UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

FACULTAD DE INGENIERÍA

**PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS DE
INFORMACIÓN**

**Modelo de gestión de riesgos de seguridad de la información para pymes en el
Perú**

TESIS

Para optar el título profesional de Ingeniero de Sistemas de Información

AUTOR(ES)

García Porras, Johari Chris (0000-0003-4677-0214)

Huamani Pastor, Sarita Cecilia (0000-0001-8635-5598)

ASESOR

Chinchay Celada, Milton Enrique (0000-0003-2450-5380)

Lima, 10 de junio de 2019

DEDICATORIA

*Dedicado a nuestras familias quienes nos dieron su apoyo total e incondicional a lo largo
de nuestra carrera universitaria.*

AGRADECIMIENTOS

Agradecemos a nuestro asesor, Milton Chinchay, y a nuestro profesor cliente, Rómulo Lomparte, quienes nos apoyaron durante toda la elaboración de este proyecto.

A Rubén Cerda y al personal de la empresa de productos de arcilla cerámica, quienes fueron de gran apoyo para la implementación de este proyecto.

RESUMEN

Actualmente, toda empresa debería tener el conocimiento de qué tan importante es y cómo debe tratarse la información para su negocio, ya que es uno de sus activos más importante. Lamentablemente, no todas tienen claro su valor, exponiéndose a grandes pérdidas. Según un estudio de EY, el 41% de empresas consideran que poseen probidades mínimas para detectar un ataque sofisticado. El motivo principal son las restricciones presupuestarias y la falta de recursos especializados.

Para proteger la información, las empresas deben determinar su exposición al riesgo, lo recomendable es emplear metodologías, marcos de referencia o estándares de análisis de riesgo de seguridad de la información. Este proyecto consiste en implementar un modelo de gestión de riesgos de seguridad de la información para Pymes, integrando la metodología OCTAVE-S y la norma ISO/IEC 27005. Se abarca el análisis de las metodologías y normas de gestión de riesgos, el diseño del modelo de gestión de riesgos de seguridad de la información, la validación del modelo en una Pyme en el proceso de ventas.

La integración proporciona una identificación oportuna y eficaz de los riesgos del enfoque cualitativo y permite aprovechar los valores identificados para los activos del enfoque cuantitativo. Asimismo, permite identificar los principales riesgos valorizándolos, para luego proceder a un tratamiento de acuerdo a las necesidades de la empresa. Se espera que este modelo ayude en la gestión de riesgos de seguridad de la información dentro de las Pymes, para poder reducir el impacto de riesgos a los que pueden estar expuestas.

Palabras clave: Modelo de Gestión de riesgos; Seguridad de la Información; OCTAVE; ISO/IEC 27005.

Information security risk management model for Peruvian SMEs

ABSTRACT

Nowadays, every company should be aware of the importance and the way business information should be treated since it is one of their most important assets. Unfortunately, not all are sure about their actual value, and so, they may be exposed to large losses. According to EY, 41% of companies consider that they have minimum probabilities to detect a sophisticated attack. The main reason that hinders the effectiveness of information security is due to budgetary restrictions and the lack of specialized resources.

To protect the information, companies must determine their risk exposure, for which it's advisable to use methodologies, reference frameworks or standards for information security risk analysis. This project consists on implementing an information security risk management model for SMEs, integrating the OCTAVE-S methodology and the ISO/IEC 27005 standard. This covers the analysis of methodologies and risk management standards, the design of the information security risk management model, the validation of the model in a SME in the sales process.

This integration provides a timely and effective identification of the risks of the qualitative approach and makes it possible to take advantage of the values identified for the assets of the quantitative approach. Furthermore, this allows identifying the main information security risks by rating and treating them according to the needs of the company. It's expected that this model will help in the management of information security risks within SMEs, in order to reduce the impact of risks to which they may be exposed.

Keywords: Risk Management model, Information Security, OCTAVE, ISO/IEC 27005.

TABLA DE CONTENIDOS

CAPÍTULO 1: DESCRIPCIÓN DEL PROYECTO.....	1
1.1 OBJETIVO DEL PROBLEMA	1
1.2 DOMINIO DEL PROBLEMA.....	1
1.3 PLANTEAMIENTO DE LA SOLUCIÓN	2
1.4 OBJETIVOS DEL PROYECTO	3
1.4.1 Objetivo general	3
1.4.2 Objetivos específicos.....	3
1.5 INDICADORES DE ÉXITO	3
1.6 PLANIFICACIÓN DEL PROYECTO	4
1.6.1 Alcance	4
1.6.2 Plan de gestión del tiempo.....	5
1.6.3 Plan de gestión de recursos humanos	6
1.6.4 Plan de comunicaciones.....	8
1.6.5 Plan de gestión de riesgos.....	11
2 CAPÍTULO 2: STUDENT OUTCOMES.....	13
2.1 STUDENT OUTCOMES (ABET).....	13
2.1.1 Student outcome A: Aplicar conocimientos de matemáticas, ciencias, computación e ingeniería.....	13
2.1.2 Student outcome B: Diseña y conduce experimentos en base al análisis e interpretar los datos	14
2.1.3 Student outcome C: Diseñar sistemas, componentes o procesos para encontrar soluciones en la atención de necesidades teniendo en cuenta restricciones económicas, sociales, políticas, éticas de salud y seguridad y otras propias del entorno empresarial.....	15
2.1.4 Student outcome D: Participar en equipos multidisciplinarios, liderando o desarrollando eficientemente sus tareas con profesionales de diferentes campos o campos de aplicación.....	16
2.1.5 Student outcome E: Identificar, formular y resolver problemas de ingeniería	

2.1.6	Student outcome F: Proponer soluciones de ingeniería con responsabilidad profesional y ética.....	18
2.1.7	Student outcome G: Comunicar oralmente o por escrito ideas o resultados de manera clara y efectiva	20
2.1.8	Student outcome H: Identificar el impacto de las soluciones de ingeniería en el contexto global, económico y del entorno de la sociedad	21
2.1.9	Student outcome I: Reconocer la necesidad de mantener sus conocimientos actualizados	21
2.1.10	Student outcome J: Analizar hechos del mundo contemporáneo identificando el impacto en el desempeño profesional de ingeniería	22
2.1.11	Student outcome K: Utilizar las técnicas, herramientas y metodologías necesarias para la práctica de la ingeniería.....	23
2.1.12	Student outcome J-CAC: Comprende y brinda soporte para el uso, entrega y gestión de información dentro de un entorno de Sistemas de Información.....	24
2.2	COMPETENCIAS WASC	24
2.2.1	Comunicación escrita	25
2.2.2	Comunicación oral.....	26
2.2.3	Ciudadanía	26
2.2.4	Pensamiento innovador.....	28
2.2.5	Pensamiento crítico.....	29
2.2.6	Pensamiento cuantitativo	30
2.2.7	Manejo de la información.....	31
3	CAPÍTULO 3: ESTADO DEL ARTE	32
3.1	REVISIÓN LITERARIA	32
3.2	ESTADO DEL ARTE	32
4	CAPÍTULO 4: MARCO TEÓRICO	43
4.1	SEGURIDAD DE LA INFORMACIÓN	44
4.2	GESTIÓN DE RIESGOS	45
4.2.1	Metodología OCTAVE.....	46
4.2.2	ISO/IEC 27005	52
4.3	CONCEPTOS RELACIONADOS A LA INTEGRACIÓN	54
4.3.1	Activo crítico	54

4.3.2	Amenaza	55
4.3.3	Catálogo de prácticas.....	55
4.3.4	Clases de componentes.....	55
4.3.5	Criterios de evaluación de impacto	55
4.3.6	Criterios de evaluación de probabilidad	55
4.3.7	Estado del semáforo.....	56
4.3.8	Frecuencia anualizada.....	56
4.3.9	Impacto	56
4.3.10	Lista de acción	56
4.3.11	Perfil de amenaza.....	56
4.3.12	Perfil de amenaza genérico.....	57
4.3.13	Prácticas estratégicas	57
4.3.14	Prácticas operativas	57
4.3.15	Prácticas de seguridad	57
4.3.16	Probabilidad.....	58
4.3.17	Puntos de acceso.....	58
4.3.18	Puntos de acceso intermedios	58
4.3.19	Requisitos de seguridad	58
4.3.20	Riesgo	58
4.3.21	Rutas de acceso a la red.....	59
4.3.22	Sistema de interés	59
4.3.23	Tiempo entre eventos.....	59
4.3.24	Ubicación de almacenamiento de datos.....	59
4.3.25	Valor de impacto	59
4.3.26	Valor de probabilidad	59
4.3.27	Vulnerabilidades.....	60
5	CAPÍTULO 5: DESARROLLO DEL PROYECTO.....	60
5.1	METODOLOGÍA DEL PROYECTO.....	60
5.2	ELECCIÓN DE METODOLOGÍA O NORMA	60
5.3	MODELO DE GESTIÓN DE RIESGOS.....	66
5.3.1	Selección de equipo de trabajo	68
5.3.2	Fase 1: Construcción de perfil de amenazas.....	71

5.3.2.1	Proceso 1: Identificar información Organizacional (OCTAVE-S) – Establecimiento del contexto (ISO/IEC 27005)	71
5.3.2.1.1	Actividad P1-1: Establecer criterio de impacto (OCTAVE-S) – Establecimiento del contexto y Comunicación del riesgo (ISO/IEC 27005)	72
5.3.2.1.2	Actividad P1-2: Identificar activos organizacionales (OCTAVE-S) – Identificación del riesgo (Identificación de los activos) y Comunicación del riesgo (ISO/IEC 27005)	76
5.3.2.1.3	Actividad P1-3: Evaluar prácticas organizacionales (OCTAVE-S) – Identificación del riesgo (Identificación de vulnerabilidades) y Comunicación del riesgo (ISO/IEC 27005)	79
5.3.2.2	Proceso 2: Crear perfil de amenaza (OCTAVE-S).....	83
5.3.2.2.1	Actividad P2-1: Seleccionar activos críticos (OCTAVE-S) – Identificación del riesgo (Identificación de los activos) y Comunicación del riesgo (ISO/IEC 27005)	83
5.3.2.2.2	Actividad P2-2: Identificar requerimientos de seguridad para activos críticos (OCTAVE-S) – Identificación del riesgo (Identificación de los activos) y Comunicación de los activos (ISO/IEC 27005)	84
5.3.2.2.3	Actividad P2-3: Identificar amenazas de los activos críticos (OCTAVE-S) – Identificación del riesgo (Identificación de las amenazas e Identificación de las consecuencias) y Comunicación del riesgo (ISO/IEC 27005)	85
5.3.3	Fase 2: Identificar vulnerabilidades de infraestructura.....	88
5.3.3.1	Proceso 3: Examinar la infraestructura computacional en relación a los activos claves	88
5.3.3.1.1	Actividad P3-1: Examinar rutas de acceso (OCTAVE-S) – Identificación del riesgo (Identificación de los activos) y Comunicación del riesgo (ISO/IEC 27005)	88
5.3.3.1.2	Actividad P3-2: Analizar procesos relacionados con tecnología (OCTAVE-S) – Identificación del riesgo (Identificación de los activos, Identificación de controles existentes, Identificación de vulnerabilidades, Identificación de las consecuencias) y Comunicación del riesgo (ISO/IEC 27005)	90
5.3.4	Fase 3: Planes y estrategia de seguridad.....	94
5.3.4.1	Proceso 4: Identificar y analizar riesgos	94
5.3.4.1.1	Actividad P4-1: Evaluar el impacto de las amenazas (OCTAVE-S) –Estimación del riesgo (Evaluación de las consecuencias) y Comunicación del riesgo (ISO/IEC 27005)	94
5.3.4.1.2	Actividad P4-2: Establecer criterios basados en la frecuencia (OCTAVE-S) – Estimación del riesgo (Evaluación de la probabilidad de incidentes) y Comunicación del riesgo (ISO/IEC 27005)	96
5.3.4.1.3	Actividad P4-3: Evaluar probabilidades de amenazas (OCTAVE-S) – Estimación del riesgo (Nivel de estimación del riesgo) y Comunicación del riesgo (ISO/IEC 27005)	97
5.3.4.2	Proceso 5: Desarrollar estrategia de protección y planes de mitigación .	99
5.3.4.2.1	Actividad P5-1: Describir estrategia de protección actual (OCTAVE-S) – Evaluación del riesgo y Comunicación del riesgo (ISO/IEC 27005)	99
5.3.4.2.2	Actividad P5-2: Seleccionar enfoques de mitigación (OCTAVE-S) y calcular riesgo – Evaluación, Tratamiento, Aceptación y Comunicación del riesgo (ISO/IEC 27005).....	104
5.3.4.2.3	Actividad P5-3: Desarrollar plan de mitigación (OCTAVE-S) – Tratamiento, Aceptación y Comunicación del riesgo (ISO/IEC 27005)	109

