados al sistema
	Acceso no autorizado al sistema
Criminal informático	Acoso cibernético
	Actos fraudulentos (reproducción de archivos, suplantación, interceptación)
	Información corrupta
	Suplantación de identidad
	Intrusión en el sistema
Terrorista	Guerra de información
	Ataque al sistema (negación distribuida del servicio)
	Penetración al sistema
	Adulteración del sistema
Espionaje industrial	Explotación económica
	Robo de información

Origen de la amenaza	Amenaza
	Intrusión a información personal
	Ingeniería social
	Penetración al sistema
	Acceso no autorizado al sistema
Gente de adentro de la institución (empleados mal capacitados, resentidos, maliciosos, deshonestos o despedidos)	Asalto a un empleado
	Chantaje
	Intromisión a información personal
	Abuso informático
	Fraude y robo
	Soborno por información
	Ingreso de datos falsificados o corruptos
	Intercepción
	Códigos maliciosos (virus, bomba lógica, troyanos, etc.)
	Venta de información personal
	Intrusión en el sistema
	Disfunciones del sistema (bugs)
	Sabotaje al sistema

Nota: Adaptado de ISO/IEC 27005

4.2.6.3 Análisis del riesgo

El propósito del análisis del riesgo es comprender la naturaleza del riesgo y sus características incluyendo el nivel del riesgo. Este proceso depende de la información obtenida del proceso de identificación del riesgo. Existen dos aspectos importantes que determinarán el análisis del riesgo: probabilidad e impacto.

4.2.6.3.1 Probabilidad

La estimación de la probabilidad de ocurrencia del riesgo se establece de acuerdo con la tabla 41.

Tabla 41

Probabilidad de ocurrencia del riesgo

Valor	Estimación	Descripción
1	Muy baja	1 vez cada 20 años
2	Baja	1 vez cada 5 años
3	Media	1 vez al año
4	Alta	1 vez cada 6 meses
5	Muy alta	1 vez al mes

Nota: Elaboración propia

4.2.6.3.2 Impacto

La estimación del impacto que los riesgos pueden producir en los activos al materializarse una amenaza, se establece de acuerdo a la tabla 42.

Tabla 42
Impacto del riesgo

Valor	Estimación	Descripción
1	Insignificante	Los procesos no se verán afectados y pueden continuar su desarrollo con normalidad. No genera pérdidas económicas.
2	Menor	Los procesos son afectados de manera que se necesitará a lo más una hora para continuar con el desarrollo normal. Perdidas económicas mínimas.
3	Medio	Los procesos son afectados de manera que se tomarán horas para resolver el problema y continuar su desarrollo con normalidad.
4	Critico	Los procesos son afectados y podría tomar días para resolver el problema y continuar su desarrollo con normalidad. Se genera altas pérdidas financieras.
5	Catastrófico	Los procesos son afectados y podría tomar muchos días en solucionar el problema y continuar su desarrollo con normalidad. Se genera enormes pérdidas económicas.

Nota: Elaboración propia

4.2.6.4 Evaluación del riesgo

El propósito de la valoración del riesgo es apoyar a la toma de decisiones, esto implica comparar los resultados del análisis del riesgo con los criterios del riesgo establecidos para determinar cuándo se requiere una acción adicional. Según a la norma ISO 31000, en este proceso, en base al resultado del análisis del riesgo se determinan cuáles deben ser tratados y priorizados para implementar el tratamiento.

4.2.6.4.1 Cálculo del riesgo

Este se realiza en base a la relación de la probabilidad y el impacto; y se determina mediante la siguiente fórmula y tal como se muestra en la tabla 43.

$$\text{Riesgo} = \text{Probabilidad} \times \text{Impacto}$$

Tabla 43
Cálculo del riesgo

<u>PROBABILIDAD</u>	<u>IMPACTO</u>				
	Insignificante (1)	Menor (2)	Medio (3)	Crítico (4)	Catastrófico (5)
Muy baja (1)	1	2	3	4	5
Baja (2)	2	4	6	8	10
Media (3)	3	6	9	12	15
Alta (4)	4	8	12	16	20
Muy alta (5)	5	10	15	20	25

Nota: Elaboración propia

La tabla 44, nos muestra el nivel de riesgo, el rango y su descripción, que representan el grado o nivel de riesgo al que los activos de información podrían estar expuestos si una vulnerabilidad se materializara.

Tabla 44
Criterios de valoración de la magnitud del riesgo

Nivel de Riesgo	Rango	Descripción
Bajo	[1 - 7]	Se necesitan acciones correctivas y un plan que debe ser desarrollado para incorporar estas medidas en un plazo razonable de tiempo. Podría tomar a lo más una hora para poder continuar con las actividades. Las pérdidas financieras son ínfimas.
Medio	[8 - 14]	El sistema existente puede seguir funcionando, pero un plan de acción correctivo debe ser puesto en marcha. Podría tomar horas para poder resolver el problema, para así continuar con los procesos y no incurrir en más pérdidas financieras.
Alto	[15 - 25]	Es necesaria la implementación de medidas correctivas. Podría tomar días para resolver el problema causando altas pérdidas financieras.

Nota: Elaboración propia

4.2.6.4.2 Nivel de aceptación del riesgo

Se aceptará los riesgos y oportunidades cuyo rango este entre [1 – 7] en el cálculo del riesgo. También, se puede apreciar los criterios de aceptación del riesgo en la tabla 45.

Tabla 45
Criterios de aceptación del riesgo

Nivel de Riesgo	Rango	Descripción
Bajo	[1 - 7]	Totalmente tolerable
Medio	[8 - 14]	Regularmente tolerable
Alto	[15 - 25]	No tolerable

Nota: Elaboración propia

De esta manera, se obtiene la matriz de riesgos cualitativa que permitirá evaluar los riesgos identificados en la Municipalidad Distrital de El Agustino, estableciendo como apetito del riesgo los que se encuentran con un nivel de aceptación calificados como “medio” y “alto”, que serán analizados en la etapa del tratamiento del riesgo. En la figura 73, se puede apreciar la línea del apetito de riesgo a tratar.

Figura 73. Apetito del riesgo para el tratamiento de riesgos
Elaboración propia

4.2.6.5 Tratamiento del riesgo

Esta etapa viene hacer el conjunto de decisiones tomadas con respecto a cada activo de información. Es así que, tal como se muestra en la tabla 46, se han establecido las siguientes opciones de tratamiento para los riesgos identificados.

Tabla 46
Opciones de tratamiento de riesgo

Tratamiento	Descripción
Aceptar	Es reconocer y asumir las consecuencias del riesgo sin tomar ninguna medida, a menos que el riesgo se materialice.
Transferir	Es trasladar el impacto o consecuencia del riesgo a un tercero, junto con la responsabilidad.
Reducir	Es actuar para reducir la probabilidad de ocurrencia o el impacto de un riesgo, a través de la selección e implementación de controles.
Evitar	Es no iniciar o no continuar con la actividad que motiva el riesgo. Por ejemplo: cambiar el objetivo que se encuentra amenazado, reducir el alcance, etc.

Nota: Elaboración propia

4.2.7 Plan de tratamiento del riesgo – PTR

La norma ISO/IEC 27001:2013 en los requisitos 6.1.3e y 6.2 define como obligatoria la información documentada del plan de tratamiento de riesgo; es así, que una vez que hemos seleccionado aquellos riesgos considerados no aceptables, tenemos que aplicar nuevos controles para reducir la probabilidad e impacto y convertirlos en riesgos residuales. Para ello, primero determinamos los controles que necesitamos implementar, en segundo lugar, planificamos su implementación, y por último realizamos un seguimiento para valorar los resultados obtenidos, todo esto formará el PTR del diseño de nuestro SGSI.

El plan de tratamiento de riesgo presenta un costo y tiempo aproximado de realización del plan, los cuales se han estimado con las tablas 47 y 48 respectivamente. Dicho plan se puede revisar en el anexo 8 – Plan de tratamiento de riesgo.

Tabla 47
Costo aproximado para el PTR

Valor	Descripción
4	Mayor a S/. 50,000
3	S/. 25,000 a S/. 50,000
2	S/. 15,000 a S/. 25,000
1	Menor a S/. 15,000
D	Desconocido

Nota: Elaboración propia

Tabla 48
Tiempo aproximado para el PTR

Clasificación	Descripción
C	Corto plazo (Menos de 6 meses)
M	Mediano plazo (De 6 a 12 meses)
L	Largo plazo (Mas de 1 año)
D	Desconocido

Nota: Elaboración propia

4.2.8 Declaración de aplicabilidad – SOA

Es el documento donde se definen los controles del anexo A de la norma ISO/IEC 27001:2013 que son aplicables al Sistema de Gestión de Seguridad de la Información. Y para nuestro proyecto, según el requisito 6.1.3 d de la norma ISO/IEC 27001:2013 generar una Declaración de Aplicabilidad, después de haber identificado los controles para todos los riesgos con un nivel **No aceptable** para la municipalidad, se pasa a mencionar y justificar cuales son aplicables o no al entorno de la entidad.

En la tabla 49 se muestra los campos de identificación que tiene la declaración de aplicabilidad. Se puede revisar completo en el anexo 9 – Declaración de Aplicabilidad.

Tabla 49
Campos de identificación de la Declaración de Aplicabilidad

Campos	Descripción
Cláusula:	Clausulas o dominios de seguridad de la información.
Objetivo de control:	Referido a cada cláusula de la norma.
Control:	Se describe un tema específico para el riesgo asociado.
Aplicabilidad:	Si es aplicable o no a la municipalidad.
Justificación:	Razón por la que se aplica o no el control.

Nota: Elaboración propia

4.2.9 Programa de capacitación y concientización

De acuerdo a la norma ISO/IEC 27001:2013 capítulo 7 soporte y los requisitos 7.2 y 7.3, que hacen referencia a las competencias y conocimiento respectivamente, se debe formar y capacitar al personal en temas de seguridad de la información, para lo cual se desarrolló un programa de capacitación y concientización, que se puede ver a detalle en el anexo 10 (Programa de concientización y capacitación).

4.3 Etapa 3: Ejecución del proyecto

4.3.1 Manual del SGSI

El objetivo del manual del Sistema de Gestión de Seguridad de la Información es mostrar las directivas, acciones, lineamientos y políticas a seguir para una posterior implementación de un SGSI.

Este manual se basa en los lineamientos solicitados por la norma ISO/IEC 27001:2013 y tiene como alcance el proceso de recaudación y fiscalización tributaria del área de rentas de la municipalidad. El contenido del manual aplica a todo el personal de la entidad.

El manual en su totalidad se puede revisar en el anexo 11 – Manual del Sistema de Seguridad de la Información.

5 PRUEBAS, RESULTADOS Y VALIDACIÓN

En este capítulo se describen las pruebas, resultados y los métodos de validación que se han aplicado al diseño del Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para la Municipalidad Distrital de El Agustino, cumpliendo con los objetivos a través de los indicadores de logro planteados al inicio del proyecto.

5.1 Etapa 4: Evaluación del proyecto

5.1.1 Método de trabajo para la validación de las pruebas

Para ello se propone un flujo de trabajo, donde se identifican las acciones a realizar con el fin de validar los objetivos estratégicos planteados y realizar el seguimiento al SGSI. Dicho flujo se muestra en la figura 74.

Figura 74. Flujo de trabajo para la validación de las pruebas
Elaboración propia

Pruebas. - En esta fase se selecciona el método de validación para hacer frente al objetivo específico. Además, se indica las actividades y recursos necesarios para la realización de la respectiva evaluación.

Ejecución. - En esta fase se ejecuta el método de validación seleccionado.

Resultado. - En esta fase se revisan los resultados obtenidos en las pruebas realizadas y se valida con los indicadores de logro y métricas.

Plan de mejoras. - En esta fase corresponde al ciclo de mejora continua para las pruebas y resultados, ya que se proponen mejoras a los objetivos específicos planteados si fuera el caso.

5.1.2 Objetivo específico 1

Tabla 50.

Indicadores de logro y métricas del objetivo 1

Objetivo Específico	Indicador de logro	Métrica
Determinar el estado actual de cumplimiento de la norma ISO/IEC 27001:2013 en la MDEA	Informe del análisis de brechas de la MDEA	<p>Porcentaje de cumplimiento de las cláusulas de la norma ISO/IEC 27001:2013</p> <p>Porcentaje de cumplimiento de los dominios de la norma ISO/IEC 27001:2013.</p>

Nota: Elaboración propia

Pruebas

Indicador 1					
Id	Met-01	Fecha	30/01/2020	Versión	1
Nombre	Porcentaje de cumplimiento de las cláusulas de la norma ISO/IEC 27001:2013				
Objetivo	Determinar el nivel de madurez tanto de la norma como de los controles del sistema de seguridad de la información				
Fuente de datos	Informe de análisis GAP - Análisis de brechas				
Fórmula del cálculo	Estado de cumplimiento del SGSI = $(\frac{\Sigma \text{Nivel de madurez actual}}{\text{Cantidad de cláusulas aplicables}}) \times 100\%$				
	Nivel de madurez de controles = $(\frac{\Sigma \text{Cantidad de grado de cumplimiento}}{\text{Cantidad de controles aplicables}}) \times 100\%$				
Características del indicador					
<div><div><div></div><div>81 – 100 % Completamente implementado</div></div><div><div></div><div>61 – 80 % Parcialmente implementado</div></div><div><div></div><div>41 – 60 % Diseñado</div></div><div><div></div><div>21 – 40 % Parcialmente diseñado</div></div><div><div></div><div>1 – 20 % No diseñado</div></div></div>

5: Nivel óptimo alcanzado

4. Nivel deseado, se debe monitorizar y medir

3: Existen procedimientos, sin embargo, hay incumplimientos

2: No existen procedimientos, se requiere observación para no llegar al nivel rojo

1: Se requiere intervención reevaluación de los riesgos

Responsable	Coordinador del plan de seguridad de la información.
Frecuencia	Recolección: Semestral Reporte: Semestral
Formato de reporte	Gráfico de barras codificadas por colores
Descripción 1	
<p>Para este indicador se utiliza el informe del análisis de brechas – GAP Análisis (anexo 2 y 3) en el cual se encuentra detallado el nivel de madurez con respecto a la norma y de cada uno de los controles de seguridad de la información. Pero para ello, también ha sido necesario realizar una encuesta dirigida al área de rentas, a donde pertenece exclusivamente el proceso de recaudación y fiscalización tributaria.</p> <p>Finalmente, se utiliza las evaluaciones de cumplimiento de los capítulos de la norma ISO/IEC 27001:2013 y de los dominios de la norma ISO/IEC 27002:2013.</p> <p>Cada indicador representa valores, que son:</p>	

- Requisitos: Que mide el grado de cumplimiento actual de las cláusulas del 4 al 10 de la norma ISO/IEC 27001:2013.
- Controles: Que mide el grado de cumplimiento actual de los dominios del 5 al 18 de la norma ISO/IEC 27002:2013.

Para su cálculo se usarán las fórmulas de cálculo descritas, para luego obtener gráficas que permitan entender mejor el reporte. Finalmente, la revisión de las métricas será semestral, considerando que esa será la frecuencia de actualización por parte del coordinador del Sistema de Gestión de Seguridad de la Información.

Resultados 1

Figura 75. Cláusulas vs Nivel de madurez
Elaboración propia

De acuerdo a la figura 75, se observa que todas las cláusulas de la norma ISO/IEC 27001:2013 se encuentran en un nivel de madurez “No diseñado”. Eso nos lleva a inferir que, de existir procedimientos de control, estos no se encuentran bien definidos por la entidad, por lo que esta se encuentra en un nivel 1 "No diseñado".

Resultados 2

Figura 76. Dominios vs Nivel de madurez
Elaboraci3n propia

De acuerdo a la figura 76, se observa que la mayor3a de los controles se encuentra en un nivel de madurez “Sin control” y “Control inicial”, siendo los de mayor cantidad los que se encuentran en un nivel inicial. Eso nos lleva a inferir que, de existir controles y procedimientos, estos no se encuentran bien definidos por la entidad. Por lo que la Municipalidad Distrital de El Agustino se limita a encontrarse en un nivel de “Control inicial” con respecto a la mudurez de sus controles.

Adem3s, con el af3n de lograr la validez de la investigaci3n se realizaron encuestas a los trabajadores del 3rea de rentas. Dicha encuesta consisti3 en 15 preguntas dicot3micas para medir opiniones y el estado b3sico de seguridad de la informaci3n dentro del 3rea de rentas, todo esto con la finalidad de corroborar el estado de la seguridad de la informaci3n.

A continuaci3n, se muestran los resultados de la encuesta aplicada a los 12 trabajadores del 3rea.

Análisis de las encuestas realizadas

Pregunta 1

Tabla 51

Encuesta aplicada a la pregunta 1

Indicador	Parámetro	Cantidad	Porcentaje
¿En la MDEA existe un Sistema de Gestión de Seguridad de la Información?	Si	0	0%
	No	12	100%
	En blanco	0	0%

Nota: Elaboración propia

Figura 77. Frecuencia de respuesta de la pregunta 1
Elaboración propia

Interpretación: De la figura 77, se observa que el 100% afirma que no existe un Sistema de Gestión de Seguridad de la Información.

Conclusión: Que se necesita con urgencia el diseño e implementación de un SGSI dentro de la municipalidad.

Pregunta 2

Tabla 52
Encuesta aplicada a la pregunta 2

Indicador	Parámetro	Cantidad	Porcentaje
¿Cree usted que el diseño e implementación de un Sistema de Gestión Seguridad de la Información permitirá mejorar la seguridad de información de su área de trabajo?	Si	0	92%
	No	11	0%
	En blanco	1	8%

Nota: Elaboración propia

Figura 78. Frecuencia de respuesta de la pregunta 2
Elaboración propia

Interpretación: De la figura 78, se observa que del 100 % de trabajadores el 92 % están de acuerdo de que el diseño e implementación de un SGSI mejorará la seguridad de la información del área de rentas.

Conclusión: Se puede concluir que la mayoría de los trabajadores del área de rentas son conscientes del beneficio que traerá el diseño de un SGSI.

Pregunta 3

Tabla 53.
Encuesta aplicada a la pregunta 3

Indicador	Parámetro	Cantidad	Porcentaje
¿Cree usted que en su área de trabajo se logrará un cambio positivo con la aplicación de un Sistema de Gestión de Seguridad de la Información?	Si	11	92%
	No	0	0%
	En blanco	1	8%

Nota: Elaboración propia

Figura 79. Frecuencia de respuesta de la pregunta 3
Elaboración propia

Interpretación: De la figura 79, se observa que del 100% de trabajadores el 92% considera o cree que con la aplicación de un SGSI se lograrán cambios positivos en la seguridad de la información, mientras que el 8% considera que no.

Conclusión: Se puede concluir que casi todos los trabajadores del área de rentas son conscientes de los beneficios que traerá el diseño e implementación de un SGSI.

Pregunta 4

Tabla 54
Encuesta aplicada a la pregunta 4

Indicador	Parámetro	Cantidad	Porcentaje
¿Aprobaría usted la implementación del Sistema de Gestión de la Seguridad de la Información en su área de trabajo?	Si	12	100%
	No	0	0%
	En blanco	0	0%

Nota: Elaboración propia

Figura 80. Frecuencia de respuesta de la pregunta 4
Elaboración propia

Interpretación: De la figura 80, se observa que el 100% de los trabajadores están dispuestos a aprobar el diseño e implementación de un SGSI.

Conclusión: Se puede concluir todos los trabajadores del área de rentas están dispuestos a colaborar en el diseño e implementación del sistema.

Pregunta 5

Tabla 55
Encuesta aplicada a la pregunta 5

Indicador	Parámetro	Cantidad	Porcentaje
¿Aprobaría usted programas dirigidos a todos los empleados para concientizar sobre la seguridad de la información en su área de trabajo?	Si	12	100%
	No	0	0%
	En blanco	0	0%

Nota: Elaboración propia

Figura 81. Frecuencia de respuesta de la pregunta 5
Elaboración propia

Interpretación: De la figura 81, se observa que el 100% de los trabajadores del área de rentas están dispuestos a participar en programas de concientización sobre seguridad de la información.

Conclusión: Se puede concluir que todos los trabajadores están dispuestos a participar de programas de concientización sobre seguridad de la información,

Pregunta 6

Tabla 56
Encuesta aplicada a la pregunta 6

Indicador	Parámetro	Cantidad	Porcentaje
¿Considera usted que en su área de trabajo existe información que debe ser protegida?	Si	12	100%
	No	0	0%
	En blanco	0	0%

Nota: Elaboración propia

Figura 82. Frecuencia de respuesta de la pregunta 6
Elaboración propia

Interpretación: De la figura 82, se observa que el 100% de los trabajadores considera que en el área de rentas existe información sensible que debe ser protegida.

Conclusión: Se concluye que todos los trabajadores del área de rentas son conscientes de la existencia de información sensible y que esta debe ser protegida con la implementación de un SGSI.

Pregunta 7

Tabla 57

Encuesta aplicada a la pregunta 7

Indicador	Parámetro	Cantidad	Porcentaje
¿Ha recibido usted capacitación sobre seguridad de la información de acuerdo a su función laboral?	Si	2	17%
	No	9	75%
	En blanco	1	8%

Nota: Elaboración propia

Figura 83. Frecuencia de respuesta de la pregunta 7
Elaboración propia

Interpretación: De la figura 83, que del 100% de los trabajadores el 17% indica haber recibido capacitación sobre seguridad de la información, el 8% no sabe, frente a un 75% que indica no haber recibido capacitación.

Conclusión: Se concluye que por el alto porcentaje que no ha recibido capacitación sobre temas de seguridad de información, es más probable que la información se vea afectada en sus dimensiones de confidencialidad, integridad y disponibilidad.

Pregunta 8

Tabla 58
Encuesta aplicada a la pregunta 8

Indicador	Parámetro	Cantidad	Porcentaje
¿Cuenta usted con un computador o laptop para realizar sus funciones?	Si	10	83%
	No	2	17%
	En blanco	0	0%

Nota: Elaboración propia

Figura 84. Frecuencia de respuesta de la pregunta 8
Elaboración propia

Interpretación: De la figura 84, se observa que del 100% de trabajadores el 83% cuenta con una computadora para realizar sus funciones en la entidad y el 17% no tiene.

Conclusión: El 17% de los trabajadores que no cuentan con una computadora para llevar a cabo sus funciones es porque se considera que las funciones que realizan no lo ameritan, por ejemplo, personal que trabaja en campo.

Pregunta 9

Tabla 59
Encuesta aplicada a la pregunta 9

Indicador	Parámetro	Cantidad	Porcentaje
¿Cuenta usted con un clave de acceso para ingresar a su computador o laptop?	Si	9	90%
	No	1	10%
	En blanco	0	0%

Nota: Elaboración propia

Figura 85. Frecuencia de respuesta de la pregunta 9
Elaboración propia

Interpretación: De la figura 85, se observa que del 100% de trabajadores que usan computador o laptop para realizar sus funciones, el 90% cuenta con una clave de acceso, mientras que el 10% no cuentan con una clave.

Conclusión: Se concluye que existe un alto porcentaje que tienen sus claves de acceso, pero que es necesario que tomen medidas para que ese porcentaje que no tienen también puedan tener esa medida de seguridad.

Pregunta 10

Tabla 60

Encuesta aplicada a la pregunta 10

Indicador	Parámetro	Cantidad	Porcentaje
Cuándo su computador esta desatendido ¿se activa el bloqueo de pantalla con contraseña para proteger la información?	Si	7	70%
	No	2	20%
	En blanco	1	10%

Nota: Elaboración propia

Figura 86. Frecuencia de respuesta de la pregunta 10

Elaboración propia

Interpretación: De la figura 86, se observa que del 100% de trabajadores el 70% que usan las computadoras afirman que sí se activa el bloqueo de pantalla cuando el equipo esta desatendido, mientras que el 20% indica que no y el 10% indica que no sabe.

Conclusión: Se concluye que es necesario verificar que todos los equipos cuenten con esta medida de seguridad.

Pregunta 11

Tabla 61
Encuesta aplicada a la pregunta 11

Indicador	Parámetro	Cantidad	Porcentaje
¿En lo que va del año ha sufrido modificación o pérdida de información ya sea por virus, acceso de personas no autorizadas, deterioro, extravió, etc.?	Si	8	75%
	No	4	25%
	En blanco	0	0%

Nota: Elaboración propia

Figura 87. Frecuencia de respuesta de la pregunta 11
Elaboración propia

Interpretación: De la figura 87, se observa que el 58% indica haber sido víctima de modificación o pérdida de información, mientras que el 42% indica que no.

Conclusión: Se concluye que es necesario la verificar e implementar nuevas medidas de seguridad en la entidad.

Pregunta 12

Tabla 62
Encuesta aplicada a la pregunta 12

Indicador	Parámetro	Cantidad	Porcentaje
¿En lo que va del año se ha divulgado la información sensible para la MDEA sin su autorización o conocimiento?	Si	7	58%
	No	3	25%
	En blanco	2	17%

Nota: Elaboración propia

Figura 88. Frecuencia de respuesta de la pregunta 12
Elaboración propia

Interpretación: De la figura 88, se observa que del 100% de los encuestados el 58% afirma que en lo que va del año se ha divulgado información sensible de la entidad, mientras que el 25% indica que no y el 17% no sabe.

Conclusión: Se concluye que es necesario la verificar e implementar nuevas medidas de seguridad en la entidad para evitar que se divulgue información sensible de la entidad.

Pregunta 13

Tabla 63
Encuesta aplicada a la pregunta 13

Indicador	Parámetro	Cantidad	Porcentaje
¿Su área de trabajo cuenta con software antivirus actualizado?	Si	7	58%
	No	3	25%
	En blanco	2	17%

Nota: Elaboración propia

Figura 89. Frecuencia de respuesta de la pregunta 13
Elaboración propia

Interpretación: De la figura 89, se observa que del 100% de encuestados el 58% indica que sus equipos si cuentan con antivirus actualizado, mientras que el 33% indica que no y el 8% no sabe.

Conclusión: Se concluye que necesario verificar que todos los equipos cuenten con esta medida para evitar posibles riesgos de seguridad.

Pregunta 14

Tabla 64
Encuesta aplicada a la pregunta 14

Indicador	Parámetro	Cantidad	Porcentaje
¿Realiza usted copias de seguridad para proteger su información?	Si	9	75%
	No	3	25%
	En blanco	0	0%

Nota: Elaboración propia

Figura 90. Frecuencia de respuesta de la pregunta 14
Elaboración propia

Interpretación: De la figura 90, se observa que del 100% de encuestados el 75% si realiza copias de seguridad para proteger su información en sus propios equipos mientras que el 25% no lo realiza. Indicando que los que si realizan las copias de seguridad lo hacen en los propios equipos de trabajo.

Conclusión: Se concluye que los trabajadores que realizan sus propias copias de seguridad la mayoría están contenidos en sus propios equipos, lo que sigue siendo un riesgo de pérdida de información si le sucediera algo al equipo, siendo necesario establecer planes de contingencia.

Pregunta 15

Tabla 65
Encuesta aplicada a la pregunta 15

Indicador	Parámetro	Cantidad	Porcentaje
¿Considera que su oficina está protegida contra amenazas externas o ambientales que ocasionan pérdidas de información?	Si	9	75%
	No	3	25%
	En blanco	0	0%

Nota: Elaboración propia

Figura 91. Frecuencia de respuesta de la pregunta 15
Elaboración propia

Interpretación: De la figura 91, se observa que el 100% de los trabajadores considera que el área de rentas es vulnerable a amenazas externas o ambientales que pueden ocasionar pérdidas de información.

Resultados

Finalmente, según el semáforo de colores presentado, la Municipalidad Distrital de El Agustino se posiciona en un nivel rojo. Esto claramente porque no existen políticas, procedimientos y lineamientos correctamente definidos y documentados de seguridad de la información.

Plan de mejoras

Es necesario volver a emplear este procedimiento, luego de haber implementado el diseño propuesto con el fin de evaluar la evolución del Sistema de Gestión de Seguridad de la Información.

5.1.3 Objetivo específico 2

Tabla 66

Indicadores de logro y métricas del objetivo 2

Objetivo Específico	Indicador de logro	Métrica
Identificar los activos críticos de información del proceso de recaudación y fiscalización tributaria de la MDEA	Inventario de activos de la información.	Porcentaje de activos críticos de información.

Nota: Elaboración propia

Pruebas

Indicador 2					
Id	Met-02	Fecha	30/01/2020	Versión	1
Nombre	Porcentaje de activos críticos de información				
Objetivo	Determinar la cantidad de activos críticos de información que se han identificado en el proceso de recaudación y fiscalización tributaria.				
Fuente de datos	Inventario de activos de información				
Fórmula del cálculo	$\% \text{ de activos críticos} = \left(\frac{\text{Cantidad de activos críticos}}{\text{Cantidad total de activos de información}} \right) \times 100\%$				
Característica del indicador					
<div><div><div></div><div></div><div></div></div><div><div>Mayor a 60%</div><div>Entre 30 – 60%</div><div>Menor a 30%</div></div></div>					

<p>Rojo: La mayoría de los activos de información son críticos</p> <p>Amarillo: Casi la mayoría de los activos son críticos</p> <p>Verde: Los activos de información críticos son menos</p>	
Responsables	Coordinador del SGSI Propietario del proceso
Frecuencia	Recolección: Bimestral Análisis y reporte: Semestral Revisión de métricas: Anual
Formato de reporte	Gráfico de barras codificadas por colores
Descripción	
<p>Para este indicador se utiliza el inventario de activos que se encuentra en el anexo 5, en el cual se encuentra el registro de cada uno de los activos que maneja el proceso de recaudación y fiscalización tributaria de la Municipalidad Distrital de El Agustino.</p> <p>Para obtener el inventario de activos se utilizó como herramienta el Diagrama Tortuga (anexo 13) y también una encuesta (anexo 14). La encuesta fue dirigida a los trabajadores del área de rentas y a la subgerencia de planeamiento, gestión de procesos y tecnologías de información; y con ello se logró determinar cuáles son los activos de información involucrados en dicho proceso.</p> <p>Luego, se valorizó los activos según su grado de importancia y criticidad para la municipalidad. Primero, se valoriza la afectación o pérdida que le puede generar a la entidad en los aspectos financiero, legal y de imagen, puesto que si se materializase una amenaza sobre el activo afecte su confidencialidad, integridad y disponibilidad. En la tabla 34 se detalla los criterios de valorización.</p> <p>Para demostrar este objetivo, el indicador representa dos valores, que son:</p> <ul style="list-style-type: none"> – Críticos: Cantidad de activos que han sido valorizados como “Medio” y “Alto” – Total: Cantidad de activos de información valorizados. <p>Para su cálculo se usará la fórmula de cálculo descrita en el indicador, para luego obtener gráficas que permitan entender mejor el reporte. La revisión de las métricas será anual, considerando que esta será la frecuencia con el que será actualizado por parte de los responsables.</p>

Nota: Elaboración propia

Como ejemplo de lo realizado para cada activo, se ha tomado dos activos que a continuación pasamos a describir en la tabla 67.

Tabla 67

Identificación y evaluación de activos

Identificación y evaluación de activos		
ID Activo	D01	Base de datos
Descripción	Base de datos donde se guardan todos los datos de los contribuyentes de la municipalidad	
Categoría	Datos	

Actividades	<ul style="list-style-type: none">- Se evalúa la frecuencia de uso del activo junto con el subgerente de TI, determinando que tiene una frecuencia de uso alta.- Se evalúa la clasificación junto con el subgerente de TI, determinando que es un activo confidencial, que debe mantenerse en estricta reserva.- Se evalúa el valor y criticidad junto con el subgerente de TI, determinando que los valores son: confidencial (4), integridad (4) y disponibilidad (4) teniendo como promedio el valor de 4.		
Valor	4	Nivel de criticidad	Alto
ID Activo	SW01	Sistema de recaudación tributaria municipal	
Descripción	Sistema que permite realizar la determinación y liquidación de los tributos de los contribuyentes.		
Categoría	Software		
Actividades	<ul style="list-style-type: none">- Se evalúa la frecuencia de uso juntamente con el gerente de rentas, determinando que su frecuencia de uso es Alta.- Se evalúa la clasificación junto con el gerente de rentas, determinando que es un activo confidencial, que debe mantenerse en estricta reserva.- Se evalúa el valor y criticidad junto con el subgerente de TI, determinando que los valores son: confidencial (4), integridad (4) y disponibilidad (4) teniendo como promedio el valor de 4.		
Valor	4	Nivel de criticidad	Alto

Nota: Elaboración propia

Resultados

Comparando estos resultados con los rangos del semáforo establecido para el indicador, estos activos de información se encuentran en un nivel rojo, es decir más de la mitad de los activos tienen un nivel de criticidad medio y alto. Por lo tanto, la entidad tiene que hacer uso de una metodología que le permita gestionar de forma adecuada sus activos de información.

Plan de mejoras

Dado que el proyecto solo abarca el diseño del Sistema de Gestión de Seguridad de la Información, no se incluye mejoras de implementación. Sin embargo, se recomienda la revisión y realización de las pruebas en una frecuencia semestral, ya que algún activo de información ha podido cambiar su valor de criticidad o impacto en el negocio.

5.1.4 Objetivo específico 3

Tabla 68

Indicadores de logro y métricas del objetivo 3

Objetivo Específico	Indicador de logro	Métrica
Identificar los riesgos de los activos críticos de información.	Matriz de gestión riesgos	Porcentaje de riesgos críticos de los activos de información

Nota: Elaboración propia

Pruebas

Indicador 3					
Id	Met-03	Fecha	30/01/2020	Versión	1
Nombre	Porcentaje de riesgo críticos de los activos de información				
Objetivo	Identificar los principales riesgos de los activos de información que podrían afectar el proceso de recaudación y fiscalización tributaria.				
Fuente de datos	Matriz de riesgos				
Fórmula del cálculo	$\% \text{ de riesgos críticos} = \left(\frac{\sum \text{Cantidad de riesgos críticos}}{\sum \text{Cantidad de riesgos totales}} \right) \times 100\%$				
Característica del indicador					
<div> </div> <p>Rojo: La mayoría de los riesgos de los activos son críticos</p> <p>Amarillo: Casi la mitad de los riesgos de los activos son críticos</p> <p>Verde: La cantidad de riesgos críticos de los activos son minoría.</p>					
Responsable	Coordinador del plan de seguridad de la información.				
Frecuencia	Recolección: Semestral Reporte: Semestral				

Formato de reporte	Gráfico de barras codificadas por colores								
Descripción									
<p>Para este indicador se utiliza el informe de la matriz de análisis y evaluación de riesgos (anexo 9). Así mismo, se tomó en cuenta los incidentes que se han ido suscitando en la entidad y que fueron reportados por los trabajadores al área de TI. Este indicador evaluará dos valores, que son:</p> <ul style="list-style-type: none"> - Críticos: Cantidad de riesgos reportados. - Total: Cantidad de riesgos totales identificados. <p>La finalidad es visualizar que tanto se estaría perdiendo en caso se materialice los riesgos críticos de seguridad de la información.</p> <p>Para su cálculo se usará la fórmula descrita en el indicador, a efectos de poder obtener posteriormente una gráfica que nos permita entender el reporte.</p> <p>La revisión de estas métricas deberá ser anual, dado que se realizará una nueva gestión de riesgos cada año.</p>									
Resultados
<table border="1"> <caption>Cantidad vs Riesgos críticos</caption> <thead> <tr> <th>Nivel de Riesgo</th> <th>Porcentaje</th> </tr> </thead> <tbody> <tr> <td>Alto</td> <td>44%</td> </tr> <tr> <td>Medio</td> <td>56%</td> </tr> <tr> <td>Bajo</td> <td>0%</td> </tr> </tbody> </table>		Nivel de Riesgo	Porcentaje	Alto	44%	Medio	56%	Bajo	0%
Nivel de Riesgo	Porcentaje								
Alto	44%								
Medio	56%								
Bajo	0%								
<p><i>Figura 93. Cantidad vs Riesgos críticos</i> Elaboración propia</p> <p>De acuerdo a la figura 93, se observa que el 56%, es decir más de la mitad de los riesgos de seguridad de la información se encuentran en un nivel de riesgo “Medio” y un 44% tiene</p>									

un nivel de riesgo “Alto”. Por consiguiente, pese a que la municipalidad ha realizado esfuerzos para gestionar los riesgos de seguridad de la información, la mayoría de estos riesgos críticos asociados a acciones por parte del personal de la entidad.

Como ejemplo de lo realizado en la gestión de riesgos, se ha tomado dos activos que a continuación pasamos a describir en la tabla 69.

Tabla 69
Evaluación de activos

Evaluación de activos			
Id activo	SW02	Base de datos	
Actividad Nº1	<ul style="list-style-type: none">- Se evalúa la amenaza junto al subgerente de TI y se determina que podría haber modificación deliberada de la información del contribuyente.- Se evalúa la vulnerabilidad junto al subgerente de TI y se evidencia la falta de control en el acceso a consultas a la base de datos.- Se evalúa el riesgo junto al subgerente de TI y se evidencia una posible modificación en los montos a pagar por impuestos de autoavalúo y arbitrios.		
Id riesgo	R05 10	Nivel riesgo	Alto
Actividad Nº2	<ul style="list-style-type: none">- Se evalúa la amenaza junto al subgerente de TI y se determina que podría ocurrir un ingreso lógico no autorizado.- Se evalúa la vulnerabilidad junto al subgerente de TI y se evidencia el incumplimiento de permisos, privilegios y accesos de control en la base de datos.- Se evalúa el riesgo junto al subgerente de TI y se evidencia la posible alteración de la información de los contribuyentes, generando pérdidas económicas a la entidad.		
ID riesgo	R01	Nivel riesgo	Alto
Id activo	SW01	Sistema de recaudación tributaria municipal	
Actividad	<ul style="list-style-type: none">- Se evalúa la amenaza junto al subgerente de TI y se determina que en el sistema podría ocurrir un procesamiento ilegal de datos.		

	<ul style="list-style-type: none"> - Se evalúa la vulnerabilidad junto al subgerente de TI y se evidencia la falta registros de acceso al sistema. - Se evalúa el riesgo junto al subgerente de TI y se evidencia la posible modificación o pérdida de información para producir otro tipo de información. 		
ID riesgo	R28	Nivel riesgo	Alto

Nota: Elaboración propia

Resultados

Comparando los resultados con los rangos del semáforo establecido para el indicador, estos se encuentran en un nivel rojo, puesto que la entidad aún no cuenta con una metodología que le permita gestionar de manera adecuada los riesgos detectados a sus activos de información.

Plan de mejora

Dado que el proyecto abarca solo el diseño del Sistema de Gestión de Seguridad de la Información, no se incluyen mejoras en la implementación de la metodología de riesgos. Sin embargo, se recomienda la revisión de los riesgos sobre los activos en una frecuencia semestral.

5.1.5 Objetivo específico 4

Tabla 70

Indicadores de logro y métricas del objetivo 4

Objetivo Específico	Indicador de logro	Métrica
Determinar los controles para el plan de tratamiento de riesgo de la seguridad de la información.	Declaración de aplicabilidad (SOA)	Porcentaje de controles aplicables sobre los activos críticos de información

Nota: Elaboración propia

Pruebas

Indicador 4					
Id	Met-04	Fecha	30/01/2020	Versión	1
Nombre	Porcentaje de controles aplicables sobre los activos críticos de información.				
Objetivo	Identificar el avance en la implementación de los controles de la norma ISO/IEC 27001:2013.				