5.3.4.2.4	Actividad P5-4: Identificar riesgo residual - Tratamiento, Aceptación y Comunicación del riesgo (ISO/IEC 27005).....	111
5.3.4.2.5	Actividad P5-5: Identificar cambios a la estrategia de protección (OCTAVE-S) – Comunicación del riesgo (ISO/IEC 27005).....	113
5.3.4.2.6	Actividad P5-6: Identificar siguientes pasos (OCTAVE-S) – Comunicación del riesgo (ISO/IEC 27005)	115
5.4	VALIDACIÓN DE EXPERTOS.....	116
5.5	IMPACTO ECONÓMICO DEL PROYECTO	118
5.5.1	Costo del proyecto	118
5.5.2	Beneficios del proyecto y recuperación por parte de la empresa	119
5.6	INFORMACIÓN BÁSICA DE LA EMPRESA.....	120
5.7	MODELO A IMPLEMENTAR EN PROCESO DE VENTAS	121
5.8	PLAN DE CONTINUIDAD	122
5.8.1	Post Implementación del modelo	122
5.8.2	Método de adaptabilidad	122
5.8.3	Certificaciones	126
5.9	HOJA DE RUTA	126
5.9.1	Objetivo de los proyectos	128
5.9.2	Beneficios	129
5.9.3	Lista de prioridad de implementación del proyecto	130
5.9.4	Plan de migración orientado en el tiempo	132
5.9.4.1	Plan de migración	132
5.9.4.2	Beneficios de la migración	132
5.9.4.3	Costo estimado de la migración.....	133
5.9.5	Recomendaciones en la implementación.....	136
5.9.5.1	Criterios de efectividad de los proyectos.....	136
5.9.5.2	Riesgos y problemas	137
6	CAPÍTULO 6: RESULTADOS DEL PROYECTO.....	137
6.1	RESULTADOS DEL PROYECTO 2017.....	137
6.1.1	Selección de equipo de trabajo	137
6.1.2	Fase 1: Construcción perfiles de amenaza.....	137
6.1.3	Fase 2: Identificar vulnerabilidades de infraestructura.....	151
6.1.4	Fase 3: Desarrollar estrategias y planes de seguridad	154
6.2	RESULTADOS DEL PROYECTO 2018.....	170

6.2.1	Selección de equipo de trabajo	170
6.2.2	Fase 1: Construcción perfiles de amenaza.....	170
6.2.3	Fase 2: Identificar vulnerabilidades de infraestructura.....	176
6.2.4	Fase 3: Desarrollar estrategias y planes de seguridad	177
6.3	COMPARATIVA DE RIESGO SEGÚN EL AÑO 2017 Y 2018.....	196
7	CAPÍTULO 7: GESTIÓN DEL PROYECTO.....	197
7.1	PRODUCTO FINAL.....	197
7.2	GESTIÓN DEL PROYECTO.....	197
7.2.1	Gestión del tiempo.....	197
7.2.2	Gestión de los Recursos Humanos	199
7.2.3	Gestión de las Comunicaciones	199
7.2.4	Gestión de los Riesgos.....	200
7.2.5	Lecciones aprendidas.....	202
8	CONCLUSIONES	203
9	RECOMENDACIONES	204
10	REFERENCIAS.....	204

ÍNDICE DE TABLAS

Tabla 1 Plan de Gestión del Tiempo - Fases e Hitos del Proyecto.....	5
Tabla 2 Plan de Gestión de Riesgos - Tabla de riesgos.....	9
Tabla 3 Plan de Gestión de Riesgos - Tabla de riesgos.....	12
Tabla 4 Tipos de incidentes reportados	34
Tabla 5 Estudios con enfoque cualitativo.....	35
Tabla 6 Estudios con enfoque cuantitativo.....	37
Tabla 7 Estudios con enfoque híbrido	38
Tabla 8 Marco de comparación de metodologías de análisis de riesgo.....	41
Tabla 9 Comparativo de marcos de referencia de gestión de riesgos de seguridad de la información.....	43
Tabla 10 OCTAVE-S – Procesos y actividades de la fase 1	49
Tabla 11 OCTAVE-S – Procesos y actividades de la fase 2	50
Tabla 12 OCTAVE-S – Procesos y actividades de la fase 3	51
Tabla 13 Costo del proyecto	119
Tabla 14 Beneficios.....	119
Tabla 15 Retorno de inversión y tiempo de recuperación	120
Tabla 16 Ciclo PDCA - Post Implementación del modelo.....	122
Tabla 17 Lista de proyectos.....	126
Tabla 18 Lista de prioridad de implementación del proyecto	130
Tabla 19 Tabla de costo estimado de herramienta automatizada	133
Tabla 20 Tabla de costo estimado de Monitoreo de controles	133
Tabla 21 Tabla de costo estimado del tablero	134
Tabla 22 Tabla de costo estimado de chat box	135
Tabla 23 Tabla de costo estimado de herramienta de gestión de riesgos	135
Tabla 24 Tabla de costo estimado de aplicación móvil.....	136
Tabla 25 Estándares de calidad ambiental para el aire	141
Tabla 26 Límite máximos permisibles de emisiones atmosféricas	141
Tabla 27 Comparativo de Riesgo 2017 - 2018	196
Tabla 28 Gestión del Tiempo - Fases e Hitos del Proyecto.....	198
Tabla 29 Gestión de los Recursos Humanos - Stakeholders	199
Tabla 30 Gestión de los riesgos – Matriz de riesgos	200

ÍNDICE DE FIGURAS

Figura 1. Total de incidentes de seguridad reportadas.	34
Figura 2. OCTAVE equilibra tres aspectos	47
Figura 3. Fases de OCTAVE.	48
Figura 4. Roadmap OCTAVE Allegro.	52
Figura 5. Proceso de gestión de riesgos de seguridad de la información.	54
Figura 6. Criterios de evaluación.....	61
Figura 7. Valorización de criterios de evaluación.	62
Figura 8. Comparativo de metodologías - 1	63
Figura 9. Comparativo de metodologías - 2	64
Figura 10. Valoración.....	65
Figura 11. Modelo de gestión de riesgos de seguridad de la información para pymes.	68
Figura 12. Formato de selección de equipo de trabajo – Negocio.	69
Figura 13. Formato de selección de equipo de trabajo – TI.	70
Figura 14. Formato de selección de equipo de trabajo – Operativas.....	70
Figura 15. Hoja de trabajo de evaluación de impacto – Inicio.	73
Figura 16. Hoja de trabajo de evaluación de impacto – Reputación/Confianza del cliente.	73
Figura 17. Hoja de trabajo de evaluación de impacto – Finanzas.	74
Figura 18. Hoja de trabajo de evaluación de impacto – Productividad.	74
Figura 19. Hoja de trabajo de evaluación de impacto – Vida/Salud de los clientes.....	75
Figura 20. Hoja de trabajo de evaluación de impacto – Multas.	75
Figura 21. Hoja de trabajo de Identificación de activos – Activos de la organización.	77
Figura 22. Lista de activos.....	77
Figura 23. Lista de activos – Valoración del activo.	78
Figura 24. Hoja de trabajo Evaluación de prácticas organizacionales.	79
Figura 25. Hoja de trabajo Evaluación de prácticas organizacionales – Concientización de la seguridad y capacitación.....	80
Figura 26. Hoja de trabajo Evaluación de prácticas organizacionales – Concientización de la seguridad y capacitación.....	80
Figura 27. Hoja de trabajo Evaluación de prácticas organizacionales – Valorización de prácticas de seguridad.....	81
Figura 28. Lista de vulnerabilidades.....	82
Figura 29. Hoja de trabajo Evaluación de prácticas organizacionales – Resultados.....	82

Figura 30. Hoja de trabajo Lista de acciones.....	83
Figura 31. Hoja de trabajo Notas y recomendaciones.	83
Figura 32. Hoja de trabajo Información de activos críticos.	84
Figura 33. Hoja de trabajo Información de activos críticos - Justificación, activos relacionados.	84
Figura 34. Hoja de trabajo Información de activos críticos - Requisito de seguridad más importante.....	85
Figura 35. Hoja de trabajo Perfil de riesgos.	85
Figura 36. Hoja de trabajo Perfil de riesgos – Actor, Motivo y Resultado.	86
Figura 37. Hoja de trabajo Perfil de riesgos – Motivo.	87
Figura 38. Hoja de trabajo Perfil de riesgos – Historia.	87
Figura 39. Lista de escenarios de incidentes.	88
Figura 40. Hoja de trabajo de rutas de acceso a la red – Sistema de interés.	89
Figura 41. Hoja de trabajo de rutas de acceso a la red.	89
Figura 42. Hoja de trabajo Revisión de infraestructura - Clases.	91
Figura 43. Hoja de trabajo Revisión de infraestructura – Activos críticos.....	91
Figura 44. Hoja de trabajo Revisión de infraestructura – Responsabilidad.	92
Figura 45. Hoja de trabajo Revisión de infraestructura – Responsabilidad.	93
Figura 46. Hoja de trabajo Revisión de infraestructura – Protección.....	93
Figura 47. Hoja de trabajo Revisión de infraestructura – Notas/Problemas.	94
Figura 48. Hoja de trabajo Perfil de riesgos – Valores de impacto.	95
Figura 49. Hoja de trabajo Criterios de Evaluación de Probabilidad.	96
Figura 50. Lista de escenarios de incidentes - Valorización de incidente.	97
Figura 51. Hoja de trabajo Perfil de riesgos – Valor probabilidad.....	98
Figura 52. Lista de escenarios de incidentes - Probabilidad.....	99
Figura 53. Hoja de trabajo Estrategia de protección.	100
Figura 57. Hoja de trabajo Estrategia de protección - Semáforo.....	100
Figura 55. Hoja de trabajo Estrategia de protección - Características.....	101
Figura 56. Hoja de trabajo Estrategia de protección - Responsabilidad.....	102
Figura 57. Hoja de trabajo Estrategia de protección - Procedimientos.	103
Figura 58. Hoja de trabajo Estrategia de protección - Formación.....	103
Figura 59. Hoja de trabajo Estrategia de protección - Cuestiones de colaboración.	104
Figura 60. Hoja de trabajo Estrategia de protección - Verificación.	104

Figura 61. Hoja de trabajo Perfil de Riesgo – Áreas de prácticas de seguridad.....	105
Figura 62. Impacto por probabilidad.	106
Figura 63. Lista riesgos con prioridad.	107
Figura 64. Hoja de trabajo Perfil de Riesgo – Enfoques.	108
Figura 65. Lista de riesgos aceptados.	109
Figura 66. Guía de Mitigación - Inicio.	110
Figura 67. Hoja de trabajo – Plan de mitigación.	110
Figura 68. Lista de controles.	111
Figura 69. Lista de controles – Valor control.	112
Figura 70. Hoja de Estrategia de Protección – Políticas de seguridad y regulaciones.	113
Figura 71. Hoja de Estrategia de Protección – Monitoreo y Auditoría de la seguridad TI.	114
Figura 72. Hoja de Estrategia de Protección – Monitoreo y Auditoría de la seguridad TI – Cambiar.	114
Figura 73. Hoja de Siguiendo pasos.....	115
Figura 74. Formato "MGRSIPP Principal".	116
Figura 75. Expertos en seguridad.	117
Figura 76. Expertos en seguridad.	118
Figura 77. Proceso de producción.	121
Figura 78. Marco de referencia y proceso ISO 31000.....	124
Figura 79. Hoja de ruta.	128
Figura 80. Plan de migración.....	132
Figura 81. Estructura organizativa.....	138
Figura 82. Combustible utilizado por productores ladrilleros.	139
Figura 83. Buenas prácticas de producción.	139
Figura 84. Compromisos para la mitigación de cambios climáticos.	140
Figura 85. Proceso de venta de empresa de productos de arcilla cerámica.....	143
Figura 86. Relación de ventas con procesos internos y entidades externas.	144
Figura 87. HT-Criterio de evaluación de impacto - Reputación / Confianza cliente.	145
Figura 88. HT-Criterio de evaluación de impacto - Finanzas.	145
Figura 89. HT-Criterio de evaluación de impacto - Productividad.	145
Figura 90. HT-Criterio de evaluación de impacto - Multas / Sanciones Legales.....	145
Figura 91. Lista de activos.....	146