Fuente de datos	Declaración de Aplicabilidad
Fórmula del cálculo	$\% \text{ de controles aplicables} = \left(\frac{\text{Número de controles aplicables}}{\text{Número total de controles}} \right) \times 100\%$
Características del indicador
<p>Rojo: Nivel óptimo de implementación de los controles</p> <p>Amarillo: Nivel satisfactorio de implementación de los controles</p> <p>Verde: Nivel mínimo de implementación de los controles</p>	
Responsable	Coordinador del plan de seguridad de la información.
Frecuencia	Se debe seguir el PTR, dado que ahí se encuentra el tiempo aproximado de implementación de cada control de seguridad de la información.
Formato de reporte	Tabla con la cantidad de controles aplicables y no aplicables y un gráfico circular de colores.
Descripción	
<p>Para este indicador se utiliza el informe de la Declaración de Aplicabilidad - SOA (anexo 9).</p> <p>Se enumeran todos los controles del anexo A de la norma ISO/IEC 27001:2013 que aplican en el Plan de Tratamiento de Riesgo - PTR, para salvaguardar los activos de información. Este indicador evaluará dos valores, que son:</p> <ul style="list-style-type: none"> - Controles aplicables: Cantidad de controles aplicables - Total: Cantidad total de controles de la norma <p>La finalidad es conocer en qué porcentaje los controles de la norma son aplicables al diseño del SGSI.</p> <p>Para su cálculo se usará la fórmula descrita en el indicador, a efectos de poder obtener posteriormente una gráfica que nos permita entender el reporte.</p>	

Resultados

Tabla 71

Controles aplicables de seguridad de la información

Cláusulas	Aplicables	No aplicables
5. Políticas de seguridad de la información	2	0
6. Organización de la seguridad de la información	2	5
7. Seguridad en los recursos humanos	5	1
8. Gestión de activos	7	3
9. Control de acceso	12	2
10. Criptografía	0	2
11. Seguridad física y ambiental	10	5
12. Seguridad de las operaciones	8	6
13. Seguridad de las comunicaciones	5	2
14. Adquisición, desarrollo y mantenimiento de sistemas	1	12
15. Relaciones con los proveedores	1	4
16. Gestión de incidentes de seguridad de la información	2	5
17. Aspectos de seguridad de la información en la gestión de continuidad del negocio	3	1
18. Cumplimiento	4	4
Total de controles	62	52

Nota: Elaboración propia

En la tabla 71, podemos apreciar que de los 114 controles de la norma ISO/IEC 27001:2013, los que son aplicables al diseño de este Sistema de Gestión de Seguridad de la Información son 62 y no aplicables 52, que representan en porcentaje el 54% y 46% respectivamente, tal como se puede observar en la figura 94.

Figura 94. Porcentaje de controles aplicables
Elaboración propia

Nota: Elaboración propia

Resultados

Comparando los resultados con los rangos del semáforo establecido para el indicador, este se encuentra en un nivel verde, es decir que implementando los controles propuestos aplicables el avance de implementación con respecto a la ISO/IEC estaría en un rango de 50 a 70% con respecto a la norma.

Plan de mejora

Dado que el proyecto abarca solo el diseño del SGSI, no se incluyen mejoras. Sin embargo, es necesario que se ejecute el plan de tratamiento de riesgo propuesto ya que existe un alto grado de criticidad en los activos de información y en una frecuencia semestral realizar el SOA para ir revisando el avance de implementación.

5.2 Etapa 5: Cierre del proyecto

Terminado y verificado todas las etapas del proyecto en conjunto con la alta dirección de la Municipalidad Distrital de El Agustino, se acordó realizar el acta de cierre del proyecto para que sirva como un certificado del diseño del Sistema de Gestión de Seguridad de la Información para la entidad. Dicha acta se encuentra en el anexo 16 - Acta de cierre de proyecto.

6 CONCLUSIONES

Habiendo finalizado el diseño del Sistema de Gestión de Seguridad de la Información para la Municipalidad Distrital de El Agustino, se ha podido llegar a las siguientes conclusiones:

- Se concluye que, del análisis de brechas realizado en la entidad para determinar el estado inicial tanto de las cláusulas y de los dominios, la MDEA se encuentra en un nivel inicial, es decir que no cuenta con las medidas de seguridad adecuadas o de tenerlos no se encuentran correctamente definidos.
- Se concluye que, de la identificación, clasificación y valorización de los activos de información del proceso de recaudación y fiscalización tributaria perteneciente al área de rentas, existen varios activos de información con nivel de criticidad alta representando el 72% del total de activos, que deben ser protegidos para la continuidad del negocio.
- Se concluye que, de la identificación de los riesgos de los activos de información del proceso de recaudación y fiscalización tributaria perteneciente al área de rentas, existen varios activos de información que tienen un nivel de riesgo alto con un 44% y medio con 56%, por lo cual es oportuno implementar controles y medidas de seguridad para la protección de los activos de información.
- Se concluye que, de la elaboración del Plan de Tratamiento de Riesgos para el proceso de recaudación y fiscalización tributaria perteneciente al área de rentas, se puede reducir cuantitativamente los riesgos de los activos de información hasta alcanzar un nivel aceptable por la entidad, ya que estos fueron diseñados a medida
- Finalmente, se concluye que, diseñar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 protegerán de una forma adecuada los activos de información del proceso de recaudación y fiscalización tributaria del área de rentas.

7 RECOMENDACIONES

- Se recomienda realizar la implementación del Sistema de Gestión de Seguridad de la Información para mitigar los riesgos de los activos de información de la Municipalidad Distrital de El Agustino.
- Se recomienda aplicar el mantenimiento periódico a las políticas de seguridad de la información, ya que nos encontramos en un entorno cambiante donde se introducen nuevas tecnologías y las amenazas pueden cambiar.
- Se recomienda revisar la metodología de gestión de riesgos con la finalidad de evaluar su eficacia y aplicar mejoras en su implementación.
- Se recomienda concientizar a los trabajadores en lo relacionado a la seguridad de la información mediante capacitaciones y charlas informativas, con el fin de que adquieran las competencias y destrezas necesarias referente a la seguridad de la información.
- Se recomienda a la Municipalidad Distrital de El Agustino asignar un presupuesto orientado a la implementación de los controles del Sistema de Gestión de Seguridad de la Información, capacitaciones y charlas de concientización, y las revisiones periódicas que se darán para asegurar la continuidad del sistema.
- Se recomienda evaluar y certificar los procesos de la entidad bajo la norma ISO/IEC 27001.

8 REFERENCIAS

- Abril, A., Pulido, J., & Bohada, J. (2013). *Análisis de riesgos en seguridad de la información*. Ciencia, Innovación y Tecnología, 1, 40-53. Recuperado a partir de <https://www.jdc.edu.co/revistas/index.php/rciyt/article/view/121>.
- Acta de transferencia (2018). *Municipalidad Distrital de El Agustino*.
- Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2003). *Introduction to the OCTAVE Approach*. Pittsburgh: Networked Systems Survivability Program.
- Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2005). *OCTAVE-S Implementation Guide - Introduction to OCTAVE-S*. Pittsburgh.
- Alemán, H. & Rodríguez, C. (2015). *Metodologías para el Análisis de Riesgos en los SGSI*. Revista Especializada en Ingeniería, 9, 73-85.
- Alexander, A. (2007). *Diseño de un Sistema de Gestión de Seguridad de Información Óptica ISO/IEC 27001:2005*. Bogotá: Alfaomega Colombiana S.A.
- Aliaga, L. (2013). *Diseño de un Sistema de Gestión de Seguridad de Información para un Instituto Educativo*. (Tesis de Licenciatura, Pontificia Universidad Católica del Perú, Facultad de Ciencias e Ingeniería. Lima, Perú).
- Angarita, J & Bautista, C. (2014). *Diseño de un Sistema de Gestión de la Seguridad de la Información ISO 27001 para la alcaldía de Floridablanca y Plan de acción para su implementación según la guía PMBOK*. (Proyecto de grado, Universidad Industrial de Santander, Facultad de Ingenierías Fisiomecánicas. Bucaramanga, Colombia).
- Autoridad Nacional de Protección de Datos Personales (APDP). (2013). *El Derecho Fundamental a la Protección de Datos Personales. Guía para el ciudadano*.
- Caralli, R., Stevens, J., Young, L. & Wilson, W. (2007). *Introducing OCTAVE Allegro: Improving the Information Security Assessment Process*. Carnegie Mellow University.
- Cardoso, O. (2014). *Modelado de Procesos de Seguridad de la Información basado en el estándar O-ISM3*. (Trabajo final de especialización en Seguridad Informática, Universidad de Buenos Aires, Facultad de Ciencias Económicas, Cs. Exactas y Naturales e Ingeniería. Ibagué, Colombia).

- Castillo, R. (2016). *Sistema de Gestión de Seguridad de la Información en la Municipalidad Distrital de Pira aplicando la Norma ISO/IEC 27001:2013*. (Tesis de licenciatura, Universidad Católica los Ángeles de Chimbote, Facultad de Ingeniería. Huaraz, Perú).
- Ccesa, M. (2017). *Diseño de un Sistema de Gestión de Seguridad de la Información bajo la NTP ISO/IEC 27001:2014 para la Municipalidad Provincial de Huamanga, 2016*. (Tesis de licenciatura, Universidad Nacional de San Cristóbal de Huamanga, Facultad de Ingeniería. Ayacucho, Perú).
- Club de la Securite de L'information Francais (CLUSIF). (2010). *MEHARI 2010 Introducción*.
- Congreso de la República del Perú (2013) Ley N° 29733. *Ley de Protección de Datos Personales*.
- Consultores en Seguridad de la Información (CSI). (2016). *Seguridad Informática vs Seguridad de la Información*. Maestro de la computación [Entrada en blog] Recuperado de <https://www.maestrodelacomputacion.net/seguridad-informatica-seguridad-de-la-informacion/>. [Consulta: 20 de diciembre de 2019].
- Dávila, M. (2018). *Evaluación de un Sistema de Gestión de Seguridad de la Información basado en la Norma ISO 27001:2013, en la Municipalidad Distrital de José Crespo y Castillo – Aucayucu; 2018*. (Tesis de licenciatura, Universidad Católica los Ángeles de Chimbote, Facultad de Ingeniería. Chimbote, Perú).
- De la Cruz, R. (2016). *Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016*. (Tesis de licenciatura, Universidad Nacional Pedro Ruiz Gallo, Facultad de Ingeniería. Lambayeque, Perú).
- Deloitte (2015). *COSO Evaluación de Riesgos* [Presentación de servicios de auditoría]. México.
- Equipo Lteam (4 de junio de 2019). ISO 3100:2018 Gestión del Riesgo [Archivo de video]. Recuperado de <https://www.youtube.com/watch?v=k5gblbzHeFI> [Consulta: 20 de enero de 2020].

- Ernst & Young Global (2018) *¿La ciberseguridad es algo más que protección?* Encuesta Global de Seguridad de Información 2018-19.
- García, Félix (2019). *E-Pulpo – Plataforma GRC para la gestión integral de la seguridad IT* [XII Jornadas STIC CCN-CERT] (Video YouTube: <https://www.youtube.com/watch?v=VBHjp0wtHF4>) [Consulta: 20 de setiembre de 2019].
- Gómez, A, (2011). *Enciclopedia de la Seguridad Informática*. Segunda Edición. DF: Alfaomenga.
- Gómez, L. & Fernández, P. (2015). *Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad*. Madrid, España.
- Gutiérrez, C. (2013). *MAGERIT: Metodología práctica para gestionar riesgos*. Recuperado de <https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/> [Consulta: 5 de setiembre de 2019].
- Holguín, F & Lema, L. (14 de enero de 2019). *Modelo para Medir la Madurez del Análisis de Riesgo de los Activos de Información en el contexto de las Empresas Navieras*. Revista Ibérica de Sistemas e Tecnologias de Informação. Recuperado de http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1646-98952019000100002 [Consulta: 22 de enero de 2020].
- Instituto Nacional de Ciberseguridad (INCIBE). (2015). *Gestión de riesgos. Una guía de aproximación para el empresario*. Recuperado de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf [Consulta: 22 de enero de 2020].
- Instituto Nacional de Ciberseguridad (INCIBE). (2016). *Gestión de riesgos. Una guía para la aproximación del empresario*.
- Instituto Nacional de Ciberseguridad (INCIBE). (2017). *Análisis de riesgos en 6 pasos*. Recuperado de <https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo> [Consulta: 22 de enero de 2020].
- Instituto Nacional de Tecnologías de la Comunicación (INTECO) (27 de abril de 2010). *Los activos de Seguridad de la Información* [Archivo de video]. Recuperado de

<https://www.youtube.com/watch?v=THnQ2FH7NtU&list=PLyQDCKiQR7I7EvAEHSR9MN2Maw5sZVShd&index=7> [Consulta: 10 octubre de 2019].

International Organization for Standardization and International Electrotechnical Commission ISO/IEC 17799:2005. *Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión e la seguridad de la información*. (2da Edición).

International Organization for Standardization and International Electrotechnical Commission ISO/IEC 27001:2013. *Tecnologías de la Información – Técnicas de Seguridad – Sistemas de gestión de seguridad de la información – Requerimientos*.

International Standard ISO/IEC 27005 (2018). *Information Technology – Security techniques – Information Security Risk Management*. Third edition.

ISACA (2009). *Marco de Riesgos de TI*. Madrid, España.

ISACA (2012). *COBIT 5 – Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*. Madrid, España.

ISACA (2012). *COBIT 5 Introducción* [Presentación Traducción al Español Cortesía de ISACA Capítulo de Panamá].

ISOTools Excellence (2016). *La norma ISO 27002 complemento para la ISO 27001* [Blog especializado en Sistemas de Gestión de Seguridad de la Información]. Recuperado de <https://www.pmg-ssi.com/2016/06/la-norma-iso-27002-complemento-para-la-iso-27001/> [Consulta: 27 de setiembre de 2019].

ISOTools Excellence (2018). *Norma ISO 31000: El valor de la gestión de riesgos en las organizaciones*.

Landeta, F. & Quille, D. (2016). *Análisis y diseño de un Sistema de Gestión de Seguridad de la Información en base a las normas ISO 27001 y 27002 para la Superintendencia de Control del Poder de Mercado*. (Tesis de licenciatura, Universidad Politécnica Salesiana, Facultad de Ingeniería. Quito, Ecuador).

López, A. & Ruiz, J. (2012). *El Portal de ISO 27001 en español*. Recuperado de <http://www.iso27000.es/> [Consulta: 8 de setiembre de 2019].

- MAGERT (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Versión 3. Madrid: España.
- Manual de Organización y Funciones (MOF). (2019). *Municipalidad Distrital de El Agustino*.
- Medina, J. (2015). *Análisis del estado actual de la gestión de la seguridad de la información en la sede principal de Corporinoquia*. (Master Universitario en Seguridad Informática, Universidad Internacional de La Rioja. Yopal, Colombia).
- Municipio al día - *Información confiable para la gestión*. [Entrada de blog]. Recuperado de <https://municipioaldia.com/municipalidades-del-peru/> [Consulta: 20 de diciembre de 2019].
- National Institute of Standards and Technology (NIST) (2012). *Information Security. Guide for Conducting Risk Assessments. NIST Special Publication 800-30*.
- National Institute of Standards and Technology (NIST) (2013). *Security and Privacy Controls for Federal Information Systems and Organizations. NIST Special Publication 800-53*. Revision 4.
- Norma Internacional ISO 31000. *Gestión del Riesgo – Directrices*. Segunda edición 2018-02.
- Norma Técnica Peruana (NTP) ISO/IEC 27001:2014 EDI. *Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la información. Requisitos*. (2da. Edición).
- Norma Técnica Peruana (NTP) ISO/IEC 27002:2017. *Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información*.
- Olivan, A. (2017). *Guía de controles de Ciberseguridad para la protección integral de la Pyme*. (Máster Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones. UOC/UAB/URV/UIB).
- Professional Evaluation and Certification Board (PECB) (2016). *Implementador Líder – Certificado en la ISO 27001*. Versión 4.8.
- Prensa El Agustino (2018). Recuperado de <https://prensaelagustino1.wordpress.com/>.

- PricewaterHouse (2018). *Encuesta Global sobre Delitos Económicos y Fraude 2018*. Lima, Perú. PwC Perú.
- PricewaterHouse (2018). *Resultados de la Encuesta Global de Seguridad de la Información*. Buenos Aires, Argentina. PwC Argentina.
- Professional Evaluation and Certification Board (PECB). (2016). *Information Security Training. Implementador Líder Certificado en la norma ISO/IEC 27001*. Guía del participante.
- Reglamento de Organización y Funciones (ROF). (2019). *Ordenanza N° 592 Municipalidad Distrital de El Agustino*.
- Sánchez, M. (2015). *Auditoria Informática*. Recuperado de <https://chauri201511701014974.wordpress.com/> [Consulta: 9 de setiembre de 2019].
- Santonja, J. (2019). *Análisis y correlación entre probabilidad e impacto de los riesgos*. (Trabajo fin de máster, Universidad de Alicante).
- Seminario, H. (2015). *¿Qué es la Seguridad de la Información?* [Presentación para el curso de Seguridad de la Información]. Lima: Universidad Peruana de Ciencias Aplicadas.
- Seminario, H. (2015). *Análisis y Evaluación de Riesgos* [Presentación para el curso de Seguridad de la Información]. Lima: Universidad Peruana de Ciencias Aplicadas.
- Tarrillo, E. & Correa, J. (2015). *Metodología para un Sistema de Gestión de la Seguridad de la Información basado en la Norma Técnica Peruana NTP – 17799 en la Administración de la Municipalidad Distrital de Lambayeque Setiembre 2013 – Febrero 2014*. (Tesis de licenciatura, Universidad Nacional Pedro Ruiz Gallo, Facultad de Ingeniería. Lambayeque, Perú).
- Torres, M. (2018). *Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI), basada en la norma ISO/IEC 27001:2013, para el proceso de pos-venta de un integrador de soluciones en Telecomunicaciones*. (Tesis de Licenciatura, Universidad Peruana de Ciencias Aplicadas, Facultad de Redes y Comunicaciones. Lima, Perú).
- Tupia, M. (2010). *Administración de la Seguridad de la Información*. Primera edición. Lima, Perú.

9 GLOSARIO

Activo

Cualquier cosa que tenga valor para la organización.

Ataque

Cualquier acción deliberada con el objetivo de violar los mecanismos de seguridad de un sistema de información.

Autenticidad

Aseguramiento de la identidad u origen.

Amenazas

“Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización”

Disponibilidad

Propiedad de ser accesible y utilizable cuando lo requiera una entidad autorizada.

Confidencialidad

Propiedad por la cual no se pone a disposición o revela información a personas, entidades o procesos no autorizados.

Control

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Disponibilidad

Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y a sus activos asociados.

Evento de seguridad

Momento en que la amenaza existe y pone en riesgo activos, procedimientos o información.

Gestión de riesgos

Selección de implementación de medidas de seguridad para conocer, prevenir, impedir, reducir o controlar los riesgos identificados. La gestión de riesgos se basa en resultados obtenidos en el análisis de riesgos.

Impacto

El impacto en un activo es la consecuencia sobre éste de la materialización de una amenaza”. Se relaciona con la severidad de las consecuencias en caso de que ocurra o se materialice un riesgo, estas consecuencias suelen traducirse en pérdidas monetarias, confianza, oportunidades de negocio, etc.

Integridad

Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.

ISO/IEC 27001

Norma que establece los requisitos para un Sistema de Gestión de la Seguridad de la Información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.

Medida de seguridad

Procedimiento o mecanismo tecnológico que reduce el riesgo.

Plan de tratamiento de riesgos

Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Riesgo

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños y / o perjuicios a la Organización.

Seguridad

Capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la

disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

Seguridad de la información

Conservación de la confidencialidad, integridad, y disponibilidad de la información; además, otras propiedades

Seguridad Informática

Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

Sistema de Gestión de Seguridad de la Información

“Es aquella parte del sistema general de gestión que comprende la política, la estructura organizativa, los recursos necesarios, los procedimientos y los procesos necesarios para implementar la gestión de seguridad de la información en una organización” (Gómez, Álvaro 2011:52)

Tratamiento del riesgo

Proceso de selección e implementación de medidas para modificar el riesgo.

Valor de un activo

Estimación del costo inducido por la materialización de una amenaza.

Vulnerabilidad

Debilidad de un activo o control que puede ser explotada por una o más amenazas.

10 SIGLARIO

APDP	Autoridad Nacional de Protección de Datos Personales
COBIT	Control Objectives for Information and Related Technology
CRAMM	CCTA Risk Analysis and Management Method
IEC	International Electrotechnical Commission
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
LAN	Local Area Network
LPDP	Ley de Protección de Datos Personales
MDEA	Municipalidad Distrital de El Agustino
MEHARI	Method for Harmonized Analysis of Risk
NIST	National Institute of Standards and Technology
NTP	Norma Técnica Peruana
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
O-ISM3	Open Information Security Management Maturity Model
PTR	Plan de Tratamiento de Riesgos
SGSI	Sistema de Gestión de Seguridad de la Información

11 ANEXOS

Anexo 1 – Acta de constitución del proyecto

ACTA DE CONSTITUCIÓN DEL PROYECTO			
Versión 1			
1. Información General			
Nombre del Proyecto:	Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para la Municipalidad Distrital de El Agustino	Fecha de preparación:	14/08/2019
Preparado por:	Lisbet Monteza Mera		
Revisado por:	Ing. Roger Arturo Chuctaya Yauri		
Autorizado por:	Víctor Salcedo Ríos		
2. Descripción del Proyecto			
En el proyecto se diseña un SGSI basado en la norma internacional ISO/IEC 27001:2013, que Proteger adecuadamente los activos de información de la municipalidad distrital de El Agustino. Tiene una duración de 5 meses para su diseño.			
3. Necesidad del Proyecto			
Proteger adecuadamente los activos de información de la municipalidad distrital de El Agustino.			
3. Objetivos del Proyecto			
<ul style="list-style-type: none">• Identificar los activos críticos de información del proceso de Recaudación y Fiscalización Tributaria perteneciente al área de rentas de la MDEA.• Identificar los riesgos de los activos críticos de información.• Determinar los controles para el plan de tratamiento de riesgo de la seguridad de la información.• Determinar el estado actual de cumplimiento de la MDEA con respecto a los requisitos de la norma ISO/IEC 27001:2013.			
4. Alcance del Proyecto			
El proyecto contempla el diseño de un SGSI para el proceso de Recaudación y Fiscalización Tributaria perteneciente a la Gerencia de Rentas.			

Anexo 2 – Análisis GAP de las cláusulas de la norma ISO/IEC 27001:2013

Cláusula	Requisitos ISO 27001:2013	Estado	Nivel de madurez	Comentario o Sugerencia
4	CONTEXTO DE LA ORGANIZACIÓN			
4.1	Comprender la organización y su contexto			
	La organización debe determinar los asuntos externos e internos que son importantes para su objetivo y que afecte su capacidad para lograr el(los) resultados(s) esperado(s) de su sistema de gestión de la seguridad de la información.	No diseñado	1	La MDEA posee documentos de su misión, visión y los objetivos estratégicos. Pero no contempla puntos sobre seguridad de la información. Se sugiere establecer objetivos de seguridad de la información que estén alineados a los objetivos estratégicos.
4.2	Comprender las necesidades y expectativas de las partes interesadas			
	La organización debe determinar: a) Las partes interesadas que son pertinentes para el sistema de gestión de la seguridad de la información.	No diseñado	1	Se recomienda determinar las partes interesadas y comprender las necesidades y expectativas de la entidad, referente a la seguridad de la información.
	b) Los requisitos de estas partes interesadas que sean pertinentes para la seguridad de la información.	No diseñado	1	Se recomienda determinar los requisitos relevantes a la seguridad de la información.
4.3	Determinar el alcance del sistema de gestión de seguridad de la información			
	La organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance.	No diseñado	1	Se recomienda determinar el alcance del SGSI.

Cláusula	Requisitos ISO 27001:2013	Estado	Nivel de madurez	Comentario o Sugerencia
	Cuando se determina el alcance la organización debe considerar: a) Los aspectos externos e internos referidos en el 4.1	No diseñado	1	Se recomienda tener en cuenta los aspectos externos e internos relevantes a la seguridad de la información para determinar el alcance.
	b) Los requisitos referidos en el 4.2	No diseñado	1	Se recomienda determinar el alcance teniendo en cuenta los requisitos de las partes interesadas.
	c) Interfases y dependencias entre las actividades por la organización y aquellas realizadas por otras organizaciones	No diseñado	1	Se recomienda tener presente las interfases y dependencias entre las actividades realizadas por la entidad y las que son realizadas por otras entidades.
	El alcance está disponible como información documentada.	No diseñado	1	Se recomienda que una vez determinado el alcance del SGSI, este sea documentado y colocado en un lugar accesible a las partes interesadas.
4.4	Sistema de gestión de seguridad de la información			
	La organización debe establecer, implementar, mantener y mejorar la manera continua un sistema de gestión de la seguridad de la información, según los requerimientos de esta norma.	No diseñado	1	Se recomienda establecer un plan para la mejora continua del SGSI conforme a la norma ISO/IEC 27001:2013.
5	LIDERAZGO			
5.1	Liderazgo y compromiso			

Cláusula	Requisitos ISO 27001:2013	Estado	Nivel de madurez	Comentario o Sugerencia
	La alta dirección debe demostrar liderazgo y compromiso con respecto al SGSI al: a) asegurar que los objetivos de la política de seguridad de la información y la seguridad de la información se establezcan y sean compatibles con la dirección estratégicas de la organización;	Parcialmente diseñado	2	Es necesario establecer una política de seguridad de la información que sea compatible con la dirección estratégica de la entidad.
	b) asegurar la integración de los requisitos del sistema de gestión de la seguridad de la información a los procesos de la organización;	Parcialmente diseñado	2	Afianzar la integración del SGSI con los procesos de la entidad.
	c) asegurar que los recursos necesarios para el SGSI estén disponibles;	Parcialmente diseñado	2	La alta dirección debe asegurar los recursos necesarios para la implementación del SGSI; es decir, que debe disponer de un presupuesto para gestionar el proyecto del SGSI.
	d) comunicar la importancia de la gestión de seguridad de la información efectiva y del cumplimiento de los requisitos del SGSI;	No diseñado	1	Es necesario que la alta dirección deba comunicar la importancia de una gestión efectiva de la seguridad de la información.
	e) asegurar que el SGSI logre su(s) resultado(s) esperado(s);	No diseñado	1	
	f) dirigir y apoyar a las personas para que contribuyan a la eficacia del SGSI;	No diseñado	1	
	g) promover la mejora continua;	No diseñado	1	

Cláusula	Requisitos ISO 27001:2013	Estado	Nivel de madurez	Comentario o Sugerencia
	h) apoyar otros roles de gestión relevantes para demostrar su liderazgo, según corresponda a sus áreas de responsabilidad;	No diseñado	1	
5.2	Política			
	a) La alta dirección debe establecer una política de seguridad de la información que sea pertinente con el objetivo de la organización.	No diseñado	1	Es necesario establecer la política de seguridad de la información de acuerdo al propósito de la municipalidad, además de incluir los objetivos de seguridad de la información (cláusula 6.2), mantenerla disponible y comunicada a toda la entidad.
	b) La alta dirección debe establecer una política de seguridad de la información que incluya los objetivos de seguridad de la información o que proporcione el marco de trabajo para establecer los objetivos de seguridad de la información.	No diseñado	1	
	c) La alta dirección debe establecer una política de seguridad de la información que incluya un compromiso para la mejora continua del sistema de gestión de la seguridad de la información.	No diseñado	1	
	d) La política de seguridad de la información debe ser comunicada dentro de la organización y estar disponible para las partes interesadas, según corresponda.	No diseñado	1	
	e) La política de seguridad de la información debe estar disponible como información documentada.	No diseñado	1	Es indispensable documentar la política de seguridad de la información.

Cláusula	Requisitos ISO 27001:2013	Estado	Nivel de madurez	Comentario o Sugerencia
	f) La política de seguridad de la información debe ser comunicada dentro de la organización.	No diseñado	1	Es necesario establecer medios para comunicar la política de la seguridad de la información, por ejemplo por medio de email, intranet, etc.
	g) La política de seguridad de la información debe estar disponible para las partes interesadas, según corresponda.	No diseñado	1	Es necesario establecer medios para comunicar la política de seguridad de la información a las partes interesadas.
5.3	Roles, responsabilidades y autoridades organizacionales			
	La alta dirección debe asegurar que las responsabilidades y las autoridades para los roles pertinentes a la seguridad de la información son asignados y comunicados.	Parcialmente diseñado	2	La alta dirección debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la seguridad de la información estén asignadas y comunicadas.
	a) La alta dirección debe asignar la responsabilidad y la autoridad para asegurar que el SGSI cumpla con los requisitos de esta norma.	No diseñado	1	Es necesario que la alta dirección designe a un responsable auditor que compruebe que el SGSI está de acuerdo con la norma ISO/IEC 270001:2013.
	b) La alta dirección debe asignar la responsabilidad y la autoridad para informar a la alta dirección sobre el desempeño del SGSI.	Parcialmente diseñado	2	Se debe asignar un responsable que reporte a la alta dirección sobre el desempeño del SGSI.
6	PLANIFICACIÓN			
6.1	Acciones para tratar los riesgos y las oportunidades			
6.1.1	Generalidades			

Cláusula	Requisitos ISO 27001:2013	Estado	Nivel de madurez	Comentario o Sugerencia
	Al planificar el SGSI, la organización debe considerar los requisitos tratados en 4.1 y 4.2, y determinar los riesgos y oportunidades que necesitan ser cubiertos para: a) asegurar que el S.GSI pueda lograr los resultados esperados; b) evitar o disminuir efectos no deseados; y c) lograr una mejora continua	No diseñado	1	Es necesario que al planificar el SGSI se tenga en cuenta las cláusulas 4.1 y 4.2 a fin de determinar los riesgos y oportunidades que necesitan ser tratados para asegurar que el SGSI logre los resultados esperados, prevenir o reducir efectos indeseados y lograr una mejora continua. Es necesario también elaborar un plan de acción para el tratamiento de riesgos y oportunidades, y su integración e implementación en el SGSI, asimismo considerar indicadores para evaluar la efectividad de las acciones.
	La organización debe planificar: d) acciones para abordar estos riesgos y oportunidades; y	No diseñado	1	Es necesario planificar acciones que traten estos riesgos y oportunidades.
	e) como: 1. integrar e implementar las acciones en los procesos del sistema de gestión de seguridad de la información; y 2. evaluar la eficacia de estas acciones	No diseñado	1	Es necesario planificar la integración e implementación de las acciones para la gestión del riesgo.
6.1.2	Evaluación de riesgo de la seguridad de la información			

Cláusula	Requisitos ISO 27001:2013	Estado	Nivel de madurez	Comentario o Sugerencia
	La organización debe definir y aplicar un proceso de evaluación de riesgo de la seguridad de la información que: a) establezca y mantenga los criterios de riesgo de la seguridad de la información que incluya: 1. los criterios de aceptación del riesgo; y 2. los criterios para realizar las evaluaciones de riesgo de la seguridad de la información;	No diseñado	1	Es necesario definir y aplicar un procedimiento que establezca y mantenga criterios de aceptación y valoración de riesgos de seguridad de la información.
	b) asegure que las evaluaciones de riesgo de la seguridad de la información producen resultados consistentes, válidos y comparables, una y otra vez;	No diseñado	1	Definir y aplicar un procedimiento que asegure que las valoraciones repetidas de riesgos de seguridad de la información produzcan resultados consistentes, válidos y comparables.
	c) identifica los riesgos de la seguridad de la información: 1. aplica el proceso de evaluación del riesgo de la seguridad de la información para identificar los riesgos asociados a la pérdida de la confidencialidad, integridad y disponibilidad para la información dentro del alcance del SGSI; y 2. identifica los propietarios del riesgo;	No diseñado	1	Es necesario establecer un procedimiento o acoger una metodología de gestión de riesgos de seguridad de la información.

Cláusula	Requisitos ISO 27001:2013	Estado	Nivel de madurez	Comentario o Sugerencia
	d) analiza los riesgos de la seguridad de la información; 1. evalúa las posibles consecuencias que podrían resultar si los riesgos identificados en 6.1.2 c) 1. se hicieran realidad; 2. evalúa la probabilidad realista de la ocurrencia de los riesgos identificados en 6.1.2 c) 1.; y 3. determina los niveles de riesgo;	No diseñado	1	Determinar los niveles de riesgo teniendo en cuenta el impacto y la probabilidad del riesgo.
	e) evalúa los riesgos de la seguridad de la información; 1. compara los resultados del análisis de riesgo con los criterios de riesgo definidos en 6.1.2 a); y 2. prioriza los riesgos analizados para el tratamiento de riesgo.	No diseñado	1	Evaluar los riesgos de acuerdo con los criterios de riesgos establecidos en 6.1.2 a), priorizando estos riesgos para su respectivo tratamiento.
	La organización debe conservar la información documentada acerca del proceso de evaluación de riesgo de la seguridad de la información.	No diseñado	1	Es indispensable documentar el procedimiento de valoración del riesgo de seguridad de la información.
6.1.3	Tratamiento de riesgos de la seguridad de la información			
	La organización debe definir y aplicar un proceso de tratamiento de riesgo de la seguridad de la información para:	No diseñado	1	Es necesario definir y aplicar un procedimiento para el tratamiento de riesgos de seguridad de la información.

Cláusula	Requisitos ISO 27001:2013	Estado	Nivel de madurez	Comentario o Sugerencia
	a) seleccionar las opciones apropiadas de tratamiento de riesgo de la seguridad de la información, tomando en consideración los resultados de la evaluación de riesgo;	No diseñado	1	Es importante tener en cuenta los resultados de la valoración de riesgos al seleccionar las opciones de tratamiento de riesgos de seguridad de la información.
	b) determinar todos los controles que son necesarios para implementar las opciones de tratamiento de riesgo de la seguridad de la información escogida;	No diseñado	1	Es necesario determinar los controles necesarios para el tratamiento de riesgos de seguridad de la información.
	c) comparar los controles definidos en 6.1.3 b) más arriba con aquellos en Anexo A y verificar que ningún control necesario fue omitido;	No diseñado	1	Comparar los controles adoptados para el tratamiento de riesgos de seguridad de la información con los controles proporcionados en el anexo A de la norma ISO/IEC 27001:2013 para evitar omitir algún control.
	d) generar una Declaración de Aplicabilidad que contenga los controles necesarios [consultar 6.1.3 b) y c)], y además la justificación de inclusiones, sean estas implementadas o no y la justificación para exclusiones de controles de Anexo A;	No diseñado	1	Se debe elaborar la Declaración de Aplicabilidad con los controles a implementar y/o justificaciones de omisión de algunos controles del Anexo A.
	e) formular un plan de tratamiento del riesgo de seguridad de la información; y	No diseñado	1	Se debe elaborar un plan de tratamiento de riesgos de seguridad de la información.

Cláusula	Requisitos ISO 27001:2013	Estado	Nivel de madurez	Comentario o Sugerencia
	f) obtener la aprobación del propietario del riesgo del plan de tratamiento del riesgo de la seguridad de la información y la aceptación de los riesgos de la seguridad de la información residual.	No diseñado	1	Es importante reunirse con los propietarios de los riesgos y obtener la aprobación del plan de tratamiento de riesgos y aceptación de los riesgos residuales de la seguridad de la información.
	La organización debe conservar la información documentada acerca del proceso de tratamiento del riesgo de la seguridad de la información.	No diseñado	1	Es indispensable documentar el procedimiento de tratamiento de riesgos de seguridad de la información.
6.2	Objetivos de seguridad de la información y planificación para conseguirlos			
	La organización debe establecer los objetivos de seguridad de la información en niveles y funciones relevantes.	No diseñado	1	Establecer los objetivos de seguridad de la información alineados a los objetivos estratégicos de la organización.
	Los objetivos de seguridad de la información deben:	No diseñado	1	Se debe elaborar los objetivos de seguridad de la información, estos deben ser consistentes con la política de la seguridad de la información, ser medibles, conforme a los requisitos de seguridad de la información y la gestión de riesgos. Asimismo, deben ser comunicados y actualizados.
	a) ser consistentes con la política de seguridad de la información;	No diseñado	1	
	b) ser medible (si es posible);	No diseñado	1	
	c) tomar en consideración los requisitos de seguridad de la información aplicable y los resultados de la evaluación de riesgo y el tratamiento de riesgo;	No diseñado	1	
	d) ser comunicados; y	No diseñado	1	
	e) estar actualizados según corresponda.	No diseñado	1	

Cláusula	Requisitos ISO 27001:2013	Estado	Nivel de madurez	Comentario o Sugerencia
	La organización debe conservar la información documentada sobre los objetivos de la seguridad de la información. Al planificar cómo lograr sus objetivos de seguridad de la información, la organización debe determinar: f) qué se hará; g) qué recursos se necesitarán; h) quién será responsable; i) cuándo se terminará; y j) cómo se evaluarán los resultados.	No diseñado	1	Se debe documentar los objetivos de la seguridad de la información. Dentro del proyecto de implementación del SGSI es necesario mirar los pasos a realizar, los recursos necesarios, los responsables, tiempo final y métodos o procedimientos para evaluar los resultados.
7	SOPORTE			
7.1	Recursos			
	La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI.	No diseñado	1	Es necesario asignar presupuesto para la implementación, mantenimiento y mejora continua del SGSI.
7.2	Competencia			
	La organización debe determinar las competencias necesarias de las personas que trabajan bajo su control que afecta su desempeño de seguridad de la información.	No diseñado	1	Determinar las competencias del personal a su cargo para un correcto desempeño del SGSI, cuando sea necesario tomar acciones para adquirir las competencias necesarias

Cláusula	Requisitos ISO 27001:2013	Estado	Nivel de madurez	Comentario o Sugerencia
	a) Determinar la competencia necesaria de la(s) persona(s) que trabajan bajo su control que afecta su desempeño en seguridad de la información;	Parcialmente diseñado	2	sobre la seguridad de la información, documentar las competencias como evidencia.
	b) Asegurar que estas personas son competentes sobre la base de educación, capacitación, o experiencia adecuados;	Parcialmente diseñado	2	
	c) Cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la efectividad de las acciones tomadas; y	Parcialmente diseñado	2	
	d) Retener información documentada apropiada como evidencia de competencia.	No diseñado	1	
7.3	Conocimiento			
	Las personas que trabajen bajo el control de la organización deben estar al tanto de:	No diseñado	1	Es necesario concientizar al personal que trabaja en la organización sobre la importancia de la seguridad de la información, la política de seguridad y el papel crucial que cumple cada uno de ellos en el correcto desempeño de SGSI, asimismo concientizarlos sobre las consecuencias de no cumplir con los requisitos del SGSI.
	a) la política de seguridad de la información.	No diseñado	1	Elaborar la política de seguridad de la información

Cláusula	Requisitos ISO 27001:2013	Estado	Nivel de madurez	Comentario o Sugerencia
	b) su contribución a la efectividad del SGSI, incluyendo los beneficios de un mejor desempeño de la seguridad de la información;	Parcialmente diseñado	2	Se han realizado algunos cursos y talleres a los que han asistido el personal de la subgerencia de TI. Pero no hay evidencia de capacitaciones para el resto del personal de la entidad.
	c) las implicancias de no tener conformidad con los requisitos del sistema de gestión de seguridad de la información.	No diseñado	1	Se puede implementar la norma ISOIEC 27001:2013 por cumplimiento legal.
7.4	Comunicación			
	<p>La organización debe determinar la necesidad de comunicaciones internas y externas que sean pertinentes al SGSI que incluya:</p> <ul style="list-style-type: none"> - qué comunicar; - cuándo comunicarlo; - con quién comunicarlo; y - los procesos que se verán afectados por la comunicación. 	Parcialmente diseñado	2	<p>Es necesario establecer comunicación con la secretaria de gobierno digital, autoridad responsable de formular y proponer las políticas nacionales y sectoriales en materia de informática y gobierno digital, además de promover el desarrollo e implementación de la seguridad de la información en las entidades públicas del estado.</p> <p>Se recomienda documentar los procedimientos de comunicación y mantenerlos como evidencia.</p>
7.5	Información documentada			
7.5.1	General			

Cláusula	Requisitos ISO 27001:2013	Estado	Nivel de madurez	Comentario o Sugerencia
	El sistema de gestión de la seguridad de la información debe incluir: a) información documentada necesaria para esta norma; y	No diseñado	1	Se sugiere iniciar la elaboración de la documentación necesaria exigida por la norma ISO/IEC 27001:2013 y lograr la efectividad del SGSI.
	b) información documentada, definida por la organización como necesaria para la efectividad del sistema de gestión de la seguridad de la información.	No diseñado	1	
7.5.2	Creación y actualización			
	Al crear y actualizar la información documentada, la organización debe asegurar la correspondiente: a) identificación y descripción (por ejemplo, un título, fecha, autor o número de referencia);	No diseñado	1	Es necesario asegurar la creación de los documentos exigidos por la norma ISO/IEC 27001:2013, determinar las herramientas y formatos de los documentos, así como los medios y procedimientos para su aprobación, revisión y actualización.
	b) formato (por ejemplo, idioma, versión de software, gráficos) y medio (por ejemplo, papel, digital); y	No diseñado	1	
	c) revisión y aprobación para conveniencia y suficiencia.	No diseñado	1	
7.5.3	Control de la información documentada			