Figura 92. Evaluación de prácticas organizacionales.....	147
Figura 93. Lista de vulnerabilidades de prácticas de seguridad.	147
Figura 94. Lista de activos críticos.....	148
Figura 95. Lista de vulnerabilidades de activos críticos.....	149
Figura 96. Amenazas relacionadas a activos críticos.	150
Figura 97. HT-Rutas de acceso.....	151
Figura 98. HT-Rutas de acceso.....	151
Figura 99. HT-Revisión de Infraestructura-Relación activos críticos.....	152
Figura 100. Lista de activos.....	153
Figura 101. Información de activos críticos.	154
Figura 102. Lista de vulnerabilidades.....	154
Figura 103. HT-Perfil de riesgos.	155
Figura 104. HT-Perfil de riesgos.	156
Figura 105. HT-Perfil de riesgos – Probabilidad.....	157
Figura 106. HT-Perfil de riesgos – Probabilidad.....	158
Figura 107. HT-Perfil de riesgos – Área de práctica de seguridad.....	159
Figura 108. HT-Perfil de riesgos – Área de práctica de seguridad.....	160
Figura 109. HT-Perfil de riesgos – Área de práctica de seguridad.....	161
Figura 110. Nivel de riesgo.	161
Figura 111. Cálculo del riesgo de activos críticos.....	162
Figura 112. Lista riesgos con prioridad.....	163
Figura 113. Enfoques.....	164
Figura 114. Enfoques.....	165
Figura 115. Riesgo Residual.....	166
Figura 116. Agrupación de Amenazas.	167
Figura 117. Agrupación de Vulnerabilidades.....	167
Figura 118. Riesgo inherente por activo.....	168
Figura 119. Agrupación de controles.	168
Figura 120. Riesgo residual por activo.	169
Figura 121. Riesgo por activo.....	169
Figura 122. Riesgo residual por activo.	170
Figura 123. Lista de activos.....	171
Figura 124. Evaluación de prácticas organizacionales.....	172

Figura 125: Lista de vulnerabilidades de prácticas de seguridad.	172
Figura 126: Lista activos críticos.....	173
Figura 127: Lista de vulnerabilidades de activos críticos.....	174
Figura 128: Amenazas relacionadas a activos críticos.	175
Figura 129: HT-Rutas de acceso.	176
Figura 130: HT-Rutas de acceso.	176
Figura 131: HT-Revisión de Infraestructura-Relación activos críticos.....	177
Figura 132: HT-Perfil de riesgos.	178
Figura 133: HT-Perfil de riesgos.	179
Figura 134: HT-Perfil de riesgos.	180
Figura 135: HT-Perfil de riesgos - Probabilidad.	181
Figura 136: HT-Perfil de riesgos - Probabilidad.	182
Figura 137: HT-Perfil de riesgos - Probabilidad.	183
Figura 138: HT-Perfil de riesgos – Área de práctica de seguridad.	184
Figura 139: HT-Perfil de riesgos – Área de práctica de seguridad.	185
Figura 140: HT-Perfil de riesgos – Área de práctica de seguridad.	186
Figura 141. Nivel de riesgo.	186
Figura 142. Cálculo del riesgo de activos críticos.....	187
Figura 143. Lista riesgos con prioridad.....	188
Figura 144. Enfoques.....	189
Figura 145. Enfoques.....	190
Figura 146. Enfoques.....	191
Figura 147. Riesgo residual.	192
Figura 148. Agrupación de amenazas.....	193
Figura 149. Agrupación de vulnerabilidades.....	193
Figura 150. Riesgo por activo.....	194
Figura 151. Agrupación de controles.	194
Figura 152. Riesgo residual por activo.....	195
Figura 153. Riesgo por activo.....	195
Figura 154. Riesgo residual por activo.....	196

CAPÍTULO 1: DESCRIPCIÓN DEL PROYECTO

En este capítulo se abarca el propósito del proyecto de tesis, el problema, la causa y la solución. Además, se da a conocer cuál es el objetivo general, así como los específicos. Se define el alcance del proyecto de tesis y los indicadores de éxitos para medir el cumplimiento del proyecto. Adicionalmente, se listan los posibles riesgos que pueden hacer peligrar la culminación del proyecto.

1.1 Objetivo del problema

El presente estudio busca diseñar e implementar un modelo de gestión de riesgos de seguridad de la información para Pymes en el Perú, integrando la metodología de Gestión de Riesgos OCTAVE-S con la norma ISO/IEC 27005, dentro de una empresa de producto de arcilla cerámica específicamente en el proceso de ventas.

1.2 Dominio del problema

Elaborar una gestión de los riesgos de seguridad de la información para garantizar que los activos principales cuenten con el nivel de protección deseada por la organización. Esta situación expone a los activos de la organización a amenazas que podrían explotar las vulnerabilidades existentes, generando un potencial impacto considerable en el negocio.

Las empresas no son conscientes de los riesgos a los que están expuestos sus activos de información, por ello suelen ser reactivas, actuando normalmente luego de producido algún incidente o al momento de ser requerido por algún ente supervisor; debido a que no cuentan con los conocimientos o especialistas para gestionar o proteger su información. El contar con una metodología que les brinde un enfoque práctico para la evaluación periódica de los riesgos de seguridad les permitirá asegurar un nivel mínimo de protección requerido para sus activos de información más importantes.

Según un estudio realizado por Deloitte, “Evolución de la gestión de ciber riesgo y Seguridad de la información”, 4 de cada 10 empresas han sufrido una brecha de seguridad en los últimos 24 meses, refiriéndose al 2016 y menos del 1% cuenta con indicadores que evalúen la gestión de ciber riesgos y de seguridad de la información, mencionan que el principal obstáculo es la falta de presupuesto o recursos con un 51%.

Un informe de Ernst & Young, “Seguridad de la información en un mundo sin fronteras”, menciona que una compañía de petróleo y gas creía que no tenía problemas de fuga de datos; sin embargo, debido a un ataque que sufrió uno de sus pares, la empresa decidió contratar

un proveedor externo para asegurar que su información estuviera segura, se descubre que se le estaba robando información sensible acerca de su propiedad intelectual patentada y vendiéndola en el extranjero. Con base en los resultados, la organización replanteó completamente su enfoque para manejar la información.

Según la encuesta Latinoamérica de seguridad de la información realizada por la asociación colombiana de ingenieros de sistemas, muestra que un 29% de las pequeñas empresas desarrollan evaluaciones de seguridad, las medianas, 29% y las grandes 41%. Asimismo, muestra que un 53% de las empresas encuestadas no se basa en alguna metodología para la gestión de riesgos. El principal obstáculo es la falta de cultura de seguridad con un 38%.

1.3 Planteamiento de la solución

El presente proyecto consiste en diseñar e implementar un modelo de gestión de riesgos de seguridad de la información, integrando la metodología OCTAVE-S y la norma ISO/IEC 27005, para desarrollar un soporte metodológico que permita realizar una gestión de los riesgos de seguridad de la información conforme a lo requerido por la norma ISO, para ser aplicado al proceso de ventas de una empresa de producto de arcilla cerámica, por motivos de seguridad no se revelará el nombre de dicha empresa.

Este análisis permitirá identificar los principales riesgos de seguridad de la información, para luego proceder a su tratamiento de acuerdo a las necesidades de la empresa.

Entre los beneficios que se obtendrían podemos mencionar los siguientes:

- Entendimiento de la importancia de la seguridad de la información en la empresa.
- Reducir los principales riesgos a los que está expuesta la información.
- Reducir gastos generados por la potencial pérdida de la disponibilidad, confidencialidad o integridad de información.
- Mejorar la cultura de seguridad de la información.
- Establecer un enfoque práctico para la evaluación periódica de los riesgos de seguridad.

1.4 Objetivos del proyecto

1.4.1 Objetivo general

Implementar un modelo de gestión de riesgos de seguridad de la información para una empresa de productos de arcilla cerámica, basado en la metodología OCTAVE-S y la norma ISO/IEC 27005.

1.4.2 Objetivos específicos

OE1: Analizar metodologías y normas de gestión de riesgos de seguridad de la información basándose en factores de evaluación.

OE2: Diseñar un modelo de gestión de riesgos de seguridad de la información, basado en la metodología OCTAVE-S y la norma ISO/IEC 27005.

OE3: Validar el modelo de gestión de riesgos de seguridad de la información, basado en la metodología OCTAVE-S y la norma ISO/IEC 27005 con expertos y evaluarlo en el proceso de ventas de una empresa de productos de arcilla cerámica.

OE4: Elaborar un plan de continuidad que garantice un adecuado nivel de seguridad en los procesos críticos.

1.5 Indicadores de éxito

Para cada objetivo específico el indicador es el siguiente:

Para OE1:

IE1: Conformidad del profesor cliente sobre el análisis de las metodologías y normas basado en factores de evaluación.

Para OE2:

IE2: Conformidad del profesor cliente del diseño del modelo de gestión de riesgos de seguridad de la información basado en la metodología OCTAVE-S y la norma ISO/IEC 27005.

Para OE3:

IE3: Conformidad de los expertos y conformidad del responsable asignado por la empresa de productos de arcilla cerámica sobre la implementación del modelo ejecutado específicamente en el proceso de ventas.

Para OE4:

IE4: Conformidad del profesor cliente sobre el plan de continuidad elaborado.

1.6 Planificación del proyecto

El seguimiento del proyecto se realiza gracias a la documentación brindada por PMBOK, con dichos documentos controlamos el avance del proyecto y los agentes externos e internos que se relacionan a este, así como los riesgos.

1.6.1 Alcance

El proyecto como alcance desarrolla los siguientes entregables:

1. Documentos de gestión de proyecto. (PMBOK)
2. Modelo de Gestión de Riesgos de Seguridad de la Información.
3. Lista de roles de equipo de análisis de riesgos.
4. Breve descripción del proceso de ventas.
5. Análisis de riesgos del proceso de ventas escogido:
 - a. Descripción de actividades realizadas por la empresa para gestionar los riesgos de seguridad de información.
 - b. Lista de los activos.
 - c. Lista de vulnerabilidades.
 - d. Perfil de riesgos (amenazas, probabilidad, prácticas de seguridad y enfoque).
 - e. Lista de escenarios de incidentes con sus respectivas consecuencias.
 - f. Lista de riesgos con prioridad.
 - g. Lista de riesgos aceptados con su respectiva justificación.
 - h. Estrategia de protección.
 - i. Planes de mitigación de riesgos.
 - j. Lista de controles.
 - k. Lista de acciones.

1. Resultados de encuestas y hojas de trabajo.
6. Hoja de Ruta.
7. Perfil de proyecto.
8. Plan de Continuidad.
9. Lecciones aprendidas.
10. Acta de cierre y aceptación.
11. Paper.
12. Memoria.
13. Poster de proyecto.

1.6.2 Plan de gestión del tiempo

Tabla 1

Plan de Gestión del Tiempo - Fases e Hitos del Proyecto

Hito del proyecto	Fecha Estimada	Entregables incluidos	Prioridad
Aprobación del Project Charter	2017-01 Semana 4	Project Charter	Alta
Exposición parcial TP1	2017-01 Semana 6	Project Charter, Plan de Trabajo, Entregables de Gestión	Alta
Aprobación del diseño del Modelo de Gestión de riesgos de SI	2017-01 Semana 15	Diseño del Modelo de Gestión de riesgos de SI	Alta
Exposición final TP1	Semana 16	Modelo de Gestión de riesgos de SI y Memoria	Alta
Validación del Modelo de Gestión de riesgos de SI	2017-02 Semana 21	Modelo de Gestión de riesgos de SI	Alta
Exposición parcial TP2	2017-02 Semana 25	Modelo de Gestión de riesgos de SI, Memoria	Alta
Aprobación Hoja de Ruta y Perfil de proyecto	2017-02 Semana 26	Hoja de Ruta Perfil de proyecto	Alta
Aprobación del Plan de Continuidad	2017-02 Semana 27	Plan de Continuidad	Alta
Aprobación de la Memoria y paper	2017-02 Semana 28	Memoria, Paper	Alta

Exposición final TP2	2017-02 Semana 32	Modelo de Gestión de riesgos de SI, Perfil de Proyecto, Lecciones aprendidas, Plan de Continuidad, Memoria, Paper, Poster	Alta
----------------------	----------------------	---	------

Fuente: Elaboración propia

1.6.3 Plan de gestión de recursos humanos

Los roles involucrados en el desarrollo del proyecto son los siguientes:

Comité de proyectos: rol conformado por la Directora de la Escuela de Sistemas y Computación y los coordinadores de las carreras de Sistemas de Información (Jimmy Armas), Ciencias de la Computación (Pedro Shiguihara) e Ingeniería de Software (Luis Vives). Encargados de validar los proyectos presentados por los alumnos de cada carrera, así también como validar el cumplimiento de los Students Outcomes. Con respecto a la participación en el proyecto, el comité realizará las siguientes funciones:

- Validar objetivos del proyecto.
- Seguimiento del proyecto en coordinación con gerente general y profesor gerente.
- Validar cambios en el proyecto.
- Presentar oportunidades de mejora del proyecto durante la sustentación.
- Aprobar la finalización del proyecto.

Gerente General: rol encargado de dar seguimiento a los proyectos de Sistemas de Información, Ciencias de la Computación e Ingeniería de Software (Emilio Herrera). Con respecto a la participación en el proyecto, el gerente general realizará las siguientes funciones:

- Coordinar funciones de empresas virtuales.
- Coordinar avance de proyectos con Profesores Gerentes de cada empresa virtual.
- Brindar información recibida por parte del Comité de proyectos.

Profesor Cliente: rol encargado de asesorar a los jefes de proyecto de cada proyecto asignado. Con respecto a la participación en el proyecto, el profesor cliente realizará las siguientes funciones:

- Definición de Requerimientos.
- Aprobación de la propuesta de solución.
- Aprobación de documentación técnica.
- Revisión de memoria, capítulos 5 y 6.
- Revisor Responsable.
- Aprobación de la memoria.

Profesor Gerente: rol encargado de dar seguimiento a cada proyecto asignado según la empresa a la que pertenecen (Julio Quispe (TP1) y Milton Chinchay (TP2)). Con respecto a la participación en el proyecto, el profesor gerente realizará las siguientes funciones:

- Aprobación de Plan de Trabajo.
- Seguimiento al Plan de Trabajo.
- Aprobación de documentos técnicos.
- Revisión de memoria, capítulos 1, 2, 7, conclusiones y recomendaciones.

Co-Autor de paper: rol encargado de dar seguimiento al avance del paper a elaborar de cada proyecto. En este caso el co-autor asignado para TP1 son Julio Quispe y Pedro Shiguihara, y para TP2, David Mauricio. Con respecto a la participación en el proyecto, el co-autor realizará las siguientes funciones:

- Aprobación del paper.
- Revisión memoria, capítulos 3 y 4.

Jefe de proyecto: rol encargado de desarrollar y gestionar el proyecto. Con respecto a la participación en el proyecto, el jefe de proyecto realizará las siguientes funciones:

- Cumplir con el plan de trabajo.
- Cumplir el objetivo general y los objetivos específicos del proyecto.
- Coordinar con profesor cliente y profesor gerente las revisiones y aprobaciones de los entregables.
- Presentar avance parcial y final frente a profesor gerente y comité de proyectos.

Cliente: rol designado a la empresa, este rol será ejecutado por los responsables de la empresa designados con los que se validará el proyecto. Con respecto a la participación en el proyecto, el cliente realizará las siguientes funciones:

- Brindar información de la empresa.
- Validar el modelo diseñado en el proyecto.

Analista IT Services: rol encargado de revisar la calidad de los entregables de cada proyecto, así como realizar pruebas de calidad de los softwares. Con respecto a la participación en el proyecto, el analista de IT Services realizará las siguientes funciones:

- Realizar matriz de incidencias relacionadas a cada entregable del proyecto.

1.6.4 Plan de comunicaciones

Todas las reuniones deben seguir las siguientes pautas:

- En caso de tener un nuevo miembro en cada reunión, se hará la respectiva presentación de este ante los asistentes.
- Se manejará una agenda para cada reunión de acuerdo a los temas de interés a tratarse, así como también las tareas pendientes de reuniones anteriores. Para este caso, se debe tener en cuenta el entregable a realizar según el diccionario EDT.
- Cada punto de la agenda contará con un nivel de prioridad a ser tratado.
- Se cuenta con un horario específico para cada reunión, sin embargo, será necesario confirmar/recordar la reunión vía correo electrónico un día antes como máximo.
- En caso se deba postergar una reunión, se deberá justificar y además acordar el nuevo día de esta.
- Al finalizar cada reunión se deberá recopilar lo tratado, resaltando los acuerdos para posteriormente elaborar el acta de reunión.
- Todas las actas de reunión deberán ser firmadas por el jefe de proyecto, asistente de proyecto y gerente general o cliente, respectivamente.
- Toda la remisión de correos electrónicos debe seguir las siguientes pautas:
- Cada correo electrónico debe ser redactado de una manera formal.

- Todo correo electrónico al cliente debe ser copiado a todo el equipo de proyecto; en especial a gerente, jefe, asistente de proyecto
- Los correos electrónicos entre el gerente de la empresa y el cliente, deberá ser enviado por el jefe de proyecto para establecer un estándar en la conexión.
- En caso de envíos de solicitud de servicios a empresas externas, se debe copiar al correo de la empresa.

Tabla 2
Plan de Gestión de Riesgos - Tabla de riesgos

Info. requerida	Contenido	Resp. de elaborar	Para entrega a Stakeholders	Método de comunicación a utilizar	Frec.	Código EDT
Iniciación del proyecto	Información de iniciación de proyecto – Project Charter.	Jefes de Proyecto	<ul style="list-style-type: none"> - Comité de proyectos - Gerente General - Profesor Cliente - Profesor Gerente 	<ul style="list-style-type: none"> - Envío de documentos Word vía correo electrónico. - Presentación física de Project Charter. - Reuniones presenciales. - Exposición. 	Una sola vez	1.1
Planificación del proyecto	Cronograma del Proyecto, Diccionario EDT, Matriz de Riesgos, Matriz de Trazabilidad, Matriz RAM, Plan de Gestión de Calidad, Plan de Gestión de Comunicaciones, Plan de Gestión de	Jefes de Proyecto	<ul style="list-style-type: none"> - Comité de proyectos - Gerente General - Profesor Cliente - Profesor Gerente 	<ul style="list-style-type: none"> - Envío de documentos Word vía correo electrónico. - Reuniones presenciales y digitales. - Exposición. 	Una sola vez	1.2

	Riesgos, Plan de Gestión de RRHH, Plan de Gestión del Cronograma, Plan de Gestión de Alcance, Registro de Interesados, plan de Gestión del Alcance, Plan de Gestión del Cronograma y Lista de equipo de análisis de riesgos, breve descripción del proceso de ventas y modelo de gestión de riesgos de SI.					
Ejecución del proyecto	Descripción de actividades realizadas por la empresa para gestionar los riesgos de seguridad de información, Lista de los activos, Lista de vulnerabilidades, Perfil de riesgos, Lista de escenarios de incidentes con sus respectivas consecuencias, Lista de riesgos con	Jefes de Proyecto	<ul style="list-style-type: none"> - Comité de proyectos - Gerente General - Profesor Cliente - Profesor Gerente - Co autor 	<ul style="list-style-type: none"> - Envío de documentos Word vía correo electrónico. - Reuniones presenciales y digitales. - Exposición. 	Semana	1.3

	prioridad., Lista de riesgos aceptados con su respectiva justificación, Estrategia de protección de toda la organización, Plan de mitigación de riesgos, Lista de controles, Lista de acciones, Hoja de Ruta, Perfil de proyecto, Plan de Continuidad, Memoria, Lecciones aprendidas, Paper y poster.					
Cierre de proyecto	Acta de Aceptación y Cierre.	Jefes de Proyecto	<ul style="list-style-type: none"> - Comité de proyecto - Gerente General - Profesor Cliente - Profesor Gerente 	<ul style="list-style-type: none"> - Envío de documentos Word vía correo electrónico. - Reuniones presenciales y digitales. - Exposición. 	Una sola vez	1.4

Fuente: Elaboración por Jefes de Proyecto

1.6.5 Plan de gestión de riesgos

A continuación, se presentan los riesgos identificados para el proyecto, así también se muestra su probabilidad e impacto si el riesgo llegase a ocurrir. A partir de ello, se muestran las estrategias planteadas para mitigar el riesgo.

Tabla 3
Plan de Gestión de Riesgos - Tabla de riesgos

#	Riesgo	Probabilidad	Impacto	Estrategia de mitigación
1	Cambios en el proyecto	Baja	Muy alto	Definir adecuadamente el alcance y mantener el lineamiento.
2	Retraso de proyecto	Muy Baja	Muy alto	Definir plan de trabajo y colocar el avance.
3	Desaprobación del profesor cliente o gerente en un documento	Baja	Muy alto	Reuniones constantes con aprobadores. Si persiste, establecer una reunión con el Gerente General para explicar el caso y se pueda aprobar el documento.
4	Deficiente comunicación entre jefes de proyecto	Baja	Muy alto	Diálogo constante, compartir problemas del proyecto y solucionarlos.
5	Falta de información	Baja	Muy alto	Definir documentos a utilizar antes de empezar los entregables.
6	Cancelación de reuniones	Media	Muy alto	Definir plan de trabajo y compartirlo con profesores.
7	Pérdida de información del proyecto	Baja	Muy alto	Establecer un repositorio en cada laptop de los JP para contar con versiones anteriores.
8	Falta de interés por parte de la empresa.	Media	Media	Establecer reuniones constantes con el contacto de la empresa y obtener la mayor información posible. O solicitar otro personal de apoyo.

9	Rechazo frente a las recomendaciones brindadas luego de la ejecución del proyecto.	Baja	Media	Establecer comunicación con el contacto de la empresa y el gerente para mantenernos informadas sobre los controles implantados y el seguimiento de los mismos.
---	--	------	-------	--

Fuente: Elaboración propia.

2 CAPÍTULO 2: STUDENT OUTCOMES

En el presente capítulo se definen los Student Outcomes y competencias que certifican la carrera de Ingeniería de Sistemas de Información. Asimismo, se incluye cómo el proyecto “Modelo de Gestión de Riesgos de Seguridad de la Información para Pymes en el Perú” cumple con dichos objetivos.

2.1 Student Outcomes (ABET)

Los Student Outcomes describen lo que los estudiantes deben saber y ser capaces de hacer antes de la graduación. Estos se refieren a los conocimientos, habilidades y comportamientos que los estudiantes adquieren a medida que avanzan a través de su carrera (ABET, 2017).

ABET es una acreditadora de programas universitarios en las disciplinas de ciencias aplicadas y naturales, computación, ingeniería y tecnología de ingeniería en los niveles de asociado, licenciatura y maestría. Con la acreditación ABET, los estudiantes, los empleadores y la sociedad pueden confiar en que un programa que cumple con los estándares de calidad que producen los graduados preparados para ingresar a una fuerza laboral global (ABET, 2017).