Cláusula	Requisitos ISO 27001:2013	Estado	Nivel de madurez	Comentario o Sugerencia
	La información documentada necesaria por el sistema de gestión de la seguridad de la información y por la norma debe ser controlada para asegurar que: a) está disponible y apropiada para su uso, donde y cuando sea necesario; y	No diseñado	1	Es necesario controlar que la documentación exigida por la norma ISO/IEC 27001:2013 esté disponible y protegida en los tres pilares de la seguridad que son confidencialidad, integridad y disponibilidad.
	b) está debidamente protegida (por ejemplo, de pérdidas de confidencialidad, uso inapropiado o pérdida de integridad).	No diseñado	1	
	Para el control de la información documentada, la organización debe abordar las siguientes actividades, según corresponda: c) distribución, acceso, recuperación y uso;	No diseñado	1	Establecer procedimientos de control para la información documentada, esto es distribución, acceso, uso, almacenamiento, preservación, control de cambios, retención y disposición.
	d) almacenamiento y conservación, incluida la conservación de la legibilidad;	No diseñado	1	
	e) control de cambios (por ejemplo, control de versión); y	No diseñado	1	
	f) retención y disposición.	No diseñado	1	
	Información documentada de origen externo, determinada por la organización, de ser necesario, para la planificación y operación del sistema de gestión de la seguridad de la información debe ser identificado como apropiado y controlado.	No diseñado	1	Es necesario la revisión de documentación de origen externo tal como la NTP ISO/IEC 27001:2014, Ley de Protección de datos Personales, Resoluciones Ministeriales, etc., para empezar la planificación e implementación del SGSI en la MDEA.
8	OPERACIÓN			

Cláusula	Requisitos ISO 27001:2013	Estado	Nivel de madurez	Comentario o Sugerencia
8.1	Planificación y control operacional			
	La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información y para implementar las acciones definidas en 6.1. La organización además debe implementar los planes para lograr los objetivos de seguridad de la información, definidos en 6.2.	No diseñado	1	Es debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información e implementar las acciones determinadas en 6.1. Asimismo, implementar planes para lograr los objetivos de seguridad de la información determinados en 6.2.
	La organización debe mantener la información documentada hasta que sea necesario y tener la certeza que los procesos se llevaron a cabo según lo planeado.	Parcialmente diseñado	2	Se debe mantener la información documentada para estar segura de que los procesos se han llevado a cabo tal como fueron planificados.
	La organización debe controlar los cambios planeados y revisar las consecuencias de los cambios no planeados, al tomar acciones para mitigar cualquier efecto adverso, según sea necesario.	Parcialmente diseñado	2	Es necesario controlar los cambios planeados y revisar las consecuencias de cambios no intencionados, actuar para mitigar cualquier efecto adverso según sea necesario.
	La organización debe asegurar de que los procesos externalizados se determinan y controlan.	Parcialmente diseñado	2	Asegurar que los procesos tercerizados son determinados y controlados.
8.2	Evaluación de riesgos de seguridad de la información			

Cláusula	Requisitos ISO 27001:2013	Estado	Nivel de madurez	Comentario o Sugerencia
	La organización debe realizar evaluaciones de riesgo de la seguridad de la información, en intervalos planificados o cuando se propongan u ocurran cambios significativos, considerando los criterios establecidos en el 6.1.2.	No diseñado	1	Es necesario planificar los intervalos de tiempo en los que se llevarán a cabo las evaluaciones de riesgos de seguridad de la información, además, de documentar los resultados de éstas evaluaciones.
	La organización debe conservar la información documentada de los resultados de las evaluaciones de riesgo de la seguridad de la información.	No diseñado	1	Disponer de información documentada de los resultados de las evaluaciones de riesgos de seguridad de la información.
8.3	Tratamiento de riesgos de seguridad de la información			
	La organización debe implementar el plan de tratamiento de riesgo de la seguridad de la información.	No diseñado	1	Es necesario implementar el plan de tratamiento de riesgo de seguridad de la información en la entidad.
	La organización debe conservar la información documentada de los resultados del tratamiento de riesgo de la seguridad de la información.	No diseñado	1	Se debe documentar los resultados del tratamiento de riesgo de seguridad de la información.
9	EVALUACIÓN DEL DESEMPEÑO			
9.1	Monitoreo, medición, análisis y evaluación			

Cláusula	Requisitos ISO 27001:2013	Estado	Nivel de madurez	Comentario o Sugerencia
	La organización debe evaluar el desempeño de la seguridad de la información y la efectividad del SGSI. La organización debe determinar: a) qué se necesita monitorear y medir, incluidos los controles y procesos de la seguridad de la información;	No diseñado	1	Establecer procedimientos para realizar el monitoreo, medición, análisis y evaluar el desempeño de la seguridad de la información y la efectividad del SGSI. Documentar los resultados del monitoreo, medición, análisis y evaluación del SGSI. Evaluar el desempeño de la seguridad de la información y la efectividad del SGSI.
	b) los métodos para monitorear, medir, analizar y evaluar, según corresponda, para asegurar resultados válidos;	No diseñado	1	Es necesario determinar qué es lo que necesita ser monitoreado y medido, los métodos para el monitoreo, medición, análisis y evaluación, cuándo debe realizarle el monitoreo y medición, cuándo deben ser analizados y evaluados los resultados de monitoreo y medición y quién es el responsable de monitorear y medir, analizar y evaluar los resultados.
	c) cuándo se deben llevar a cabo el monitoreo y la medición;	No diseñado	1	
	d) quién debe monitorear y medir;	No diseñado	1	
	e) cuándo se deben analizar y evaluar los resultados del monitoreo y la medición; y	No diseñado	1	
	f) quién debe analizar y evaluar estos resultados.	No diseñado	1	
	La organización debe conservar la información documentada correspondiente, como evidencia de los resultados de monitoreo y medición.	No diseñado	1	Es necesario guardar información documentada apropiada como evidencia del monitoreo y los resultados de la medición.
9.2	Auditoría interna			

Cláusula	Requisitos ISO 27001:2013	Estado	Nivel de madurez	Comentario o Sugerencia
	La organización debe llevar a cabo auditorías internas en intervalos planificados para proporcionar información sobre si el sistema de gestión de la seguridad de la información: a) cumple con: 1. los propios requisitos de la organización para su sistema de gestión de la seguridad de la información; y 2. los requisitos de esta norma;	No diseñado	1	Es necesario que la entidad lleve a cabo auditorías internas en periodos planificados para proporcionar información del SGSI.
	b) está debidamente implementada y mantenida. La organización debe:	No diseñado	1	
	c) planificar, establecer, implementar y mantener programa(s) de auditoría, incluida la frecuencia, métodos, responsabilidades, requisitos de planificación e informes. El (los) programa(s) de auditoría debe(n) considerar la importancia de los procesos en cuestión y los resultados de las auditorías anteriores;	No diseñado	1	
	d) definir los criterios de auditoría y el alcance para cada auditoría;	No diseñado	1	
	e) seleccionar auditores y realizar auditorías que aseguren la objetividad y la imparcialidad del proceso de auditoría;	No diseñado	1	
	f) asegurar que los resultados de las auditorías son informados a la dirección pertinente; y	No diseñado	1	

Cláusula	Requisitos ISO 27001:2013	Estado	Nivel de madurez	Comentario o Sugerencia
	g) conservar la información documentada como evidencia de los programas de auditoría y los resultados de la auditoría.	No diseñado	1	
9.3	Revisión por la gerencia			
	La alta dirección debe revisar el sistema de gestión de la seguridad de la información en los plazos planificados para asegurar su conveniencia, suficiencia y efectividad continua. La revisión de la dirección debe considerar: a) el estado de las acciones, a partir de las revisiones de gestión anteriores;	No diseñado	1	Las revisiones por parte de la gerencia deben incluir el estado de las acciones con relación a las revisiones anteriores, cambios externos e internos, retroalimentación sobre el desempeño de la seguridad de la información. Retroalimentación de las partes interesadas, resultados de la evaluación y estado del plan de tratamiento de riesgos y oportunidades de mejora continua.
	b) los cambios en los asuntos externos e internos que son pertinentes al sistema de gestión de la seguridad de la información;	No diseñado	1	
	c) los comentarios sobre el desempeño de la seguridad de la información, incluidas tendencias en: 1. no conformidades y acciones correctivas; 2. resultados del monitoreo y mediciones; 3. resultados de auditoría; y 4. cumplimiento de los objetivos de seguridad de la información;	No diseñado	1	
	d) comentarios de las partes interesadas;	No diseñado	1	

Cláusula	Requisitos ISO 27001:2013	Estado	Nivel de madurez	Comentario o Sugerencia
	e) resultados de la evaluación de riesgo y el estado del plan de tratamiento de riesgo; y	No diseñado	1	
	f) las oportunidades para la mejora continua.	No diseñado	1	
	Los resultados de la revisión de dirección deben incluir las decisiones relacionadas a las oportunidades de mejora y cualquier necesidad de cambios al SGSI.	No diseñado	1	
	La organización debe conservar la información documentada como evidencia de los resultados de las revisiones de gestión.	No diseñado	1	
10	MEJORAS			
10.1	No conformidades y acción correctiva			
	<p>Cuando ocurre una no conformidad, la organización debe:</p> <p>a) reaccionar frente a la no conformidad y si corresponde:</p> <ol style="list-style-type: none"> 1. tomar acciones para controlarlo y corregirlo; y 2. encargarse de las consecuencias; 	No diseñado	1	Se debe implantar el SGSI y elaborar un plan de mejora continua para actualizar el SGSI de acuerdo a los cambios y novedades de la organización, las tecnologías, las amenazas, etc., tratando de mantener los riesgos controlados en todo momento.

Cláusula	Requisitos ISO 27001:2013	Estado	Nivel de madurez	Comentario o Sugerencia
	b) evaluar la necesidad de acción para eliminar las causas de no conformidad, y que así esto no vuelva a ocurrir o que ocurra en otro lugar, al: 1. revisar la no conformidad; 2. determinar las causas de las no conformidades; y 3. determinar si existe una no conformidad similar o podría ocurrir.	No diseñado	1	
	c) implementar cualquier acción necesaria;	No diseñado	1	
	d) revisar la efectividad de cualquier acción correctiva implementada; y	No diseñado	1	
	e) hacer cambios al sistema de gestión de la seguridad de la información, si es necesario.	No diseñado	1	
	Las acciones correctivas deben ser pertinentes a los efectos de las no conformidades halladas.	No diseñado	1	
	La organización debe conservar la información documentada como evidencia de: f) la naturaleza de las no conformidades y las subsecuentes acciones implementadas, y	No diseñado	1	
	g) los resultados de cualquier acción correctiva.	No diseñado	1	
10.2	Mejora continua			
	La organización debe mejorar de manera continua la convivencia, suficiencia y efectividad del SGSI.	No diseñado	1	

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD			PREGUNTA	ESTADO	NIVEL DE MADUREZ	COMENTARIO
5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN						
5.1 Orientación de la dirección de gestión para la seguridad de la información						
Objetivo: Proporcionar orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y las leyes pertinentes						
5.1.1	Políticas de seguridad de la información	<i>Control</i> La dirección debe definir, aprobar, publicar y comunicar a todos los empleados y a las partes externas pertinentes un grupo de políticas para la seguridad de la información	¿Existen políticas publicadas y aprobadas para apoyar la seguridad de la información?	Sin control	0	La MDEA no cuenta con ningún documento de política de seguridad de la información aprobado por la alta dirección.
5.1.2	Revisión de las políticas de seguridad de la información	<i>Control</i> Se deben revisar las políticas de seguridad de la información a intervalos planificados, o si se producen cambios significativos, para asegurar su conveniencia, suficiencia, y eficacia continua.	¿Las políticas de seguridad de la información son revisadas y actualizadas?	Sin control	0	La MDEA no cuenta con ningún documento de política de seguridad de la información aprobado por la alta dirección.
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN						
6.1 Organización interna						
Objetivo: Establecer un marco de trabajo de la dirección para comenzar y controlar la implementación y funcionamiento de la seguridad de la información dentro de la organización.						
6.1.1	Roles y responsabilidades de la seguridad de la información	<i>Control</i> Todas las responsabilidades de la seguridad de la información deben ser definidas y asignadas.	¿Están definidas todas las responsabilidades de seguridad de la información?	Control repetible	2	La MDEA no cuenta con un responsable de la seguridad de la información, por lo tanto no están definidas en ningún documento las responsabilidades para la seguridad de la información.
6.1.2	Segregación de funciones	<i>Control</i> Se deben segregar las funciones y las áreas de responsabilidad para reducir las oportunidades de modificaciones no autorizadas o no intencionales, o el uso indebido de los activos de la organización.	¿Se han segregado las diversas áreas de responsabilidad sobre la seguridad de la información para evitar usos y accesos indebidos?	Control inicial	1	Existen algunos roles definidos; sin embargo, el gerente de TI es quien asume la responsabilidad de la seguridad de la información.
6.1.3	Contacto con autoridades	<i>Control</i> Se deben mantener los contactos apropiados con las autoridades pertinentes.	¿Existe un proceso definido para contactar con las autoridades competentes ante incidentes relacionados con la seguridad de la información?	Control inicial	1	Existe un contacto con el MEF por razones administrativas y financieras; pero no así existe un mecanismo de reporte en temas de seguridad de la información ni mucho menos una sucesión de responsabilidades.

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD			PREGUNTA	ESTADO	NIVEL DE MADUREZ	COMENTARIO
6.1.4	Contacto con grupos especiales de interés	<i>Control</i> Se deben mantener los contactos apropiados con los grupos especiales de interés u otros foros especializados en seguridad, así como asociaciones de profesionales.	¿Existen definidos contactos con grupos de interés especial o asociaciones profesionales?	Sin control	0	En la MDEA no existe una lista de contactos o asociaciones profesionales para llamar en caso de necesitarse.
6.1.5	Seguridad de la información en la gestión del proyecto	<i>Control</i> Se debe abordar la seguridad de la información en la gestión de proyecto, sin importar el tipo de proyecto.	¿Los proyectos consideran aspectos relacionados con la seguridad de la información?	Control inicial	1	Cada uno de los proyectos que se llevan a cabo en la MDEA tiene su propia evaluación de riesgos, sin embargo estas no han sido orientadas a la seguridad de la información,
6.2 Dispositivos móviles y trabajo remoto						
Objetivo: Garantizar la seguridad del trabajo remoto y el uso de dispositivos móviles						
6.2.1	Política de dispositivos móviles	<i>Control</i> Se debe adoptar una política y medidas de apoyo a la seguridad para gestionar los riesgos presentados al usar dispositivos móviles.	¿Existen reglas definidas para el manejo seguro de los dispositivos móviles?	Sin control	0	En la MDEA no existen reglas definidas para el uso de dispositivos móviles en cuanto a la seguridad de la información.
6.2.2	Teletrabajo	<i>Control</i> Una política y medidas de seguridad de apoyo deben ser implementadas para proteger información a la que se accede, se procesa o almacena en sitios de teletrabajo.	¿Se aplican criterios de seguridad para los accesos de teletrabajo?	Sin control	0	En la MDEA no se realiza teletrabajo.
7. SEGURIDAD EN LOS RECURSOS HUMANOS						
7.1 Antes del empleo						
Objetivo: Asegurar que los empleados y contratistas entiendan sus responsabilidades, y que sean aptos para los roles para los cuales están siendo considerados.						
7.1.1	Selección	<i>Control</i> Las verificaciones de los antecedentes de todos los candidatos a ser empleados deben ser llevadas a cabo en concordancia con las leyes, regulaciones y ética relevantes, y debe ser proporcional a los requisitos del negocio, la clasificación de la información a la que se tendrá acceso y los riesgos percibidos.	¿La organización realiza verificaciones de antecedentes de los candidatos para el empleo o para los contratistas?	Control definido	3	El área de RRHH viene realizando las verificaciones de los antecedentes policiales y penales de los candidatos al puesto de trabajo.
7.1.2	Términos y condiciones del empleo	<i>Control</i> Los acuerdos contractuales con los empleados y contratistas deben estipular responsabilidades de éstos y de la organización respecto de la seguridad de la información.	¿Existen acuerdos con los empleados y contratistas donde se especifiquen las responsabilidades de seguridad de la información?	Control inicial	1	En los contratos se firman acuerdos de responsabilidad, sin embargo no existen acuerdos de confidencialidad de la información establecidos.

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD			PREGUNTA	ESTADO	NIVEL DE MADUREZ	COMENTARIO
7.2 Durante el empleo						
Objetivo: Asegurar que los empleados y contratistas sean conscientes y cumplan con sus responsabilidades de seguridad de la información.						
7.2.1	Responsabilidades de la gerencia	<i>Control</i> La gerencia debe requerir a todos los empleados y contratistas aplicar la seguridad de la información en concordancia con las políticas y procedimientos establecidos por la organización.	¿El cumplimiento de las responsabilidades sobre la seguridad de la información es exigida de forma activa a empleados y contratistas?	Sin control	0	No se ha encontrado evidencia de una política de seguridad de la información.
7.2.2	Conciencia, educación y capacitación sobre la seguridad de la información.	<i>Control</i> Todos los empleados de la organización y, cuando fuera relevante, los contratistas deben recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos de la organización, según sea relevante para la función del trabajo que cumplen.	¿Existen procesos de información, formación y concientización sobre las responsabilidades sobre la seguridad de la información?	Control inicial	1	En la MDEA no se brinda formación y/o capacitación a los usuarios en temas de seguridad de la información. Pero si cuando ingresan se les brinda los accesos a la información y se les informa su uso.
7.2.3	Proceso disciplinario	<i>Control</i> Debe haber un proceso disciplinario formal y comunicado para tomar acción contra los empleados que hayan cometido una infracción a la seguridad de la información.	¿Existe un plan disciplinario donde se comunica a los empleados y contratistas las consecuencias de los incumplimientos sobre las políticas de la seguridad de la información?	Sin control	0	Si no se cuenta con una política de seguridad de la información, por ende no existe un plan disciplinario por incumplimiento a la seguridad de la información.
7.3 Terminación y cambio de empleo						
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.						
7.3.1	Terminación o cambio de responsabilidades del empleo	<i>Control</i> Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos luego de la terminación o cambio de empleo deben ser definidos, comunicados al empleado o contratista y forzar el cumplimiento.	¿Existen acuerdos que cubren las responsabilidades de seguridad de la información que siguen siendo válidas después de la terminación del empleo?	Sin control	0	En el contrato no existe algún termino expreso de indicaciones de los aspectos de seguridad de la información o divulgación de información sensible,
8. GESTIÓN DE ACTIVOS						
8.1 Responsabilidad por los activos						
Objetivo: Identificar los activos de la organización y definir responsabilidades de protección apropiadas.						
8.1.1	Inventario de activos	<i>Control</i> Información, otros activos asociados con información e instalaciones de procesamiento de información deben ser identificados y un inventario de estos activos debe ser elaborado y mantenido.	¿Se ha realizado un inventario de activos que den soporte al negocio y de información?	Control inicial	1	La MDEA cuenta con un inventario de activos físicos pero no cuenta con un inventario de activos de información.

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD			PREGUNTA	ESTADO	NIVEL DE MADUREZ	COMENTARIO
8.1.2	Propiedad de los activos	<i>Control</i> Los activos mantenidos en el inventario deben ser propios.	¿Se ha identificado al responsable de cada activo en cuanto a su seguridad?	Sin control	0	No existe un inventario de activos de información.
8.1.3	Uso aceptable de los activos	<i>Control</i> Las reglas para el uso aceptable de la información y activos asociados con la información y con las instalaciones de procesamiento de la información deben ser identificadas, documentadas e implementadas.	¿Se han establecido normas para el uso de activos en relación a su seguridad?	Sin control	0	No se cuenta con documentos de los activos, ni se encuentra definido su uso aceptable con la seguridad de la información.
8.1.4	Retorno de activos	<i>Control</i> Todos los empleados y usuarios de partes externas deben retornar todos los activos de la organización en su posesión a la conclusión de su empleo, contrato o acuerdo.	¿Existe un procedimiento para la devolución de activos cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato?	Control repetible	2	Cuando se termina un contrato y al momento de firmarlo el usuario debe entregar todo los bienes asignados como equipos, información, permisos, etc.
8.2 Clasificación de la información						
Objetivo: Asegurar que la información recibe un nivel apropiado en concordancia con su importancia para la organización.						
8.2.1	Clasificación de la información	<i>Control</i> La información deber ser clasificada en términos de los requisitos legales, valor, criticidad y sensibilidad respecto a una divulgación o modificación no autorizada.	¿Se clasifica la información según su confidencialidad o su importancia en orden a establecer medidas de seguridad específicas?	Control inicial	1	La información no se encuentra clasificada, sin embargo, los empleados saben que la información que manejan es confidencial y crítica.
8.2.2	Etiquetado de la información	<i>Control</i> Un conjunto apropiado de procedimientos para el etiquetado de la información debe ser desarrollado e implementado en concordancia con el esquema de clasificación de la información adoptado por la organización.	¿Existen procedimientos que definan el etiquetado de los activos?	Sin control	0	La MDEA no tiene procedimientos para el etiquetado y manejo de información, ya que tampoco existe una clasificación de los activos de información.
8.2.3	Manejo de activos	<i>Control</i> Los procedimientos para el manejo de activos deber ser desarrollados e implementados en concordancia con el esquema de clasificación de la información adoptado por la organización.	¿Existen procedimientos para el manipulado de la información de acuerdo a su clasificación?	Control inicial	1	No existen procedimientos establecidos para la manipulación de los activos dentro de la MDEA.
8.3 Manejo de los medios						
Objetivo: Prevenir la divulgación, modificación, remoción o destrucción no autorizada de información almacenada en medios.						

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD			PREGUNTA	ESTADO	NIVEL DE MADUREZ	COMENTARIO
8.3.1	Gestión de los medios removibles	<i>Control</i> Se debe implementar procedimientos para la gestión de medios removibles en concordancia con el esquema de clasificación adoptado por la organización.	¿Existen procedimientos que definen cómo manejar los soportes extraíbles (uso, cifrado, borrado, etc.)?	Control repetible	2	Existen algunos cuidados al manejar los medios extraíbles, pero no hay controles establecidos.
8.3.2	Disposición de medios	<i>Control</i> Se debe poner a disposición los medios de manera segura cuando ya no se requieran, utilizando procedimientos formales.	¿Existen procedimientos formales para la eliminación de medios?	Control inicial	1	Cuando un medio se daña o no sirve se da de baja en el sistema de control patrimonial. Sin embargo, no hay un control establecido para su disposición final.
8.3.3	Transferencia de medios físicos	<i>Control</i> Los medios que contienen información deben ser protegidos contra el acceso no autorizado, el mal uso o la corrupción durante el transporte.	¿Son protegidos los medios que contienen información sensible durante el transporte?	Sin control	0	En la MDEA no se han establecido mecanismos de protección de medios físicos.
9. CONTROL DE ACCESO						
9.1 Requisitos de la empresa para el control de acceso						
Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de la información.						
9.1.1	Política de control de acceso	<i>Control</i> Una política de control de acceso deber ser establecida, documentada y revisada en requisitos del negocio y de seguridad de la información.	¿Existe una política para definir los controles de acceso a la información que tengan en cuenta el acceso selectivo a la información según las necesidades de cada actividad o puesto de trabajo?	Sin control	0	No existe una política de control de acceso a la información definida formalmente.
9.1.2	Acceso a redes y servicios de red	<i>Control</i> Los usuarios deben tener acceso solamente a la red y a servicios de red que hayan sido específicamente autorizadas a usar.	¿Se establecen accesos limitados a los recursos y necesidades de red según perfiles determinados?	Control repetible	2	Existe un procedimiento establecido para brindar acceso a usuarios nuevos en los servicios de red. Pero no cuentan con controles sobre permisos especiales.
9.2 Gestión de acceso de usuario						
Objetivo: Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios.						
9.2.1	Registro y baja de usuarios	<i>Control</i> Un proceso formal de registro y baja de usuarios deber ser implementado para permitir la asignación de derechos de acceso.	¿Existen procesos formales de registros y baja de usuarios?	Control repetible	2	No hay una política establecida de altas y bajas de usuarios, el procedimiento se realiza pero no está documentado
9.2.2	Aprovisionamiento de acceso a usuario	<i>Control</i> Un proceso formal de aprovisionamiento de acceso a usuarios debe ser implementado para asignar o revocar los derechos de acceso para todos los tipos de usuarios a todos los sistemas y servicios.	¿Existen procesos formales para asignación de perfiles de acceso?	Control repetible	2	Si existe la creación de grupos de usuarios por área, donde se le asignan roles y privilegios; sin embargo, no se encuentra documentado.

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD			PREGUNTA	ESTADO	NIVEL DE MADUREZ	COMENTARIO
9.2.3	Gestión de derechos de acceso privilegiados.	<i>Control</i> La asignación y uso de derechos de acceso privilegiado debe ser restringida y controlada.	¿Se define un proceso específico para la asignación y autorización de permisos privilegiados de administración de accesos?	Sin control	0	No existe un control sobre los accesos privilegiados en la red. Muchos acceden a redes sociales y YouTube.
9.2.4	Gestión de información de autenticación secreta de usuarios.	<i>Control</i> La asignación de información de autenticación secreta deber ser controlada a través de un proceso de gestión formal.	¿Las contraseñas y otra información de autenticación secreta, son proporcionadas de forma segura?	Control repetible	2	La autenticación no se entrega de manera secreta, ya que es brindada por personal de TI.
9.2.5	Revisión de los derechos de acceso de usuarios	<i>Control</i> Los propietarios de los activos deben revisar los derechos de acceso de usuario a intervalos regulares.	¿Se establecen periodos concretos para renovación de permisos de acceso?	Sin control	0	No existe un procedimiento que indique la revisión de los accesos de los usuarios a la red.
9.2.6	Remoción o ajuste de derechos de acceso	<i>Control</i> Los derechos de acceso a información e instalaciones de procesamientos de información de todos los empleados y de los usuarios de partes	¿Existen un proceso definido para la revocación de permisos cuando se finalice una actividad, puesto de trabajo o cese de contratos?	Control definido	3	Al finalizar el contrato se quita los privilegios y permisos asignados. El área de RRHH informa al área de TI cuando finaliza la relación laboral.
9.3 Responsabilidades de los usuarios						
Objetivo: Hacer que los usuarios respondan por la salvaguarda de su información de autenticación.						
9.3.1	Uso de información confidencial para la autenticación	<i>Control</i> Los usuarios deben ser exigidos a que sigan las prácticas de la organización en el uso de información de autenticación secreta.	¿Existen reglas para los usuarios sobre cómo proteger las contraseñas y otra información de autenticación?	Sin control	0	No existen reglas y no se ha brindado capacitación sobre ello. Ya que muchas veces las intercambian por razones laborales.
9.4 Control de acceso a sistema y aplicación						
Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.						
9.4.1	Restricción del acceso a la información	<i>Control</i> El acceso a la información y a las funciones del sistema de aplicación debe ser restringido en concordancia con la política de control de acceso.	¿El acceso a la información en los sistemas es restringido según la política de control de acceso?	Sin control	0	No hay una política de control de acceso que defina restricciones para las aplicaciones.
9.4.2	Procedimientos seguros de inicio de sesión	<i>Control</i> Donde la política de control de acceso lo requiera, el acceso a los sistemas y a las aplicaciones debe ser controlado por un procedimiento de ingreso seguro.	¿Se han implementado procesos de acceso seguro para el inicio de sesión considerando limitaciones de intentos de acceso, controlando la información en pantalla, etc.?	Control inicial	1	Si bien hay controles de acceso a la red, no así para las aplicaciones.
9.4.3	Sistema de gestión de contraseñas	<i>Control</i> Los sistemas de gestión de contraseñas deber ser interactivos y deben asegurar contraseñas de calidad.	¿Los sistemas de gestión de contraseñas utilizados por los usuarios de la organización les ayuda a manejar de forma segura su información de autenticación?	Sin control	0	No existe una política de contraseñas que establezca fechas de cambio.

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD			PREGUNTA	ESTADO	NIVEL DE MADUREZ	COMENTARIO
9.4.4	Uso de programas utilitarios privilegiados	<i>Control</i> El uso de programas utilitarios que podrían ser capaces de pasar por alto los controles del sistema y de la aplicaciones deber ser restringido y controlarse estrictamente.	¿El uso de herramientas de utilidad es controlado y limitado a empleados específicos?	Sin control	0	No está restringido. Cualquier empleado puede instalar programas no autorizados.
9.4.5	Control de acceso al código fuente de los programas	<i>Control</i> El acceso al código fuente de los programas debe ser restringido.	¿Se restringe el acceso a códigos fuente de programas y se controla cualquier tipo de cambio a realizar?	Control repetible	2	El código fuente de los programas o aplicaciones se encuentra restringido y solo el administrador del mismo tiene acceso a ellos.
10. CRIPTOGRAFÍA						
10.1 Controles criptográficos						
Objetivo: Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.						
10.1.1	Política sobre el uso de controles criptográficos	<i>Control</i> Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	¿Existe una política para regular la encriptación y existen otros controles criptográficos?	Sin control	0	No existe implementado ninguna política para el uso de controles criptográficos.
10.1.2	Gestión de claves	<i>Control</i> Una política sobre el uso, protección y tiempo de vida de las claves criptográficas debe ser desarrollada e implementada a través de todo su ciclo de vida.	¿Existe un control del ciclo de vida de las claves criptográficas?	Sin control	0	No existe implementado ninguna política para el uso de controles criptográficos.
11. SEGURIDAD FÍSICA Y AMBIENTAL						
11.1 Áreas seguras						
Objetivo: Impedir acceso físico no autorizado, daño e interferencia a la información y a las instalaciones de procesamiento de la información de la organización.						
11.1.1	Perímetro de seguridad física	<i>Control</i> Perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de la información.	¿Se establecen perímetros de seguridad física donde sea necesario con barreras de acceso?	Control repetible	2	El ingreso a las instalaciones de la MDEA, se hace por la puerta principal contralada por personal de seguridad, pero no hay un correcto control sobre el ingreso de personas.
11.1.2	Controles de ingreso físico	<i>Control</i> Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo al personal autorizado.	¿Existen controles de acceso a personas autorizadas en áreas restringidas?	Sin control	0	No existe un control físico adecuado en el ingreso de personas a las área de renta y caja.

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD			PREGUNTA	ESTADO	NIVEL DE MADUREZ	COMENTARIO
11.1.3	Seguridad de oficinas, áreas e instalaciones	<i>Control</i> Seguridad física para oficinas, áreas e instalaciones debe ser diseñada e implementada.	¿Se establecen medidas de seguridad para zonas de oficinas para proteger la información de pantallas, etc. en áreas accesibles a personal externo?	Sin control	0	No existe un control físico adecuado en el ingreso de personas a las área de renta y caja.
11.1.4	Protección contra amenazas externas y ambientales	<i>Control</i> Protección física contra desastres naturales, ataque malicioso o accidentes debe ser diseñada y aplicada.	¿Existen instaladas alarmas, sistemas de protección contra incendios y otros sistemas?	Control repetible	2	la MDEA tiene extintores para combatir el fuego. Pero no existe una política que vele por la infraestructura en caso de desastres naturales como sismos y/o terremotos.
11.1.5	Trabajo en áreas seguras	<i>Control</i> Procedimientos para el trabajo en áreas seguras debe ser diseñado y aplicado.	¿Existen definidos procedimientos para las zonas seguras?	Sin control	0	No existe un control físico adecuado en el ingreso de personas a las área de renta y caja.
11.1.6	Áreas de despacho y carga	<i>Control</i> Los puntos de acceso, como las áreas de despacho, carga y otros puntos en donde personas no autorizadas pueden ingresar al local deben ser controlados, y si fuera posible, aislarlos de las instalaciones de procesamiento de la información para evitar el acceso no autorizado.	¿Se controlan las áreas de carga y descarga con procedimientos de control de mercancías entregadas, etc.?	Sin control	0	No existe un control físico adecuado en el ingreso de personas a las área de renta y caja.
11.2 Equipos						
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos e interrupción de las operaciones de la organización.						
11.2.1	Emplazamiento y protección de los equipos	<i>Control</i> Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.	¿Se protegen los equipos tanto del medioambiente como de accesos no autorizados?	Control repetible	2	Los equipos de cómputo están asegurados a los mismos módulos y el CPU cuenta con candado, evitando que sean abiertos.
11.2.2	Servicios de suministro	<i>Control</i> Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro.	¿Se protegen los equipos contra fallos de suministro de energía?	Control inicial	1	Cada equipo cuenta con un UPS, pero muchos de ellos se encuentran dañados.
11.2.3	Seguridad del cableado	<i>Control</i> El cableado de energía y telecomunicaciones que llevan datos o servicios de información de soporte debe ser protegido de la interceptación, interferencia o daño.	¿Existen protecciones para los cableados de energía y de datos?	Sin control	0	No hay lineamientos que velen por la adecuada protección del cableado.

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD			PREGUNTA	ESTADO	NIVEL DE MADUREZ	COMENTARIO
11.2.4	Mantenimiento de equipos	<i>Control</i> Los equipos deben mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.	¿Se planifican y realizan tareas de mantenimiento sobre los equipos?	Sin control	0	No se cuenta con un procedimiento ni un plan de mantenimiento de los equipos de cómputo.
11.2.5	Remoción de activos	<i>Control</i> Los equipos, la información o el software no deben ser retirados de su lugar sin autorización previa.	¿Se controlan y autorizan la salida de equipos, aplicaciones, etc. que puedan tener información?	Control repetible	2	No se permite la salida de ningún bien de la entidad, sin previa autorización del área encargada.
11.2.6	Seguridad de equipos y activos fuera de las instalaciones	<i>Control</i> La seguridad debe ser aplicada a los activos que están fuera de su lugar tomando en cuenta los distintos riesgos de trabajar fuera de las instalaciones de la organización.	¿Se consideran medidas de protección específicas para equipos que se utilicen fuera de las instalaciones de la propia empresa?	Sin control	0	No hay medidas de seguridad para los equipos que se encuentran fuera de las instalaciones de la MDEA.
11.2.7	Disposición o reutilización segura de equipos	<i>Control</i> Todos los elementos del equipo que contengan medios de almacenamiento deben ser verificados para asegurar que cualquier dato sensible y software con licencia se haya eliminado o se haya sobre escrito de manera segura antes de su disposición o reutilización.	¿Se establecen protocolos para proteger o eliminar información de equipos de baja o que van a ser reutilizados?	Sin control	0	No existen protocolos para eliminar información de los equipos de baja o que van a ser reutilizados.
11.2.8	Equipos de usuario desatendidos	<i>Control</i> Los usuarios deben asegurarse de que el equipo desatendido tenga la protección apropiada.	¿Se establecen normas para proteger la información de equipos cuando los usuarios abandonan el puesto de trabajo?	Sin control	0	No existen protocolos para proteger la información de equipos cuando los usuarios dejan su puesto de trabajo.
11.2.9	Política de escritorio limpio y pantalla limpia	<i>Control</i> Una política de escritorio limpio de papeles y de medios de almacenamiento removibles, así como una política de pantalla limpia para las instalaciones de procesamiento de la información debe ser adoptada.	¿Se establecen reglas de comportamiento para abandonos momentáneos o temporales del puesto de trabajo?	Sin control	0	No se tiene una política de escritorio limpio.
12. SEGURIDAD DE LAS OPERACIONES						
12.1 Procedimientos y responsabilidades operativas						
Objetivo: Asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras						
12.1.1	Procedimientos operativos documentados	<i>Control</i>	¿Se documentan los procedimientos y se establecen responsabilidades?	Control inicial	1	No todos los procedimientos del área de rentas se encuentran documentados.

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD			PREGUNTA	ESTADO	NIVEL DE MADUREZ	COMENTARIO
12.1.2	Gestión de cambios	<i>Control</i> Los cambios en la organización, procesos de negocio, instalaciones de procesamiento de la información y sistemas que afectan la seguridad de la información deben ser controlados.	¿Se controla que la información sobre procedimientos se mantenga actualizada?	Sin control	0	No todos los procedimientos del área de rentas se encuentran documentados.
12.1.3	Gestión de la capacidad	<i>Control</i> El uso de recursos debe ser monitoreado, afinado y se debe hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.	¿Los recursos son monitoreados y se realizan planes para asegurar su capacidad para cumplir con la demanda de los usuarios?	Control repetible	2	Se lleva a cabo a través del plan de adquisición de cada área.
12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones	<i>Control</i> Los entornos de desarrollo, pruebas y operaciones deben ser separados para reducir los riesgos de acceso no autorizado o cambios al entorno operativo.	¿Los entornos de desarrollo y pruebas están convenientemente separados de los entornos de producción?	Sin control	0	En la MDEA solo hay una oficina de TI, donde se desarrollan todas las actividades y proyectos de las diferentes temáticas.
12.2 Protección contra códigos maliciosos						
Objetivo: Asegurar que la información y las instalaciones de procesamiento de la información estén protegidas contra códigos maliciosos.						
12.2.1	Controles contra códigos maliciosos	<i>Control</i> Controles de detección, prevención y recuperación para proteger contra códigos maliciosos deben ser implementados, en combinación con una concientización apropiada de los usuarios.	¿Existen sistemas de detección para software malicioso o malware?	Control repetible	2	Se cuenta con sistema antivirus en casi todos los equipos de cómputo.
12.3 Respaldo						
Objetivo: Proteger contra la pérdida de datos						
12.3.1	Respaldo de la información	<i>Control</i> Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	¿Existe un política de backup definida y se lleva a cabo correctamente?	Sin control	0	No se tiene controles adecuados para realizar las copias de respaldo de acuerdo con los requisitos de seguridad de la información.
12.4 Registros y monitoreo						
Objetivo: Registrar eventos y generar evidencia						

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD			PREGUNTA	ESTADO	NIVEL DE MADUREZ	COMENTARIO
12.4.1	Registro de eventos	<i>Control</i> Registros (logs) de eventos de actividades de usuarios, excepciones, fallas y eventos de seguridad de la información deben ser producidos, mantenidos y regularmente revisados.	¿Se realiza un registro de eventos? (intentos de acceso fallidos/exitosos, desconexiones del sistema, alertas de fallos, etc.)	Sin control	0	No se tiene procedimientos para el registro de logs, identificación de cambios, etc.
12.4.2	Protección de información de registros	<i>Control</i> Las instalaciones para registros (logs) y la información de los registros (logs) deben ser protegidas contra la adulteración y el acceso no autorizado.	¿Se ha establecido un sistema de protección para los registros mediante segregación de tareas o copias de seguridad?	Sin control	0	No se cuenta con controles que resguarden los registros provenientes de los sistemas de información.
12.4.3	Registros del administrador y del operador	<i>Control</i> Las actividades del administrador del sistema y del operador del sistema deben ser registradas y los registros (logs) deben ser protegidos y revisados regularmente.	¿Se protege convenientemente y de forma específica los accesos de los administradores?	Sin control	0	No se cuenta con controles que resguarden los registros de los operadores de red.
12.4.4	Sincronización de reloj	<i>Control</i> Los relojes de todos los sistemas de procesamiento de la información relevantes dentro de una organización o dominio de seguridad deben estar sincronizados a una fuente de tiempo de referencia única.	¿Existe un control de sincronización de los distintos sistemas?	Control inicial	1	En la MDEA los relojes se encuentran sincronizados con una misma fuente horaria.
12.5 Control del software operacional						
Objetivo: Asegurar la integridad de los sistemas operacionales						
12.5.1	Instalación de software en sistemas operacionales	<i>Control</i> Procedimientos deben ser implementados para controlar la instalación de software en sistemas operacionales.	¿Las instalaciones de nuevas aplicaciones de software o modificaciones son estrictamente controladas?	Sin control	0	No se controla la instalación de software en los equipos.
12.6 Gestión de vulnerabilidad técnica						
Objetivo: Asegurar la integridad de los sistemas operacionales						
12.6.1	Gestión de vulnerabilidades técnicas	<i>Control</i> Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el riesgo asociado.	¿Se establecen métodos de control para vulnerabilidades técnicas "hacking ético", etc.?	Sin control	0	No se tiene información sobre vulnerabilidades técnicas de los sistemas, ni registro de ataques presentados. Además, tampoco se cuenta con personal capacitado para afrontar las vulnerabilidades que pudieran existir.