ABET es una organización no gubernamental sin fines de lucro reconocida por el Consejo de Acreditación para la Educación Superior (CHEA).

2.1.1 Student outcome A: Aplicar conocimientos de matemáticas, ciencias, computación e ingeniería

El Student Outcome A se refiere a la aplicación de los conocimientos de matemáticas, ciencia e ingeniería que han sido adquiridos por el estudiante durante los años de estudio de su carrera universitaria.

El presente proyecto logra cumplir este Student Outcome, gracias a la realización de tareas durante el proyecto, se utilizan conocimientos de ingeniería en la debida realización de una gestión de proyectos basado en la guía PMBOK, aplicando los tiempos necesarios y asignación de recursos, así como la identificación de posibles riesgos asociados al proyecto añadiendo conocimientos de matemáticas valorizando su impacto, A continuación, se presenta la evidencia necesaria para validar el cumplimiento de este outcome:

- Documentos de gestión
 - o MGRSIPP – Project Charter v3.8
 - o MGRSIPP – Cronograma v2.8
 - o MGRSIPP – Diccionario EDT v2.12
 - o MGRSIPP – Matriz de Riesgos v2.4
 - o MGRSIPP – Plan de Gestión de RRHH v2.6

Se aplican conocimientos de ingeniería y de conocimientos matemáticos para la realización de un comparativo de las distintas metodologías y normas de gestión de riesgos basados en factores de evaluación los cuales fueron valorizados, para las hojas y listas de trabajo desarrolladas para poder calcular el riesgo se aplicaron conocimientos matemáticos. A continuación, se presenta la evidencia necesaria para validar el cumplimiento de este outcome:

- MGRSIPP – Benchmarking
- Hojas y listas de trabajo del Modelo de Gestión de Riesgos

2.1.2 Student outcome B: Diseña y conduce experimentos en base al análisis e interpretar los datos

El Student Outcome B se refiere al diseño de experimentos, realización de experimentos, análisis de datos y a la debida interpretación de datos por parte del estudiante (The Foundation Coalition, 2005).

El presente proyecto logra cumplir este Student Outcome, gracias al análisis que se realiza en el comparativo de las metodologías y normas de gestión de riesgos escogiendo la más adecuada para la realización de este proyecto basado en ciertos criterios de evaluación, gracias a ello se pudo diseñar el modelo de gestión de riesgos de seguridad de la información

para pymes, se realiza la evaluación de la situación actual de la empresa en seguridad de la información basándose en la ISO/IEC 27002, encontrando un bajo nivel de protección. Mediante la información recopilada se realiza la evaluación del modelo en la empresa de productos de arcilla cerámica, asimismo, se realiza la validación del modelo por expertos en seguridad de la información. A continuación, se presenta la evidencia necesaria para validar el cumplimiento de este outcome:

- MGRSIPP – Benchmarking
- MGRSIPP – Situación actual de Seguridad de la Información de la empresa
- MGRSIPP – Modelo de Gestión de Riesgos de Seguridad de la información para Pymes en el Perú
- Hojas y Listas de trabajo evaluadas en la empresa de productos de arcilla cerámica.
- Acta de validación del objetivo 3 del proyecto MGRSIPP.

2.1.3 Student outcome C: Diseñar sistemas, componentes o procesos para encontrar soluciones en la atención de necesidades teniendo en cuenta restricciones económicas, sociales, políticas, éticas de salud y seguridad y otras propias del entorno empresarial

El Student Outcome C se refiere a la capacidad con la que cuenta el estudiante de diseñar un sistema, componente o proceso para satisfacer las necesidades deseadas dentro de limitaciones realistas tales como económicas, política, ética, salud y seguridad, manufacturabilidad y sostenibilidad (The Foundation Coalition, 2005).

El presente proyecto logra cumplir este Student Outcome, gracias a la realización y mapeo del proceso de ventas de la empresa de productos de arcilla cerámica, ya que no se contaba con este. Asimismo, se realiza el diseño del modelo de gestión de riesgos de seguridad de la información basado en la metodología OCTAVE-S y la norma ISO/IEC 27005, logrando modificar las hojas de trabajo e incluir el diseño de listas para el análisis completo de una gestión de riesgos. A continuación, se presenta la evidencia necesaria para validar el cumplimiento de este outcome:

- MGRSIPP – Descripción del proceso de ventas de empresa de productos de arcilla cerámica

- Modelo de Gestión de Riesgos de Seguridad de la Información
- Hojas y listas de trabajo del Modelo de Gestión de Riesgos de Seguridad de la Información

Las Pymes peruanas cuentan con un bajo presupuesto para temas relacionados a seguridad de la información, se realiza la factibilidad económica del proyecto, logrando mostrar que si dicho modelo se implementa en las empresas con los requisitos mostrados se obtendrían beneficios relacionados a disminución de horas de trabajo, disminución de mano de obra en recuperar información y reducción de costos por personal adicional, es así como se haya el retorno de inversión del proyecto, el cual es de 6 meses, como se puede observar la empresa recuperaría en poco tiempo su inversión.

Relacionado al tema social, el modelo permite a las Pymes realizar las evaluaciones de gestión de riesgos periódicamente, y, sobre todo, mejorar la cultura de seguridad de la información dentro de la empresa, ya que el personal interno también desempeña un papel importante dentro de la evaluación. Asimismo, los altos directivos tomarán conciencia de los riesgos presentes, y tomarán mejores decisiones al respecto.

Relacionado al tema de la política, lo enfocamos a la política dentro de la empresa, el modelo contempla que se estén realizando y contemplando las políticas básicas para resguardar la información. Asimismo, se verifica que tan bien se están realizando las prácticas de seguridad según las áreas plasmadas por la metodología OCTAVE-S. Asimismo, se trata de que las empresas contemplen como acciones preventivas los controles mostrados en la ISO/IEC 27001.

Relacionado al tema de la ética, el modelo cumple con los componentes esenciales para la protección de los activos de información y la información relacionada a estos. Se buscó enfocarse en los criterios de confiabilidad, integridad y disponibilidad.

2.1.4 Student outcome D: Participar en equipos multidisciplinarios, liderando o desarrollando eficientemente sus tareas con profesionales de diferentes campos o campos de aplicación

El Student Outcome D se refiere a la capacidad del estudiante de participar en equipos de trabajo multidisciplinarios para lograr el éxito del proyecto.

El presente proyecto logra cumplir este Student Outcome, gracias al cronograma del proyecto donde se observa las reuniones pactadas con los interesados del proyecto, asimismo se cuenta con las actas de reuniones que lo validan. Para la adecuada comunicación entre jefes de proyectos e interesados se genera un plan y una matriz de comunicaciones. A continuación, se presenta la evidencia necesaria para validar el cumplimiento de este outcome:

- MGRSIPP – Cronograma v2.8
- MGRSIPP – Plan de Gestión de Comunicaciones v2.1
- MGRSIPP – Matriz De Comunicaciones v2.7
- Actas de reuniones con profesor gerente, profesor cliente y con el personal de apoyo de la empresa de productos de arcilla cerámica

Asimismo, durante el desarrollo del proyecto se solicita los servicios de la empresa IT Services para la validación de la calidad de los entregables del proyecto conformada por alumnos del Taller de Desempeño. Durante el Taller de Proyectos 1, se mantuvo comunicación con el gerente alumno Robert Tovar y los analistas asignados Luis Felipe Sánchez y Henry Pérez, obteniendo la constancia de servicio de validación y verificación ITS. Durante el Taller de Proyectos 2, se mantuvo comunicación con el profesor Jaylli Arteaga Sánchez y los alumnos asignados, manteniendo mayor comunicación con la responsable asignada Yelithza Ramírez Alamo. A continuación, se presenta la evidencia necesaria para validar el cumplimiento de este outcome:

- Constancia_ITS
- Actas de reunión con la responsable del equipo de Taller de Desempeño

El proyecto cuenta con la realización de un poster, por lo cual se tuvo contacto con una alumna de la carrera de Diseño Profesional Gráfico de la UPC, del décimo ciclo, Jenny Puchurrí Gutierrez, quien fue la encargada del diseño del mismo según lo explicado por los jefes de proyecto.

- Actas de reunión con la alumna de Diseño Profesional Gráfico
- MGRSIPP - Poster

2.1.5 Student outcome E: Identificar, formular y resolver problemas de ingeniería

El Student Outcome E se refiere a la capacidad del estudiante de identificar y analizar situaciones o problemas de ingeniería para poder encontrar la solución respectiva.

El presente proyecto logra cumplir este Student Outcome, gracias a la realización del Project Charter, donde se identifica la problemática de ingeniería y se asocian sus causas. Asimismo, se realiza un comparativo de metodologías y normas para encontrar la mejor solución a la problemática. La resolución de esta problemática se demuestra en el modelo de gestión de riesgos de seguridad de la información para pymes presentado en este documento, así como su desarrollo, donde se explica cada una de las fases y los procesos respectivos. Para validar el modelo, este se implementa en una empresa de productos de arcilla cerámica, donde validaron la utilidad del modelo para identificar y reducir sus riesgos, así como la flexibilidad de este, asimismo, se realizó la validación del modelo con tres expertos de seguridad de la información. A continuación, se presenta la evidencia necesaria para validar el cumplimiento de este outcome:

- MGRSIPP – Project Charter v3.8
- MGRSIPP – Benchmarking
- MGRSIPP – Memoria 1.12
- Modelo de Gestión de Riesgos de Seguridad de la Información para Pymes en el Perú
- Aprobación Objetivo específico 3, Indicador específico 3, carta de la empresa de productos de arcilla cerámica y actas de validación de los expertos

2.1.6 Student outcome F: Proponer soluciones de ingeniería con responsabilidad profesional y ética

El Student Outcome F se refiere a la capacidad del estudiante de completar un proyecto considerando la responsabilidad que conlleva y las prácticas éticas.

El presente proyecto logra cumplir este Student Outcome, gracias a la responsabilidad presentada durante la gestión del proyecto, sobretodo en el cumplimiento de los entregables y en las fechas pactadas para las reuniones, las cuales se encuentran evidenciadas en el cronograma del proyecto y en las actas de reuniones. Asimismo, para evidenciar el comportamiento ético durante este proyecto, se realizan las referencias necesarias de los autores que aportaron ideas para este proyecto, evidencia la ética que debe tener todo

profesional respecto a trabajos de investigación. A continuación, se presenta la evidencia necesaria para validar el cumplimiento de este outcome:

- MGRSIPP – Cronograma 2.8
- MGRSIPP – Plan de Gestión del Cronograma v2.2
- MGRSIPP – Project Charter v3.8
- MGRSIPP – Memoria 1.12
- Actas de Reuniones con profesor gerente, profesor cliente, IT Services, personal de la empresa de productos de arcilla cerámica y la alumna de diseño

Asimismo, el proyecto se implementa dentro de una Pyme de productos de arcilla – cerámica, donde se cumple el principio de confidencialidad no revelando el nombre de la misma, ni información sensible.

Además, se ha cumplido con el Código de Ética del Ingeniero establecido por la ABET, donde los principios fundamentales a cumplir son:

- Usar los conocimientos y habilidades para mejorar el bienestar humano: en el proyecto se ha buscado solucionar una problemática planteada en el Project Charter, usando los conocimientos de ingeniería y matemáticas se logra diseñar un modelo para conseguir el objetivo principal y apoyar a las Pymes del Perú logrando que los trabajadores cuenten con un proceso más agilizado.
- Ser honesto e imparcial, y servir con fidelidad al público, a sus empleados, y a sus clientes: durante las presentaciones del proyecto, durante la implementación del modelo siempre se tomó en cuenta las observaciones y decisiones dadas por los trabajadores de la empresa, presentando los resultados obtenidos los cuales fueron aprobados por los mismos trabajadores y la gerencia, dicha implementación se realizó bajo el principio de confiabilidad, ya que no se debía divulgar la información.
- Luchar por aumentar el nivel de competencia y el prestigio de ingeniería como profesión: la implementación del modelo logra identificar el riesgo dentro del proceso de ventas de la pyme, asimismo los trabajadores involucrados aumentaron su conocimiento en gestión de riesgos y seguridad de la información a quienes se les explicó el proceso que debían realizar, logrando la aprobación por parte de la gerencia de la implementación del

modelo debido a los resultados presentados y a los controles propuestos para disminuir el riesgo.