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD			PREGUNTA	ESTADO	NIVEL DE MADUREZ	COMENTARIO
12.6.2	Restricciones sobre la instalación de software	<i>Control</i> Reglas que gobiernan la instalación de software por parte de los usuarios deben ser establecidas e implementadas.	¿Se establecen medidas restrictivas para la instalación de software en cuanto a personal autorizado evitando las instalaciones por parte de usuarios finales?	Sin control	0	No hay lineamientos establecidos para la instalación de software por parte de los usuarios en sus equipos asignados.
12.7 Consideraciones para la auditoría de los sistemas de información						
Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operacionales						
12.7.1	Controles de auditoría de los sistemas de información	<i>Control</i> Requisitos de las auditorías y las actividades que involucran la verificación de sistemas operacionales deben ser cuidadosamente planificados y acordados para minimizar la interrupción a los procesos del negocio.	¿Están las auditorías de sistemas de información planeadas y se ejecutan correctamente?	Sin control	0	No se realizan auditorías a los sistemas de información y mucho menos están planificadas.
13. SEGURIDAD DE LAS COMUNICACIONES						
13.1 Gestión de seguridad de la red						
Objetivo: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información de apoyo.						
13.1.1	Controles de la red	<i>Control</i> Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y las aplicaciones.	¿En el entorno de red se gestiona la protección de los sistemas mediante controles de red y de elementos conectados?	Control inicial	1	Mediante un usuario y contraseña se accede a la red de datos. Pero se carece de una buena restricción a aplicaciones o puertos que causan saturación a la red.
13.1.2	Seguridad de servicios de red	<i>Control</i> Mecanismos de seguridad, niveles de servicio y requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en acuerdos de servicios de red, ya sea que estos servicios se provean internamente o sean tercerizados.	¿Se establecen condiciones de seguridad en los servicios de red tanto propios como subcontractados?	Control repetible	2	Los servicios de red solo lo autorizan personal de la subgerencia de TI. Aun así, no hay procedimientos bien definidos que mantengan la seguridad de los servicios de red de las diferentes áreas.
13.1.3	Segregación en redes	<i>Control</i> Grupos de servicios de información, usuarios y sistemas de información deben ser segregados en redes.	¿Existe separación o segregación de redes tomado en cuenta condiciones de seguridad y clasificación de activos?	Sin control	0	No se tiene una segregación de red que garantice la seguridad de la información por áreas.
13.2 Transferencia de información						
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.						

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD			PREGUNTA	ESTADO	NIVEL DE MADUREZ	COMENTARIO
13.2.1	Políticas y procedimientos de transferencia de la información	<i>Control</i> Políticas, procedimientos y controles de transferencia formales deben aplicarse para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.	¿Se establecen políticas y procedimientos para proteger la información en los intercambios?	Sin control	0	No se tiene una política definida para la transferencia o intercambio de información.
13.2.2	Acuerdo sobre transferencia de información	<i>Control</i> Los acuerdos deben dirigir la transferencia segura de información del negocio entre la organización y partes externas.	¿Se delimitan y establecen acuerdos de responsabilidad en intercambios de información con otras entidades?	Sin control	0	No hay acuerdos de transferencia o intercambio de información.
13.2.3	Mensajes electrónicos	<i>Control</i> La información involucrada en mensajería electrónica debe ser protegida apropiadamente.	¿Se establecen normas o criterios de seguridad en mensajería electrónica?	Control inicial	1	El servidor de correo electrónico no se encuentra configurado correctamente, ya que permite el envío de correos masivos y de gran tamaño.
13.2.4	Acuerdos de confidencialidad o no divulgación	<i>Control</i> Requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deben ser identificados, revisados regularmente y documentados.	¿Se establecen acuerdos de confidencialidad antes de realizar intercambios de información con otras entidades?	Sin control	0	No se encuentran definidos claramente.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS						
14.1 Requisitos de seguridad de los sistemas de información						
Objetivo: Garantizar que la seguridad de la información es una parte integral de los sistemas de información a través del ciclo de vida completo. Esto también incluye los requisitos para sistemas de información que proporcionen servicios sobre redes públicas.						
14.1.1	Análisis y especificación de requisitos de seguridad de la información	<i>Control</i> Requisitos relacionados a la seguridad de la información deben ser incluidos en los requisitos para los sistemas de información nuevos o las mejoras para los sistemas de información existentes.	¿Se definen y documentan los requisitos de seguridad de la información para los nuevos sistemas de información?	Sin control	0	No existen políticas definidas para mantener la seguridad de los sistemas de información.
14.1.2	Aseguramiento de servicios de aplicaciones sobre redes públicas	<i>Control</i> La información relacionada a servicios de aplicación que pasan por redes públicas debe ser protegida de la actividad fraudulenta, disputas contractuales, y su divulgación y modificación no autorizada.	¿Se consideran requisitos de seguridad específicos para accesos externos o de redes públicas a los sistemas de información?	Sin control	0	No existen políticas sobre PKI que permitan asegurar los tres pilares (CID) de la seguridad en los sistema de información.

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD			PREGUNTA	ESTADO	NIVEL DE MADUREZ	COMENTARIO
14.1.3	Protección de las transacciones de servicios de aplicación	<i>Control</i> La información implicada en transacciones de servicio de aplicación de debe proteger para evitar la transmisión incompleta, la omisión de envío, la alteración no autorizada del mensaje, la divulgación no autorizada, la duplicación o repetición no autorizada del mensaje.	¿Se establecen medidas de protección para transacciones online?	Control repetible	2	No se cuenta con medidas apropiadas de protección para los pagos online.
14.2 Seguridad en los procesos de desarrollo y soporte						
Objetivo: Garantizar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.						
14.2.1	Política de desarrollo seguro	<i>Control</i> Reglas para el desarrollo de software y sistemas deben ser establecidas y aplicadas a desarrollos dentro de la organización.	¿Se establecen procedimientos que garanticen el desarrollo seguro del software?	Sin control	0	No existen políticas y/o procedimientos para el desarrollo seguro de software.
14.2.2	Procedimientos de control de cambio del sistema	<i>Control</i> Cambios a los sistemas dentro del ciclo de vida del desarrollo deben ser controlados por medio del uso de procedimientos formales de control de cambios.	¿Se gestiona el control de cambios en relación al impacto que puedan tener en los sistemas?	Sin control	0	No existen procedimientos formales de control de cambios en los sistemas.
14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	<i>Control</i> Cuando se cambian las plataformas operativas, las aplicaciones críticas para el negocio deben ser revisadas y probadas para asegurar que no haya impacto adverso en las operaciones o en la seguridad de la organización.	¿Se establecen procedimientos de revisión después de efectuar cambios o actualizaciones?	Control inicial	1	Se realizan pruebas básicas relacionadas al funcionamiento del nuevo sistema o aplicativo.
14.2.4	Restricciones sobre cambios a los paquetes de software	<i>Control</i> Modificaciones a los paquetes de software deben ser disuadidas, limitadas a los cambios necesarios y todos los cambios deben ser estrictamente controlados.	¿Se establecen procesos formales para cambios de versiones o nuevas funcionalidades para software de terceros?	Sin control	0	No existe un proceso formal para la realización de cambio de versiones o funcionalidades nuevas.
14.2.5	Principios de ingeniería de sistemas seguros	<i>Control</i> Principios para la ingeniería de sistemas seguros deben ser establecidos, documentados, mantenidos y aplicados a cualquier esfuerzo de implementación de sistemas de información.	¿Se definen políticas de seguridad de la información en procesos de ingeniería de sistemas?	Sin control	0	No se cuenta con una política de seguridad de la información de desarrollo seguro de software.

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD			PREGUNTA	ESTADO	NIVEL DE MADUREZ	COMENTARIO
14.2.6	Ambientes de desarrollo seguro	<i>Control</i> Las organizaciones deben establecer y proteger apropiadamente los ambientes de desarrollo seguros para los esfuerzos de desarrollo e integración de sistemas que cubren todo el ciclo de vida del desarrollo del sistema.	¿Es seguro el ambiente de desarrollo de software?	Sin control	0	No se tiene un ambiente de desarrollo seguro de software.
14.2.7	Desarrollo contratado externamente.	<i>Control</i> La organización debe supervisar y monitorear la actividad de desarrollo de sistemas contratado externamente.	¿Se acuerdan los requisitos de seguridad de la información para software desarrollado por terceros?	Control inicial	1	A través de los contratos de desarrollo de software, se asigna un personal que supervise el desarrollo del sistema.
14.2.8	Pruebas de seguridad del sistema	<i>Control</i> Pruebas de funcionalidad de la seguridad deben ser llevadas a cabo durante el desarrollo.	¿Se realizan pruebas funcionales de seguridad de los sistemas antes de su fase de producción?	Control inicial	1	A través de los contratos de desarrollo de software, se asigna un personal que supervise el desarrollo del sistema.
14.2.9	Pruebas de aceptación del sistema	<i>Control</i> Programas de pruebas de aceptación y criterios relacionados deben ser establecidos para nuevos sistemas de información, actualizaciones y nuevas versiones.	¿Se establecen protocolos y pruebas de aceptación de sistemas para nuevos sistemas y actualizaciones?	Control inicial	1	Se realizan pruebas de aceptación y cumplimiento de los requerimientos del nuevo sistema.
14.3 Datos de prueba						
Objetivo: Asegurar la protección de datos utilizados para las pruebas						
14.3.1	Protección de datos de prueba	<i>Control</i> Los datos de prueba deben ser seleccionados cuidadosamente, protegidos y controlados.	¿Se utilizan datos de prueba en los ensayos o pruebas de los sistemas?	Control inicial	1	Aunque los datos de prueba son seleccionados por el desarrollador, no existe un procedimiento que garantice la correcta eliminación de la información de los datos de prueba.
15. RELACIONES CON LOS PROVEEDORES						
15.1 Seguridad de la información en las relaciones con los proveedores						
Objetivo: Asegurar protección a los activos de la organización que son accesibles por los proveedores.						
15.1.1	Política de seguridad de la información para las relaciones con los proveedores	<i>Control</i> Requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso por parte del proveedor a los activos de la organización deben ser acordados con el proveedor y documentados.	¿Existe una política de seguridad de la información para proveedores que acceden a activos de la información de la empresa?	Sin control	0	No existe una política de seguridad de la información concerniente a los proveedores.

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD			PREGUNTA	ESTADO	NIVEL DE MADUREZ	COMENTARIO
15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	<i>Control</i> Todos los requisitos relevantes de seguridad de la información deben ser establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proveer componentes de infraestructura de TI para la información de la organización.	¿Se han establecido requisitos de seguridad de la información en contratos con terceros?	Control inicial	1	Se tiene acuerdos con proveedores de servicios, pero no bien definido el tema de seguridad de la información
15.1.3	Cadena de suministro de tecnología de información y comunicación	<i>Control</i> Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.	¿Se fijan requisitos para extender la seguridad de la información a toda la cadena de suministros?	Sin control	0	No se tiene acuerdos con proveedores de servicios bien definidos.
15.2 Gestión de entrega de servicios del proveedor						
Objetivo: Mantener un nivel de seguridad de la información y entrega de servicios acordado en línea con los acuerdos con proveedores.						
15.2.1	Monitoreo y revisión de servicios de los proveedores	<i>Control</i> Las organizaciones deben monitorear, revisar y auditar regularmente la entrega de servicios por parte de los proveedores.	¿Se controla el cumplimiento de los requisitos establecidos con proveedores externos?	Sin control	0	No se tiene procedimientos definidos para el monitoreo, revisión y supervisión de los servicios presados por los proveedores externos.
15.2.2	Gestión de cambios a los servicios de proveedores	<i>Control</i> Los cambios a la provisión de servicios por parte de proveedores, incluyendo el mantenimiento y mejoramiento de políticas, procedimientos y controles existentes de seguridad de la información deben ser gestionados tomando en cuenta la criticidad de la información del negocio, sistemas y procesos involucrados y una reevaluación de riesgos.	¿Se controlan los posibles impactos en la seguridad ante cambios de servicios de proveedores externos?	Sin control	0	No se tiene acuerdos con proveedores de servicios bien definidos, por lo que tampoco se cuenta con un plan de gestión de riesgos.
16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN						
16.1 Gestión de incidentes de seguridad de la información y mejoras						
Objetivo: Asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades.						
16.1.1	Responsabilidades y procedimientos	<i>Control</i> Las responsabilidades de gestión y los procedimientos deben ser establecidos para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.	¿Se definen responsabilidades y procedimientos para responder a los incidentes de la seguridad de la información?	Control inicial	1	Se cuenta con procedimientos para tratar los incidentes que se escalan al área de soporte; sin embargo no se encuentran documentados y no hay un registro de dichos eventos.

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD			PREGUNTA	ESTADO	NIVEL DE MADUREZ	COMENTARIO
16.1.2	Reporte de eventos de seguridad de la información	<i>Control</i> Los eventos de seguridad de la información deben ser reportados a través de canales de gestión apropiados tan rápido como sea posible.	¿Se han implementado canales adecuados para la comunicación de incidentes en la seguridad de la información?	Control repetible	2	Cuando ocurre un incidente, el personal lo reporta a la subgerencia de TI, este al jefe inmediato y luego a la alta dirección. Existe procedimientos pero no se cuenta con una política que lo sustente y se divulgue.
16.1.3	Reporte de debilidades de seguridad de la información	<i>Control</i> Empleados y contratistas que usan los sistemas y servicios de información de la organización deben ser exigidos a advertir y reportar cualquier debilidad observada o de la que se sospecha en cuanto a seguridad de la información en los sistemas o servicios.	¿Se promueven y se hayan establecidos canales para comunicar o identificar puntos débiles en la seguridad de la información?	Sin control	0	Se carece de una guía donde indique los canales para comunicar los puntos débiles de seguridad de la información.
16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	<i>Control</i> Los eventos de seguridad de la información deben ser evaluados y debe decidirse si son clasificados como incidentes de seguridad de la información.	¿Se ha establecido un proceso para gestionar los incidentes en la seguridad de la información?	Sin control	0	No se cuenta con un procedimiento formal para realizar un correcto escalamiento de incidentes de seguridad de la información.
16.1.5	Respuesta a incidentes de seguridad de la información	<i>Control</i> Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.	¿Existen mecanismos para dar una respuesta a los eventos de la seguridad de la información?	Control inicial	1	Se atiende los incidentes de seguridad reportados, pero no hay procedimientos documentados, registro de bitácoras, etc.
16.1.6	Aprendizaje de los incidentes de seguridad de la información	<i>Control</i> El conocimiento adquirido a partir de analizar y resolver los incidentes de seguridad de la información debe ser utilizado para reducir la probabilidad o el impacto de incidentes futuros.	¿La información proporcionada por los eventos en la seguridad de la información son tratados para tomar medidas preventivas?	Sin control	0	No se cuenta con una bitácora de conocimiento.
16.1.7	Recolección de evidencia	<i>Control</i> La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	¿Existe un proceso para recopilar evidencias sobre los incidentes en la seguridad de la información?	Sin control	0	No existe procedimientos para identificar y recopilar evidencias sobre los incidentes en la seguridad de la información.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO						
17.1 Continuidad de seguridad de la información						
Objetivo: La continuidad de seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio de la organización.						

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD			PREGUNTA	ESTADO	NIVEL DE MADUREZ	COMENTARIO
17.1.1	Planificación de continuidad de seguridad de la información	<i>Control</i> La organización debe determinar sus requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre.	¿Se ha elaborado un plan de continuidad del negocio ante incidentes de seguridad de la información?	Sin control	0	No existe un plan de continuidad del negocio.
17.1.2	Implementación de continuidad de seguridad de la información	<i>Control</i> La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de seguridad de la información durante una situación adversa.	¿Se ha implementado las medidas de recuperación previstas en el plan de continuidad del negocio?	Sin control	0	No existe un plan de continuidad del negocio.
17.1.3	Verificación, revisión y evaluación de continuidad de seguridad de la información	<i>Control</i> La organización debe verificar los controles de continuidad de seguridad de la información que han establecido e implementado a intervalos regulares para asegurarse que son válidos y efectivos durante situaciones adversas.	¿Se han verificado o probado las acciones previstas en el plan de continuidad del negocio?	Sin control	0	No existe un plan de continuidad del negocio.
17.2 Redundancias						
Objetivo: Asegurar la disponibilidad de las instalaciones y procedimientos de la información.						
17.2.1	Instalaciones de procesamiento de la información	<i>Control</i> Las instalaciones de procesamiento de la información deben ser implementadas con redundancia suficiente para cumplir con los requisitos de disponibilidad.	¿Se ha evaluado la necesidad de redundar los activos críticos de la información?	Sin control	0	No existe un plan de continuidad del negocio.
18. CUMPLIMIENTO						
18.1 Cumplimiento con requisitos legales y contractuales						
Objetivo: Evitar infracciones de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad.						
18.1.1	Identificación de requisitos contractuales y de legislación aplicables	<i>Control</i> Todos los requisitos legislativos, estatutarios, regulatorios y contractuales relevantes así como el enfoque de la organización para cumplir con estos requisitos deben ser explícitamente identificados, documentados y mantenidos al día para cada sistema de información y para la organización.	¿Son conocidos los requisitos legislativos, regulatorios, contractuales y cualquier otro requisito relativo a seguridad?	Control inicial	1	Se tiene conocimiento de la Ley de Protección de Datos Personales; sin embargo no se cuenta con una adecuación de la misma.

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD			PREGUNTA	ESTADO	NIVEL DE MADUREZ	COMENTARIO
18.1.2	Derechos de propiedad intelectual	<i>Control</i> Procedimientos apropiados deben ser implementados para asegurar el cumplimiento de requisitos legislativos, regulatorios y contractuales relacionados a los derechos de propiedad intelectual y uso de productos de software propietario.	¿Existen procedimientos implementados sobre la propiedad intelectual?	Control repetible	2	Las PCs y servidores cuentan con sistemas operativos licenciados, pero algunos equipos cuentan con software ilegales.
18.1.3	Protección de registros	<i>Control</i> Los registros deben ser protegidos de cualquier pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.	¿Se establecen criterios para clasificación de registros y medidas de protección según niveles?	Control repetible	2	Se realiza a través de los sistemas de información y los backups de registros en la base de datos. Pero no se tiene una política que indique el tiempo de conservación de la información.
18.1.4	Privacidad y protección de datos personales	<i>Control</i> La privacidad y la protección de datos personales deben ser aseguradas tal como se requiere en la legislación y regulación relevantes donde sea aplicable.	¿Se establecen medidas para la protección de datos personales de acuerdo con la legislación vigente?	Sin control	0	No se tiene una política de protección de datos personales.
18.1.5	Regulación de controles criptográficos	<i>Control</i> Controles criptográficos deben ser utilizados en cumplimiento con todos los acuerdos, legislación y regulación relevantes.	¿Si se utiliza el cifrado, se establecen controles criptográficos de acuerdo a la legislación?	Sin control	0	No se ha definido ningún procedimiento para el uso de controles criptográficos.
18.2 Revisiones de seguridad de la información						
Objetivo: Asegurar que la seguridad de la información está implementada y es operada de acuerdo con las políticas y procedimientos organizativos.						
18.2.1	Revisión independiente de la seguridad de la información	<i>Control</i> El enfoque de la organización para manejar la seguridad de la información y su implementación (por ejemplo objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) debe ser revisado independientemente a intervalos planeados o cuando ocurran cambios significativos.	¿Se revisan los controles de la seguridad de la información por personal independiente a los responsables de implementar los controles?	Sin control	0	No se tiene un SGSI.
18.2.2	Cumplimiento de políticas y normas de seguridad	<i>Control</i> Los gerentes deben revisar regularmente el cumplimiento del procesamiento de la información y de los procedimientos dentro de su área de responsabilidad con las políticas, normas y otros requisitos de seguridad apropiados.	¿Se revisa periódicamente el cumplimiento de las políticas y controles de la seguridad de la información?	Sin control	0	No se tiene un SGSI.

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD			PREGUNTA	ESTADO	NIVEL DE MADUREZ	COMENTARIO
18.2.3	Revisión del cumplimiento técnico	<i>Control</i> Los sistemas de información deben ser revisados regularmente respecto al cumplimiento de las políticas y normas de seguridad de la información de la organización.	¿Se realizan evaluaciones sobre el correcto funcionamiento de las medidas técnicas de protección para la seguridad de la información?	Sin control	0	No se tiene un SGSI.

Anexo 4 – Política de Seguridad

POLÍTICA	Código: PS-001
		Versión: 0.1
	Política de Seguridad de la Información	Fecha: 30/10/2019
		Autor: Lisbet Monteza

1. Resumen

La política que se presenta describe los lineamientos de seguridad en los que se debe manejar la entidad, el tratamiento de los activos según su categoría, los roles y responsabilidades y las posibles sanciones por el incumplimiento de las políticas de seguridad de la información.

2. Objetivo

Establecer las normas relacionadas para la gestión de la seguridad de la información que permita proteger adecuadamente los activos de información frente a las amenazas a las cuales se encuentra expuesta la municipalidad, fin de asegurar la confidencialidad, integridad y disponibilidad de la información.

3. Alcance

El cumplimiento de la política de seguridad de la información tiene carácter obligatorio para todo el personal de la municipalidad contratado bajo cualquier modalidad, proveedores de servicio y terceros que estén relacionados con los procesos incluidos en el alcance del Sistema de Gestión de Seguridad de la Información.

4. Base Normativa

- Ley N° 29733 – Ley de Protección de Datos Personales (LPDP), su reglamento y su directiva.
- Resolución N° 129-2014/CNB-INDECOPI aprueba la Norma Técnica Peruana NTP ISO/IEC 27001:2014 – Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos. 2° Edición.
- Resolución Ministerial N°004-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 en todas las instituciones integrantes del Sistema Nacional de Informática.
- Reglamento de Organización y Funciones (ROF) de la Municipalidad Distrital de El Agustino.

5. Términos y definiciones

Activo de información. - En relación con la seguridad de la información, es cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, personas, edificios, etc.) que tenga valor para la organización.

Amenaza. - Causa potencial de un incidente no deseado que puede provocar daños a un sistema o a la organización.

Confidencialidad. - Propiedad que determina que la información no está disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Datos personales sensibles. - Son aquellos que identifican directa o indirectamente a una persona natural (titular de los datos): nombre, fecha de nacimiento, dirección de domicilio y correo electrónico; número de DNI, RUC, teléfono, celular, seguro social y placa de vehículo; imagen; firma manuscrita y electrónica; y otros datos no sensibles establecidos en los formularios aprobados con Resolución Directoral N° 001-2013-JUS/DGPDP.

Disponibilidad. - Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Impacto. - Cambio adverso en el nivel de los objetivos del negocio logrado.

Riesgo. - Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Sistema de información. – Es todo sistema soportado por una infraestructura tecnológica como, por ejemplo, el Sistema de caja, servicio tecnológico de control de acceso a la red de datos, etc.

Seguridad de la información. - Preservación de la confidencialidad, integridad y disponibilidad de la información.

SGSI. - Sistema de Gestión de Seguridad de la Información.

6. Roles y responsabilidades

Los responsables de la seguridad de la información tienen los siguientes roles y responsabilidades:

- **CGSI - Comité de Gestión de Seguridad de la Información**

- Revisar y aprobar las políticas específicas de seguridad de la información.
 - Proveer los recursos necesarios para la seguridad de la información.
 - Asignar los roles específicos y responsabilidades en materia de seguridad dentro de la entidad.
 - Iniciar planes y programas para lograr y mantener la concientización de la seguridad de la información.
 - Velar por el cumplimiento de programas de seguridad, normas y leyes vigentes.
- **GISI – Comité Interdisciplinario de Seguridad de la Información**
 - Asegurar que las actividades de seguridad sean ejecutadas en cumplimiento con la política de seguridad de la información.
 - Aprobar las principales iniciativas para incrementar la seguridad de la información.
 - Permitir que el personal exprese sus inquietudes sobre asuntos de seguridad.
 - Aprobar metodologías y procesos de seguridad de la información.
 - Promover la difusión y apoyo a la seguridad de la información dentro de la municipalidad.
- **OSI – Oficial de Seguridad de la Información**
 - Diseñar y coordinar la implementación de las políticas, normas y procedimientos de seguridad de la información.
 - Identificar los riesgos y amenazas a los que están expuestos los activos de información de la municipalidad.
 - Establecer un cronograma de revisión de vulnerabilidades y coordinar planes de mitigación.
 - Supervisar el cumplimiento de los controles de seguridad de la información.
 - Desarrollar programas de capacitación y concientización sobre seguridad de la información al personal de la municipalidad.
 - Controlar la documentación del SGSI.
 - Organizar la realización de las auditorías internas y externas del SGSI.
 - Supervisar permanentemente las diferentes áreas de la municipalidad referente a la seguridad de la información.
 - Elaborar y actualizar el plan de seguridad de la información.
 - Liderar los proyectos de mejora del SGSI.

- **Propietario, custodio y usuario de los activos de información**

Propietario

- Conocer, identificar y clasificar aquellos activos de información de los cuales son dueños.
- Determinar los criterios y niveles de acceso a los activos de información de su propiedad.
- Asegurar que los activos de información que tienen son manejados y administrados correctamente.
- Reportar al oficial de seguridad de la información sobre cualquier vulnerabilidad detectada que afecte sus activos de información.
- Verificar que los controles de seguridad aplicados sean consistentes con la clasificación realizada.
- En coordinación con el oficial de seguridad de la información, revisar y evaluar los resultados de la implementación de los controles aplicados a los activos de su propiedad.

Custodio

- Dar acceso a los usuarios de acuerdo con las especificaciones establecidas por los propietarios.
- Administrar los accesos a los activos de información.
- Cumplir las políticas, procedimientos y controles implementados para la protección de los activos asignados para su custodia.
- Administrar los procedimientos de backup, recuperación y restauración de información.
- Comunicar al propietario del activo de información las amenazas y vulnerabilidades que encuentre durante el desarrollo de sus actividades.

Usuario

- Cumplimiento de las políticas y directivas de seguridad de la información.
- Mantener la confidencialidad de las contraseñas para el acceso a aplicaciones, sistemas de información y recursos informáticos.
- Utilizar la información de la municipalidad solo para el cumplimiento de sus funciones y/o fines de la entidad.
- Reportar incidentes y debilidades de seguridad de la información.

7. Política de Seguridad de la Información

La Municipalidad Distrital de El Agustino entiende que la información, tanto propia como de sus contribuyentes, es un activo clave e importante para la entidad. Es por ello que se compromete a la búsqueda de la confidencialidad, integridad y disponibilidad de la información según lo indicado en el alcance del Sistema de Gestión de Seguridad de la Información.

De acuerdo a ello, la alta dirección de la municipalidad se compromete en diseñar, implementar, operar y mejorar el SGSI según los principios enunciados en la norma internacional para la seguridad de la información ISO/IEC 27001:2013, por lo que se compromete a:

- Proteger los activos de información frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información.
- Proporcionar los recursos necesarios para asegurar la implementación de las medidas de control necesarias para evitar que los riesgos de la seguridad de la información se materialicen.
- Mejorar el nivel de conciencia de seguridad de la información en los funcionarios, colaboradores y contribuyentes de los servicios de la municipalidad
- Mejorar continuamente la eficacia del Sistema de Gestión de Seguridad de la Información a fin de minimizar constantemente los riesgos de seguridad de la información.
- Cumplir con los requisitos legales y regulatorios que afectan a la municipalidad respecto a la seguridad de la información.

8. Políticas específicas

Las políticas específicas proporcionan principios y guías en aspectos específicos de la seguridad de la información, están alineadas y soportadas por la política general de seguridad de la información. Estas son:

- Política de gestión de accesos
- Política de gestión de contraseñas
- Políticas de escritorio y pantalla limpia

- Política de incidentes de seguridad
- Política de gestión de activos

9. Sanciones

El incumplimiento de las disposiciones establecidas en las políticas de seguridad de la información tendrá como resultado la aplicación de diversas sanciones disciplinarias de acuerdo al reglamento interno de la municipalidad, que serán aplicadas conforme a la naturaleza y gravedad de aspecto no cumplido, antecedentes del trabajador, reincidencia y circunstancias en el que se cometió la falla.

De acuerdo a la gravedad de la falla cometida, se podrá aplicar las siguientes sanciones:

- Amonestación verbal. - Se impondrán a los trabajadores que comentan por primera vez y que sean faltas leves.
- Amonestación por escrito. - Se impondrán a los trabajadores que sean reincidentes en faltas leves o si realizan faltas que se consideren que debe haber una amonestación más que verbal.
- Suspensión de labores. - Se impondrá a los trabajadores que hayan sido amonestados de manera reiterativa tanto verbal como escrita o que cometan faltas que no constituyan causal de despido.
- Despido. - Se retirará al trabajador de su puesto de trabajo anulando su contrato laboral.

Las sanciones no necesariamente se impondrán en forma progresiva. La gravedad de la falta determinará la sanción a imponerse.

10. Revisiones de la Política

La revisión de la política del Sistema de Gestión de Seguridad de la Información deberá realizarse una vez al año con la presencia de los miembros del Comité de Seguridad de la Información y del Oficial de Seguridad de la Información de la Municipalidad Distrital de El Agustino.

11. Revisión del Alcance del SGSI

La revisión del alcance del SGSI, se realizará una vez al año o cuando existan algunos cambios importantes en los procesos pertinentes al alcance actual del Sistema de Gestión de Seguridad de la Información.

12. Información de Contacto

La persona encargada de velar por el funcionamiento correcto del Sistema de Gestión de Seguridad de la Información y de responder por todos los temas relacionados es el Oficial de Seguridad de la Información.

Anexo 5 - Inventario de activos de información

N°	Nombre del activo	Descripción del activo	ID Categoría	Ubicación del activo (Física o lógica)	Proceso del activo	Responsabilidad del activo			Clasificación			Frecuencia de Uso		
						Usuario	Custodio	Propietario	Confidencial	Interna	Pública	Diario	Mensual	Anual
Datos / Documentos														
1	Base de Datos Catastro	Información sobre las características físicas de los predios, así como de los usos y actividades desarrolladas en ellas.	D01	Servidor	Recaudación y fiscalización tributaria	Persona de la subgerencia de catastro	Analista de TI	Gerente de rentas		X		X		
2	Base de Datos Declaración jurada de autoevalúo	Documento que contiene información de los dos formularios HR y PU.	D02	Servidor	Recaudación y fiscalización tributaria	Persona autorizada de la subgerencia de recaudación y fiscalización	Analista de TI	Gerente de rentas		X		X		
3	Declaración jurada de autoevalúo física	Documento que contiene información de los dos formularios HR y PU.	D03	Gabinetes ubicados en el área de rentas	Recaudación y fiscalización tributaria	Persona autorizada de la subgerencia de recaudación y fiscalización	Subgerente de recaudación y fiscalización	Gerente de rentas		X		X		
4	Formulario PU (Predio Urbano)	Información del inmueble para determinar el valor del bien o autoevalúo.	D04	Servidor y gabinetes ubicados en el área de rentas	Recaudación y fiscalización tributaria	Persona autorizada de la subgerencia de recaudación y fiscalización	Subgerente de recaudación y fiscalización	Gerente de rentas		X		X		
5	Formulario HR (Hoja Resumen)	Documento que el contribuyente declara toda la información referente a sí mismo, como de cada uno de los autoevaluó o valorizaciones del predio que son de su propiedad. Resumen de sus bienes.	D05	Servidor y gabinetes ubicados en el área de rentas	Recaudación y fiscalización tributaria	Persona autorizada de la subgerencia de recaudación y fiscalización	Subgerente de recaudación y fiscalización	Gerente de rentas		X		X		
6	Cuponera	Documento de actualización del valor de los predios que anualmente efectúa la municipalidad.	D06	Servidor y gabinetes ubicados en el área de rentas	Recaudación y fiscalización tributaria	Persona autorizada de la subgerencia de recaudación y fiscalización	Subgerente de recaudación y fiscalización	Gerente de rentas		X			X	
7	Emisión de requerimiento de DDJJ	Documento que da inicio al proceso de fiscalización, es emitido al domicilio fiscal del contribuyente indicando el día y la hora de la fiscalización.	D07	Servidor y gabinetes ubicados en el área de rentas	Recaudación y fiscalización tributaria	Persona autorizada de la subgerencia de recaudación y fiscalización	Subgerente de recaudación y fiscalización	Gerente de rentas		X			X	

N°	Nombre del activo	Descripción del activo	ID Categoría	Ubicación del activo (Física o lógica)	Proceso del activo	Responsabilidad del activo			Clasificación			Frecuencia de Uso		
						Usuario	Custodio	Propietario	Confidencial	Interna	Pública	Diario	Mensual	Anual
8	Notificaciones de orden de pago	Emisión de requerimiento	D08	Servidor y gabinetes ubicados en el área de rentas	Emitir notificaciones de pago de tributos	Persona autorizada de la subgerencia de recaudación y fiscalización	Subgerente de recaudación y fiscalización	Gerente de rentas		X		X		
9	Comprobante de pago	Documento que emite el asesor de rentas luego de haberse efectuado el pago.	D09	Caja	Recaudación y fiscalización tributaria	Personal de caja	Jefe de caja	Gerente de rentas		X		X		
10	Acta de inspección predial - Acta de inspección no realizad - Acta de acuerdo de inspección	Actas realizadas en el domicilio fiscal del contribuyente.	D10	Servidor y gabinetes ubicados en el área de rentas	Recaudación y fiscalización tributaria	Persona autorizada de la subgerencia de recaudación y fiscalización	Subgerente de recaudación y fiscalización	Gerente de rentas		X		X		
Software														
11	Sistema de Recaudación Tributaria Municipal	Sistema del MEF, que permite a la municipalidad realizar la determinación y liquidación de los tributos de los contribuyentes.	SW01	Servidor	Recaudación y fiscalización tributaria	Personal autorizado de la subgerencia de recaudación y fiscalización tributaria	Analista de TI	Gerente de rentas	X			X		
12	Módulo de Catastro	Sistema para registrar las fichas catastrales como ficha urbana individual, ficha urbana de bienes comunes, etc.	SW02	Servidor	Recaudación y fiscalización tributaria	Personal autorizado de la subgerencia de catastro	Analista de TI	Gerente de rentas		X		X		
13	Módulo de Caja	Sistema para realizar el pago de tributos e impuesto predial.	SW03	Servidor	Cobranza de las obligaciones tributarias	Personal autorizado de caja	Analista de TI	Jefe de caja	X			X		
14	Módulo de Fiscalización	Sistema que ayuda a la municipalidad a realizar el proceso de fiscalización tributaria del impuesto predial, arbitrios municipales y multas tributarias desde el requerimiento de verificación del predio, registro de la información detectada en campo, emisión de las resoluciones de determinación por impuesto predial y arbitrios municipales, resolución de	SW04	Servidor	Recaudación y fiscalización tributaria	Personal autorizado de la subgerencia de recaudación y fiscalización tributaria	Analista de TI	Gerente de rentas		X		X		

N°	Nombre del activo	Descripción del activo	ID Categoría	Ubicación del activo (Física o lógica)	Proceso del activo	Responsabilidad del activo			Clasificación			Frecuencia de Uso		
						Usuario	Custodio	Propietario	Confidencial	Interna	Pública	Diario	Mensual	Anual
		multa hasta el envío a cobranza coactiva.												
15	Office	Swite ofimática que permite diseñar y producir documentos.	SW05	Computadoras de los usuarios	Todos los procesos	Personal autorizado de la subgerencia de recaudación y fiscalización tributaria	Analista de TI	Subgerente de TI		X		X		
16	Sistema Operativo	Que contiene las aplicaciones utilizadas en la entidad.	SW06	Computadoras de los usuarios	Todos los procesos	Personal autorizado de la subgerencia de recaudación y fiscalización tributaria	Analista de TI	Subgerente de TI		X		X		
17	Antivirus	Programa que sirve para detectar y eliminar virus informáticos.	SW07	Computadoras de los usuarios	Gestión de seguridad de la información	Personal autorizado del área de rentas	Analista de TI	Subgerente de TI		X		X		
Hardware														
18	Computadoras	Equipo informático que permite a los usuarios de la municipalidad la realización de sus funciones.	HW01	Oficina de rentas, plataforma de rentas, caja	Todos los procesos	Personal autorizado del área de rentas	Soporte de TI	Gerente de rentas		X		X		
19	Servidores	Equipo informático que soporta las aplicaciones de la municipalidad.	HW02	Datacenter	Gestión de infraestructura tecnológica	Personal autorizado de la subgerencia de TI	Soporte de TI	Subgerente de TI	X			X		
20	Impresoras	Equipo que permite obtener documentos digitales en físicos.	HW03	Oficina de rentas, plataforma de rentas, caja	Todos los procesos	Personal autorizado del área de rentas	Soporte de TI	Subgerente de TI		X		X		
21	Equipo POS (Point of sale)	Dispositivo para realizar el pago con tarjeta de crédito o débito de los impuestos prediales y arbitrios municipales.	HW04	Caja	Cobranza de las obligaciones tributarias	Personal autorizado de caja	Jefe de caja	Gerente de rentas		X		X		
22	Laptops	Equipo informático que utiliza el gerente del área.	HW05	Oficina de renta	Recaudación y fiscalización tributaria	Gerente de rentas	Gerente de rentas	Gerente de rentas		X		X		
Red de comunicaciones														
23	Red LAN	Red de comunicación cableada, que permite la comunicación entre los diferentes equipos de cómputo.	RC01	Todas las áreas de rentas	Todos los procesos	Personal autorizado del área de rentas	Soporte de TI	Subgerente de TI		X		X		

N°	Nombre del activo	Descripción del activo	ID Categoría	Ubicación del activo (Física o lógica)	Proceso del activo	Responsabilidad del activo			Clasificación			Frecuencia de Uso		
						Usuario	Custodio	Propietario	Confidencial	Interna	Pública	Diario	Mensual	Anual
24	Red WIFI	Red de comunicación inalámbrica que permite la comunicación	RC02	Todas las áreas de rentas	Recaudación y fiscalización tributaria	Personal autorizado del área de rentas	Soporte de TI	Subgerente de TI		X		X		
25	Líneas telefónicas	Red de comunicación telefónica	RC03	Todas las áreas de rentas	Todos los procesos	Personal autorizado del área de rentas	Soporte de TI	Subgerente de TI		X		X		
Servicios														
26	Internet	Servicio que permite la interconexión de la municipalidad con la información.	S01	Todas las áreas de rentas	Todos los procesos	Soporte de TI	Soporte de TI	Subgerente de TI		X		X		
27	Pago en línea - VisaNet	Forma electrónica (a través de internet) de pagar los tributos y arbitrios municipales..	S02	Alojado en la página Web de la municipalidad	Cobranza de las obligaciones tributarias	Analista de TI	Analista de TI	Subgerente de TI	X			X		
28	Correo electrónico institucional	Servicio de correo electrónico para los diversos trabajadores	S03	Servidor	Todos los procesos	Analista de TI	Analista de TI	Subgerente de TI		X		X		
29	Página Web	Medio por donde se brinda información pública de la municipalidad.	S04	Servidor	Todos los procesos	Analista de TI	Analista de TI	Subgerente de TI			X	X		
30	Energía eléctrica	Servicio eléctrico que permite que funcionen los equipos de hardware.	S05	Sub estación de la entidad	Todos los procesos	Servicios generales	Personal especializado de servicios generales	Jefe de servicios generales		X		X		
Personal														
31	Gerente de rentas	Responsable de administrar y operar los servicios administrativos tributarios municipales.	P01	No aplica	Recaudación y fiscalización tributaria	Gerente de rentas	Gerente de rentas	Gerencia de Recursos Humanos	X			X		
32	Subgerente de recaudación y fiscalización tributaria	Responsable de administrar las cobranzas de los diferentes tributos municipales.	P02	No aplica	Recaudación y fiscalización tributaria	Subgerente de recaudación y fiscalización	Gerente de rentas	Gerencia de Recursos Humanos	X			X		
33	Administrativos	Personal que labora en las oficinas de rentas y recaudación y fiscalización tributaria.	P03	Área de rentas	Recaudación y fiscalización tributaria	Personal autorizado de recaudación y fiscalización tributaria	Gerente de rentas	Gerencia de Recursos Humanos	X			X		

N°	Nombre del activo	Descripción del activo	ID Categoría	Ubicación del activo (Física o lógica)	Proceso del activo	Responsabilidad del activo			Clasificación			Frecuencia de Uso		
						Usuario	Custodio	Propietario	Confidencial	Interna	Pública	Diario	Mensual	Anual
34	Asesor de rentas	Persona que se encarga de la recepción de los formularios HR, PU, además de brindar información de los autoavalúos, licencias de funcionamiento, etc.	P04	Módulo de rentas	Recaudación y fiscalización tributaria	Personal autorizado de recaudación y fiscalización tributaria	Gerente de rentas	Gerencia de Recursos Humanos	X			X		
34	Cajero	Personal que se encarga de recepcionar el pagó de los impuestos prediales, arbitrios municipales, etc.	P05	Caja	Cobranza de las obligaciones tributarias	Personal autorizado de caja	Jefe de caja	Gerencia de Recursos Humanos	X			X		
35	Inspector municipal	Personal que se encarga de realizar las inspecciones de los domicilios de los vecinos de la municipalidad	P06	Área de rentas	Fiscalización tributaria	Personal autorizado de recaudación y fiscalización tributaria	Subgerente de recaudación y fiscalización	Gerencia de Recursos Humanos	X			X		
36	Personal de limpieza	Personal que se encarga de la limpieza de la entidad.	P07	No aplica	Todos los procesos	Personal autorizado de limpieza	Jefe de mantenimiento	Gerencia de Recursos Humanos		X		X		
Instalaciones														
37	Oficina de rentas	Lugar donde se realizan las actividades propias al proceso de recaudación y fiscalización tributaria	I01	Instalaciones de la municipalidad	Todos los procesos	Personal autorizado de recaudación y fiscalización tributaria	Subgerente de recaudación y fiscalización	Gerente de rentas		X		X		
38	Caja	Módulos donde se realiza el pago de los impuestos prediales y arbitrios municipales.	I02	Instalaciones de la municipalidad	Cobranza de las obligaciones tributarias	Personal autorizado de caja	Jefe de caja	Gerente de rentas		X		X		
39	Módulos de rentas	Módulo donde se solicita autoevaluaos, licencias de funcionamiento, consultas de predios, etc.	I03	Instalaciones de la municipalidad	Recaudación y fiscalización tributaria	Personal autorizado de recaudación y fiscalización tributaria	Subgerente de recaudación y fiscalización	Gerente de rentas		X		X		
40	Datacenter	Espacio donde se encuentran los recursos para el procesamiento de la información de la municipalidad.	I04	Oficina de TI	Todos los procesos	Personal autorizado de soporte TI	Soporte de TI	Subgerente de TI	X			X		
Soporte de información														
41	Cintas de backup	Cintas donde se almacena los backups de la información.	SI01	Oficina de TI	Gestión de seguridad de la información	Personal autorizado de soporte TI	Soporte de TI	Subgerente de TI	X					X

N°	Nombre del activo	Descripción del activo	ID Categoría	Ubicación del activo (Física o lógica)	Proceso del activo	Responsabilidad del activo			Clasificación			Frecuencia de Uso		
						Usuario	Custodio	Propietario	Confidencial	Interna	Pública	Diario	Mensual	Anual
42	Discos duros de backup	Unidad externa donde se guarda el backup de información.	SI02	Oficina de TI	Gestión de seguridad de la información	Personal autorizado de soporte TI	Soporte de TI	Subgerente de TI	X				X	
Equipo auxiliar														
43	UPS	Sistema de almacenamiento ininterrumpida	EA01	Oficina de rentas, plataforma de rentas, caja	Todos los procesos	Personal autorizado de soporte TI	Soporte de TI	Subgerente de TI		X		X		
44	Aire acondicionado	Sistema de refrigeración del aire que se utiliza para refrescar los ambientes.	EA02	Datacenter	Gestión de seguridad de la información	Personal autorizado de soporte TI	Soporte de TI	Subgerente de TI		X		X		
45	Mobiliario	Estantes, armarios, escritorios, archivadores, etc.	EA03	Oficina de rentas, plataforma de rentas, caja	Todos los procesos	Personal autorizado de recaudación y fiscalización tributaria	Subgerente de recaudación y fiscalización	Gerente de patrimonio		X		X		

Anexo 6 – Valorización de activos

N°	Nombre del activo	ID Categoría	Confidencialidad				Integridad				Disponibilidad				VF	Criticidad
			F	L	I	VFC	F	L	I	VFI	F	L	I	VFD		
1	Base de Datos Catastro	D01	4	5	4	4	5	5	2	4	3	1	3	2	4	Alto
2	Base de Datos Declaración jurada de autoavalúo	D02	4	5	4	4	5	5	2	4	3	1	3	2	4	Alto
3	Declaración jurada de autoavalúo física	D03	4	5	4	4	5	4	2	4	4	2	2	3	4	Alto
4	Formulario PU (Predio Urbano)	D04	4	5	4	4	5	4	2	4	4	2	2	3	4	Alto
5	Formulario HR (Hoja Resumen)	D05	4	5	4	4	5	4	2	4	4	2	2	3	4	Alto
6	Cuponera	D06	3	4	2	3	4	3	1	3	4	2	1	2	3	Medio
7	Emisión de requerimiento de DDJJ	D07	1	2	1	1	1	1	1	1	2	1	1	1	1	Bajo
8	Notificaciones de orden de pago	D08	1	2	1	1	1	1	1	1	2	1	1	1	1	Bajo
9	Comprobante de pago	D09	1	1	1	1	1	2	2	2	2	1	1	1	1	Bajo
10	Acta de inspección predial - Acta de inspección no realizad - Acta de acuerdo de inspección	D10	2	4	2	3	2	3	2	2	1	2	1	1	2	Bajo
11	Sistema de Recaudación Tributaria Municipal	SW01	5	4	5	5	5	5	5	5	4	4	4	4	5	Alto
12	Módulo de Catastro	SW02	5	4	5	5	5	5	3	4	4	4	4	4	4	Alto

N°	Nombre del activo	ID Categoría	Confidencialidad				Integridad				Disponibilidad				VF	Criticidad
			F	L	I	VFC	F	L	I	VFI	F	L	I	VFD		
13	Módulo de Caja	SW03	5	3	5	4	5	5	5	5	5	2	2	3	4	Alto
14	Módulo de Fiscalización	SW04	5	3	5	4	5	5	5	5	5	2	1	3	4	Alto
15	Office	SW05	1	1	1	1	1	1	1	1	1	1	1	1	1	Bajo
16	Sistema Operativo	SW06	1	1	1	1	3	2	2	2	4	5	4	4	2	Medio
17	Antivirus	SW07	0	2	0	1	0	2	0	1	2	2	2	2	1	Bajo
18	Computadoras	HW01	2	3	4	3	4	4	4	4	3	4	4	4	4	Alto
19	Servidores	HW02	4	4	4	4	5	4	4	4	5	4	5	5	4	Alto
20	Impresoras	HW03	1	1	1	1	3	1	1	2	3	1	1	2	1	Bajo
21	Equipo POS (Point of sale)	HW04	1	1	2	1	1	1	1	1	3	1	1	2	1	Bajo
22	Laptops	HW05	2	3	4	3	4	4	4	4	3	4	4	4	4	Alto
23	Red LAN	RC01	3	2	3	3	2	3	2	2	3	2	3	3	3	Medio
24	Red WIFI	RC02	2	2	2	2	2	1	2	2	3	2	3	3	2	Bajo
25	Líneas telefónicas	RC03	2	2	2	2	2	1	2	2	3	2	3	3	2	Bajo
26	Internet	S01	2	2	2	2	3	1	4	3	5	2	4	4	3	Medio
27	Pago en línea - VisaNet	S02	4	3	3	3	4	3	4	4	5	2	4	4	4	Alto
28	Correo electrónico institucional	S03	4	2	4	3	4	3	4	4	3	2	3	3	3	Medio
29	Página Web	S04	4	2	4	3	4	3	4	4	3	2	3	3	3	Medio
30	Energía eléctrica	S05	1	1	1	1	1	1	1	1	4	2	3	3	2	Bajo
31	Gerente de rentas	P01	5	5	4	5	5	5	4	5	3	2	4	3	4	Alto
32	Subgerente de recaudación y fiscalización tributaria	P02	5	5	4	5	5	5	4	5	3	2	4	3	4	Alto
33	Administrativos	P03	5	5	4	5	5	5	4	5	3	2	4	3	4	Alto
34	Asesor de rentas	P04	5	5	4	5	5	5	4	5	4	2	4	3	4	Alto

N°	Nombre del activo	ID Categoría	Confidencialidad				Integridad				Disponibilidad				VF	Criticidad
			F	L	I	VFC	F	L	I	VFI	F	L	I	VFD		
34	Cajero	P05	5	5	4	5	5	5	4	5	4	2	4	3	4	Alto
35	Inspector municipal	P06	5	5	4	5	5	5	4	5	4	2	4	3	4	Alto
36	Personal de limpieza	P07	5	5	4	5	5	5	4	5	4	2	4	3	4	Alto
37	Oficina de rentas	I01	4	1	4	3	5	1	4	3	5	2	4	4	3	Medio
38	Caja	I02	4	1	4	3	5	3	4	4	5	3	4	4	4	Alto
39	Módulos de rentas	I03	4	1	4	3	5	1	4	3	5	2	4	4	3	Medio
40	Datacenter	I04	5	2	4	4	5	2	4	4	5	2	4	4	4	Alto
41	Cintas de backup	SI01	5	4	4	4	5	4	4	4	5	3	4	4	4	Alto
42	Discos duros de backup	SI02	3	1	1	2	4	1	1	2	3	1	1	2	2	Bajo
43	UPS	EA01	3	1	3	2	4	1	3	3	5	1	4	3	3	Medio
44	Aire acondicionado	EA02	3	1	3	2	4	1	3	3	5	1	4	3	3	Medio
45	Mobiliario	EA03	1	1	1	1	1	1	1	1	2	1	2	2	1	Bajo

Anexo 7 – Análisis y Evaluación de Riesgo

Nº	Activo o grupo de activos	Categoría de activo	Amenaza	Vulnerabilidad	Propietario	Probabilidad	Impacto	Riesgo	Nivel de riesgo	Tolerancia	Apetito del riesgo	Id Riesgo
1	Base de Datos	Datos	Acceso lógico no autorizado	Incumplimiento de permisos, privilegios y control de acceso	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R001
		Datos	Alteración accidental de la información	SQL Injection	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R002
		Datos	Divulgación de la información	Personal no tiene claro la función la gestión de seguridad de la información	Subgerente de TI	3	5	15	Alto	No tolerable	Riesgo no aceptable	R003
		Datos	Errores del administrador del equipo o sistema	Procedimiento de operación no se encuentra documentada	Subgerente de TI	4	4	16	Alto	No tolerable	Riesgo no aceptable	R004
		Datos	Modificación deliberada de la información	Falta de políticas de seguridad de la información	Subgerente de TI	4	5	20	Alto	No tolerable	Riesgo no aceptable	R005
		Datos	Suplantación de la identidad del usuario	Credenciales compartidas entre usuarios	Subgerente de TI	3	5	15	Alto	No tolerable	Riesgo no aceptable	R006
		Datos	Manipulación de la información	Falta de una adecuada clasificación de la información sensible	Subgerente de TI	3	5	15	Alto	No tolerable	Riesgo no aceptable	R007
		Datos	Indisponibilidad parcial o permanente	Falta de respaldo de información	Subgerente de TI	3	5	15	Alto	No tolerable	Riesgo no aceptable	R008
		Datos	Abuso de derechos	Falta de políticas de intercambio de información	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R009
		Datos	Procesamiento ilegal de datos	No existe una correcta restricción de accesos	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R010
2	DD JJ física (Autoevalúo) Formulario PU Formulario HR	Documentos	Fuga de información	Falta de políticas de seguridad de la información	Gerente de rentas	3	5	15	Alto	No tolerable	Riesgo no aceptable	R011
		Documentos	Modificación deliberada de la información	Falta de políticas de seguridad de la información	Gerente de rentas	3	4	12	Medio	No tolerable	Riesgo no aceptable	R012
		Documentos	Divulgación de la información	Falta de capacitación y concientización del personal	Gerente de rentas	3	4	12	Medio	No tolerable	Riesgo no aceptable	R013
		Documentos	Robo de documentación	Falta de protección física de las puertas y ventanas del área.	Gerente de rentas	4	4	16	Alto	No tolerable	Riesgo no aceptable	R014
		Documentos	Destrucción del documento por estar almacenado a la intemperie	Suceptibilidad a la humedad, polvo y corrosión	Gerente de rentas	3	4	12	Medio	No tolerable	Riesgo no aceptable	R015
		Documentos	Divulgación de la información	Falta una política de intercambio de información	Gerente de rentas	3	4	12	Medio	No tolerable	Riesgo no aceptable	R016
		Documentos	Divulgación de la información	No hay acuerdos de confidencialidad de la información.	Gerente de rentas	3	5	15	Alto	No tolerable	Riesgo no aceptable	R017

Nº	Activo o grupo de activos	Categoría de activo	Amenaza	Vulnerabilidad	Propietario	Probabilidad	Impacto	Riesgo	Nivel de riesgo	Tolerancia	Apetito del riesgo	Id Riesgo
		Documentos	Manipulación de la información	Falta de procedimientos del área	Gerente de rentas	4	4	16	Alto	No tolerable	Riesgo no aceptable	R018
3	Sistema de Recaudación Tributaria Municipal Sistema de Caja Sistema de Fiscalización Sistema de Catastro	Software	Robo de información	Falta de capacitación y concientización del personal	Gerente de rentas	3	5	15	Alto	No tolerable	Riesgo no aceptable	R019
		Software	Errores de mantenimiento / Actualizaciones de programas (software)	Falta de capacitación técnica	Gerente de rentas	3	5	15	Alto	No tolerable	Riesgo no aceptable	R020
		Software	Errores de configuración	Falta de capacitación técnica	Subgerente de TI	3	5	15	Alto	No tolerable	Riesgo no aceptable	R021
		Software	Suplantación de la identidad del usuario	Credenciales compartidas entre usuarios	Subgerente de TI	4	3	12	Medio	No tolerable	Riesgo no aceptable	R022
		Software	Manipulación de la información	No existe clasificación de la información	Subgerente de TI	3	5	15	Alto	No tolerable	Riesgo no aceptable	R023
		Software	Acceso lógico no autorizado	Incumplimiento de permisos, privilegios y control de acceso	Subgerente de TI	3	5	15	Alto	No tolerable	Riesgo no aceptable	R024
		Software	Manipulación de la información / Acceso lógico no autorizado	Falta de políticas de seguridad de la información	Gerente de rentas	3	5	15	Alto	No tolerable	Riesgo no aceptable	R025
		Software	Mal funcionamiento del software	Saturación del sistema	Gerente de rentas	3	5	15	Alto	No tolerable	Riesgo no aceptable	R026
		Software	Infección de código malicioso (virus, spyware, ransomware, etc.)	Inyección de código / Inyecciones de Comandos de Sistema Operativo	Gerente de rentas	3	5	15	Alto	No tolerable	Riesgo no aceptable	R027
		Software	Procesamiento ilegal de datos	No se cuenta con un registro de acceso a los sistemas	Gerente de rentas	3	5	15	Alto	No tolerable	Riesgo no aceptable	R028
		Software	Vulnerabilidades de los programas	Error de diseño / Problemas de cifrado o encriptado	Gerente de rentas	3	4	12	Medio	No tolerable	Riesgo no aceptable	R029
		Software	Abuso de derechos	Falta de acuerdos de confidencialidad de la información	Gerente de rentas	3	4	12	Medio	No tolerable	Riesgo no aceptable	R030
		Software	Vencimiento de licencia de uso	No se realiza seguimiento a la renovación de las licencias	Gerente de rentas	3	4	12	Medio	No tolerable	Riesgo no aceptable	R031
		Software	Abuso de privilegios de acceso	Incumplimiento de permisos, privilegios y control de acceso	Gerente de rentas	3	5	15	Alto	No tolerable	Riesgo no aceptable	R032
4	Servidor	Hardware	Abuso de privilegios de acceso	Incumplimiento de permisos, privilegios y control de acceso	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R033
		Hardware	Manipulación de la información	Procedimientos de operación no documentados	Subgerente de TI	3	5	15	Alto	No tolerable	Riesgo no aceptable	R034

Nº	Activo o grupo de activos	Categoría de activo	Amenaza	Vulnerabilidad	Propietario	Probabilidad	Impacto	Riesgo	Nivel de riesgo	Tolerancia	Apetito del riesgo	Id Riesgo
		Hardware	Abuso de derechos	Facilidad de acceso al equipo	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R035
		Hardware	Acceso físico no autorizado	Acceso físico no controlado / No se tienen controles para la seguridad física	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R036
		Hardware	Destrucción del equipo debido a que se encuentra en una zona insegura	Inadecuada ubicación del data center	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R037
		Hardware	Inoperatividad del equipo	Inestabilidad de la energía eléctrica.	Subgerente de TI	3	5	15	Alto	No tolerable	Riesgo no aceptable	R038
		Hardware	Pérdida de comunicación	Cableado estructurado desordenado en el gabinete	Subgerente de TI	3	5	15	Alto	No tolerable	Riesgo no aceptable	R039
		Hardware	Falla de funcionamiento de hardware debido al polvo, corrosión, congelamiento, etc.	Antigüedad del equipo / Falta de mantenimientos planificados	Subgerente de TI	4	4	16	Alto	No tolerable	Riesgo no aceptable	R040
		Hardware	Errores del administrador del equipo o sistema	Falta capacitación en seguridad / Procedimientos de operación no documentados / Falta de técnicas de programación de software seguro	Subgerente de TI	4	4	16	Alto	No tolerable	Riesgo no aceptable	R041
		Hardware	Errores de mantenimiento / Actualizaciones de equipos	Temperatura y humedad no controlados	Subgerente de TI	3	5	15	Alto	No tolerable	Riesgo no aceptable	R042
		Hardware	Caída del sistema por agotamiento de recursos (Saturación)	Errores de gestión de recursos	Subgerente de TI	4	5	20	Alto	No tolerable	Riesgo no aceptable	R043
		Hardware	Pérdida de energía eléctrica	Red inestable de energía	Jefe de Logística	3	5	15	Alto	No tolerable	Riesgo no aceptable	R044
5	Computadoras Laptops	Hardware	Robo de equipo	No hay control en la asignación de equipos	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R045
		Hardware	Manipulación incorrecta de los equipos	Falta de políticas de seguridad de la información	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R046
		Hardware	Acceso lógico no autorizado	Falta de políticas de seguridad de la información	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R047
		Hardware	Robo de información	Falta de concientización en seguridad al personal.	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R048
		Hardware	Acceso físico no autorizado / pérdida de equipo	No se tienen mecanismos para la seguridad física de activos	Subgerente de TI	3	5	15	Alto	No tolerable	Riesgo no aceptable	R049
		Hardware	Falla del funcionamiento del hardware	Falta de mantenimiento preventivo / No se	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R050

Nº	Activo o grupo de activos	Categoría de activo	Amenaza	Vulnerabilidad	Propietario	Probabilidad	Impacto	Riesgo	Nivel de riesgo	Tolerancia	Apetito del riesgo	Id Riesgo
				tienen mecanismos para evitar los efectos de la contaminación								
		Hardware	Procesamiento ilegal de datos	Falta de políticas de seguridad de la información	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R051
		Hardware	Infección de código malicioso	Equipos sin antivirus	Subgerente de TI	3	5	15	Alto	No tolerable	Riesgo no aceptable	R052
		Hardware	Pérdida de información	Falta de backup de información de los equipos	Subgerente de TI	3	5	15	Alto	No tolerable	Riesgo no aceptable	R053
		Hardware	Pérdida de energía eléctrica	Red inestable de energía	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R054
6	Red local	Red de comunicaciones	Procesamiento ilegal de datos	Falta de control de accesos a los servicios de red	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R055
		Red de comunicaciones	Acceso físico no autorizado	Acceso físico no controlado	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R056
		Red de comunicaciones	Destrucción de los equipos	No se tienen controles para la seguridad física	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R057
		Red de comunicaciones	Intercepción de señales	Cableado estructurado sin protección	Subgerente de TI	3	5	15	Alto	No tolerable	Riesgo no aceptable	R058
		Red de comunicaciones	Falla del equipo de comunicaciones	Falta de mantenimiento preventivo	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R059
		Red de comunicaciones	Saturación del sistema	Errores de gestión de recursos	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R060
		Red de comunicaciones	Inoperatividad de los equipos	Equipos sin antivirus	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R061
		Red de comunicaciones	Bajo rendimiento	Arquitectura insegura	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R062
		Red de comunicaciones	Pérdida de energía eléctrica	No tener mecanismos alternos para el suministro de energía	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R063
7	Internet	Servicios	Abuso de derechos	Falta de políticas de control y uso de internet	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R064

Nº	Activo o grupo de activos	Categoría de activo	Amenaza	Vulnerabilidad	Propietario	Probabilidad	Impacto	Riesgo	Nivel de riesgo	Tolerancia	Apetito del riesgo	Id Riesgo
		Servicios	Robo o pérdida de información	Falta de políticas de control y uso de internet	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R065
		Servicios	Acceso físico no autorizado	Acceso físico no controlado	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R066
		Servicios	Abuso de derechos	Falta de políticas de control y uso de internet	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R067
		Servicios	Inoperatividad del sistema	No se cuenta con herramientas de monitoreo	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R068
		Servicios	Incumplimiento de los acuerdos de niveles de servicio	No se cuenta con herramientas de monitoreo	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R069
		Servicios	Infección de código malicioso (virus, spyware, ransomware, etc.)	Falta de controles de seguridad	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R070
		Servicios	Inoperatividad del sistema / Pérdida de actividad de labores	Falta de contingencia	Subgerente de TI	3	5	15	Alto	No tolerable	Riesgo no aceptable	R071
8	Página Web Pago en línea	Servicios	Caída de servicios	No se cuenta con herramientas de monitoreo	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R072
		Servicios	Abrir una URL que redirecciona a un lugar malicioso	Incumplimiento de los acuerdos de niveles de servicio	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R073
		Servicios	Pago a webs fraudulentas / Phishing	Incumplimiento de los acuerdos de niveles de servicio	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R074
		Servicios	Caída de los servicios que soporta la página web	Falta de contingencia y un esquema de alta disponibilidad	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R075
9	Correo electrónico institucional	Servicios	Manipulación de la información.	Falta de cierre de inicio de sesión en cada logueo realizado	Subgerente de TI	3	5	15	Alto	No tolerable	Riesgo no aceptable	R076
		Servicios	Acceso lógico no autorizado	Incumplimiento de permisos, privilegios y control de acceso	Subgerente de TI	3	5	15	Alto	No tolerable	Riesgo no aceptable	R077
		Servicios	Espionaje de contraseñas	Mala gestión de contraseñas	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R078
		Servicios	Procesamiento ilegal de datos	Ausencia de políticas para el envío de correos (tamaño, destinatario, adjuntos, etc.)	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R079
		Servicios	Correos entrantes con contenido malicioso y/o spam.	Ausencia de mecanismos de protección contra correo del tipo spam	Subgerente de TI	3	5	15	Alto	No tolerable	Riesgo no aceptable	R080
		Servicios	Robo de información	Ausencia de políticas para el envío de correos (tamaño, destinatario, adjuntos, etc.)	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R081

Nº	Activo o grupo de activos	Categoría de activo	Amenaza	Vulnerabilidad	Propietario	Probabilidad	Impacto	Riesgo	Nivel de riesgo	Tolerancia	Apetito del riesgo	Id Riesgo
10	Gerente de rentas Subgerente de recaudación y fiscalización Asesor de rentas Cajero Inspector municipal Personal de limpieza	Personal	Indisponibilidad del personal por huelgas, absentismo laboral, bajas no justificadas, etc.	No hay formación de personal alterno / Funciones no segregadas	Gerente de RRHH	4	4	16	Alto	No tolerable	Riesgo no aceptable	R082
		Personal	Inatención en los trabajos asignados	Falta de supervisión en los trabajos	Gerente de RRHH	3	4	12	Medio	No tolerable	Riesgo no aceptable	R083
		Personal	Fuga de información	Dispositivos de entrada y salida de datos no controlados	Gerente de RRHH	4	4	16	Alto	No tolerable	Riesgo no aceptable	R084
		Personal	Incumplimiento de las normas establecidas respecto a seguridad de la información	Falta de procedimiento sancionador	Gerente de RRHH	4	4	16	Alto	No tolerable	Riesgo no aceptable	R085
		Personal	Abuso de derechos	Falta de conciencia acerca de la seguridad.	Gerente de RRHH	4	4	16	Alto	No tolerable	Riesgo no aceptable	R086
		Personal	Apropiación indebida de activos	Falta de procedimientos de entrega de equipos	Gerente de RRHH	4	4	16	Alto	No tolerable	Riesgo no aceptable	R087
		Personal	Robo o pérdida de información	Falta de protección física de las puertas del área	Gerente de RRHH	4	4	16	Alto	No tolerable	Riesgo no aceptable	R088
		Personal	Manipulación de la información	Falta de capacitación en seguridad de la información	Gerente de RRHH	4	4	16	Alto	No tolerable	Riesgo no aceptable	R089
		Personal	Procesamiento ilegal de datos / Fuga de información	Falta de políticas para el uso correcto de correo y medios de comunicaciones	Gerente de RRHH	4	4	16	Alto	No tolerable	Riesgo no aceptable	R090
11	Data Center Oficinas Administrativas Caja Módulo de rentas	Instalaciones	Robo de información y equipos	Acceso físico no controlado	Gerente de rentas	3	4	12	Medio	No tolerable	Riesgo no aceptable	R091
		Instalaciones	Acceso físico no autorizado	Falta de protección física de las puertas del área	Gerente de rentas	3	5	15	Alto	No tolerable	Riesgo no aceptable	R092
		Instalaciones	Incendio	No cuentan con extintores ni sistema contra incendios / Tomas eléctricas en mal estado	Gerente de rentas	3	5	15	Alto	No tolerable	Riesgo no aceptable	R093
		Instalaciones	Terremoto (Sismos)	Fallas estructurales de las instalaciones	Gerente de rentas	2	5	10	Medio	No tolerable	Riesgo no aceptable	R094
		Instalaciones	Ataque destructivo (vandalismo, terrorismo, acción militar)	Inseguridad en el contexto social	Gerente de rentas	3	5	15	Alto	No tolerable	Riesgo no aceptable	R095
		Instalaciones	Inundación	Conexiones de agua cerca del área de procesamiento de datos	Gerente de rentas	3	4	12	Medio	No tolerable	Riesgo no aceptable	R096
		Instalaciones	Perdida de energía eléctrica	Tomas eléctricas en mal estado	Gerente de rentas	3	4	12	Medio	No tolerable	Riesgo no aceptable	R097
12	Sistema operativo	Software	Instalación de software no licenciado	No hay lineamientos para el uso de software licenciado	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R098

Nº	Activo o grupo de activos	Categoría de activo	Amenaza	Vulnerabilidad	Propietario	Probabilidad	Impacto	Riesgo	Nivel de riesgo	Tolerancia	Apetito del riesgo	Id Riesgo
		Software	Errores de mantenimiento / Actualizaciones de programas (software)	Falta de capacitación técnica	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R099
		Software	Abuso de privilegios de acceso	Incumplimiento de permisos, privilegios y control de acceso	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R100
		Software	Vulnerabilidades de los programas (Software)	Error de Diseño / Problemas de cifrado o encriptado	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R101
		Software	Abuso de privilegios de acceso	Incumplimiento de permisos, privilegios y control de acceso	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R102
		Software	Vencimiento de licencia de uso (Software)	Falta de seguimiento a la renovación de las licencias	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R103
		Software	Acceso lógico no autorizado	Incumplimiento de permisos, privilegios y control de acceso / No se tiene sistema de bloqueo de ataques	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R104
		Software	Difusión de software dañino (malware)	Inyección de código / Inyecciones de comandos de sistema operativo	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R105
13	UPS Aire acondicionado	Equipo auxiliar	Mal funcionamiento debido al polvo, corrosión, congelamiento / Falla del funcionamiento del equipo	Falta de mantenimiento preventivo / No se tienen mecanismos para evitar los efectos de la contaminación	Subgerente de TI	3	5	15	Alto	No tolerable	Riesgo no aceptable	R106
		Equipo auxiliar	Manipulación de los equipos	Procedimientos de operación no documentados	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R107
		Equipo auxiliar	Falla del funcionamiento del sistema de climatización	No se cuenta con mecanismos para controlar la temperatura y humedad en niveles apropiados	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R108
		Equipo auxiliar	Corte del suministro eléctrico	No tener mecanismos alternos para el suministro eléctrico	Subgerente de TI	3	5	15	Alto	No tolerable	Riesgo no aceptable	R109
14	Cintas de backup	Sistema de Información	Divulgación de información	El personal no tiene claro la función de la gestión de la seguridad de la información	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R110
		Sistema de Información	Avería de los medios de almacenamiento de información (cintas, cd / dvd, hard disk, etc.)	Manejo inadecuado del equipo	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R111
		Sistema de Información	Robo o pérdida de información	No se tienen mecanismos para la seguridad física de activos	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R112

Nº	Activo o grupo de activos	Categoría de activo	Amenaza	Vulnerabilidad	Propietario	Probabilidad	Impacto	Riesgo	Nivel de riesgo	Tolerancia	Apetito del riesgo	Id Riesgo
		Sistema de Información	Manipulación de los equipos	Procedimientos de operación no documentados	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R113
		Sistema de Información	Falta de soportes de información (cintas, discos externos, cd, dvd)	No se tiene contratado un proveedor de medios de soporte	Subgerente de TI	3	4	12	Medio	No tolerable	Riesgo no aceptable	R114

Anexo 8 - Plan de Tratamiento de Riesgo

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
1	Base de Datos	R001	Acceso lógico no autorizado	Reducir	A.9.1.1 Política de control de acceso.	9.1.1 - Una política de control de acceso debería estar establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.	Se elaborará una política de control de accesos. Se emplearan controles de acceso lógico: * Uso de clave alfanumérica generada de 8 dígitos. * Bloqueo de cuenN6:N59ta por intentos fallidos. * Se revisará de manera trimestral el control de acceso a las bases de datos. * Se revisaran los registros log de autenticación y acceso a las bases de datos. * Se realizará la instalación de parches de seguridad según recomendación de fabricante.	1	C	Abr-20	Oct-20	1	4	4	TT	Administrador de accesos
		R002	Alteración accidental de la información	Reducir	A.12.6.1 Gestión de la vulnerabilidades técnicas	12.6.1 - Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debería ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debería ser evaluada y las medidas apropiadas deberían ser tomadas para resolver el riesgo asociado.	Se realizan pruebas de ethical hacking de manera anual. Se realizan cambios en la plataforma según la recomendación del fabricante ante cualquier vulnerabilidad detectada	1	C	Abr-20	Oct-20	1	4	4	TT	Analista TI
		R003	Divulgación de la información	Reducir	A.7.2.2 Conciencia, educación y capacitación sobre seguridad de la información.	7.2.2 - Todos los empleados de la organización y, cuando fuera relevante, los contratistas deberían recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos de la organización, según sea relevante para la función del trabajo que cumplen.	Se realizaran charlas y talleres de concientización al personal en temas de seguridad de la información al ingreso a su puesto de trabajo; además de manera programada durante el año.	1	M	Abr-20	Abr-21	1	5	5	TT	Oficial de seguridad de la información

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
		R004	Errores del administrador del equipo o sistema	Reducir	A.12.1.1 Procedimientos operativos documentados	12.1.1 - Los procedimientos operativos deberían estar documentados y puestos a disposición de todos los usuarios que los necesitan.	Se realizara la revisión y/o actualización de los procedimientos e instructivos operativos del área de rentas, caja, etc.	1	M	Abr-20	Abr-21	1	4	4	TT	Analista TI
		R005	Modificación deliberada de la información	Reducir	A.5.1.1 Políticas para la seguridad de la información. A.18.2.2 Cumplimiento de políticas y normas de seguridad.	5.1.1 - Un conjunto de políticas para la seguridad de la información debería ser definido, aprobado por la gerencia, publicado y comunicado a los empleados y a las partes externas relevantes. 18.2.2 - Los gerentes deberían revisar regularmente el cumplimiento del procesamiento de la información y de los procedimientos, dentro de su área de responsabilidad con las políticas, normas y otros requisitos de seguridad apropiados.	Se elaborará la política de seguridad de la información y será difundida a los empleados por diferentes medios (email, charlas, murales, etc.). El cumplimiento de todas las políticas y normas de seguridad de la información de la entidad, se verificará con los reportes e informes por parte de la estructura organizacional del SGSI.	1	C	Abr-20	Oct-20	1	4	4	TT	Oficial de seguridad de la información
		R006	Suplantación de la identidad del usuario	Reducir	A.7.2.2 Conciencia, educación y capacitación sobre seguridad de la información.	7.2.2 - Todos los empleados de la organización y, cuando fuera relevante, los contratistas deberían recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos	Se realizarán charlas de concienciación en temas de seguridad al ingreso al proyecto, así como de manera programada en el año	1	M	Abr-20	Abr-21	2	3	6	TT	Oficial de seguridad de la información
		R007	Manipulación de la información	Reducir	A.8.2.3 Manejo de activos.	8.2.3 - Los procedimientos para el manejo de activos deberían ser desarrollados e implementados en concordancia con el esquema de clasificación de la información adoptado por la organización.	Se realizará la clasificación de la información de acuerdo a los requisitos definidos por la entidad como, por ejemplo: legales, criticidad, divulgación, etc. De la misma manera, se implementará los procedimientos para el manejo de la base de datos con la información de los contribuyentes.	1	C	Abr-20	Oct-20	1	5	5	TT	Analista TI

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
		R008	Indisponibilidad parcial o permanente	Reducir	A.12.3.1 Respaldo de la información	12.3.1 - Copias de respaldo de la información del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada	Se realizarán y/o revisarán el cronograma de backup de la información del área de rentas.	1	C	Abr-20	Oct-20	1	4	4	TT	Soporte TI
		R009	Abuso de derechos	Reducir	A.13.2.1 Políticas y procedimientos de transferencia de la información. A.13.2.4 Acuerdos de confidencialidad o no divulgación.	13.2.1 - Políticas, procedimientos y controles de transferencia formales deberían aplicarse para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación. 13.2.4 - Requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deberían estar identificados, revisados regularmente y documentados.	Se elaborará la política de intercambio de información, que permitirá la protección de la información por cualquier medio de comunicación. Además se revisarán los acuerdos de confidencialidad y no divulgación de la información, que el personal de la entidad deberá cumplir con todos los lineamientos indicados en la política.	1	C	Abr-20	Oct-20	1	4	4	TT	Oficial de seguridad de la información
		R010	Procesamiento ilegal de datos	Reducir	A.9.4.1 Restricción de acceso a la información.	9.4.1 - El acceso a la información y a las funciones del sistema de aplicación debería ser restringido en concordancia con la política de control de acceso.	Se revisarán los lineamientos de la política de control de acceso a la base de datos, que permita controlar de forma segura el ingreso.	1	C	Abr-20	Oct-20	1	4	4	TT	Analista TI

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
2	DD JJ física (Autoavalúo) Formulario PU Formulario HR	R011	Fuga de información	Reducir	A.5.1.1 Políticas para la seguridad de la información. A.18.2.2 Cumplimiento de políticas y normas de seguridad.	5.1.1 - Un conjunto de políticas para la seguridad de la información debería ser definido, aprobado por la gerencia, publicado y comunicado a los empleados y a las partes externas relevantes. 18.2.2 - Los gerentes deberían revisar regularmente el cumplimiento del procesamiento de la información y de los procedimientos, dentro de su área de responsabilidad con las políticas, normas y otros requisitos de seguridad apropiados.	Se elaborará la política de seguridad de la información y será difundida al personal por diversos medios (email, talleres, plan de capacitación y concientización).	1	C	Abr-20	Nov-20	1	5	5	TT	Oficial de seguridad de la información
		R012	Modificación deliberada de la información	Reducir	A.5.1.1 Políticas para la seguridad de la información.	5.1.1 - Un conjunto de políticas para la seguridad de la información debería ser definido, aprobado por la gerencia, publicado y comunicado a los empleados y a las partes externas relevantes.	Se elaborará la política de seguridad de la información y será difundida al personal por diversos medios (email, talleres, plan de capacitación y concientización).	1	C	Abr-20	Oct-20	1	4	4	TT	Oficial de seguridad de la información
		R013	Divulgación de la información	Reducir	A.7.2.2 Conciencia, educación y capacitación sobre seguridad de la información.	7.2.2 - Todos los empleados de la organización y, cuando fuera relevante, los contratistas deberían recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos	Se realizarán charlas de concientización en temas de seguridad de la información al personal que ingresa a la entidad; además, de manera programada durante el año.	1	M	Abr-20	Abr-21	1	4	4	TT	Oficial de seguridad de la información

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
		R014	Robo de documentación	Reducir	A.11.1.1 Perímetro de seguridad física. A.11.1.2 Controles de ingreso físico. A.11.1.3 Asegurar oficinas, áreas e instalaciones	11.1.1 - Los perímetros de seguridad deberían ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de la información. 11.1.2 - Las áreas seguras deberían estar protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo al personal autorizado. 11.1.3 .- La seguridad física para oficinas, áreas e instalaciones debería ser diseñada e implementada	Se definirán los parámetros de seguridad más seguros para la seguridad en las áreas de rentas y caja. Se debe evitar el ingreso de personas no autorizadas al área.	D	M	Abr-20	Abr-21	1	4	4	TT	Jefe de seguridad Gerente de rentas
		R015	Destrucción del documento por estar almacenado a la intemperie	Reducir	A.11.1.4 - Protección contra amenazas externas y ambientales	11.1.4 - La protección física contra desastres naturales, ataque malicioso o accidentales debería estar diseñada y aplicada.	Se implementara módulos para el adecuado archivamiento de los documentos sensibles, además se realizará la digitalización de los documentos en orden de antigüedad.	D	L	Abr-20	Dic-21	1	4	4	TT	Gerente de rentas
		R016	Divulgación de la información	Reducir	A.13.2.1 Política y procedimientos de transferencia de información. A.13.2.4 Acuerdos de confidencialidad o no divulgación	13.2.1 - Políticas, procedimientos y controles de transferencia formales deberían aplicarse para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación. 13.2.4 - Requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deberían estar identificados, revisados regularmente y documentados.	Se realizará la política y procedimientos para el intercambio de información. Además, se procederá a crear una política contra la divulgación de información no autorizada por medio de cláusulas de confidencialidad.	2	C	Abr-20	Oct-20	1	4	4	TT	Oficial de seguridad de la información

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
		R017	Divulgación de la información	Reducir	A.18.1.3 Protección de registros. A.18.1.4 Privacidad y protección de datos personales.	18.1.3 - Los registros deberían ser protegidos de cualquier pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio. 18.1.4 - La privacidad y protección de los datos personales deberían estar aseguradas tal como se requiere en la legislación y regulación relevantes donde sea aplicable.	Se realizará las políticas de protección de datos personales, teniendo en cuenta la Ley N° 29733 - LPDP.	2	C	Abr-20	Oct-20	1	5	5	TT	Oficial de seguridad de la información
		R018	Manipulación de la información	Reducir	A.12.1.1 Procedimientos operativos documentados.	12.1.1 - Los procedimientos operativos deberían estar documentados y puestos a disposición de todos los usuarios que los necesitan.	Se elaborarán los procedimientos e instructivos operativos del área o procesos.	2	C	Abr-20	Oct-202	1	4	4	TT	Gerente de rentas
3	Sistema de Recaudación Tributaria Municipal Sistema de Caja Sistema de Fiscalización	R019	Robo de información	Reducir	A.5.1.1 Políticas para la seguridad de la información. A.18.2.2 Cumplimiento de políticas y normas de seguridad.	5.1.1 - Un conjunto de políticas para la seguridad de la información debería ser definido, aprobado por la gerencia, publicado y comunicado a los empleados y a las partes externas relevantes. 18.2.2 - Los gerentes deberían revisar regularmente el cumplimiento del procesamiento de la información y de los procedimientos, dentro de su área de responsabilidad con las políticas, normas y otros requisitos de seguridad apropiados.	Se elaborará la política de seguridad de la información y será difundida a los empleados por diferentes medios (email, charlas, murales, etc.). El cumplimiento de todas las políticas y normas de seguridad de la información de la entidad, se verificará con los reportes e informes por parte de la estructura organizacional del SGSI.	1	C	Abr-20	Oct-202	1	5	5	TT	Oficial de seguridad de la información