- Apoyar las sociedades profesionales y técnicas de sus respectivas disciplinas: se cuenta con el apoyo entre la universidad, los jefes de proyecto y los trabajadores de la Pyme de productos de arcilla – cerámica.

2.1.7 Student outcome G: Comunicar oralmente o por escrito ideas o resultados de manera clara y efectiva

El Student Outcome G se refiere a la capacidad del estudiante de comunicar sus ideas o resultados de manera efectiva.

El presente proyecto logra cumplir este Student Outcome, gracias a las reuniones semanales realizadas con el profesor gerente, el profesor cliente y el co-autor para la revisión de avances o validaciones necesarias. Asimismo, las reuniones con el personal de la empresa de productos de arcilla cerámica para poder mostrar los resultados obtenidos de la implementación del modelo. El proyecto cuenta con entregables que han sido revisados por IT Services, quienes son los encargados de verificar la calidad de cada uno de los entregables; uno de los entregables, el paper, es validado por el co-autor asignado. Adicionalmente, se realizaron pre-sustentaciones frente al profesor gerente y sustentaciones ante el comité explicando el presente proyecto. Cabe resaltar que los resultados también se encuentran evidenciados en el cumplimiento de los indicadores del proyecto. A continuación, se presenta la evidencia necesaria para validar el cumplimiento de este outcome:

- Actas de reunión con profesor gerente, profesor cliente, con el personal de la empresa de productos de arcilla cerámica
- Constancia ITS
- Acta de conformidad del paper
- Aprobaciones de los indicadores específicos (IE1, IE2, IE3 y IE4)

2.1.8 Student outcome H: Identificar el impacto de las soluciones de ingeniería en el contexto global, económico y del entorno de la sociedad

El Student Outcome H se refiere a la amplia formación del estudiante para comprender el impacto de las soluciones de ingeniería en un contexto global, económico, ambiental y social (The Foundation Coalition, 2005).

El presente proyecto logra cumplir este Student Outcome, gracias a la identificación de la problemática en el documento del Project Charter, donde se puede evidenciar el impacto que se tiene frente a la sociedad y frente a la empresa donde se implementará el modelo. Adicionalmente, se realiza un análisis de la situación actual de la empresa de productos de arcilla cerámica para poder validar el bajo nivel de seguridad de la información en la que se encontraba. Para poder encontrar la solución más adaptable a las empresas pymes, las cuales cuentan con poco presupuesto para los temas de seguridad de la información, se realizó un análisis comparativo entre metodologías y normas de gestión de riesgos para identificar el más idóneo. Asimismo, el impacto económico generado por esta problemática se evidencia durante las exposiciones mostrando el impacto global, latinoamericano y en el Perú, también se menciona en el paper presentado para este proyecto. La implementación del modelo dentro de una Pyme permite reducir los gastos relacionados a seguridad, asimismo contribuye a la cultura en seguridad de la información dentro de la misma. A continuación, se presenta la evidencia necesaria para validar el cumplimiento de este outcome:

- MGRSIPP – Project Charter v3.8
- MGRSIPP – Memoria 1.12
- MGRSIPP – Benchmarking
- MGRSIPP – Situación actual de Seguridad de la Información de la empresa
- MGRSIPP – Paper

2.1.9 Student outcome I: Reconocer la necesidad de mantener sus conocimientos actualizados

El Student Outcome H se refiere al reconocimiento de la necesidad y la capacidad de participar en el aprendizaje permanente (The Foundation Coalition, 2005).

El presente proyecto logra cumplir este Student Outcome, gracias a la realización de un comparativo de metodologías y normas de gestión de riesgos que han sido desarrolladas a

través de los años, donde se ha podido observar cómo estas han podido evolucionar o actualizar para el mejor entendimiento o simplemente para que estas se puedan adaptar mejor. Asimismo, se realiza investigaciones de otros autores, quienes realizaron artículos en revistas, donde se observa que comparan las metodologías y dan un aporte propio para que esta pueda mejorar, o cómo sería mejor si ciertas metodologías se integran. De esta manera, se puede evidenciar que las investigaciones realizadas hasta la actualidad relacionada a metodologías y normas de gestión de riesgos, demuestran que se debe tener actualizado el conocimiento en estos temas para poder mejorar y proponer modelos de metodologías que se puedan adaptar a la necesidad de cada empresa en la que se realizará la implementación. Asimismo, en la Hoja de Ruta se muestra cómo el proyecto puede adaptarse a través del tiempo, y cómo las actualizaciones lograran el cambio futuro del proyecto. A continuación, se presenta la evidencia necesaria para validar el cumplimiento de este outcome:

- MGRSIPP – Benchmarking
- MGRSIPP – Paper
- MGRSIPP – Hoja de Ruta v1.3

2.1.10 Student outcome J: Analizar hechos del mundo contemporáneo identificando el impacto en el desempeño profesional de ingeniería

El Student Outcome J se refiere a la capacidad del estudiante de identificar importantes problemas contemporáneos que involucren ingeniería, proponer y discutir formas en que los ingenieros pueden contribuir a la solución (The Foundation Coalition, 2005).

El presente proyecto logra cumplir este Student Outcome, gracias a la realización del documento Project Charter, donde desde el inicio del proyecto se muestra el problema y cuál sería la posible solución para este. Asimismo, en el documento de situación actual de la empresa, donde se observa cómo una empresa puede encontrarse en seguridad de la información, es decir, en qué nivel. Este documento ayuda a validar que en dicha empresa se puede implementar el modelo para obtener los resultados esperados. Para contemplar el análisis del mundo contemporáneo, se realizaron las investigaciones necesarias en relación a las metodologías y normas de gestión de riesgos, para poder elaborar un comparativo de estas y determinar mediante factores de evaluación cual era la más apropiada para este proyecto, teniendo en cuenta el impacto que podría tener. El impacto en el desempeño profesional de ingeniería según el proyecto son los siguientes:

- Mejorar la implementación de una gestión de riesgos dentro de una empresa Pyme haciéndola más dinámica y menos complicada.
- Lograr que la gestión de riesgos a implementar cuente con todos los componentes necesarios.
- Lograr la inclusión de empleados necesarios a la implementación de gestión de riesgos, quienes tengan el conocimiento necesario sobre su área de trabajo.

A continuación, se presenta la evidencia necesaria para validar el cumplimiento de este outcome:

- MGRSIPP – Project Charter v3.8
- MGRSIPP – Benchmarking
- MGRSIPP – Situación actual de Seguridad de la Información de la empresa
- MGRSIPP – Paper

2.1.11 Student outcome K: Utilizar las técnicas, herramientas y metodologías necesarias para la práctica de la ingeniería

El Student Outcome K se refiere a la capacidad del estudiante utilizar técnicas, herramientas y metodologías necesarias para la práctica de la ingeniería.

El presente proyecto logra cumplir este Student Outcome, gracias a la utilización de la metodología PMBOK, para la debida gestión del proyecto, la comparación entre las metodologías y normas analizadas, la metodología OCTAVE-S y la norma ISO/IEC 27005 para el diseño del modelo de gestión de riesgos de seguridad de la información. Asimismo, se utilizó la herramienta Bizagi para poder diagramar el proceso de ventas de la empresa de productos de arcilla cerámica. Adicionalmente, para la realización del poster se utilizó la herramienta Illustrator. A continuación, se presenta la evidencia necesaria para validar el cumplimiento de este outcome:

- Documentos de gestión
- MGRSIPP – Benchmarking
- MGRSIPP – Descripción del proceso de ventas de la empresa de productos de arcilla cerámica

- MGRSIPP – Poster

2.1.12 Student outcome J-CAC: Comprende y brinda soporte para el uso, entrega y gestión de información dentro de un entorno de Sistemas de Información

El Student Outcome J-CAC se refiere a la capacidad del estudiante de validar que la solución es viable a través del tiempo.

El presente proyecto logra cumplir este Student Outcome, gracias a la realización de un plan de continuidad que garantice un adecuado nivel de seguridad en los procesos críticos y la continuidad del proyecto dentro de la empresa que lo implemente. Asimismo, por la realización de una hoja de ruta, la cual indica cómo el proyecto puede mejorar a través del tiempo, y cómo genera nuevos proyectos a partir de ello. A continuación, se presenta la evidencia necesaria para validar el cumplimiento de este outcome:

- MGRSIPP – Plan de Continuidad v1.1
- MGRSIPP – Hoja de Ruta v1.3

2.2 Competencias WASC

La competencia en la evaluación del aprendizaje del estudiante, es una habilidad específica, cuerpo de conocimiento o disposición; también puede referirse a la capacidad del estudiante para demostrar ese aprendizaje. La "competencia" a veces se usa indistintamente con "resultado", "objetivo" y "capacidad" (WASC Senior College and University Commission).

WASC Senior College and University Commission (WSCUC) es una de las agencias acreditadoras en educación superior más importante del mundo, la cual valida la calidad académica de las universidades de los Estados de California y Hawaii y la zona del Pacífico, evaluando de forma integral el cumplimiento de la misión, los resultados de aprendizaje de los estudiantes, asociados a su modelo educativo y al perfil de cada uno de sus programas, sus recursos físicos, académicos y administrativos, así como su sistema de calidad y mejora continua (UPC Alumni, 2016).

El Departamento de Educación de los EE. UU. Reconoce a la Comisión Superior de Universidades y Universidades de WASC (WSCUC) como una entidad que certifica la elegibilidad institucional para recibir fondos federales en una serie de programas, incluido el acceso de los estudiantes a la ayuda financiera federal (WASC Senior College and University Commission).

2.2.1 Comunicación escrita

La comunicación por medio del lenguaje escrito con fines informativos, persuasivos y expresivos. La comunicación escrita puede aparecer en muchas formas o géneros. La comunicación escrita exitosa depende del dominio de las convenciones del lenguaje escrito, facilidad con estructuras culturalmente aceptadas para la presentación y el argumento, conocimiento de la audiencia y otros factores específicos de la situación (WASC Senior College and University Commission).

El presente proyecto logra cumplir esta competencia, gracias a que este cuenta con entregables, los cuales han sido revisados por IT Services, quienes son los encargados de verificar la calidad de cada uno de ellos, ya sea en estructura o redacción; asimismo, uno de los entregables es un paper del proyecto, el cual es validado por el co-autor asignado donde se tiene que utilizar un léxico variado, preciso, académico y especializado así también como en los otros entregables. Adicionalmente, se realizaron pre-sustentaciones frente al profesor gerente y sustentaciones ante el comité explicando el presente proyecto. A continuación, se presenta la evidencia necesaria para validar el cumplimiento de esta competencia:

- Documentos de gestión de proyecto (PMBOK)
- Modelo de Gestión de Riesgos de Seguridad de la Información
- Lista de roles de equipo de análisis de riesgos
- Breve descripción del proceso de ventas
- Análisis de riesgos del proceso de ventas escogido
- Hoja de Ruta
- Perfil de proyecto
- Plan de Continuidad
- Lecciones aprendidas
- Acta de cierre y aceptación
- Paper
- Memoria
- Poster de Proyecto

2.2.2 Comunicación oral

La comunicación se logra a través del lenguaje hablado con fines informativos, persuasivos y expresivos. Además del habla, la comunicación oral puede emplear ayudas visuales, lenguaje corporal, entonación y otros elementos no verbales para apoyar la transmisión del significado y la conexión con la audiencia. La comunicación oral puede incluir discursos, presentaciones, debates, diálogos y otras formas de comunicación interpersonal, ya sea en persona o mediada tecnológicamente (WASC Senior College and University Commission).

El presente proyecto logra cumplir esta competencia, gracias a las reuniones semanales realizadas con el profesor gerente, el profesor cliente y el co-autor para la revisión de avances o validaciones necesarias. Asimismo, las reuniones con el personal de la empresa de productos de arcilla cerámica para poder mostrar los resultados obtenidos de la implementación del modelo. Adicionalmente, las pre-sustentaciones frente al profesor gerente y sustentaciones ante el comité explicando el presente proyecto, así como la exposición del paper en el Congreso COPIOS 2017 realizado en la Universidad San Marcos y en el Congreso Internacional de Investigación en Ciencias y Humanidades (SHIRCON) en la Universidad de Ciencias y Humanidades. A continuación, se presenta la evidencia necesaria para validar el cumplimiento de esta competencia:

- Actas de reunión con profesor gerente, profesor cliente, con el personal de la empresa de productos de arcilla cerámica
- Pre - sustentaciones y sustentaciones
- Exposición del Paper en Congreso COPIOS 2017
- Exposición del Paper en Congreso SHIRCON 2018

2.2.3 Ciudadanía

La ciudadanía es la capacidad para valorar la convivencia humana en sociedades plurales, reflexionando acerca de las dimensiones morales de las propias acciones y decisiones, asumiendo la responsabilidad por las consecuencias en el marco del respeto de los derechos y deberes ciudadanos.

El presente proyecto logra cumplir esa competencia, gracias a la identificación de la problemática en el documento del Project Charter, donde se puede evidenciar el impacto que se tiene frente a la sociedad y frente a la empresa donde se implementará el modelo,

asimismo también se muestra cual sería la posible solución a implementar. Para poder encontrar la solución más adaptable a las empresas pymes, las cuales cuentan con poco presupuesto para los temas de seguridad de la información, se realizó un análisis comparativo entre metodologías y normas de gestión de riesgos para identificar el más idóneo, llegando a un acuerdo con el profesor cliente de cuál era la más apropiada mediante diálogos y presentaciones sobre lo planteado. Dentro del contexto social, como ya se mencionó las pymes no cuentan con un presupuesto suficiente para poder realizar un análisis de riesgo o utilizar un método de gestión de riesgos dentro de ellas, ello se evidencia en una encuesta Latinoamérica mostrando que el 38% de las empresas encuestadas no contaba con el apoyo económico necesario. Dentro del contexto político, enfocándonos en las normas, no se tiene una norma establecida para la aplicación obligatoria de una gestión de riesgos, se tiene una norma para las empresas para certificarse en la ISO/IEC 27001, la cual sigue los lineamientos de un sistema de gestión seguridad de la información, debería ser importante que las empresas implementaran una gestión de riesgos para poder evitar impactos monetarios altos por ciertos ataques informáticos o de revelación. Dentro del tema cultural, la situación actual de las pymes en seguridad de la información es muy baja, según un informe de Deloitte solo el 1% de las empresas utiliza indicadores de ciber riesgos o de seguridad de la información, asimismo la encuesta antes mencionada muestra que solo el 29% de las empresas medianas y el 29% de las empresas pequeñas realizan una gestión de riesgos dentro de su empresa, por lo que podemos observar la cultura en seguridad de la información no está bien desarrollada dentro de las pymes. El presente proyecto ayudaría a las pymes a poder reducir el riesgo presente en ellas, así como tener el conocimiento de sus activos más críticos, y también a desarrollar una cultura dentro de la empresa en seguridad de la información, ya que el personal también participa de la evaluación. A continuación, se presenta la evidencia necesaria para validar el cumplimiento de esta competencia:

- MGRSIPP – Project Charter v3.8
- MGRSIPP – Benchmarking
- MGRSIPP – Memoria 1.12

2.2.4 Pensamiento innovador

El pensamiento innovador es la capacidad para detectar necesidades y oportunidades para generar proyectos o propuestas innovadoras, viables y rentables. Planifica y toma decisiones eficientes orientadas al objetivo del proyecto.

El presente proyecto logra cumplir esa competencia, gracias a la identificación de la problemática en el documento del Project Charter, donde se identifica la necesidad de las pymes de proteger su información. A partir de ello, se busca la solución de implementar una metodología, donde se decide realizar un análisis comparativo entre metodologías y normas de gestión de riesgos para identificar el más idóneo, se encuentra que la norma ISO/IEC 27005 era la más idónea debido a que enfocaba en la necesidad de seguridad de la información, esta norma no contaba con un metodología por lo que dentro del comparativo se identifica a OCTAVE como la más idónea, ya que estaba enfocada en la misma necesidad pero con algunas deficiencias, así se seleccionó el método OCTAVE-S el cual está enfocada en pequeñas y medianas empresas. Debido a que se observa que OCTAVE-S no contaba con todos los lineamientos de la norma, se decide modificar la estructura de sus procesos, añadiendo procesos o listas necesarias que sí contemplaba la ISO/IEC 27005. A partir de ello, se logra diseñar el modelo de gestión de riesgos de seguridad de la información, el cual cuenta con los principales componentes de una gestión de riesgos y enfocado en la seguridad de la información, adicionalmente se logra que el modelo pueda cuantificar el riesgo inherente y el riesgo residual. Se logra también brindar controles para reducir el riesgo, así como los principales indicadores para monitorearlos, los cuales están estructurados como lo mencionan la ISO/IEC 27004.

Todo el proyecto se logra gracias a la realización de una estructura de plan de trabajo donde se muestran las tareas principales a realizar para el avance del proyecto, asimismo el proyecto sigue la metodología PMBOK, en donde se detallan las tareas, entregables, los tiempos, los recursos a necesitar, así como las comunicaciones.

Para demostrar que el proyecto es rentable y viable, se realiza el impacto económico donde se aprecia un aproximado del costo del proyecto, así como el retorno de inversión para este, demostrando que en solo seis meses la empresa podría recuperar lo invertido si gestionara los recursos mencionados.

A continuación, se presenta la evidencia necesaria para validar el cumplimiento de esta competencia:

- MGRSIPP – Project Charter v3.8
- MGRSIPP – Benchmarking
- Modelo de Gestión de Riesgos de Seguridad de la Información
- Documentos de gestión
- MGRSIPP – Costo del proyecto

2.2.5 Pensamiento crítico

El pensamiento crítico es la capacidad de pensar de una manera clara, razonada, reflexiva, informada por evidencia y dirigida a decidir qué creer o hacer. Las disposiciones que apoyan el pensamiento crítico incluyen la apertura de mente y la motivación para buscar la verdad (WASC Senior College and University Commission).

El presente proyecto logra cumplir esa competencia, gracias a la identificación de la problemática en el documento del Project Charter, a partir de ello se muestran tres principales causas:

- Las empresas no son conscientes de los riesgos a los que están expuestos sus activos de información, por ello suelen ser reactivas, actuando normalmente luego de producido algún incidente o al momento de ser requerido por algún ente supervisor; debido a que no cuentan con los conocimientos o especialistas para gestionar o proteger su información. Según un estudio realizado por Deloitte, “Evolución de la gestión de ciber riesgo y Seguridad de la información”, 4 de cada 10 empresas han sufrido una brecha de seguridad en los últimos 24 meses, refiriéndose al 2016 y menos del 1% cuenta con indicadores que evalúen la gestión de ciber riesgos y de seguridad de la información, mencionan que el principal obstáculo es la falta de presupuesto o recursos con un 51%.
- Las empresas son reactivas. Un informe de Ernst & Young, “Seguridad de la información en un mundo sin fronteras”, menciona que una compañía de petróleo y gas creía que no tenía problemas de fuga de datos; sin embargo, debido a un ataque que sufrió uno de sus pares, la empresa decidió contratar un proveedor externo para asegurar que su información estuviera segura, se descubre que se le estaba robando información sensible

acerca de su propiedad intelectual patentada y vendiéndola en el extranjero. Con base en los resultados, la organización replanteó completamente su enfoque para manejar la información.

- Falta de cultura en seguridad de la información. Según la encuesta Latinoamérica de seguridad de la información realizada por la asociación colombiana de ingenieros de sistemas, muestra que un 29% de las pequeñas empresas desarrollan evaluaciones de seguridad, las medianas, 29% y las grandes 41%. Asimismo, muestra que un 53% de las empresas encuestadas no se basa en alguna metodología para la gestión de riesgos. El principal obstáculo es la falta de cultura de seguridad con un 38%.

El contar con una metodología que les brinde un enfoque práctico para la evaluación periódica de los riesgos de seguridad permitiría a las empresas asegurar un nivel mínimo de protección requerido para sus activos de información más importantes.

Asimismo, en el presente documento se muestra los distintos puntos de vista de diferentes autores que también realizaron comparaciones entre metodologías de gestión de riesgos, mostrando sus aportes, lo cual fue de ayuda para la comparativa y para tomar la decisión sobre qué metodología escoger para este proyecto. Dichos aportes también se encuentran reflejados en el paper.

A continuación, se presenta la evidencia necesaria para validar el cumplimiento de esta competencia:

- MGRSIPP – Project Charter v3.8
- MGRSIPP – Memoria 1.12 (Introducción, Capítulo 1 y Estado del arte)
- MGRSIPP – Benchmarking
- Paper

2.2.6 Pensamiento cuantitativo

El razonamiento cuantitativo es la capacidad de aplicar conceptos matemáticos a la interpretación y análisis de información cuantitativa para resolver una amplia gama de problemas, desde los que surgen en la investigación pura y aplicada hasta cuestiones y preguntas cotidianas. Puede incluir dimensiones tales como la capacidad de aplicar las habilidades matemáticas, juzgar la razonabilidad, comunicar información cuantitativa y

reconocer los límites de los métodos matemáticos o estadísticos (WASC Senior College and University Commission).

El presente proyecto logra cumplir esta competencia, gracias a la identificación de posibles riesgos asociados al proyecto, ya que estos han sido valorizados según su impacto los cuales también están reflejados en el Project Charter, así también se ha cuantificado cuanto sería el costo aproximado del costo del proyecto, y se obtuvo el retorno de inversión para este. Adicionalmente, se obtuvo un porcentaje de nivel de seguridad en la empresa donde se implementará el modelo, basado en los controles que menciona la ISO/IEC 27002, tomando la decisión de aplicar el modelo, a que el nivel obtenido fue bajo. Algunas hojas de trabajo de OCTAVE-S fueron modificadas para cuantificar campos necesarios dentro de la evaluación, así como algunas de las listas que contempla la ISO/IEC 27005, con lo que se llega a obtener el riesgo presente en la empresa (inherente y residual), basado en toma de decisiones bajo los enfoques de mitigación, aceptación, transferencia y eliminación, a partir de ello también se pudo identificar cuáles son los activos de información más críticos de la empresa. A continuación, se presenta la evidencia necesaria para validar el cumplimiento de esta competencia:

- MGRSIPP – Matriz de Riesgos v2.4
- MGRSIPP – Plan de Gestión de RRHH v2.6
- MGRSIPP – Costo del proyecto
- MGRSIPP – Situación actual de Seguridad de la Información de la empresa
- Hojas y listas de trabajo del Modelo de Gestión de Riesgos

2.2.7 Manejo de la información

El manejo de la información es la capacidad de identificar la información necesaria, así como de buscarla, seleccionarla, evaluarla y usarla éticamente, con la finalidad de resolver un problema.

El presente proyecto logra cumplir esta competencia, gracias a realización del Project Charter donde se puede observar la identificación del problema, la investigación realizada sobre los conceptos claves relacionados con el tema y con lo que se aplicará, esta información también se ve reflejada en la Memoria del proyecto. Se utiliza distintas referencias bibliográficas confiables, las cuales sirven para definir cada uno de los

conceptos, así como las metodologías y normas dentro de la comparativa de metodologías y normas, los aportes de los autores en el estado del arte y cómo algunas investigaciones han ayudado a la realización del modelo del presente proyecto. Asimismo, el paper del proyecto también muestra las referencias de los autores de otros papers, los cuales han servido de ayuda para la realización de la revisión literaria de ese documento. Las referencias de los entregables están ligadas a la referencia APA, mientras que el paper está ligado al tipo de referencia Vancouver para el Congreso COPIOS y la referencia IEEE, para el Congreso SHIRCON. A continuación, se presenta la evidencia necesaria para validar el cumplimiento de esta competencia:

- MGRSIPP – Project Charter v3.8
- MGRSIPP – Memoria 1.12
- MGRSIPP – Benchmarking
- Paper

3 CAPÍTULO 3: ESTADO DEL ARTE

En el presente capítulo “Estado del arte” se presenta la recopilación de investigaciones relacionadas al título del proyecto “Modelo de Gestión de Riesgos de Seguridad de la Información para Pymes en el Perú”. Estos se agrupan dependiendo de su aporte al proyecto, ya sea por el aporte al problema o por el aporte a las definiciones de la metodología OCTAVE-S y la Norma ISO/IEC 27005.