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
		R020	Errores de mantenimiento / Actualizaciones de programas (software)	Reducir	A.7.2.2 Conciencia, educación y capacitación sobre seguridad de la información.	7.2.2 - Todos los empleados de la organización y, cuando fuera relevante, los contratistas deberían recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos.	Se realizarán charlas de concienciación en temas de seguridad al ingreso al proyecto así como de manera programada en el año.	1	C	Abr-20	Oct-202	1	5	5	TT	Oficial de seguridad de la información
		R021	Errores de configuración	Reducir	A.7.2.2 Conciencia, educación y capacitación sobre seguridad de la información.	7.2.2 - Todos los empleados de la organización y, cuando fuera relevante, los contratistas deberían recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos.	Se elaborará un plan de capacitación técnica anual, según las necesidades del personal (nuevas tecnologías, plan de capacitación y concientización, etc.).	1	C	Abr-20	Oct-202	1	5	5	TT	Oficial de seguridad de la información
		R022	Suplantación de la identidad del usuario	Reducir	A.7.2.2 Conciencia, educación y capacitación sobre seguridad de la información.	7.2.2 - Todos los empleados de la organización y, cuando fuera relevante, los contratistas deberían recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos.	Se realizarán charlas de concientización en temas de seguridad de la información al personal que ingresa a la entidad; además, de manera programada durante el año.	1	C	Abr-20	Oct-202	1	5	5	TT	Oficial de seguridad de la información
		R023	Manipulación de la información	Reducir	A.8.2.3 Manejo de activos	8.2.3 - Los procedimientos para el manejo de activos deberían ser desarrollados e implementados en concordancia con el esquema de clasificación de la información adoptado por la organización.	Se desarrollará e implementará procedimientos para el manejo de los sistemas, de acuerdo al esquema de clasificación de la información adoptado por la municipalidad.	2	M	Abr-20	Abr-21	1	5	5	TT	Analista TI

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
		R024	Acceso lógico no autorizado	Reducir	A.9.1.1 Política de control de acceso. A.9.2.2 Aprovisionamiento de acceso a usuarios. A.9.2.3 Gestión de derechos de accesos privilegiados. A.9.2.4 Gestión de información de autenticación secreta de usuarios.	9.1.1 - Una política de control de acceso debería estar establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información. 9.2.2 - Un proceso formal de aprovisionamiento de acceso a usuarios debería ser implementado para asignar o revocar los derechos de acceso para todos los tipos de usuarios a todos los sistemas y servicios. 9.2.3 - La asignación y uso de derechos de acceso privilegiado debería estar restringida y controlada. 9.2.4 - La asignación de información de autenticación secreta debería revisar los derechos de acceso de usuario a intervalos regulares.	Se elaborará una política de control de accesos. Se mantendrá controlados los accesos de usuarios. Se emplearán controles de acceso lógico: - Uso de clave alfanumérica de 8 dígitos. - Bloqueo de cuenta por intentos fallidos. - Se revisará de manera trimestral el control de acceso a las bases de datos. - Se revisarán los registros log de autenticación y acceso a las bases de datos. - Se realizará la instalación de parches de seguridad según recomendación de fabricante. - Se tendrá un registro del ingreso y salida de los usuarios al sistema.	1	C	Abr-20	Oct-20	1	5	5	TT	Subgerente de TI
		R025	Manipulación de la información / Acceso lógico no autorizado	Reducir	A.9.4.1 Restricción de acceso a la información. A.9.4.2 Procedimientos de ingreso seguro. A.9.4.3 Sistema de gestión de contraseñas.	9.4.1 - El acceso a la información y a las funciones del sistema de aplicación debería ser restringido en concordancia con la política de control de accesos. 9.4.2 - Donde la política de control de acceso lo requiera, el acceso a los sistemas y a las aplicaciones debería ser controlado por un procedimiento de ingreso seguro. 9.4.3 - Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar que las contraseñas sean de calidad.	Se realizarán y/o revisarán los lineamientos de la política de control de acceso a los sistemas y aplicaciones que controle un ingreso seguro al mismo.	1	C	Abr-20	Oct-20	1	5	5	TT	Analista TI

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
		R026	Mal funcionamiento del software	Reducir	A.12.1.3 Gestión de la capacidad. A.12.6.1 Gestión de la vulnerabilidades técnicas	12.1.3 - El uso de recursos debería ser monitoreado, afinado y se debería hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema. 12.6.1 - Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debería ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debería ser evaluada y las medidas apropiadas deberían ser tomadas para resolver el riesgo asociado.	Se revisarán en ciclos programados el consumo de recursos del servidor que contiene los sistemas. Se realizarán pruebas de ethical hacking de manera anual. Se realizarán cambios en la plataforma según recomendación del fabricante ante cualquier vulnerabilidad detectada.	2	M	Abr-20	Abr-21	1	5	5	TT	Subgerente de TI
		R027	Infección de código malicioso (virus, spyware, ransomware, etc.)	Reducir	A.12.2.1 Controles contra software malicioso	12.2.1 - Controles de detección, prevención y recuperación para proteger contra el software malicioso deberían estar implementados, en combinación con una concientización apropiada de los usuarios.	Se elaborará un cronograma de instalación de parches de seguridad y fixes a nivel de base de datos y sistemas. Se elaborará los procedimientos de gestión de cambios.	1	C	Abr-20	Oct-20	1	5	5	TT	Subgerente de TI
		R028	Procesamiento ilegal de datos	Reducir	A.12.4.1 Registro de eventos. A.16.1.2 Reporte de eventos de seguridad de la información. A.16.1.3 Reporte de debilidades de seguridad de la información.	12.4.1 - Registros (logs) de eventos de actividades de usuarios, excepciones, fallas y eventos de seguridad de la información deberían ser producidos, mantenidos y regularmente revisados. 16.1.2 - Los eventos de seguridad de la información deberían ser reportados a través de canales de gestión apropiados tan rápido como sea posible. 16.1.3 - Empleados y contratistas que usan los sistemas y servicios de información de la organización deberían ser exigidos a advertir y	Se elaborará y/o revisará regularmente los registros de las actividades de los usuarios referente a los sistemas. Así mismo se llevará a cabo charlas y capacitaciones acerca del procedimiento para reportar incidentes de seguridad de la información.	1	M	Abr-20	Abr-21	1	5	5	TT	Subgerente de TI Oficial de seguridad de la información

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
						reportar cualquier debilidad observada o de la que se sospecha en cuanto a seguridad de la información en los sistemas o servicios.										
		R029	Vulnerabilidades de los programas (Software)	Reducir	A.12.6.1 Gestión de vulnerabilidades técnicas.	12.6.1 - Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debería ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debería ser evaluada y las medidas apropiadas deberían ser tomadas para resolver el riesgo asociado.	Se realizan pruebas de ethical hacking de manera anual. Se realizan cambios en la plataforma según la recomendación del fabricante ante cualquier vulnerabilidad detectada	2	M	Abr-20	Abr-21	1	5	5	TT	Subgerente de TI
		R030	Abuso de derechos	Reducir	A.13.2.4 Acuerdos de confidencialidad o no divulgación	13.2.4 - Requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deberían estar identificados, revisados regularmente y documentados.	Se creará y/o revisará las políticas contra la divulgación no autorizada y uso adecuado de la información.	1	C	Abr-20	Oct-21	1	4	4	TT	Oficial de seguridad de la información
		R031	Vencimiento de licencia de uso	Reducir	A.18.1.2 Derechos de propiedad intelectual	18.1.2 - Procedimientos apropiados deberían ser implementados para asegurar el cumplimiento de requisitos legislativos, regulatorios y contractuales, relacionados a los derechos de propiedad intelectual y uso de productos de software propietario.	Se realizará la renovación anual del mantenimiento de licencias.	D	L	Abr-20	Dic-21	1	4	4	TT	Subgerente de TI

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
		R032	Abuso de privilegios de acceso	Reducir	A.9.1.1 Política de control de acceso.	9.1.1 - Una política de control de acceso debería estar establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.	Se elaborará una Política de control de accesos. Se mantendrá controlados los accesos de usuarios. Se emplearán controles de acceso lógico: - Uso de clave alfanumérica de 8 dígitos. - Bloqueo de cuenta por intentos fallidos. - Se revisará de manera trimestral el control de acceso a las bases de datos. - Se revisarán los registros log de autenticación y acceso a las bases de datos. - Se realizará la instalación de parches de seguridad según recomendación de fabricante.	1	C	Abr-20	Oct-20	1	5	5	NT	Analista TI Subgerente de TI
4	Servidor	R033	Abuso de privilegios de acceso	Reducir	A.9.1.1 Política de control de acceso.	9.1.1 - Una política de control de acceso debería estar establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.	Se elaborará una Política de control de accesos. Se mantendrá controlados los accesos de usuarios. Se emplearán controles de acceso lógico: - Uso de clave alfanumérica de 8 dígitos. - Bloqueo de cuenta por intentos fallidos. - Se revisará de manera trimestral el control de acceso a las bases de datos. - Se revisarán los registros log de autenticación y acceso a las bases de datos. - Se realizará la instalación de parches de seguridad según recomendación de fabricante.	1	C	Abr-20	Oct-20	1	4	4	TT	Oficial de seguridad de la información

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
		R034	Manipulación de la información	Reducir	A.9.2.1 Registro y baja de usuarios. A.9.2.2 Aprovisionamiento de acceso a usuarios. A.9.2.3 Gestión de derechos de acceso privilegiados. A.9.2.5 Revisión de los derechos de acceso de usuarios	9.2.1 - Un proceso formal de registro y baja de usuarios debería estar implementado para permitir la asignación de derechos de acceso. 9.2.2 - Un proceso formal de aprovisionamiento de acceso de usuarios debería ser implementado para asignar o revocar los derechos de acceso para todos los tipos de usuarios a todos los sistemas y servicios. 9.2.3 - La asignación y uso de derechos de acceso privilegiado debería ser restringida y controlada. 9.2.5 - Los propietarios de los activos deberían revisar los derechos de acceso de usuario a intervalos regulares.	Se realizará y/o revisará los lineamientos de la política de control de acceso, con el fin de mantener controlados los accesos de los usuarios. Se implementará un proceso formal de registro y cancelación de usuarios. Además, se capacitará a los usuarios sobre la utilización de la información en los equipos informáticos.	2	C	Abr-20	Oct-20	1	5	5	TT	Oficial de seguridad de la información
		R035	Abuso de derechos	Reducir	A.9.4.1 Restricción de acceso a la información	9.4.1 - El acceso a la información y a las funciones del sistema de aplicación debería ser restringido en concordancia con la política de control de acceso.	El acceso a la información y a las configuraciones de los equipos estarán dadas en la política de control de acceso.	1	C	Abr-20	Oct-20	1	4	4	TT	Oficial de seguridad de la información
		R036	Acceso físico no autorizado	Reducir	A.11.1.2 Controles de ingreso físico	11.1.2 - Las áreas seguras deberían estar protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo al personal autorizado.	Se llevará un control de ingreso a las instalaciones del datacenter. Los que solicitaron la vista acompañaran a las visitantes durante su permanencia en las instalaciones. El ingreso será con anticipación al data center mínimo de 2 días. El personal de seguridad verificara	D	M	Abr-20	Dic-21	1	4	4	TT	Subgerente de TI

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
							los objetos de entrada y salida de las personas.									
		R037	Dstrucción del equipo debido a que se encuentra en una zona insegura	Reducir	A.11.2.1 Ubicación y protección de los equipos	11.2.1 - Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.	Se verificará la ubicación actual del servidor que se encuentra expuesto al deterioro del medio ambiente e ingreso de personal no autorizado. Se realizará el proyecto de diseño de un nuevo data center.	D	L	Abr-20	Dic-21	1	4	4	TT	Subgerente de TI
		R038	Inoperatividad del equipo	Reducir	A.11.2.2 Servicios de suministro	11.2.2 - Los equipos deberían estar protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro.	Se realizará el mantenimiento de las conexiones eléctricas y se recomendará la adquisición de un nuevo UPS.	D	M	Abr-20	Abr-21	1	5	5	TT	Subgerente de TI
		R039	Pérdida de comunicación	Reducir	A.11.2.3 Seguridad del cableado	11.2.3 - El cableado de energía y telecomunicaciones que llevan datos o servicios de información de soporte debería ser protegido de la interceptación, interferencia o daño.	Se realizará el mantenimiento del cableado estructurado. Así mismo se realizará el ordenamiento y gestión del cableado.	D	M	Abr-20	Abr-21	1	5	5	TT	Subgerente de TI
		R040	Falla de funcionamiento de hardware debido al polvo, corrosión, congelamiento, etc.	Reducir	A.11.2.4 Mantenimiento de equipos	11.2.4 - Los equipos deberían mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.	Programar y ejecutar los mantenimientos preventivos anuales.	1	M	Abr-20	Abr-21	1	4	4	TT	Subgerente de TI

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
		R041	Errores del administrador del equipo o sistema	Reducir	A.12.1.1 Procedimientos operativos documentados. A 12.6.1 Gestión de vulnerabilidades técnicas.	12.1.1 - Los procedimientos operativos deberían estar documentados y puestos a disposición de todos los usuarios que los necesitan. 12.6.1 - Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debería ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debería ser evaluada y las medidas apropiadas deberían ser tomadas para resolver el riesgo asociado.	Revisión y/o actualización de los procedimientos e instructivos operativos del área o proceso. Capacitación / actualización técnica para el personal que administra los equipos.	2	M	Abr-20	Abr-21	1	4	4	TT	Subgerente de TI
		R042	Errores de mantenimiento / Actualizaciones de equipos	Reducir	A.12.1.3 Gestión de la capacidad	12.1.3 - El uso de recursos debería ser monitoreado, afinado y se debería hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.	Revisar los controles de medición de humedad y temperatura en el datacenter. Los administradores monitorean el servicio mediante la herramienta de monitoreo Foglight, el cual permite monitorear la disponibilidad de la plataforma.	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI
		R043	Caída del sistema por agotamiento de recursos (Saturación)	Reducir	A.12.1.3 Gestión de la capacidad	12.1.3 - El uso de recursos debería ser monitoreado, afinado y se debería hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.	Se monitoreará la plataforma tecnológica con la herramienta Foglight. Los administradores tendrán un monitor especial solamente para realizar el monitoreo.	1	C	Abr-20	Oct-20	1	5	5	TT	Subgerente de TI
		R044	Pérdida de energía eléctrica	Reducir	A.17.1.1 Planificación de continuidad de seguridad de la información.	17.1.1 - La organización debería determinar sus requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre.	Se realizarán mantenimientos preventivos a los equipos de apoyo. Se realizarán mantenimientos anuales al grupo electrógeno.	1	C	Abr-20	Oct-20	1	5	5	TT	Subgerente de TI

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
5	Computadoras Laptops	R045	Robo de equipo	Reducir	A.8.1.1 Inventario de activos. A.8.1.2 Propiedad de los activos.	8.1.1 - El control de la información, otros activos asociados con la información y las instalaciones de procesamiento de información deberían ser identificadas y un inventario de estos activos debería ser elaborado y mantenido. 8.1.2 - Los activos mantenidos en el inventario deberían tener un propietario.	Se realizará y/o revisará el inventario de los equipos de cómputo con los que cuenta la entidad. Además, también se verificará en el sistema de patrimonio la asignación de los mismos.	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI
		R046	Manipulación incorrecta de los equipos	Reducir	A.8.1.3 Uso aceptable de los activos. A.8.1.4 Retorno de los activos.	8.1.3 - Las reglas para el uso aceptable de la información y los activos asociados con la información y con las instalaciones de procesamiento de la información deberían estar identificadas, documentadas e implementadas. 8.1.4 - Todos los empleados y usuarios de terceras partes deberían retornar todos los activos de la organización en su posesión a la conclusión de su empleo, contrato o acuerdo.	Se programará charlas y capacitaciones sobre seguridad de la información y el uso correcto de los activos de la entidad. Se verificarán los procedimientos de asignación y retorno de equipos del área de patrimonio.	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI
		R047	Acceso lógico no autorizado	Reducir	A.9.1.1 Política de control de acceso.	9.1.1 - Una política de control de acceso debería estar establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.	Se elaborará una Política de control de accesos. Se mantendrá controlados los accesos de usuarios. Se emplearán controles de acceso lógico: - Uso de clave alfanumérica de 8 dígitos. - Bloqueo de cuenta por intentos fallidos. - Se revisará de manera trimestral el control de acceso a las bases de datos.	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
							- Se revisarán los registros log de autenticación y acceso a las bases de datos. Se realizará la instalación de parches de seguridad según recomendación de fabricante.									
		R048	Robo de información	Reducir	A.9.4.3 Sistema de gestión de contraseñas.	9.4.3 - Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.	Se implementará la política de gestión de contraseña, para que los empleados utilicen en los equipos cómputo contraseñas robustas y seguras.	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI
		R049	Acceso físico no autorizado / pérdida de equipo	Reducir	A.11.1.2 Controles de ingreso físico	11.1.2 - Las áreas seguras deberían estar protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo al personal autorizado.	El acceso a las oficinas será previa coordinación y autorización por del jefe responsable del área. Las laptops tendrá su cadena de seguridad. Se colocará cámaras de seguridad y personal de seguridad física de la sede.	2	M	Abr-20	Abr-21	1	5	5	TT	Subgerente de TI
		R050	Falla del funcionamiento del hardware	Reducir	A.11.2.4 Mantenimiento de equipos	11.2.4 - Los equipos deberían mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.	Programar y ejecutar los mantenimientos preventivos anuales.	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI
		R051	Procesamiento ilegal de datos	Reducir	A.11.2.8 Equipos de usuarios desatendidos. A.11.2.9 Política de escritorio limpio y pantalla limpia.	11.2.8 - Los usuarios deberían asegurarse de que el equipo desatendido tenga la protección apropiada. 11.2.9 - Una política de escritorio limpio de papeles y de medios de almacenamiento removibles, así como una política de pantalla limpia para las instalaciones de procesamiento de la información debería ser adoptada.	Se creará la política de escritorio y pantalla limpia.	2	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
		R052	Infección de código malicioso	Reducir	A.12.2.1 Controles contra software malicioso.	12.2.1 - Controles de detección, prevención y recuperación para proteger contra el software malicioso deberían estar implementados, en combinación con una concientización apropiada de los usuarios.	Se verificará que cada equipo de cómputo cuente como mínimo con un antivirus estándar.	1	C	Abr-20	Oct-20	1	3	3	TT	Subgerente de TI
		R053	Pérdida de información	Reducir	A.12.3.1 Respaldo de la información.	12.3.1 - Copias de respaldo de la información del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	Se elaborará una planificación de copias de respaldo, con el fin de producir registros exactos y completos de la información.	1	C	Abr-20	Oct-20	1	5	5	TT	Subgerente de TI
		R054	Pérdida de energía eléctrica	Reducir	A.17.1.1 Planificación de continuidad de seguridad de la información.	17.1.1 - La organización debería determinar sus requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre.	Se realizarán mantenimientos anuales al grupo electrógeno.	D	M	Abr-20	Abr-21	1	4	4	TT	Subgerente de TI
6	Red local	R055	Procesamiento ilegal de datos	Reducir	A.9.1.2 Acceso a redes y servicios de red.	9.1.2 - Los usuarios deberían tener acceso solamente a la red y a servicios de red que hayan sido específicamente autorizados a usar.	La entidad dentro de su política de control de acceso debe especificar claramente el acceso de los usuarios a los servicios que integran la red de comunicaciones.	1	C	Abr-20	Oct-20	1	4	4	TT	Oficial de seguridad de la información
		R056	Acceso físico no autorizado	Reducir	A.11.1.1 Perímetro de seguridad física. A.11.1.2 Controles de ingreso físico.	11.1.1 - Los perímetros de seguridad deberían ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de la información. 11.1.2 - Las áreas seguras deberían estar protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo al personal autorizado.	El área de acceso a los equipos de red deben estar protegidos con controles de acceso apropiados para asegurar sólo el ingreso al personal autorizado.	1	C	Abr-20	Oct-20	1	4	4	TT	Oficial de seguridad de la información

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
		R057	Dstrucción de los equipos	Reducir	A.11.2.1 Ubicación y protección de los equipos.	11.2.1 - Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.	Se verificará que los equipos de comunicaciones estén ubicados y protegidos de los peligros del entorno.	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI
		R058	Intercepción de señales	Reducir	A.11.2.3 Seguridad del cableado	11.2.3 - El cableado de energía y telecomunicaciones que llevan datos o servicios de información de soporte debería ser protegido de la intercepción, interferencia o daño.	Se realizará el mantenimiento del cableado estructurado. Así mismo se realizará el ordenamiento y gestión del cableado .	2	M	Abr-20	Abr-21	1	4	4	TT	Subgerente de TI
		R059	Falla del equipo de comunicaciones	Reducir	A.11.2.4 Mantenimiento de equipos	11.2.4 - Los equipos deberían mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.	Se programará y ejecutará los mantenimientos preventivos.	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI
		R060	Saturación del sistema	Reducir	A.12.1.3 Gestión de la capacidad	12.1.3 - El uso de recursos debería ser monitoreado, afinado y se debería hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.	Se monitoreará la plataforma tecnológica mediante el uso de herramientas	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI
		R061	Inoperatividad de los equipos	Reducir	A.12.2.1 Controles contra software malicioso	12.2.1 - Controles de detección, prevención y recuperación para proteger contra el software malicioso deberían estar implementados, en combinación con una concientización apropiada de los usuarios.	Se verificará que los equipos de comunicaciones cuenten como mínimo con antivirus para la protección de código malicioso.	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI
		R062	Bajo rendimiento	Reducir	A.13.1.1 Controles de la red.	13.1.1 - Las redes deberían ser gestionadas y controladas para proteger la información en los sistemas y las aplicaciones.	Se implementará y/o revisará los controles para asegurar la correcta configuración de la red; además, de documentar la configuración y sus cambios.	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
		R063	Pérdida de energía eléctrica	Reducir	A.17.1.1 Planificación de la continuidad de la seguridad de la información. A.17.1.2 Implementación de continuidad de seguridad de la información.	17.1.1 - La organización debería determinar sus requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre. 17.1.2 - La organización debería establecer, documentar, implementar y mantener los procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de seguridad de la información durante una situación adversa.	La alta dirección junto con los integrantes de la estructura organizacional del SGSI deberán crear planes de continuidad de negocio o DRP (plan de recuperación ante desastres), estrategia útil para restablecer los servicios de TI (Hardware y Software) ante cualquier eventualidad.	D	L	Abr-20	Dic-21	1	4	4	TT	Subgerente de TI Oficial de seguridad de la información
7	Internet	R064	Abuso de derechos	Reducir	A.9.1.1 Política de control de acceso	9.1.1 - Una política de control de acceso debería estar establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.	En la política de control de accesos, se colocarán cláusulas con procedimientos referente al uso de Internet para los trabajadores de la municipalidad. Por su parte, la entidad debe supervisar continuamente que se ejecute los lineamientos indicados dentro de la política. .	1	C	Abr-20	Oct-20	1	4	4	TT	Oficial de seguridad de la información
		R065	Robo o pérdida de información	Reducir	A.9.1.2 Acceso a redes y servicios de red	9.1.2 - Los usuarios deberían tener acceso solamente a la red y a servicios de red que hayan sido específicamente autorizados a usar.	La entidad dentro de su política de control de acceso debe especificar claramente el acceso de los usuarios a los servicios que integran la red de comunicaciones.	1	C	Abr-20	Oct-20	1	4	4	TT	Oficial de seguridad de la información
		R066	Acceso físico no autorizado	Reducir	A.11.1.2 Controles de ingreso físico	11.1.2 - Las áreas seguras deberían estar protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo al personal autorizado.	Se llevará un control de ingreso a las instalaciones del datacenter.	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
		R067	Abuso de derechos	Reducir	A.12.1.1 Procedimientos operativos documentados	12.1.1 - Los procedimientos operativos deberían estar documentados y puestos a disposición de todos los usuarios que los necesiten.	Se realizará y/o revisará los procedimientos de operación para ponerlos a disposición de todos los empleados de la municipalidad. Además, el acceso a Internet se brindará solo con propósitos autorizados.	1	C	Abr-20	Oct-20	1	4	4	TT	Oficial de seguridad de la información
		R068	Inoperatividad del sistema	Reducir	A.12.1.3 Gestión de la capacidad	12.1.3 - El uso de recursos debería ser monitoreado, afinado y se debería hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.	Se mantendrá una revisión en ciclos programados del consumo de recursos del router que brinda el servicio de Internet.	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI
		R069	Incumplimiento de los acuerdos de niveles de servicio	Reducir	A.12.1.3 Gestión de la capacidad	12.1.3 - El uso de recursos debería ser monitoreado, afinado y se debería hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.	Se monitoreará la plataforma tecnológica mediante el uso de la herramienta Foglight, los administradores tendrán 2 monitores uno para sus labores operativas y otra de monitoreo.	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI
		R070	Infección de código malicioso (virus, spyware, ransomware, etc.)	Reducir	A.12.2.1 Controles contra software malicioso	12.2.1 - Controles de detección, prevención y recuperación para proteger contra el software malicioso deberían estar implementados, en combinación con una concientización apropiada de los usuarios.	Fortalecer la protección en uso del Internet mediante herramientas de seguridad como firewall, antivirus, antispam y antimalware.	2	M	Abr-20	Abr-21	1	4	4	TT	Subgerente de TI
		R071	Inoperatividad del sistema / Pérdida de actividad de labores	Reducir	A.17.2.1 Instalaciones de procesamiento de la información	17.2.1 - Las instalaciones de procesamiento de la información deberían ser implementadas con redundancia suficiente para cumplir con los requisitos de disponibilidad.	Elaborar planes de continuidad del negocio, tal como un DRP ante emergencia	2	M	Abr-20	Abr-21	1	4	4	TT	Subgerente de TI Oficial de seguridad de la información

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
8	Página Web Pago en línea	R072	Caída de servicios	Reducir	A.12.1.3 Gestión de la capacidad	12.1.3 - El uso de recursos debería ser monitoreado, afinado y se debería hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.	Se monitoreará la plataforma tecnológica mediante el uso de herramientas.	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI
		R073	Abrir una URL que redirecciona a un lugar malicioso	Reducir	A.14.1.2 Aseguramiento de servicios de aplicaciones sobre redes públicas.	14.1.2 - La información involucrada en servicios de aplicaciones que pasa sobre redes públicas debería estar protegida de actividad fraudulenta, disputa de contratos o divulgación no autorizada y modificación.	Se revisará los acuerdos de servicios de aplicaciones, que estén respaldados por un acuerdo documentado entre ambas partes incluyendo garantizar la disponibilidad, protección, etc.	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI
		R074	Pago a webs fraudulentas / Phishing	Reducir	A.14.1.3 Protección de transacciones en servicios de aplicación	14.1.3 - La información involucrada en las transacciones de servicios de aplicación debería estar protegida para prevenir transmisión incompleta, ruteo incorrecto, alteración no autorizada de mensajes, divulgación no autorizada, duplicación o respuesta no autorizada de mensajes.	Se revisarán los acuerdos con los proveedores de la entrega del servicio de pago online.	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI
		R075	Caída de los servicios que soporta la página web	Reducir	A.15.2.1 Monitoreo y e servicios del proveedor	15.2.1 - Las organizaciones deberían monitorear, revisar y auditar regularmente la entrega de servicios por parte de los proveedores.	Se revisarán los acuerdos con los proveedores de la entrega del servicio de pago online.	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
	Correo electrónico institucional	R076	Manipulación de la información.	Reducir	A.5.1.1 Políticas para la seguridad de la información. A.5.1.2 Revisión de las políticas para la seguridad de la información.	5.1.1 - Un conjunto de políticas para la seguridad de la información debería ser definido, aprobado por la gerencia, publicado y comunicado a los empleados y a las partes externas relevantes. 5.1.2 - La política para la seguridad de la información deberían ser revisadas a intervalos planificados o si ocurren cambios significativos para asegurar su conveniencia, adecuación y efectividad continua.	Se implementará y/o revisará los lineamientos de la política de seguridad de la información de la municipalidad. Para su cumplimiento se realizarán auditorías programadas. Se solicitará a la estructura organizacional del SGSI reportes sobre la seguridad de la información de la entidad, de esta manera se verá el cumplimiento e incumplimiento y las causas del mismo,; para seguidamente tomar las acciones necesarias para la reducción del incumplimiento.	1	C	Abr-20	Abr-21	1	5	5	TT	Oficial de seguridad de la información
9		R077	Acceso lógico no autorizado	Reducir	A.9.1.1 Política de control de acceso. A.9.2.2 Aprovisionamiento de acceso a usuario.	9.1.1 - Una política de control de acceso debería estar establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información. 9.2.2 - Un proceso formal de aprovisionamiento de acceso de usuarios debería ser implementado para asignar o revocar los derechos de acceso para todos los tipos de usuarios a todos los sistemas y servicios.	Se realizarán los lineamientos de la política de control de acceso. También, se deberá implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para el acceso al correo electrónico.	1	C	Abr-20	Abr-21	1	4	4	TT	Oficial de seguridad de la información

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
		R078	Espionaje de contraseñas	Reducir	A.9.4.1 Restricción de acceso a la información. A.9.4.2 Procedimiento de ingreso seguro. A.9.4.3 Sistema de gestión de contraseñas.	9.4.1 - El acceso a la información y a las funciones del sistema de aplicación debería ser restringido en concordancia con la política de control de accesos. 9.4.2 - Donde la política de control de acceso lo requiera, el acceso a los sistemas y a las aplica. 9.4.3 - Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar que las contraseñas sean de calidad.	Se creará y/o revisará la política de control de acceso que permitirá controlar el acceso al correo electrónico de forma segura.	1	C	Abr-20	Abr-21	1	4	4	TT	Oficial de seguridad de la información
		R079	Procesamiento ilegal de datos		A.13.2.1 Políticas y procedimientos de transferencia de la información. A.13.2.4 Acuerdos de confidencialidad o no divulgación.	13.2.1 - Políticas, procedimientos y controles de transferencia formales deberían aplicarse para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación. 13.2.4 - Requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deberían estar identificados, revisados regularmente y documentados.	Se implementará la política para el intercambio de información a través de cualquier tipo de comunicaciones. Ello implicará también una cláusula de confidencialidad.	1	C	Abr-20	Abr-21	1	4	4	TT	Oficial de seguridad de la información
		R080	Correos entrantes con contenido malicioso y/o spam.		A.13.2.3 Mensajes electrónicos.	13.2.3 - La información involucrada en mensajería electrónica debería estar protegida apropiadamente.	Se creará y/o revisará los lineamientos de protección de la información de mensajería electrónica. Se implementara una solución de recepción masiva de correos no deseados para que brinde seguridad al servicio.	1	C	Abr-20	Abr-21	1	4	4	TT	Oficial de seguridad de la información

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
		R081	Robo de información		A.18.1.4 Privacidad y protección de datos personales.	18.1.4 - La privacidad y protección de los datos personales deberían estar aseguradas tal como se requiere en la legislación y regulación relevantes donde sea aplicable.	La entidad debe asegurar la privacidad y protección de la información de datos personales de los contribuyentes y empleados durante el intercambio de información en el servicio de correo electrónico .	1	C	Abr-20	Abr-21	1	4	4	TT	Oficial de seguridad de la información
10	Personal	R082	Indisponibilidad del personal (Huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos)	Reducir	A.6.1.2 Segregación de funciones	6.1.2 - Las funciones y áreas de responsabilidad en conflicto deberían estar segregadas para reducir oportunidades de modificación no autorizada o no intencional o mal uso de los activos de la organización.	Elaborar esquema o plan de reemplazo o sucesión en caso de ausencia de personal del proyecto	1	M	Abr-20	Abr-21	1	4	4	TT	Gerente de rentas
		R083	Inatención en los trabajos asignados		A.7.1.1 Selección. A.7.1.2 Términos y condiciones del empleo.	7.1.1 - Las verificaciones de los antecedentes de todos los candidatos a ser empleados deberían ser llevadas a cabo en la concordancia con las leyes, regulaciones y ética relevantes y debería ser proporcional a los requisitos del negocio, la clasificación de la información a la que se tendrá acceso y los riesgos percibidos. 7.1.2 - Los acuerdos contractuales con los empleados y contratistas deberían estipular responsabilidades de éstos y de la organización respecto de la seguridad de la información.	La entidad definirá los términos y condiciones laborales; además de definir los perfiles de los trabajadores de la municipalidad.	1	C	Abr-20	Oct-20	1	4	4	TT	Gerente de RRHH

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
		R084	Fuga de información	Reducir	A.7.2.2 Conciencia, educación y capacitación sobre seguridad de la información.	7.2.2 - Todos los empleados de la organización y, cuando fuera relevante, los contratistas deberían recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos de la organización, según sea relevante para la función del trabajo que cumplen.	Se realizarán charlas de concienciación en temas de seguridad al ingreso al proyecto así como de manera programada en el año	1	C	Abr-20	Oct-20	1	4	4	TT	Oficial de seguridad de la información
		R085	Incumplimiento de las normas establecidas respecto a seguridad de la información	Reducir	A.7.2.2 Conciencia, educación y capacitación sobre seguridad de la información.	7.2.2 - Todos los empleados de la organización y, cuando fuera relevante, los contratistas deberían recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos de la organización, según sea relevante para la función del trabajo que cumplen.	Se deberán implementar las normas de seguridad establecidas a todo el personal de la entidad, que empiezan desde amonestaciones verbales, suspensión, despido, etc., de acuerdo a la gravedad del incidente.	1	C	Abr-20	Oct-20	1	4	4	TT	Oficial de seguridad de la información
		R086	Abuso de derechos	Reducir	A.7.2.2 Conciencia, educación y capacitación sobre seguridad de la información.	7.2.2 - Todos los empleados de la organización y, cuando fuera relevante, los contratistas deberían recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos de la organización, según sea relevante para la función del trabajo que cumplen.	Se elaborará y/o revisará los accesos y privilegios de los empleados de la entidad que han finalizado su labor o han cambiado de área.	1	C	Abr-20	Oct-20	1	4	4	TT	Administrador de accesos

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
		R087	Apropiación indebida de activos	Reducir	A.8.1.3 Uso aceptable de los activos. A.8.1.4 Retorno de activos.	8.1.3 - Las reglas para el uso aceptable de la información y activos asociados con la información y con las instalaciones de procesamiento de la información deberían estar identificadas, documentadas e implementadas. 8.1.4 - Todos los empleados y usuarios de terceras partes deberían retornar todos los activos de la organización en su posesión a la conclusión de su empleo, contrato o acuerdo.	Todo el personal de la entidad debe hacer buen uso de los activos que les han sido asignados. Se elaborará y/o revisará los procedimientos de entrega de bienes asignados al personal de la entidad.	1	C	Abr-20	Oct-20	1	4	4	TT	Oficial de seguridad de la información
		R088	Robo o pérdida de información	Reducir	A.9.1.1 Política de control de acceso	9.1.1 - Una política de control de acceso debería estar establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.	Se elaborará una política de control de accesos. Se capacitará al personal de la entidad sobre la utilización de contraseñas en el equipo. Se emplearán controles de acceso lógico: - Uso de clave alfanumérica generada de 8 dígitos. - Bloqueo de cuenta por intentos fallidos. - Se revisará de manera trimestral el control de acceso a las bases de datos. - Se revisarán los registros log de autenticación y acceso a las bases de datos. - Se realizará la instalación de parches de seguridad según recomendación de fabricante.	1	C	Abr-20	Oct-20	1	4	4	TT	Oficial de seguridad de la información
		R089	Manipulación de la información	Reducir	A.12.1.1 Procedimientos operativos documentados	12.1.1 - Los procedimientos operativos deberían estar documentados y puestos a disposición de todos los usuarios que los necesitan.	Se revisarán y elaborarán los procedimientos e instructivos operativos del área o procesos.	1	C	Abr-20	Oct-20	1	4	4	TT	Oficial de seguridad de la información

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
		R090	Procesamiento ilegal de datos / Fuga de información	Reducir	A.13.2.1 Políticas y procedimientos de transferencia de la información. A.13.2.2 Acuerdo sobre transferencia de información.	13.2.1 - Políticas, procedimientos y controles de transferencia formales deberían aplicarse para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación. 13.2.2 - Los acuerdos deberían dirigir la transferencia segura de información del negocio entre la organización y partes externas.	Se elaborará la política de intercambio de información. El personal de la entidad deberá cumplir los lineamientos indicados en la política.	1	C	Abr-20	Oct-20	1	4	4	TT	Oficial de seguridad de la información
11	Instalaciones Data Center / Oficinas Administrativas	R091	Robo de información y equipos	Reducir	A.9.1.1 Política de control de acceso.	9.1.1 - Una política de control de acceso debería estar establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información	La entidad deberá implementar procedimientos dentro de la política de control de acceso, que regulen el acceso a las instalaciones y equipos. Además, debe supervisar continuamente que se ejecuten los lineamientos mencionados en la política.	1	C	Abr-20	Oct-20	1	4	4	TT	Oficial de seguridad de la información
		R092	Acceso físico no autorizado		A.11.1.1 Perímetro de seguridad física. A.11.1.2 Controles de ingreso físico.	11.1.1 - Los perímetros de seguridad deberían ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de la información. 11.1.2 - Las áreas seguras deberían estar protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo al personal autorizado.	Se llevará un control de ingreso a las áreas de caja y tesorería, especialmente. El personal de seguridad verificará los objetos de entrada y salida de las personas. También, se llevará un control expreso de ingreso a las instalaciones del datacenter. Las personas que solicitan visita acompañaran a las visitantes durante su permanencia en las instalaciones. El ingreso será con anticipación al data center mínimo de 2días. El personal de seguridad verificará los objetos de entrada y salida de las personas.	1	C	Abr-20	Oct-20	1	5	5	TT	Jefe de seguridad Gerente de rentas

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
		R093	Incendio		A.11.1.2 Controles de ingreso físico.	11.1.2 - Las áreas seguras deberían estar protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo al personal autorizado.	Se realizarán las revisiones y cambios de extintores. Además, se formarán brigadistas y se revisarán la señales de evacuación en caso de emergencia.	1	C	Abr-20	Oct-20	1	5	5	TT	Jefe de seguridad Gerente de rentas
		R094	Terremoto (Sismos)		A.17.1.1 Planificación de continuidad de seguridad de la información.	17.1.1 - La organización debería determinar sus requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre.	Elaborar planes de respuesta ante emergencia (continuidad de negocio), como un DRP. Realizar simulacros periódicos, contar con brigadas de emergencia	2	M	Abr-20	Abr-21	1	5	5	TT	Subgerente de TI Oficial de seguridad de la Información
		R095	Ataque destructivo (vandalismo, terrorismo, acción militar, etc.)		A.17.1.1 Planificación de continuidad de seguridad de la información.	17.1.1 - La organización debería determinar sus requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre.	Elaborar planes de respuesta ante emergencia (continuidad de negocio), como un DRP. Realizar simulacros periódicos, contar con brigadas de emergencia	2	M	Abr-20	Abr-21	1	5	5	TT	Subgerente de TI Oficial de seguridad de la Información
		R096	Inundación	Reducir	A.17.1.1 Planificación de continuidad de seguridad de la información.	17.1.1 - La organización debería determinar sus requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre.	Elaborar planes de respuesta ante emergencia (continuidad de negocio), como un DRP. Realizar simulacros periódicos, contar con brigadas de emergencia	2	M	Abr-20	Abr-21	1	5	5	TT	Subgerente de TI Oficial de seguridad de la Información
		R097	Perdida de energía eléctrica	Reducir	A.17.1.1 Planificación de continuidad de seguridad de la información.	17.1.1 - La organización debería determinar sus requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre.	Se realizarán mantenimientos anuales al grupo electrógeno. Se realizarán mantenimientos preventivos a los equipos auxiliares.	2	M	Abr-20	Abr-21	1	5	5	TT	Subgerente de TI Oficial de seguridad de la Información

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
12	Sistema operativo	R098	Instalación de software no licenciado	Reducir	A.12.6.2 Restricciones sobre la instalación de software	12.6.2 - Reglas que gobiernen la instalación de software por parte de los usuarios deberían ser establecidas e implementadas.	Se implementará control de acceso a Internet para restringir la instalación de programas sin autorización	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI
		R099	Errores de mantenimiento / Actualizaciones de programas (software)	Reducir	A.7.2.2 Conciencia, educación y capacitación sobre seguridad de la información.	7.2.2 - Todos los empleados de la organización y, cuando fuera relevante, los contratistas deberían recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos de la organización, según sea relevante para la función del trabajo que cumplen.	Se elaborará un plan de capacitación técnica anual, según las necesidades de las actividades del personal, tales como: nuevas tecnologías, actualizaciones, etc.	2	M	Abr-20	Abr-21	1	4	4	TT	Subgerente de TI
		R100	Abuso de privilegios de acceso	Reducir	A.9.1.1 Política de control de acceso.	9.1.1 - Una política de control de acceso debería estar establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.	Se elaborará una política de control de accesos. Se capacitará al personal de la entidad sobre la utilización de contraseñas en el equipo. Se emplearán controles de acceso lógico: - Uso de clave alfanumérica generada de 8 dígitos. - Bloqueo de cuenta por intentos fallidos. - Se revisará de manera trimestral el control de acceso a las bases de datos. - Se revisarán los registros log de autenticación y acceso a las bases de datos. Se realizará la instalación de parches de seguridad según recomendación de fabricante.	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
		R101	Vulnerabilidades de los programas (Software)	Reducir	12.6.1 Gestión de vulnerabilidades técnicas	12.6.1 - Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debería ser obtenida de manera oportuna, la exposición de la organización a dichas vulnerabilidades debería ser evaluada y las medidas apropiadas deberían ser tomadas para resolver el riesgo asociado.	Se realizan pruebas de ethical hacking de manera anual. Se realizan cambios en la plataforma según la recomendación del fabricante ante cualquier vulnerabilidad detectada.	2	M	Abr-20	Abr-21	1	4	4	TT	Subgerente de TI
		R102	Abuso de privilegios de acceso	Reducir	A.9.1.1 Política de control de acceso.	9.1.1 - Una política de control de acceso debería estar establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.	Se elaborará una política de control de accesos. Se capacitará al personal de la entidad sobre la utilización de contraseñas en el equipo. Se emplearán controles de acceso lógico: - Uso de clave alfanumérica generada de 8 dígitos. - Bloqueo de cuenta por intentos fallidos. - Se revisará de manera trimestral el control de acceso a las bases de datos. - Se revisarán los registros log de autenticación y acceso a las bases de datos. - Se realizará la instalación de parches de seguridad según recomendación de fabricante.	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI
		R103	Vencimiento de licencia de uso (Software)	Reducir	A.18.1.2 Derechos de propiedad intelectual	18.1.2 - Procedimientos apropiados deberían ser implementados para asegurar el cumplimiento de requisitos legislativos, regulatorios y contractuales, relacionados a los derechos de propiedad intelectual y uso de productos de software propietario.	Se realizará la renovación anual del mantenimiento de licencias.	D	M	Abr-20	Abr-21	1	4	4	TT	Subgerente de TI

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
		R104	Acceso lógico no autorizado	Reducir	A.9.1.1 Política de control de acceso.	9.1.1 - Una política de control de acceso debería estar establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la información.	Se elaborará una política de control de accesos. Se capacitará al personal de la entidad sobre la utilización de contraseñas en el equipo. Se emplearán controles de acceso lógico: - Uso de clave alfanumérica generada de 8 dígitos. - Bloqueo de cuenta por intentos fallidos. - Se revisará de manera trimestral el control de acceso a las bases de datos. - Se revisarán los registros log de autenticación y acceso a las bases de datos. - Se realizará la instalación de parches de seguridad según recomendación de fabricante. - Se monitoreará el acceso a la red (IDS/IPS)	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI
		R105	Difusión de software dañino (malware)	Reducir	A.12.2.1 Controles contra software malicioso	12.2.1 - Controles de detección, prevención y recuperación para proteger contra el software malicioso deberían estar implementados, en combinación con una concientización apropiada de los usuarios.	Elaboración y/o actualización del procedimiento de Gestión de Cambios. Se elaborará un programa de instalación de parches de seguridad fixes a nivel de base de datos y aplicaciones.	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI
13	UPS Aire acondicionado	R106	Falla del funcionamiento del equipo	Reducir	A.11.2.4 Mantenimiento de equipos	11.2.4 - Los equipos deberían mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.	Programar y ejecutar los mantenimientos preventivos (anual)	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
		R107	Manipulación de los equipos	Reducir	A.12.1.1 Procedimientos operativos documentados	12.1.1 - Los procedimientos operativos deberían estar documentados y puestos a disposición de todos los usuarios que los necesitan.	Revisión y/o actualización de los procedimientos e instructivos operativos del área o proceso	1	C	Abr-20	Oct-20	1	4	4	TT	Analista TI
		R108	Falla del funcionamiento del sistema de climatización	Reducir	A.12.1.3 Gestión de la capacidad	12.1.3 - El uso de recursos debería ser monitoreado, afinado y se debería hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.	Revisar los controles de medición de humedad y temperatura en del datacenter. Los administradores monitorean el servicio mediante la herramienta de monitoreo Foglight, el cual permite monitorear la disponibilidad de la plataforma.	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI
		R109	Corte del suministro eléctrico	Reducir	A.17.1.1 Planificación de continuidad de seguridad de la información.	17.1.1 - La organización debería determinar sus requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre.	Se realizarán mantenimientos preventivos a los equipos auxiliares. Por otro lado, se realizarán mantenimientos y pruebas anuales al grupo electrógeno.	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI
14	Cintas de backup	R110	Divulgación de información	Reducir	A.7.2.2 Conciencia, educación y capacitación sobre seguridad de la información.	7.2.2 - Todos los empleados de la organización y, cuando fuera relevante, los contratistas deberían recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos de la organización, según sea relevante para la función del trabajo que cumplen.	Se realizarán charlas de concientización en temas de seguridad al ingreso al proyecto así como de manera programada en el año	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI

N°	Activos	Id Riesgo	Riesgo	Tratamiento	Anexo relacionado	Control ISO/IEC 27002	Mecanismos de Protección Propuestos	Costo Aprox.	Tiempo Aprox.	Fecha		Riesgo Residual				Responsable
										Inicio	Fin	Probabilidad	Impacto	Riesgo	Tolerancia	
		R111	Avería de los medios de almacenamiento de información (cintas, cd / dvd, hard disk, etc)	Reducir	A.7.2.2 Conciencia, educación y capacitación sobre seguridad de la información.	7.2.2 - Todos los empleados de la organización y, cuando fuera relevante, los contratistas deberían recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos de la organización, según sea relevante para la función del trabajo que cumplen.	Se realizarán charlas de concientización en temas de seguridad al ingreso al proyecto así como de manera programada en el año	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI
		R112	Robo o pérdida de información	Reducir	A.11.1.2 Controles de ingreso físico	11.1.2 - Las áreas seguras deberían estar protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo al personal autorizado.	El acceso al datacenter y será previa coordinación y autorización con el jefe o responsable del área. Se implementará una cámaras de vigilancia dentro del área.	2	M	Abr-20	Abr-21	1	4	4	TT	Subgerente de TI
		R113	Manipulación de los equipos	Reducir	A.12.1.1 Procedimientos operativos documentados	12.1.1 - Los procedimientos operativos deberían estar documentados y puestos a disposición de todos los usuarios que los necesitan.	Revisión y/o actualización de los procedimientos e instructivos operativos del área o proceso.	1	C	Abr-20	Oct-20	1	4	4	TT	Subgerente de TI
		R114	Falta de soportes de información (cintas, discos externos, cd, dvd)	Compartir	A.15.1.2 Abordar la seguridad dentro de los acuerdos con proveedores	15.1.2 - Todos los requisitos relevantes de seguridad de la información deberían ser establecidos y acordados con cada proveedor	Se contarán con más de un proveedor de medios de respaldos de las cintas backup.	D	M	Abr-20	Abr-21	1	4	4	TT	Subgerente de TI

Anexo 9 - Declaración de Aplicabilidad

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD		¿CUMPLE? (SI/ NO)	JUSTIFICACIÓN
5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
5.1	Orientación de la dirección de gestión para la seguridad de la información		
5.1.1	Políticas de seguridad de la información	Si	Es necesario contar con una política de seguridad de la información que sirva para gestionar la seguridad de la información dentro de la municipalidad.
5.1.2	Revisión de las políticas de seguridad de la información	Si	Es necesario revisar constantemente los controles para ajustar aquellos que no estén debidamente aplicados.
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			
6.1	Organización interna		
6.1.1	Roles y responsabilidades de la seguridad de la información	Si	Es necesario definir los roles y responsabilidades a todos los que participen e interactúen en el SGSI de la municipalidad.
6.1.2	Segregación de funciones	Si	Es necesario segregar las funciones para la realización de tareas y actividades, a fin de evitar usos indebidos de los activos de la municipalidad.
6.1.3	Contacto con autoridades	No	No aplica para el alcance del SGSI.
6.1.4	Contacto con grupos especiales de interés	No	No aplica para el alcance del SGSI.
6.1.5	Seguridad de la información en la gestión del proyecto	No	No aplica para el alcance del SGSI.
6.2	Dispositivos móviles y trabajo remoto		
6.2.1	Política de dispositivos móviles	No	No aplica para el alcance del SGSI.
6.2.2	Teletrabajo	No	No aplica para el alcance del SGSI.
7. SEGURIDAD EN LOS RECURSOS HUMANOS			
7.1	Antes del empleo		
7.1.1	Selección	Si	Es necesario que el área de recursos humanos realice una exhaustiva investigación de los antecedentes del personal a fin de conocer su procedencia, si

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD		¿CUMPLE? (SI/ NO)	JUSTIFICACIÓN
			cuenta con antecedentes penales y judiciales, etc.
7.1.2	Términos y condiciones del empleo	Si	Es necesario que se establezca un documento con cláusulas de confidencialidad hacia municipalidad e incluyendo la responsabilidad, que todo el personal debe firmar.
7.2	Durante el empleo		
7.2.1	Responsabilidades de la gerencia	No	No aplica para el alcance del SGSI.
7.2.2	Conciencia, educación y capacitación sobre la seguridad de la información.	Si	Es necesario capacitar y concientizar a todo el personal en los aspectos relacionados a seguridad de la información, de acuerdo a sus funciones laborales.
7.2.3	Proceso disciplinario	Si	Es necesario establecer sanciones que se aplicarán al personal que incumpla con lo descrito en la política de seguridad de la información.
7.3	Terminación y cambio de empleo		
7.3.1	Terminación o cambio de responsabilidades del empleo	Si	Es necesario definir en los contratos los deberes y responsabilidades ante la finalización del empleo, sobre todo en relación a la confidencialidad de la información.
8. GESTIÓN DE ACTIVOS			
8.1	Responsabilidad por los activos		
8.1.1	Inventario de activos	Si	Es necesario tener un inventario de los activos con los que cuenta la municipalidad. Y como parte del proceso de diseño del SGSI se ha realizado el inventario de los activos de información.
8.1.2	Propiedad de los activos	Si	Como parte del control anterior, es necesario que cada activo tenga un responsable o identificar en custodia de quien se encuentra el activo.
8.1.3	Uso aceptable de los activos	Si	Es necesario que haya una cláusula donde los empleados se comprometan al uso

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD		¿CUMPLE? (SI/ NO)	JUSTIFICACIÓN
			aceptable de la información y de los activos de la municipalidad.
8.1.4	Retorno de activos	Si	Es necesario contar con un proceso para la devolución de los activos, ya sea cuando un empleado ha cambiado de puesto o ha terminado su vínculo laboral con la municipalidad.
8.2	Clasificación de la información		
8.2.1	Clasificación de la información	Si	Es necesario que contar con un procedimiento que permita la clasificación de la información de acuerdo a su valor, sensibilidad, criticidad, etc., y exista un mejor entendimiento de quienes hagan uso de ellos.
8.2.2	Etiquetado de la información	No	No aplica para el alcance del SGSI.
8.2.3	Manejo de activos	Si	Es necesario tener un procedimiento para el manejo que se le debe dar a un activo; además de adoptar medidas de seguridad en función de su clasificación.
8.3	Manejo de los medios		
8.3.1	Gestión de los medios removibles	No	No aplica para el alcance del SGSI.
8.3.2	Disposición de medios	No	No aplica para el alcance del SGSI.
8.3.3	Transferencia de medios físicos	Si	Es necesario definir procedimientos que permitan que la información almacenada en estos no sea divulgada, modificada o eliminada.
9. CONTROL DE ACCESO			
9.1	Requisitos de la empresa para el control de acceso		
9.1.1	Política de control de acceso	Si	Es necesario establecer políticas que permitan el acceso a la información de acuerdo a privilegios establecidos según sus funciones.
9.1.2	Acceso a redes y servicios de red	Si	Es necesario establecer una política referente al uso de los servicios de red, con el fin de gestionar los accesos de acuerdo a las funciones asignadas.

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD		¿CUMPLE? (SI/ NO)	JUSTIFICACIÓN
9.2	Gestión de acceso de usuario		
9.2.1	Registro y baja de usuarios	Si	Es necesario contar con documentos formales autorizado por el jefe del proceso sobre la creación o baja de usuarios. Todos los usuarios con acceso a los sistemas de información deben estar registrados, además de dar de baja a los que ya no forman parte de la municipalidad.
9.2.2	Aprovisionamiento de acceso a usuario	Si	Es necesario implementar un procedimiento donde se concedan o retiren permisos en función de las necesidades de acceso de los usuarios.
9.2.3	Gestión de derechos de acceso privilegiados.	Si	Es necesario establecer privilegios de acceso a la información de acuerdo al desempeño de sus funciones.
9.2.4	Gestión de información de autenticación secreta de usuarios.	Si	Es necesario establecer un proceso de gestión formal para la asignación de información solo al personal con privilegios especiales.
9.2.5	Revisión de los derechos de acceso de usuarios	Si	Es necesario el monitoreo de los privilegios asignados a los usuarios con el fin de identificar, si los privilegios asignados son adecuados para el desarrollo de sus funciones.
9.2.6	Remoción o ajuste de derechos de acceso	Si	Es necesario dar de baja o modificar los privilegios de acceso a la información en caso de traslado del usuario o retiro de la entidad.
9.3	Responsabilidades de los usuarios		
9.3.1	Uso de información confidencial para la autenticación.	Si	Es necesario que cada empleado se responsabilice sobre el correcto uso de sus contraseñas y accesos.
9.4	Control de acceso a sistema y aplicación		
9.4.1	Restricción del acceso a la información	Si	Es necesario restringir el acceso a la información por parte de personal no autorizado.

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD		¿CUMPLE? (SI/ NO)	JUSTIFICACIÓN
9.4.2	Procedimientos seguros de inicio de sesión	Si	Es necesario establecer procedimientos que restrinjan el acceso a la información a personal no autorizado.
9.4.3	Sistema de gestión de contraseñas	Si	Es necesario establecer políticas de gestión de contraseñas donde se establezcan fechas de cambio, cantidad de caracteres a utilizar, bloqueo después de un determinado número de intentos, parámetros para creación de contraseñas seguras.
9.4.4	Uso de programas utilitarios privilegiados	No	No aplica para el alcance del SGSI.
9.4.5	Control de acceso al código fuente de los programas	No	No aplica para el alcance del SGSI.
10. CRIPTOGRAFÍA			
10.1	Controles criptográficos		
10.1.1	Política sobre el uso de controles criptográficos	No	No aplica para el alcance del SGSI.
10.1.2	Gestión de claves	No	No aplica para el alcance del SGSI.
11. SEGURIDAD FÍSICA Y AMBIENTAL			
11.1	Áreas seguras		
11.1.1	Perímetro de seguridad física	Si	Es necesario establecer un perímetro de tal forma que las áreas donde se encuentran los activos tengan acceso restringido.
11.1.2	Controles de ingreso físico	Si	Es necesario restringir el acceso a áreas como la ubicación del servidor, el centro de cableado, lugares donde se encuentra información confidencial, además de caja y tesorería.
11.1.3	Seguridad de oficinas, áreas e instalaciones	Si	Es necesario restringir el acceso a las áreas por personal no autorizado, siendo estas demarcadas con un aviso de que son sitios restringidos.
11.1.4	Protección contra amenazas externas y ambientales	Si	Es necesario establecer políticas para evitar daños contra incendios, inundaciones, terremotos, etc.
11.1.5	Trabajo en áreas seguras	No	No aplica para el alcance del SGSI.
11.1.6	Áreas de despacho y carga	No	No aplica para el alcance del SGSI.

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD		¿CUMPLE? (SI/ NO)	JUSTIFICACIÓN
11.2	Equipos		
11.2.1	Ubicación y protección de los equipos	Si	Es necesario mantener una infraestructura segura, que los equipos se encuentren ubicados en sitios seguros, a fin de protegerlos contra robos, accesos no autorizados, etc.
11.2.2	Servicios de suministro	Si	Es necesario contar con un adecuado suministro y respaldo de energía.
11.2.3	Seguridad del cableado	Si	Es necesario proteger el cableado eléctrico y de datos de posibles daños.
11.2.4	Mantenimiento de equipos	Si	Es necesario programar mantenimientos preventivos y correctivos en periodos de tiempo establecidos, con el fin de evitar daños en los servidores y equipos de cómputo.
11.2.5	Remoción de activos	No	No aplica para el alcance del SGSI.
11.2.6	Seguridad de equipos y activos fuera de las instalaciones	No	No aplica para el alcance del SGSI.
11.2.7	Disposición o reutilización segura de equipos	No	No aplica para el alcance del SGSI.
11.2.8	Equipos de usuario desatendidos	Si	Es necesario establecer políticas para los equipos cuando los usuarios no están presentes, evitando así ingresos no autorizados o robo de información.
11.2.9	Política de escritorio limpio y pantalla limpia	Si	Es necesario definir procedimientos para que los escritorios estén libres de papeles y tener políticas de pantallas limpias.
12. SEGURIDAD DE LAS OPERACIONES			
12.1	Procedimientos y responsabilidades operativas		
12.1.1	Procedimientos operativos documentados	Si	Es necesario documentar los procedimientos de seguridad tales como: copias de seguridad, mantenimiento de equipos, manejo del correo, manejo de medios, etc.; y ponerlos al alcance de todos.
12.1.2	Gestión de cambios	No	No aplica para el alcance del SGSI.

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD		¿CUMPLE? (SI/ NO)	JUSTIFICACIÓN
12.1.3	Gestión de la capacidad	Si	Es necesario que se realice un monitoreo de los recursos de tal forma que no afecten la operación, como: capacidad de banda ancha, espacio en disco, circuitos descalibrados que afecten el fluido eléctrico , equipos de cómputo lentos, etc.
12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones	No	No aplica para el alcance del SGSI.
12.2	Protección contra códigos maliciosos		
12.2.1	Controles contra códigos maliciosos	Si	Es necesario establecer políticas de seguridad referidas al uso del correo electrónico y de páginas web con contenido dudoso. Además, los equipos de cómputo deben contar con software antivirus que debe actualizarse constantemente que mitiguen las nuevas vulnerabilidades.
12.3	Respaldo		
12.3.1	Respaldo de la información	Si	Es necesario establecer políticas de respaldo de información, además de realizar las pruebas para la comprobación de que cumplen con las políticas establecidas.
12.4	Registros y monitoreo		
12.4.1	Registro de eventos	Si	Es necesario establecer procedimientos para el control y registro de los accesos al sistema y revisar las actividades del mismo, a fin de establecer medios que ayuden a repararlos o eliminarlos definitivamente.
12.4.2	Protección de información de registros	Si	Es necesario implementar controles que protejan los registros y problemas de aplicativos de la municipalidad. Solo el administrador o encargado puede tener acceso y se deben realizar copias de logs.
12.4.3	Registros del administrador y del operador	No	No aplica para el alcance del SGSI.
12.4.4	Sincronización de reloj	No	No aplica para el alcance del SGSI.

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD		¿CUMPLE? (SI/ NO)	JUSTIFICACIÓN
12.5	Control del software operacional		
12.5.1	Instalación de software en sistemas operacionales	No	No aplica para el alcance del SGSI.
12.6	Gestión de vulnerabilidad técnica		
12.6.1	Gestión de vulnerabilidades técnicas	Si	Es necesario establecer procedimientos que disminuyan las vulnerabilidades técnicas a los que están expuestos los activos tecnológicos.
12.6.2	Restricciones sobre la instalación de software	Si	Es necesario controlar la instalación de software, con el fin de que solo las personas autorizadas lo realicen.
12.7	Consideraciones para la auditoría de los sistemas de información		
12.7.1	Controles de auditoría de los sistemas de información	No	No aplica para el alcance del SGSI.
13. SEGURIDAD DE LAS COMUNICACIONES			
13.1	Gestión de seguridad de la red		
13.1.1	Controles de la red	Si	Es necesario instalar dispositivos o software que permitan controlar el acceso a la red como: firewall, segmentación de red, monitoreo de canales, Ids, autenticación de ingreso, etc.
13.1.2	Seguridad de servicios de red	No	No aplica para el alcance del SGSI.
13.1.3	Segregación en redes	No	No aplica para el alcance del SGSI.
13.2	Transferencia de información		
13.2.1	Políticas y procedimientos de transferencia de la información	Si	Es necesario establecer políticas sobre la transferencia de información y todos sus usos.
13.2.2	Acuerdo sobre transferencia de información	Si	Es necesario establecer controles que permitan respetar acuerdos de intercambio o transferencia de información.
13.2.3	Mensajes electrónicos	Si	Es necesario que haya controles referentes al uso adecuado de la mensajería electrónica. Se debe instalar programas que detecten antivirus y spam. También, realizar capacitaciones con situaciones de

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD		¿CUMPLE? (SI/ NO)	JUSTIFICACIÓN
			correos sospechosos y el uso correcto del correo electrónico.
13.2.4	Acuerdos de confidencialidad o no divulgación	Si	Es necesario que los empleados cumplan con las políticas de confidencialidad y no divulgación de información, firmadas en el contrato de ingreso a la municipalidad.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS			
14.1	Requisitos de seguridad de los sistemas de información		
14.1.1	Análisis y especificación de requisitos de seguridad de la información	No	No aplica para el alcance del SGSI.
14.1.2	Aseguramiento de servicios de aplicaciones sobre redes públicas	No	No aplica para el alcance del SGSI.
14.1.3	Protección de las transacciones de servicios de aplicación	No	No aplica para el alcance del SGSI.
14.2	Seguridad en los procesos de desarrollo y soporte		
14.2.1	Política de desarrollo seguro	No	No aplica para el alcance del SGSI.
14.2.2	Procedimientos de control de cambio del sistema	Si	Es necesario establecer procedimientos para que cada cambio que se realice a los sistemas tenga que ser controlado y documentado.
14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	No	No aplica para el alcance del SGSI.
14.2.4	Restricciones sobre cambios a los paquetes de software	No	No aplica para el alcance del SGSI.
14.2.5	Principios de ingeniería de sistemas seguros	No	No aplica para el alcance del SGSI.
14.2.6	Ambientes de desarrollo seguro	No	No aplica para el alcance del SGSI.
14.2.7	Desarrollo contratado externamente.	No	No aplica para el alcance del SGSI.

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD		¿CUMPLE? (SI/ NO)	JUSTIFICACIÓN
14.2.8	Pruebas de seguridad del sistema	No	No aplica para el alcance del SGSI.
14.2.9	Pruebas de aceptación del sistema	No	No aplica para el alcance del SGSI.
14.3	Datos de prueba		
14.3.1	Protección de datos de prueba	No	No aplica para el alcance del SGSI.
15. RELACIONES CON LOS PROVEEDORES			
15.1	Seguridad de la información en las relaciones con los proveedores		
15.1.1	Política de seguridad de la información para las relaciones con los proveedores	No	No aplica para el alcance del SGSI.
15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	No	No aplica para el alcance del SGSI.
15.1.3	Cadena de suministro de tecnología de información y comunicación	No	No aplica para el alcance del SGSI.
15.2	Gestión de entrega de servicios del proveedor		
15.2.1	Monitoreo y revisión de servicios de los proveedores	Si	Es necesario que la municipalidad monitoree, revise y audite la entrega de los servicios por parte de los proveedores.
15.2.2	Gestión de cambios a los servicios de proveedores	No	No aplica para el alcance del SGSI.
16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			
16.1	Gestión de incidentes de seguridad de la información y mejoras		
16.1.1	Responsabilidades y procedimientos	No	No aplica para el alcance del SGSI.
16.1.2	Reporte de eventos de seguridad de la información	Si	Es necesario diseñar un procedimiento para gestionar los eventos de seguridad de la información reportados por los empleados de cada uno de los controles implementados. Además, realizar capacitaciones al personal sobre sus roles y responsabilidades dentro del SGSI.

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD		¿CUMPLE? (SI/ NO)	JUSTIFICACIÓN
16.1.3	Reporte de debilidades de seguridad de la información	Si	Es necesario capacitar adecuadamente a todo el personal de la municipalidad con la finalidad de que sean capaces de detectar debilidades en el SGSI y puedan reportarlo. Así mismo, las sanciones que podrían recibir si deciden probar las debilidades encontradas.
16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	No	No aplica para el alcance del SGSI.
16.1.5	Respuesta a incidentes de seguridad de la información	No	No aplica para el alcance del SGSI.
16.1.6	Aprendizaje de los incidentes de seguridad de la información	No	No aplica para el alcance del SGSI.
16.1.7	Recolección de evidencia	No	No aplica para el alcance del SGSI.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO			
17.1	Continuidad de seguridad de la información		
17.1.1	Planificación de continuidad de seguridad de la información	Si	Es necesario para identificar los puntos débiles en cuanto a la continuidad de las operaciones.
17.1.2	Implementación de continuidad de seguridad de la información	Si	Es necesario implementar procedimientos que permitan la continuidad del negocio ante situaciones imprevistas que podrían ocasionar retrasos en las operaciones. Por ejemplo un DRP (Recuperación ante desastres).
17.1.3	Verificación, revisión y evaluación de continuidad de seguridad de la información	No	No aplica para el alcance del SGSI.
17.2	Redundancias		
17.2.1	Instalaciones de procesamiento de la información	Si	Es necesario establecer redundancias en las instalaciones donde se procesa la

OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD		¿CUMPLE? (SI/ NO)	JUSTIFICACIÓN
			información con el objetivo de que no se afecte la disponibilidad de la información.
18. CUMPLIMIENTO			
18.1	Cumplimiento con requisitos legales y contractuales		
18.1.1	Identificación de requisitos contractuales y de legislación aplicables	No	No aplica para el alcance del SGSI.
18.1.2	Derechos de propiedad intelectual	Si	Es necesario establecer políticas de derechos de propiedad intelectual y cumplir con las regulaciones vigentes. Software patentado.
18.1.3	Protección de registros	Si	Es necesario contar con un procedimiento que permita la custodia de los registros o documentación clasificada ante situaciones de robo, divulgación, modificación, etc.
18.1.4	Privacidad y protección de datos personales	Si	Es necesario establecer políticas de seguridad para cumplir con la ley de protección de datos personales.
18.1.5	Regulación de controles criptográficos	No	No aplica para el alcance del SGSI.
18.2	Revisiones de seguridad de la información		
18.2.1	Revisión independiente de la seguridad de la información	No	No aplica para el alcance del SGSI.
18.2.2	Cumplimiento de políticas y normas de seguridad	Si	Es necesario que gerente del área compruebe que los requisitos de seguridad de la información definidos en las políticas y estándares sean cumplidos.

Anexo 10 - Plan de concientización y capacitación

PROGRAMA	Código: PS-001
		Versión: 0.1
	Programa de concientización y capacitación	Fecha: 30/10/2019
		Autor: Lisbet Monteza

1. Introducción

Las tecnologías y comunicaciones se han convertido en la herramienta por excelencia para la optimización de los procesos y el funcionamiento eficaz de una empresa. Pero con el uso de las tecnologías surgen amenazas y vulnerabilidades asociadas, que pueden llegar a afectar la confidencialidad, integridad y disponibilidad de la información que se encuentra disponible en las diferentes plataformas, afectando así el normal desempeño de la municipalidad.

El Sistema de Gestión de Seguridad de la Información da pautas específicas para guiar a la entidad a mitigar las amenazas que pueden llegar a traer consigo las tecnologías implementadas, sin embargo, un plan de tratamiento de riesgo no se basa solo en el aseguramiento de plataformas y procesos, sino también debe involucrar los factores humanos, que en muchos casos, son la principal causa de los incidentes de seguridad, esto debido a que no conocen sobre seguridad de la información y su rol dentro de la entidad. Por lo que es necesario concientizarlos y capacitarlos sobre la importancia de la preservación de la confidencialidad, integridad y disponibilidad de la información.

Es así que este documento describe el plan de concientización y capacitación en seguridad de la información para la Municipalidad Distrital de El Agustino.

2. Objetivo

Desarrollar una cultura en seguridad de la información dentro de la Municipalidad Distrital de El Agustino, implementando buenas prácticas de seguridad e incentivando en los propietarios y usuarios de los sistemas de información su preocupación por el tema y su cambio de comportamiento frente al manejo de los activos de información a su cargo.

3. Alcance

Todos los trabajadores de la municipalidad distrital de El Agustino, especialmente del área de rentas y de TI, serán beneficiados con el programa al obtener un conocimiento de cómo manejar con seguridad su información.

4. Roles involucrados:

Directivos:

Los directivos de la Municipalidad Distrital de El Agustino apoyaran el desarrollo del programa de concientización y capacitación mediante las siguientes acciones:

- 1) Autorizar a los trabajadores bajo su responsabilidad para participar en las sesiones presenciales de concientización y capacitación que se desarrollen durante su vigencia.
- 2) Participar de acuerdo a su disponibilidad en las actividades presenciales del programa de concientización y capacitación.
- 3) Fomentar la aplicación de las buenas prácticas de seguridad de la información que se difundirá en el programa de concientización y capacitación.

Responsables de la seguridad de la información

- 1) Diseñar el programa de concientización y capacitación en seguridad de la información, teniendo en cuenta la misión de la municipalidad y la relevancia que se busca para la cultura de la entidad.
- 2) Identificar las necesidades y las prioridades que tenga la municipalidad respecto al tema de concientización y capacitación en seguridad de la información.
- 3) Estructurar el programa de concientización y capacitación en seguridad de la información de acuerdo con las necesidades de la municipalidad y los recursos disponibles para su ejecución.
- 4) Participar en el diseño de los materiales del programa de concientización y capacitación.
- 5) Participar en la implementación del programa de concientización y capacitación.

Líderes del proceso

- 1) Coordinar al interior de sus procesos la participación de los trabajadores en las actividades del plan de concientización y capacitación.
- 2) Vigilar que en las actividades de sus procesos se empleen las instrucciones y recomendaciones sobre la seguridad de la información en el marco del plan de concientización y capacitación.

- 3) Identificar necesidades en materia de concientización y capacitación en seguridad de la información para su proceso, trabajadores y entidad.

Funcionarios de la entidad

- 1) Participar en las actividades del programa de concientización y capacitación de acuerdo con la coordinación que se realice.
- 2) Identificar formas de implementar en sus actividades diarias las recomendaciones y buenas prácticas del programa de concientización y capacitación.
- 3) Identificar oportunidades para mejorar el programa de concientización y capacitación.

5. Metas:

El programa de concientización y capacitación en seguridad de la información tiene las siguientes metas:

- Comunicar formalmente a toda la municipalidad la existencia del sistema de gestión de seguridad de la información.
- Socializar a todo el personal de la municipalidad las políticas de seguridad de la información.
- Socializar los principales procedimientos de seguridad de la información.
- Fomentar la cultura de seguridad de la información como herramienta de protección de la información de la municipalidad.
- Divulgar a todos los funcionarios los principales riesgos de seguridad de la información.
- Explicar las normas legales que soporta el sistema de gestión de seguridad de la información.
- Explicar de manera sencilla en qué consiste diversos tipos de ataques informáticos y como controlarlos.
- Explicar los mecanismos de control dispuestos por la entidad para evitar ataques informáticos.

6. Programa de concientización

Entre los temas más importantes a tratar se encuentran:

- Políticas de seguridad de la información

- Sistema de Gestión de Seguridad de la Información
- Política de escritorio limpio
- Amenazas informáticas
- Control de acceso a los sistemas (privilegios, separación de roles)
- Uso y manejo de inventario
- Uso de correo electrónico
- Sanciones por incumplimiento de las políticas

Actividades programadas

- Charlas y conferencias
- Cursos
- Mensajes de correos electrónico
- Publicaciones en pantallas
- Elementos físicos de recordación

Materiales y recursos

- Mensajes electrónicos sobre que debe y que no debe hacerse
- Boletines vía email.
- Protector de pantalla con mensajes de concientización
- Letreros

Plan de concientización

Se presenta a continuación en la tabla 72.

Tabla 72.
Plan de concientización

N°	Tema	Objetivo	Actividad	Tiempo	Recursos	Responsable	Resultados
1	Conocimiento del Sistema de Gestión de Seguridad de la Información	Explicar a los trabajadores de la MDEA qué es y para qué sirve el Sistema de Gestión de Seguridad de la información.	Charla	30 min.	Sala de reuniones y presentación de diapositivas.	Oficial de seguridad de la información	Los participantes podrán explicar cuáles son los beneficios de contar con un Sistema de Gestión de Seguridad de la Información.
2	Conocimiento de las políticas de seguridad de la información	Explicar a los trabajadores de la MDEA, en dónde pueden consultar y cuáles son las principales políticas de seguridad de la información.	Charla	45 min.	Sala de reuniones y presentación de diapositivas y videos.	Oficial de seguridad de la información	Los participantes podrán identificar que comportamientos de seguridad de la información se consideran correctos e incorrectos.
3	Amenazas informáticas	Explicar a los trabajadores de la MDEA sobre los ataques informáticos más comunes	Charla	40 min.	Sala de reuniones y presentación de diapositivas y videos.	Expositor externo	Los participantes podrán explicar cómo pueden identificar y protegerse de los ataques informáticos más comunes.
4	Respaldo de la información	Explicar a los trabajadores de la MDEA como	Charla	30 min.	Sala de reuniones y	Expositor externo	Los participantes podrán explicar

N°	Tema	Objetivo	Actividad	Tiempo	Recursos	Responsable	Resultados
		guardar su información de su equipo de cómputo.			presentación de diapositivas.		cuáles son los medios correctos para guardar su información.
5	Gestión de incidentes de seguridad	Explicar a los trabajadores de la MDEA cuáles son los procedimientos correctos para gestionar los incidentes de seguridad de la información.	Charla	45 min.	Sala de reuniones y presentación de diapositivas y videos.	Oficial de seguridad de la información	Los participantes podrán explicar cuáles son los procedimientos para reportar incidentes de seguridad de la información.
6	Seguridad en las estaciones de trabajo	Explicar a los trabajadores de la MDEA los procedimientos para la seguridad en sus puestos de trabajo.	Charla	30 min.	Sala de reuniones y presentación de diapositivas y videos.	Oficial de seguridad de la información	Los participantes podrán explicar cuáles son las acciones a seguir para proteger sus estaciones de trabajo.

6.1. Mensajes propuestos de concientización en seguridad de la información

1. Tema: Seguridad en las estaciones de trabajo: Escritorio y pantalla limpia

Mensaje: Bloquea tu sesión cuando dejes solo tu puesto de trabajo.

2. Tema: Seguridad en las estaciones de trabajo: Contraseñas seguras

Mensaje: Utiliza contraseñas seguras, fáciles de recordar, difíciles de adivinar.

3. Tema: Seguridad en las estaciones de trabajo: Clasificar, ordenar y limpiar
Mensaje: Mantén sobre tu escritorio únicamente los documentos necesarios para la labor a realizar. Ordena tu puesto de trabajo para saber siempre dónde está cada cosa. Archiva documentos innecesarios que ya no utilices.

4. Tema: Amenazas informáticas: Phishing
Mensaje: No hagas click en links de correos sospechosos, ni respondas a correos con invitaciones engañosas.

5. Tema: Procedimientos del SGSI: Áreas seguras (espacio físico donde se almacena o procesa información)

Mensaje: Todo visitante debe estar acompañado de una persona responsable cuando visite un área segura. Cuando no están en uso las áreas seguras deben estar cerradas.

6. Tema: Procedimientos del SGSI: Transferencia de información

Mensaje: Antes de transferir información reservada o pública clasificada de la municipalidad se deben establecer acuerdos para proteger la información.

7. Programa de capacitación

Luego de haber realizado el análisis de las necesidades de la municipalidad, esta tiene la responsabilidad de determinar las competencias necesarias para cada una de las tareas requeridas, evaluar las competencias de los trabajadores y desarrollar los planes para aminorar las brechas existentes.

Es por ello que se debe formar y capacitar al personal en temas de seguridad de la información, para lo cual se desarrolló el plan de capacitación, que se puede apreciar en la tabla 73.

Tabla 73.

Plan de capacitación

N°	Nombre	Objetivo	Actividad	Tiempo	Dirigido a:
1	Gestión de seguridad de la información	Conocer los conceptos y principios de seguridad de la información propuestos por la norma ISO/IEC 27001:2013	Taller	24 hrs.	Gerente de TI
2	Formación de Auditor Líder ISO 27001:2013	Desarrollar habilidades y destrezas para planificar, ejecutar y evaluar una auditoria interna/externa de la norma ISO/IEC 27001:2013	Curso	48 hrs.	Oficial de seguridad de la información
3	Plan de continuidad del negocio (BCP)	Conocer y organizar el proceso de implementación de un plan de continuidad del negocio que se debe seguir para la protección efectiva de la información, personal y recursos en casos de un desastre.	Curso	24 hrs.	Gerente de TI

Nota: Elaboración propia

8. Glosario

Concientización. - Es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.

Ejemplo: Uso correcto de contraseñas, consecuencias reales sobre prestar una contraseña y que hacer sino recuerda la contraseña.

Entrenamiento. - Proceso utilizado para enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas a su cargo. Ejemplo: Un curso de seguridad de la información enfocado en la administración de riesgos.

Ingeniería social. – Tipo de ataque de seguridad en la cual un individuo manipula al otro con el fin de obtener información que puede ser utilizada para acceder a un sistema no autorizado, sustraer dinero o incluso suplantar la identidad de la víctima.

Es un método basado en el engaño y la persuasión que puede llevarse a cabo a través de canales tecnológicos o bien en persona, y que se utiliza para obtener información significativa o lograr que la víctima realice un determinado acto. Un ejemplo de la aplicación de esta técnica es el phishing.

Phishing. - Del inglés fishing: pesca. Fraude informático efectuado a través de una comunicación electrónica. Es un proceso fraudulento de la rama de la social cuyo objetivo es adquirir información sensible, como nombres de usuarios, contraseñas y números de tarjetas de crédito.

Política. - Declaraciones de alto nivel que expresan los objetivos a cumplir de la entidad respecto a algún tema en particular.

9. Anexo

Anexo 11 – Manual del Sistema de Gestión de Seguridad de la Información

MANUAL		Código: PS-001
			Versión: 0.1
	Sistema de Gestión de Seguridad de la Información		Fecha: 30/01/2020
			Autor: Lisbet Monteza

MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Elaborado por: Lisbet Monteza Mera	Revisado por: Ing. Roger Chuctaya Yauri	Aprobado por: Víctor Salcedo Ríos
Especialista en SI	Subgerente de TI	Alcalde

1. Introducción

La Municipalidad Distrital de El Agustino reconoce que la información es uno de los activos más importantes y críticos para el desarrollo de sus funciones. Dado que, en la gestión de los procesos estratégicos, misionales y de soporte, constantemente se está procesando, gestionando, almacenando, transfiriendo e intercambiando valiosa información que debe ser protegida. Es así que la entidad ve la necesidad de implementar un Sistema de Gestión de Seguridad de la Información para establecer los mecanismos y asegurar la confidencialidad, integridad y disponibilidad de la información que se maneja. Asimismo, lograr garantizar que los riesgos de la seguridad sobre los activos de información sean conocidos, gestionados y minimizados.

Para ello, la entidad ha adoptado los lineamientos de la norma ISO/IEC 27001:2013, la cual establece los requisitos para la implementación del SGSI, la norma ISO/IEC 31000:2018 como esquema para la gestión de riesgos y la ISO/IEC 27002 para la selección de los controles.

Es así que en este documento se presentan las políticas, lineamientos y normas de seguridad de la información definidas por la municipalidad y se convierten en la base para la implementación de los estándares, procedimientos, instructivos y controles que deberán ser implementados.

2. Objetivo

El presente manual tiene como objetivo dar a conocer los lineamientos y acciones a seguir para la posterior implementación del Sistema de Gestión de Seguridad de la Información de la municipalidad.

3. Alcance

Cumplir con los pilares de seguridad de la información, preservando la confidencialidad, integridad y disponibilidad de la información que se maneja en el área de rentas.

4. Normas aplicables

- ISO/IEC 27001:2013
- ISO/IEC 27002:2013
- ISO/IEC 31000:2018

- NTP-ISO/IEC 27001:2014

5. Términos y definiciones

Los términos relacionados a continuación están basados y referenciados para efectos del Sistema de Gestión de Seguridad de la Información, ya que muchos de ellos son citados directamente de la norma ISO/IEC 27001:2013. Estos términos permitirán una mayor comprensión del presente manual.

Activo de información. - En relación con la seguridad de la información, es cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, personas, edificios, etc.) que tenga valor para la organización.

Amenaza. - Causa potencial de un incidente no deseado que puede provocar daños a un sistema o a la organización.

Análisis de riesgo. - Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Confidencialidad. - Propiedad que determina que la información no está disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Disponibilidad. - Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Gestión de riesgos. - Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y tratamiento del riesgo.

Impacto. - Cambio adverso en el nivel de los objetivos del negocio logrado.

Integridad. - Propiedad de la información relativa a su exactitud y completitud.

Probabilidad. - Frecuencia o factibilidad de ocurrencia del riesgo.

Riesgo. - Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Seguridad de la información. - Preservación de la confidencialidad, integridad y disponibilidad de la información.

SGSI. - Sistema de Gestión de Seguridad de la Información.

6. Sistema de gestión de seguridad de la información

6.1. Visión general

La municipalidad al tener en cuenta la gran dependencia sobre sus sistemas de información y la información que maneja propia y de los contribuyentes, ha decidido adoptar un Sistema de Gestión de Seguridad de la Información bajo los lineamientos de la norma internacional ISO/IEC 27001:2013. Además, con el fin de dar cumplimiento a la Resolución Ministerial 004-2016-PCM que declara el uso obligatorio de la NTP-ISO/IEC 27001:2014.

6.2. Alcance

El alcance del Sistema de Gestión de Seguridad de la Información es al proceso de recaudación y fiscalización tributaria perteneciente al área de rentas, que abarca siguientes sub-procesos:

- Determinar las obligaciones tributarias.
- Verificar cumplimiento de obligaciones tributarias.
- Cobranza de obligaciones tributarias.
- Ejecutar incremento o disminución de valores tributarios.
- Emitir las notificaciones de pago de tributos.

6.3. Objetivos

- Proteger, conservar y asegurar la información de la MDEA y las herramientas tecnológicas utilizadas para su generación, procesamiento y disposición, con el fin de preservar la confidencialidad, integridad y disponibilidad frente a amenazas internas o externas, deliberadas o accidentales.
- Implementar y fortalecer los controles para la protección de los activos críticos.
- Educar y concientizar al personal para lograr servidores públicos competentes y comprometidos con una cultura de seguridad de la información reflejada en la aceptación y aplicación de las directrices de seguridad.
- Implementar una metodología de gestión de riesgos de seguridad de la información como herramienta para actuar proactivamente ante la presencia de situaciones que puedan afectar la continuidad, confidencialidad e integridad de la información de la MDEA.

6.4. Política de alto nivel del SGSI

En el Sistema de Gestión de Seguridad de la Información se ha definido una política de seguridad de la información el cual se expone a continuación:

POLÍTICA DEL SGSI

La Municipalidad Distrital de El Agustino (MDEA) en cumplimiento con su misión, visión y valores, comprometido con la mejora de sus procesos y generando valor económico, social y ambiental para el desarrollo del distrito, establece el diseño e implementación del Sistema de Gestión de Seguridad de la Información (SGSI) y se compromete a:

- *Proteger los activos de información frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información.*
- *Proporcionar los recursos necesarios para asegurar la implementación de las medidas de control necesarias para evitar que los riesgos de la seguridad de la información se materialicen.*
- *Mejorar el nivel de conciencia de seguridad de la información en los funcionarios, colaboradores, y contribuyentes de los servicios de la entidad.*
- *Mejorar continuamente la eficacia del SGSI a fin de minimizar constantemente los riesgos de seguridad de la información.*
- *Cumplir con los requisitos legales y regulatorios que afectan a la entidad respecto a la seguridad de la información.*

Aplicabilidad de la política del SGSI

Esta política aplica a toda la entidad, sus trabajadores, proveedores, terceros y demás partes interesadas.

6.5. Gestión de riesgos

La municipalidad aplica una metodología basada en la norma ISO/IEC 31000:2018 para la evaluación del riesgo de seguridad de la información, esta metodología tiene las siguientes fases:

- Identificación del riesgo

- Identificación de activos
- Clasificación de activos
- Valoración de activos
- Identificación de amenazas y vulnerabilidades
- Análisis del riesgo
- Evaluación del riesgo
- Tratamiento del riesgo

6.6. Criterios para la evaluación de riesgos

La municipalidad toma en cuenta las siguientes consideraciones para la evaluación de los riesgos sobre los activos de información:

- La identificación de los riesgos se hará en base al juicio de expertos, es decir el personal que está involucrado en el proceso donde interviene cada activo de información valorizado.
- Personal calificado en seguridad de la información, lo cual da una visión global de los riesgos inminentes sobre los activos de información.
- Documentación y buenas prácticas usadas en el mercado sobre los riesgos de información sobre activos de información. Ello creara conciencia en cuanto a los riesgos que puedan estar sujetos los activos de información y qué medidas adoptar en primera instancia.

Por otro lado, la valoración del riesgo sobre el activo de información se muestra a continuación en la tabla 1.

Tabla 1
Valoración del riesgo

Nivel	Rango	Descripción
Bajo	[1 - 8]	Totalmente tolerable
Medio	[9 - 14]	Regularmente tolerable
Alto	[15 - 25]	No tolerable

Elaboración propia

6.7. Opciones de tratamiento de riesgo

Las opciones de tratamiento de riesgo son:

Tabla 2
Opciones de tratamiento de riesgo

Tratamiento	Descripción
Aceptar	Es reconocer y asumir las consecuencias del riesgo sin tomar ninguna medida, a menos que el riesgo se materialice.
Transferir	Es trasladar el impacto o consecuencia del riesgo a un tercero, junto con la responsabilidad.
Reducir	Es actuar para reducir la probabilidad de ocurrencia o el impacto de un riesgo, a través de la selección e implementación de controles.
Evitar	Es no iniciar o no continuar con la actividad que motiva el riesgo. Por ejemplo: cambiar el objetivo que se encuentra amenazado, reducir el alcance, etc.

Elaboración propia

6.8. Plan de tratamiento de riesgo

Las opciones de tratamiento de riesgo adoptada por la municipalidad

Luego de haber efectuado el análisis de riesgos sobre los activos de información el Comité de Gestión de Seguridad de la Información (CGSI), el Oficial de Seguridad de la Información y el área involucrada sobre el riesgo del activo de información deberán reunirse y efectuar un plan de tratamiento de riesgos para los riesgos considerados como “Regularmente tolerable” y/o “No tolerable”. Es así que el plan de tratamiento de riesgo – PTR, tendrá el formato que se muestra en la tabla 3.

Tabla 3:
Encabezado del plan de tratamiento de riesgo

Nº	Activo o grupo de activo	Id Riesgo	Descripción del Riesgo	Nivel del Riesgo	Apetito del riesgo	Tratamiento	Cláusula anexo A ISO/IEC 27001:2013	Controles ISO/IEC 27002:2013	Comentario de la aplicación del control	Responsable del control
----	--------------------------	-----------	------------------------	------------------	--------------------	-------------	-------------------------------------	------------------------------	---	-------------------------

Elaboración propia

6.9. Declaración de Aplicabilidad

La Declaración de Aplicabilidad o SOA (Statement of Applicability) es un documento basado en el anexo A de la norma ISO/IEC 27001:2013 que contiene los 114 controles en

los 14 dominios. A través del SOA la entidad identifica los controles que serán implementados como parte del SGSI y sus excepciones.

La declaración de Aplicabilidad del Sistema de Gestión de Seguridad de la Información de la organización se encuentra dentro del presente proyecto en el anexo 9.

7. Políticas del Sistema de Gestión de Seguridad de la Información

Las políticas que conciernen al SGSI son de cumplimiento obligatorio para todo el personal de la entidad. Estas tienen el propósito de establecer las acciones necesarias para la protección de la información. Las políticas específicas son:

- Política de gestión de accesos
- Política de gestión de contraseñas
- Política de escritorio y pantalla limpia
- Política de gestión de incidentes de seguridad
- Política de gestión de activos
- Política de seguridad de las operaciones

8. Incumplimiento

El incumplimiento de lo indicado en el presente manual del SGSI tendrá como resultado la aplicación de diversas sanciones de acuerdo al reglamento interno de la municipalidad, que serán aplicadas conforme a la naturaleza y gravedad del aspecto no cumplido.

Anexo 12 – Políticas específicas

Código: PS01
	Versión 1.0
	Autor: Lisbet Monteza Mera
	Fecha: 20/01/2020
Política de gestión de accesos	

1. Resumen

El presente documento contiene una serie de lineamientos para garantizar un adecuado uso y control de acceso a los sistemas de información de la entidad, sus activos de información, el manejo de los usuarios y el monitoreo que se debe tener de estos.

2. Objetivo

Controlar el acceso a la información, definir y detallar el uso adecuado de los sistemas de información para impedir el acceso no autorizado a los sistemas de información de la entidad.

3. Alcance

Esta política se aplica a toda la información proveída por la entidad, ya sea a través de documentos físicos, carpetas compartidas, base de datos, aplicaciones, entre otros; además, para la alta gerencia, gerentes de área y empleados en general que administran y hacen uso de estas.

4. Política

Se ha establecido la siguiente política para la seguridad de la información:

4.1. Administración de usuarios

- Las cuentas de usuario que no hayan sido utilizadas en los últimos noventa días serán inhabilitadas por el área de TI. Pasado los dos años de una cuenta inhabilitada, de debe proceder a su eliminación.

- Cada personal de la MDEA (funcionarios, CAS, locadores de servicios y otros) tendrá una cuenta de usuario y contraseña única de identificación, quien será responsable de todo registro a su nombre.
- El nivel de acceso a un sistema de información se otorgará de acuerdo a:
 - Clasificación de la información.
 - Funciones del usuario.
 - Perfiles de acceso estandarizados.
 - Pedido, autorización y administración de acceso.
 - Revisión periódica.
 - Retiro y modificación de derechos de acceso.
- Está prohibido intentar ingresar a la infraestructura tecnológica con la cuenta de usuario de otro empleado de la MDEA.
- La creación, eliminación y revisión de privilegios de los usuarios de red y las aplicaciones de la MDEA deberán ser revisados regularmente según actividades programadas de la subgerencia de TI.
- Los sistemas de información, según su criticidad y uso, deberían desconectar automáticamente las sesiones de conexión tras un periodo definido de inactividad que sea configurable por cada sistema.

4.2. Contraseñas

- Cada personal de la MDEA (funcionarios, CAS, locadores de servicios y otros) deben tener una contraseña asociada que cumpla con las características de contraseñas seguras.
- La MDEA mantendrá definido para todos sus sistemas de información un esquema de construcción de contraseñas fuertes que debe ser cumplida por todo el personal.
- Es responsabilidad del personal de la MDEA (funcionarios, CAS, locadores de servicios y otros) y demás personas el velar por la confidencialidad y buen uso de su contraseña.
- No se deben almacenar contraseñas en formato legible en archivos tipo “batch”, scripts de logon automáticos, macros de software, teclas de función de terminales, computadores sin control de acceso, archivos de texto o en sitios donde personas no autorizadas puedan descubrirlos y utilizarlos.

4.3. Controles de acceso de red

- El personal de la MDEA (funcionarios, CAS, locadores de servicios y otros) y demás personas no tendrán acceso de escritura a los datos de producción por fuera de los sistemas de información, a excepción del administrador de base de datos.
- Ningún personal que trabaje en la subgerencia de TI tendrá acceso a los datos de producción, en modalidad diferente a la de consulta, a excepción del administrador de base de datos, a menos que se realice una solicitud expresa y autorización del subgerente de TI.
- La subgerencia de TI garantizará a la entidad que el personal de la MDEA (funcionarios, CAS, locadores de servicios y otros) y demás personas reportadas como ausentes por motivo de vacaciones, licencias, finalización de servicio, etc., no podrán tener acceso a la red interna de la entidad, a menos que se justifique y se realice por expresa solicitud y autorización del responsable de la subgerencia de TI.

4.4. Control de acceso a aplicaciones

- Las aplicaciones incluirán un adecuado control de acceso basado en el análisis de las funciones que la aplicación tienen desarrolladas y las autorizaciones por grupos de usuarios, roles y perfiles.

5. Roles y responsabilidades

Los roles y responsabilidades están definidas en el punto 6 de la Política de Seguridad de la Información, anexo 4.

6. Sanciones

Las sanciones aplicables son las definidas en el punto 9 de la Política General de Seguridad de la Información, anexo 4.

Código: PS01
	Versión 1.0
	Autor: Lisbet Monteza Mera
	Fecha: 20/01/2020
Política de gestión de contraseñas	

1. Resumen

El presente documento contiene una serie de lineamientos que tienen que usarse como requisito mínimo en la gestión de contraseñas.

2. Objetivo

Evitar el acceso sin autorización a los sistemas de información de la MDEA.

3. Alcance

Esta política incluye a todas las cuentas de usuarios que acceden al dominio de la MDEA, tal como el inicio de sesión en los sistemas operativos, cuentas de correo, aplicativos entre otros.

4. Política

- Las contraseñas de las cuentas de usuario deben cambiarse cada sesenta días y evitar la reutilización de las últimas 10 contraseñas, para lo cual la subgerencia de TI debe realizar las configuraciones respectivas.
- Las contraseñas deben tener cierto grado de complejidad y no contener nombres, apellidos, fechas de nacimiento, números telefónicos, ni cualquier otro tipo de información pública y/o personal del usuario.
- El usuario debe crear una contraseña que cumpla con las características de seguridad: Longitud mínima de 08 caracteres e incluso letras (mayúsculas y minúsculas), números y caracteres especiales.
- No usar la característica de “recordar contraseña” presente en los navegadores de internet.
- Las contraseñas de diferentes sistemas de información no deben ser iguales.

5. Roles y responsabilidades

Los roles y responsabilidades están definidas en el punto 6 de la Política de Seguridad de la Información, anexo 4.

6. Sanciones

Las sanciones aplicables son las definidas en el punto 9 de la Política General de Seguridad de la Información, anexo 4.

Código: PS01
	Versión 1.0
	Autor: Lisbet Monteza Mera
	Fecha: 20/01/2020
Política de escritorio y pantalla limpia	

1. Resumen

El presente documento contiene la política de escritorio limpio, que asegure que todos los documentos e información confidencial no estén visibles ni sean manipulados por un tercero cuando el trabajador no se encuentra en su área de trabajo.

2. Objetivo

Definir los lineamientos para mejorar la protección de la información almacenada en los puestos de trabajo y en el computador; y que esta sea visualizada y modificada solo por personal autorizado.

3. Alcance

Esta política incluye a todos los empleados de la MDEA.

4. Política

- La información crítica impresa o almacenada de manera electrónica debe estar protegida de accesos no autorizados, especialmente cuando no estén en uso.
- Se debe bloquear la computadora al momento de ausentarse de su estación de trabajo y al final del día deben ser apagados.
- Todo usuario debe desconectarse de las aplicaciones o de servicios de red cuando no sea necesario.
- Una vez finalizada su jornada de trabajo, los usuarios no deberán dejar hojas o papeles de trabajo sobre los escritorios. Asimismo, no deberán dejar medios de almacenamiento donde se pueda obtener información de la entidad.
- Las llaves de las gavetas del escritorio o de los estantes no deben ser descuidadas en ningún momento por el trabajador.

- Los documentos sensibles que sean desechados, deben ser debidamente destruidos sin la posibilidad de una posible reconstrucción.
- Está prohibido dejar papeles, sticker pegados en la pantalla o en lugares de fácil acceso en la cual se encuentre información de inicio de sesión o contraseñas de acceso a los sistemas de información, la cual puede ser observada o manipulada por terceras personas.

5. Roles y responsabilidades

Los roles y responsabilidades están definidas en el punto 6 de la Política de Seguridad de la Información, anexo 4.

6. Sanciones

Las sanciones aplicables son las definidas en el punto 9 de la Política General de Seguridad de la Información, anexo 4.

Código: PS01
	Versión 1.0
	Autor: Lisbet Monteza Mera
	Fecha: 20/01/2020
Política de gestión de incidentes de seguridad	

1. Resumen

El presente documento contiene los lineamientos para el correcto manejo y administración de los incidentes de seguridad sobre los activos de información. Además, constituye un documento útil para los trabajadores de la entidad para la toma de acciones sobre incidentes de seguridad.

2. Objetivo

Prevenir y limitar el impacto de la materialización de alguna amenaza sobre los activos de información de la entidad.

3. Alcance

Esta política incluye a todos los trabajadores de la entidad.

4. Política

- Todo trabajador de la entidad tiene la responsabilidad de comunicar algún incidente de seguridad que sea de su conocimiento, a su jefatura inmediata y a los responsables de la seguridad de la municipalidad.
- La entidad analizará los eventos de seguridad asociados a los activos de información a fin de revisar, evidenciar y/o determinar que se trata de un incidente de seguridad de la información. Los procedimientos y plan de respuesta deben ser determinados por los responsables de seguridad.
- Se debe establecer procedimientos para incidentes de seguridad y establecer las coordinaciones necesarias con instituciones como bomberos, PNP, servicios médicos, entre otros según corresponda.
- Los responsables de seguridad deben registrar todos los incidentes de seguridad de la información, detallando:
 - Nombre de activo afectado.

- Detalle del incidente de seguridad.
 - Riesgo asociado al incidente.
 - Controles asociados al incidente.
 - Comportamiento de los controles durante el incidente.
 - Impacto financiero, legal y de imagen el incidente.
 - Planes de acción.
- Los incidentes graves de seguridad deben ser informados a todas las gerencias de la entidad, informando el evento, el impacto hacia municipalidad y los planes de acción.
 - Una vez superado el incidente, se debe monitorear los controles asociados al incidente de seguridad, para determinar la efectividad del control y establecer si se realizó el cumplimiento de este.
 - Luego de superado el incidente, se debe determinar si es un riesgo nuevo y conocido. Si es nuevo, se debe proceder a realizar una evaluación del riesgo. Si es un riesgo conocido, se debe analizar si está dentro del apetito del riesgo o necesita ser clasificado nuevamente aumentando o disminuyendo su impacto.

5. Roles y responsabilidades

Los roles y responsabilidades están definidas en el punto 6 de la Política de Seguridad de la Información, anexo 4.

6. Sanciones

Las sanciones aplicables son las definidas en el punto 9 de la Política General de Seguridad de la Información, anexo 4.

Código: PS01
	Versión 1.0
	Autor: Lisbet Monteza Mera
	Fecha: 20/01/2020
Política de gestión de activos	

1. Resumen

El presente documento contiene los lineamientos a seguir para la gestión de activos de información de la entidad previniendo su pérdida de confidencialidad, integridad y disponibilidad.

2. Objetivo

Lograr y mantener la protección adecuada de los activos de información, asignando esto a los usuarios finales que sean responsables de administrarlos de acuerdo a sus funciones y roles.

3. Alcance

Esta política incluye a todos los trabajadores de la entidad.

4. Política

4.1. Seguridad de información digital

- Los activos de información pertenecientes a la entidad deben utilizarse exclusivamente para propósitos laborales.
- La entidad deberá proporcionar al usuario los equipos informáticos (con los sistemas de información o aplicativos instalados) y la información creada, almacenada y recibida será propiedad de la entidad. Los empleados solo podrán realizar respaldos de información pública y de archivos personales, de ser necesario copiar cualquier tipo de información clasificada o reservada se solicitará autorización al jefe inmediato; de acuerdo a las normas de clasificación de la información de los niveles de seguridad establecidos por la entidad. La sustracción, daño intencional, copia o utilización para fines distintos a las labores propias de la entidad será sancionada de acuerdo con las normas y legislación vigente.

- Los usuarios deben utilizar únicamente los programas y equipos acreditados por la subgerencia de TI.
- La subgerencia de TI, periódicamente llevara a cabo revisiones de los programas utilizados en cada equipo. La descarga, instalación o uso indebido de aplicativos no autorizados se considera como una falta a las Políticas de Seguridad de la Información de la MDEA.
- Los medios removibles deben ser inhabilitados en todos los equipos de la entidad. Si se necesita el uso de algún medio removible, debe ser solicitado a la subgerencia de TI con su respectiva justificación.
- Los usuarios no deben hacer mal uso de los equipos informáticos, enviar correos electrónicos masivos con fines no laborables y práctica de juegos en línea.
- Está prohibido el uso de correos personales.
- Para evitar comprometer información de forma accidental, se debe tener en cuenta:
 - Evitar abrir correos sospechosos o de destinatarios desconocidos.
 - Bloquear la pantalla de la computadora cuando no se encuentre en su área de trabajo.
 - Eliminar completamente documentación digital.
- El usuario será responsable de todas las transacciones o acciones efectuadas con su “cuenta de usuario”.
- Ningún usuario deberá acceder a la red o a los servicios de tecnología de la información de la entidad usando otra cuenta de usuario.
- Cada usuario será responsable de asegurar que el uso de internet no comprometa la seguridad de los recursos informáticos. La subgerencia de TI será la responsable de realizar el aseguramiento de los accesos a internet.
- Todo archivo descargado de internet deberá ser revisado para detección de virus y otros programas destructivos antes de ser instalados en los equipos de la entidad.
- Se debe respaldar periódicamente la información de la entidad, debiendo ser almacenada en lugares apropiados donde se pueda garantizar que la información está segura y pueda ser recuperada en caso de un desastre o de incidentes con los equipos de procesamiento.
- El lugar donde se almacena la información digital debe tener un mantenimiento de mínimo una vez cada seis meses.

5. Roles y responsabilidades

Los roles y responsabilidades están definidas en el punto 6 de la Política de Seguridad de la Información, anexo 4.

6. Sanciones

Las sanciones aplicables son las definidas en el punto 9 de la Política General de Seguridad de la Información, anexo 4.

Código: PS01
	Versión 1.0
	Autor: Lisbet Monteza Mera
	Fecha: 20/01/2020
Política de seguridad de las operaciones	

1. Resumen

El presente documento contiene una serie de lineamientos a seguir para una correcta gestión de las operaciones de instalaciones de la información.

2. Objetivo

Asegurar que las operaciones realizadas en la entidad sean correctas y seguras.

3. Alcance

Esta política incluye a todos los trabajadores de la entidad.

4. Política

4.1. Procedimientos y responsabilidades operativas

- Todos los procedimientos operativos, estarán documentados adecuadamente, actualizados y a disponibilidad de los usuarios a quienes compete.
- Cualquier cambio a la plataforma tecnológica de la entidad debe ser documentado y controlado por la subgerencia de TI.
- El estándar de configuración base para los equipos de cómputo sobre hardware y software es establecido por la subgerencia de TI, de acuerdo a los requerimientos del negocio y a los avances tecnológicos del mercado. Toda instalación de hardware y software solo lo realiza personal autorizado de la subgerencia de TI, quienes deben llevar un control estricto del número de licencias adquiridas por producto.
- Los usuarios de los equipos no tendrán ningún privilegio administrativo sobre el equipo asignado. Solo personal autorizado por la subgerencia de TI tendrán privilegios especiales sobre los equipos para brindar el soporte, configuración e instalación de hardware y software.

- Está prohibido el almacenamiento en el disco duro de archivos no relacionados a la entidad, como son: archivos de música, videos, juegos, protectores de pantalla, fotos, etc.
- La subgerencia de TI debe realizar estudios de proyecciones de crecimiento de los recursos (procesadores, discos duros, memorias, ancho de banda, tráfico de red, etc.) a fin de asegurar el desempeño y capacidad de la plataforma tecnológica.

4.2. Protección contra software malicioso

- Contar con un sistema de seguridad perimetral que permita prevenir, detectar y corregir intrusiones o intentos de ingreso no autorizado, el cual será administrado por la subgerencia de TI.
- La subgerencia de TI debe instalar antivirus a nivel de toda la red de la entidad para prevenir infecciones de cualquier virus.
- Todo usuario que detecte la presencia de virus debe informar a la subgerencia de TI, quienes serán los encargados de evaluar y eliminar el virus.

4.3. Respaldo de la información

- Se realizarán copias de seguridad de la base de datos un mínimo de 1 vez a la semana,
- Las copias de seguridad deben ser realizadas de manera automática y no manual, guardando versiones por fechas y no reemplazándolas en cada copia.
- Si se desea realizar una restauración parcial o completa de la información, esta debe ser solicitada a su jefatura inmediata o a los encargados de seguridad.
- Toda copia de respaldo debe estar debidamente encriptada.

5. Roles y responsabilidades

Los roles y responsabilidades están definidas en el punto 6 de la Política de Seguridad de la Información, anexo 4.

6. Sanciones

Las sanciones aplicables son las definidas en el punto 9 de la Política General de Seguridad de la Información, anexo 4.

Anexo 13 – Diagrama Tortuga

MUNICIPALIDAD DISTRITAL DE EL AGUSTINO

ENCUESTA ÁREA DE RENTAS

Instrucciones:

Para desarrollar este cuestionario, usted debe leer cada pregunta y escoger una de las alternativas propuestas con una “X” dentro de los paréntesis.

1. ¿En la MDEA existe un sistema de gestión de seguridad de la información?
Si () No ()
2. ¿Cree usted que el diseño e implementación de un sistema de gestión seguridad de la información permitirá mejorar la seguridad de información de su área de trabajo?
Si () No ()
3. ¿Cree usted que en su área de trabajo se logrará un cambio positivo con la aplicación de un sistema de gestión de seguridad de la información?
Si () No ()
4. ¿Aprobaría usted la implementación del sistema de gestión de la seguridad de la información en su área de trabajo?
Si () No ()
5. ¿Aprobaría usted programas dirigidos a todos los empleados para sensibilizar sobre la seguridad de la información en su área de trabajo?
Si () No ()
6. ¿Considera usted que en su área de trabajo existe información que debe ser protegida?
Si () No ()
7. ¿Ha recibido usted capacitación sobre seguridad de la información de acuerdo a su función laboral?
Si () No ()
8. ¿Cuenta usted con un computador o laptop para realizar sus funciones?
Si () No ()
9. ¿Cuenta usted con un clave de acceso para ingresar a su computador o laptop?
Si () No ()

10. Cuando su computador esta desatendido ¿se activa el bloqueo de pantalla con contraseña para proteger la información?
Si () No ()
11. ¿En lo que va del año ha sufrido modificación o pérdida de información ya sea por virus, acceso de personas no autorizadas, deterioro, extravió, etc.?
Si () No ()
12. ¿En lo que va del año se ha divulgado la información sensible para la MDEA sin su autorización o conocimiento?
Si () No ()
13. ¿Su área de trabajo cuenta con software antivirus actualizado?
Si () No ()
14. ¿Realiza usted copias de seguridad para proteger su información?
Si () No ()
15. ¿Considera que su oficina está protegida contra amenazas externas o ambientales que ocasionan pérdidas de información?
Si () No ()

Resolución Ministerial

N° 004-2016-PCM

Lima, - 8 ENE. 2016

CONSIDERANDO:

Que, mediante Resolución Ministerial N° 246-2007-PCM se aprobó el uso de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª. Edición", en todas las entidades del Sistema Nacional de Informática;

Que, mediante Resolución Ministerial N° 197-2011-PCM, se estableció el plazo para que determinadas entidades de la Administración Pública implementen el Plan de Seguridad de la Información dispuesto en la Norma Técnica Peruana antes señalada; posteriormente, mediante Resolución Ministerial N° 129-2012-PCM se estableció un nuevo cronograma y la incorporación del rol del oficial de seguridad para el proceso de implementación de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008;

Que, la Norma Técnica Peruana "NTP ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos", aprobada mediante Resolución N° 42-2008/INDECOPI-CNB, por la Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias del Instituto Nacional de Defensa de la Competencia y de Protección de la Propiedad Intelectual (INDECOPI) ha sido reemplazada por la nueva versión de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos. 2ª Edición" aprobada por Resolución N° 129-2014/DNB-INDECOPI;

Que, de acuerdo a lo establecido en el numeral 4.8 del artículo 4 y el artículo 49 del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por el Decreto Supremo N° 063-2007-PCM, la Presidencia del Consejo de Ministros actúa como ente rector del Sistema Nacional de Informática a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), siendo ésta la encargada de implementar la Política Nacional de Gobierno Electrónico e Informática;

Que, el "Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0" aprobado mediante Decreto Supremo N° 066-2011-PCM, establece en su Objetivo N° 7, la necesidad de promover una Administración Pública de calidad orientada a la población, determinando como parte de su Estrategia N° 4, la implementación de mecanismos para mejorar la seguridad de la información, la necesidad de contar con una Estrategia Nacional de Ciberseguridad con el objetivo de minimizar los riesgos en caso de sufrir algún tipo de incidente en los recursos informáticos del Estado, así como, la disuasión del crimen cibernético, que se producen mediante el uso de redes teleinformáticas, entre otros;

Que, la actual Política Nacional de Gobierno Electrónico 2013 – 2017, aprobada mediante el Decreto Supremo N° 081-2013-PCM, prevé determinados Lineamientos

Estratégicos para el Gobierno Electrónico en el Perú, entre otros, el relacionado con la Seguridad de la Información, el mismo que busca velar por la integridad, seguridad y disponibilidad de los datos debiendo establecerse lineamientos de seguridad de la información a fin de mitigar el riesgo de exposición de información sensible del ciudadano, correspondiendo que en uso de las funciones atribuidas al ente rector del Sistema Nacional de Informática, para el caso ONGEI-PCM, a cargo de implementar dicha Política Nacional, articular la implementación efectiva del acotado lineamiento por parte de los distintos entes del sector público;

Que, estando a lo indicado en los considerando precedentes la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros a través del Memorando N° 152-2015-PCM/ONGEI, recomienda la aplicación y uso de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades del Sistema Nacional de Informática, con la finalidad de coadyuvar con la infraestructura de Gobierno Electrónico, por considerar a la seguridad de la información, como un componente crucial para dicho objetivo;

De conformidad con lo dispuesto en la Ley N° 29158, Ley Orgánica del Poder Ejecutivo; la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado; y, el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros aprobado mediante Decreto Supremo N° 063-2007-PCM y sus modificatorias;

SE RESUELVE:

Artículo 1.- De la aprobación

Apruébese el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

Artículo 2.- Publicación

La Norma Técnica Peruana NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición" será publicada en el Portal de la Presidencia del Consejo de Ministros (www.pcm.gob.pe) y en el Portal de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) (www.ongei.gob.pe) el mismo día de la publicación de la presente resolución en el Diario Oficial El Peruano.

Artículo 3.- De la implementación

Las entidades integrantes del Sistema Nacional de Informática, tendrán un plazo máximo de dos (2) años para la implementación y/o adecuación de la presente norma.

Dichas entidades públicas tendrán un plazo de 60 días contados a partir de la fecha de publicación de la presente norma, para la presentación del cronograma de

Resolución Ministerial

implementación y/o adecuación del sistema de gestión de la Seguridad de la Información, que deberá ser presentado a la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros.

La ONGEI brindará asistencia técnica a las entidades que lo requieran. Las entidades públicas que a la fecha cuenten con la certificación ISO 27001, están exoneradas del presente proceso de implementación.

Artículo 4.- De la certificación de la norma

Las entidades que requieran certificarse de acuerdo a lo establecido en la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2 Edición"; podrán realizar dicha certificación de forma opcional y con recursos propios de cada entidad.

Artículo 5.- Del Comité de Gestión de Seguridad de la Información

Cada entidad designará un Comité de Gestión de Seguridad de la Información, conformado por:

- El/la titular de la entidad;
- El/la responsable de administración o quien haga sus veces;
- El/la responsable de planificación o quien haga sus veces;
- El/la responsable del área de informática o quien haga sus veces;
- El/la responsable de área legal o quien haga sus veces y
- El/la oficial de seguridad de la información.

Las funciones del Comité de Gestión de Seguridad de la Información, serán establecidas por cada entidad de acuerdo a la norma que se aprueba mediante el Artículo 1° de la presente Resolución Ministerial.

Artículo 6.- De la responsabilidad de la implementación

La responsabilidad de la implementación de la presente norma será del titular de cada entidad.

Artículo 7.- Déjese sin efecto

Deróguese la Resolución Ministerial N° 129-2012-PCM.

Regístrese, comuníquese y publíquese

PEDRO CATERIANO BELLIDO
Presidente del Consejo de
Ministros

Resolución Ministerial

Lima,

CONSIDERANDO: 20 JUN. 2017

N° 166-2017-PCM

Que, mediante Resolución Ministerial N° 004-2016-PCM se aprobó el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 - Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática;

Que, el Comité de Gestión de Seguridad de la Información debe contar con el liderazgo y compromiso necesario para la implementación de la citada Norma Técnica Peruana, por lo que resulta relevante precisar sus funciones tomando como referencia lo establecido en el numeral 5.1 de la NTP-ISO/IEC 27001:2014 - Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición;

Que, se requiere priorizar la implementación del Sistema de Gestión de Seguridad de la Información en las entidades públicas, sobre todo en sus procesos misionales y de soporte que resulten críticos y relevantes para su operatividad, siendo necesario contar para ello con el rol del Oficial de Seguridad de la Información, como responsable de coordinar la implementación de dicho Sistema, ello con la finalidad de coadyuvar al desarrollo del Gobierno Electrónico y la Digitalización del Estado;

Que, de acuerdo a lo establecido en los artículos 47 y 51 del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado mediante Decreto Supremo N° 022-2017-PCM, la Presidencia del Consejo de Ministros actúa como ente rector del Sistema Nacional de Informática a través de la Secretaría de Gobierno Digital (SEGD), siendo ésta la encargada de formular y proponer normas y estándares para el desarrollo e implementación de la Seguridad de la Información, así como de supervisar su cumplimiento, resulta pertinente modificar el artículo 5 de la Resolución Ministerial N° 004-2016-PCM a fin de que el Comité de Gestión de Seguridad de la Información se encuentre conformado por los funcionarios y/o directivos competentes para la ejecución de sus funciones;

De conformidad con lo dispuesto en la Ley N° 29158, Ley Orgánica del Poder Ejecutivo, y el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros aprobado mediante Decreto Supremo N° 022-2017-PCM;

SE RESUELVE:

Artículo 1.- Modificación del artículo 5 de la Resolución Ministerial N° 004-2016-PCM.

Modifíquese el artículo 5 de la Resolución Ministerial N° 004-2016-PCM, en los términos siguientes:

"Artículo 5.- Del Comité de Gestión de Seguridad de la Información"

Cada entidad designará un Comité de Gestión de Seguridad de la Información, conformado como mínimo por:

- El/la titular de la entidad o su representante.
- El/la responsable de administración o quien haga sus veces;

- El/la responsable de planificación o quien haga sus veces;
- El/la responsable del área de informática o quien haga sus veces;
- El/la responsable de área legal o quien haga sus veces y
- El/la oficial de seguridad de la información."

Artículo 2.- Incorporación del artículo 5-A a la Resolución Ministerial N° 004-2016-PCM.

Incorpórese el artículo 5-A a la Resolución Ministerial N° 004-2016-PCM, conforme al siguiente texto:

"Artículo 5-A.- De las Funciones del Comité de Gestión de Seguridad de la Información

El Comité de Gestión de Seguridad de la Información debe cumplir, como mínimo, las siguientes funciones:

- Proponer la política y objetivos de seguridad de la información alineados con el Plan Estratégico Institucional, con la Política Nacional de Gobierno Electrónico y regulación en el ámbito de seguridad de la información;
- Promover y gestionar la implementación del Sistema de Gestión de Seguridad de la Información;
- Promover la gestión de seguridad de la información en los procesos y cultura organizacional;
- Gestionar la asignación del personal y recursos necesarios para la implementación del Sistema de Gestión de Seguridad de la Información;
- Difundir la importancia de una efectiva gestión de seguridad de la información a las partes interesadas, en conformidad con los requisitos del Sistema de Gestión de Seguridad de la Información;
- Evaluar el desempeño del Sistema de Gestión de Seguridad de la Información;
- Otras funciones que se le asigne en el ámbito de su competencia y aquellas concordantes con la materia."

Artículo 3.- Priorización del Alcance del Sistema de Gestión de Seguridad de la Información

Las entidades comprendidas en el artículo 1 de la Resolución Ministerial N° 004-2016-PCM deben asegurar la implementación del Sistema de Gestión de Seguridad de la Información en su institución, priorizando en el alcance los procesos misionales y aquellos que sean relevantes para su operatividad.

Artículo 4.- Del Oficial de Seguridad de la Información

El Titular de entidad, dentro del plazo de diez (10) días hábiles, contados a partir de la publicación de la presente resolución, debe designar a un Oficial de Seguridad de la Información, quien será responsable de coordinar la implementación del Sistema de Gestión de Seguridad de la Información en la entidad.

Dicha designación debe ser puesta en conocimiento a la Secretaría de Gobierno Digital para las coordinaciones y acciones correspondientes.

Regístrese, comuníquese y publíquese.

FERNANDO ZAVALA LOMBARDI
Presidente del Consejo de Ministros

Anexo 16 – Acta de cierre del proyecto

ACTA DE CIERRE Y ENTREGA DEL PROYECTO			
Versión 1			
1. Información General			
Nombre del Proyecto:	Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para la Municipalidad Distrital de El Agustino	Fecha de entrega:	14/02/2020
Preparado por:	Lisbet Monteza Mera		
Revisado por:	Ing. Roger Arturo Chuctaya Yauri		
Aprobado por:	Víctor Salcedo Ríos		
2. Objetivos			
Objetivo general: Diseñar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para proteger adecuadamente los activos de información asociados al proceso de Recaudación y Fiscalización Tributaria de la Municipalidad Distrital de El Agustino.			
Objetivos específicos: <ul style="list-style-type: none">• Determinar el estado actual de cumplimiento de la MDEA con respecto a los requisitos de la norma ISO/IEC 27001:2013.• Identificar los activos críticos de información del proceso del área de rentas de la municipalidad distrital de El Agustino.• Identificar los riesgos de los activos críticos de información.• Determinar los controles para el plan de tratamiento de riesgo de la seguridad de la información.			
3. Entregables generados por el proyecto			
<ul style="list-style-type: none">• Políticas de Seguridad de la información.• Inventario de activos.• Plan de tratamiento de riesgos.• Declaración de aplicabilidad.• Manual de capacitación y concientización• Manual del SGSI			
4. Logros del proyecto			
Diseñar el SGSI para que la entidad pueda minimizar los riesgos a los que están expuestos los activos críticos de la información.			
5. Beneficiario del proyecto			

Municipalidad Distrital de El Agustino.

6. Comentarios generales

La entidad cuenta con el diseño del Sistema de Gestión de Seguridad de la Información basado en estándares de buenas prácticas, como es la norma ISO/IEC 27001:2013, por lo que se sugiere que establezcan el comité de seguridad de la información y puedan realizar la implementación del sistema en el tiempo más corto a fin de proteger los activos de información asociados del proceso de recaudación y fiscalización tributaria.