3.1 Revisión Literaria

Para el presente trabajo se realizaron investigaciones referentes a seguridad de la información, análisis de riesgo, gestión de riesgos, metodología de Gestión de riesgos (OCTAVE-S) e ISO/IEC 27005.

3.2 Estado del arte

En el estudio de Pacheco (2013) señala que la seguridad de la información no ha sido muy desarrollada en la educación superior, tanto pública como privada en todo el mundo. Fue a partir de la tragedia de la caída de las torres gemelas en el 2011, donde el mundo de los negocios da un giro y empieza a enfocarse en actividades relacionadas a seguridad desarrollando así las mejoras a los procesos de planes de contingencias, continuidad de

negocios y recuperación ante desastres, donde la seguridad de la información es quien dirige (Pacheco).

La seguridad en una empresa tiene muchas formas y variaciones; por ejemplo, las operaciones de seguridad, seguridad de la producción, la seguridad del personal, seguridad informática, etc.; estos dependen unos de otros para construir la seguridad total (Finne, 2000). También se define a la seguridad de información como la protección de los activos de información contra la divulgación, modificación o destrucción accidental o intencional pero no autorizada, o la incapacidad de procesar esa información (IBM Data Security Support Programs, 1984).

Según Pacheco, en diversos lugares del mundo promovieron la inclusión de programas educativos orientados en seguridad de la información, sin embargo, en Argentina las universidades solo habían destinado escasas horas a dicho tema a modo de materia optativa, y esta materia solo era dictada para las carreras de ingeniería en sistemas o informática (The Need for Formal Education on Information Security).

En el artículo de Mana Gonçalves & Neves Fernandes indica que la Policía Federal de Brasil ha desarrollado una iniciativa para combatir los delitos de seguridad de información. La Figura 1 muestra el aumento de delitos en línea, este figura muestra las estadísticas de incidentes de seguridad de la información que se han reportado en el país (Mana Gonçalves & Neves Fernandes, The Impact of Information Security on Latin America, 2009).

Figura 1. Total de incidentes de seguridad reportadas.

Elaborado por Mana Gonçalves & Neves Fernandes, The Impact of Information Security on Latin America, 2009.

Estos incidentes reportados fueron de muchos aspectos, como se puede observar en la Tabla 4.

Tabla 4

Tipos de incidentes reportados¹

Month	Worm	DoS	Inv.	Web	Scan	Fraud	Others
Jan	26.748	0	13	364	3.859	74.909	52
Feb	3.524	3	5	457	3.398	66.214	282
Mar	773	3	12	342	4.392	32.44	284
Total	31.045	6	30	1.163	11.649	173.563	618

Fuente: Elaborado por Mana Gonçalves & Neves Fernandes, The Impact of Information Security on Latin America, 2009.

¹ Worm: informes de actividades maliciosas relacionadas con el proceso automatizado de propagación de código malicioso en la red. DoS (DoS - Denial of Service): informes de ataques de denegación de servicio en los que el atacante utiliza una computadora o un conjunto de equipos para aprovechar una operación de servicio, una computadora o una red. Inv. (Invasión): un ataque exitoso que da como resultado el acceso no autorizado a una computadora o red. Web: un caso particular de un ataque específicamente dirigido a la participación de servidores web o desfiguraciones de páginas en Internet. Scan: Escanea en informes de redes informáticas, con el fin de identificar qué equipos están activos y qué servicios se proporcionan para ellos. Es ampliamente utilizado por los atacantes para identificar objetivos potenciales, ya que permite vulnerabilidades potenciales asociados a los servicios habilitados en un equipo. Fraud: un intento de fraude, o incidente que ocurre en un intento de obtener ventaja, generalmente financiero. Otros: otros tipos de incidentes.

Pacheco indica que la seguridad de la información es un aspecto clave en el funcionamiento de toda organización y es por ello que se requiere profesionales capacitados a la altura de las exigencias del mercado corporativo.

Behnia, Rashid, & Chaudhry (2012) define al análisis de riesgo como la base de la protección de la información, la gestión de riesgos y el riesgo en el proceso de protección de la información. Además, Beranek (2012) indica que el análisis de riesgos de seguridad es fundamental para la seguridad de cualquier organización, ya que esta es esencial para asegurar que los controles son totalmente proporcionales a los riesgos a los que la organización está expuesta y los procesos relevantes están en conformidad con las políticas de seguridad.

El propósito de cualquier análisis de riesgo es proporcionar a los que toman las decisiones la mejor información posible sobre la probabilidad de pérdida (Behnia, Rashid, & Chaudhry, 2012). Según Feng, Jiannan Wang, & Li, los enfoques existentes para el análisis de riesgos pueden agruparse en tres categorías principales: los enfoques cualitativos, los enfoques cuantitativos y la combinación de enfoques cuantitativos y cualitativos.

Según Behnia, Rashid, & Chaudhry indican que enfoque cualitativo clasifica la magnitud del impacto potencial de una amenaza como alta, media o baja. El enfoque cualitativo es la medida más común del impacto de los riesgos. Este método o enfoque permite a las entidades cubiertas evaluar todos los impactos potenciales, ya sean tangibles o intocables (Behnia, Rashid, & Chaudhry, 2012). La tabla 5 muestra estudios realizados según este enfoque relacionados a la gestión de riesgos.

Tabla 5
Estudios con enfoque cualitativo

N°	ESTUDIOS CON ENFOQUE CUALITATIVO	
	Estudio	Referencia
1	Método de descripción rica (RDM) el cual adopta una visión menos formal y más integrada de los activos de información y conocimiento que existen en los ambientes de trabajo modernos. Este método propuesto utiliza técnicas de análisis y recopilación de datos más relevantes de metodologías cualitativas, y se basa en la distinción	(Shedden, Ahmad, Tscherning, Smith, & Scheepers, 2016)

N°	ESTUDIOS CON ENFOQUE CUALITATIVO	
	Estudio	Referencia
	entre los aspectos formales e informales de las organizaciones y como se estos se relacionan.	
2	Modelo cualitativo EVAO que resulta ser la mejora de la metodología VECTOR mediante la adaptación de OCTAVE para en análisis de proceso de migración de software. Dicho modelo permite a los usuarios cuantificar y representar visualmente todos los aspectos posibles del riesgo para el sistema empresarial.	(Hakemi, Ryul , Jeong, Ghani, & Sanaei, 2014)
3	Modelo basado en la combinación de 6 metodologías con enfoque cualitativo identificando las características mutuas, su modelo propuesto es para cualquier organización, independiente de su tamaño, indican también que los involucrados en realizar el análisis del riesgo deben tener la habilidad, calificación, experiencia y formación requerida.	(Shamala, Ahmad, & Yusoff, 2013)
4	Modelo cualitativo basado en la integración de dos metodologías FRAPP y BITS, teniendo como metodología base a BITS. En esta integración, el autor utiliza la evaluación de los activos de FRAPP y para el resto del proceso de análisis se basa en BITS.	(Beranek, 2012)

Los enfoques cuantitativos utilizan modelos matemáticos y estadísticos para representar el riesgo a diferencia del modelo cualitativo (Feng, Harry, & Li, A security risk analysis model for information systems, 2013). La exposición al riesgo de seguridad se representa como una función de la probabilidad de las amenazas y la pérdida esperada debido a la vulnerabilidad a esas amenazas (Büyüközkan & Ruan, 2010). La tabla 6 muestra estudios realizados según este enfoque relacionados a la gestión de riesgos.

Tabla 6
Estudios con enfoque cuantitativo

N°	ESTUDIOS CON ENFOQUE CUANTITATIVO	
	Estudio	Referencia
1	Modelo sistemático, extensible y modular con el objetivo de ayudar a los gerentes a evaluar con precisión las amenazas de seguridad. Dicho modelo cuantifica el costo de la pérdida que resulta de las amenazas y vulnerabilidades teniendo de esta manera los gerentes una visión más detallada de los costos.	(Mouna, Latifa, & Ridha, 2015)
2	Modelo de análisis de riesgo de seguridad integrado con Redes Bayesianas (BNs) y optimización de colonia de hormigas, para poder desarrollar la red bayesiana se tiene que integrar las bases de datos de casos observados con experiencia y conocimiento de expertos con la finalidad de representar los factores relacionados al riesgo y mecanismos causales.	(Feng, Harry, & Li, 2013). A security risk analysis model for information systems,

Behnia, Rashid, & Chaudhry (2012) indican que los métodos cuantitativos pueden no ser capaces de modelar escenarios de riesgo complejos en la actualidad. Los métodos de análisis de riesgos basados en medidas cualitativas son más adecuados para el complicado entorno de riesgo de los sistemas de información actuales. Sin embargo, una debilidad significativa del método de análisis cualitativo es el criterio de riesgo de aquellos que crean resultados inestables. An Wang (2005) elaboró que las métricas de seguridad son más comúnmente cualitativas que cuantitativas.

En general, los riesgos de los sistemas de información se analizan mediante un análisis de riesgo probabilístico, en el que se calcula el impacto en la organización y la probabilidad de que se produzca el riesgo. La evaluación del riesgo utiliza los resultados del análisis, y si el riesgo se considera inaceptable, se implementan tratamientos de riesgo, que consiste en elegir una estrategia y medidas para controlar eventos indeseables (Wangen & Snekenes, 2014).

Debido a las fortalezas y debilidades tanto de las evaluaciones cuantitativas como cualitativas, existe un enfoque híbrido. De esta manera, la organización puede beneficiarse

de la sencillez y rapidez de las evaluaciones cualitativas, aprovechando al mismo tiempo la valoración cuantitativa de sus activos más críticos (Alireza, Rouzbeh, & Mohamed, 2015). La tabla 7 muestra estudios realizados según este enfoque relacionados a la gestión de riesgos.

Tabla 7
Estudios con enfoque híbrido

N°	ESTUDIOS CON ENFOQUE HÍBRIDO	
	Estudio	Referencia
1	Modelo para el entorno de red de una Universidad basado en OCTAVE, con el fin de reducir el riesgo de incumplimiento de la seguridad mediante el apoyo a actividades. La primera fase evalúa las amenazas y vulnerabilidades con el fin de identificar el punto débil, la segunda fase se centra en el riesgo más alto y crear un plan de mitigación y la tercera fase reconoce el requisito de cumplimiento de la gestión de la vulnerabilidad para mejorar la seguridad de la Universidad. Su objetivo es medir cuantitativamente el nivel de riesgo que permitirá a los institutos de educación superior entender los riesgos de seguridad de la información.	(Chanchala & Umesh, 2017)
2	Modelo híbrido conformado por la ISO 27005, OCTAVE-S y MAGERIT que tienen el enfoque cualitativo y para el enfoque cuantitativo se basa en el modelo IFRS (International Financial Reporting Standard). Dicho modelo fue aplicado a dos PYMES ecuatorianas, con el objetivo de generar una solución práctica de un problema de gestión de TI para lo cual se necesita el diseño formal y un proceso de evaluación que asegure la calidad de la solución	(Montenegro & Moncayo, 2016)
3	Modelo con enfoque híbrido que propone una formulación matemática del riesgo utilizando un menor nivel de granularidad de sus elementos tales como amenaza, probabilidad, criterios para determinar el valor de un	(Faris, Ghazouani, Medromi, & Sayouti, 2014).

N°	ESTUDIOS CON ENFOQUE HÍBRIDO	
	Estudio	Referencia
	activo, la exposición, la frecuencia y la medida de protección. Para el enfoque cualitativo dicho autores hicieron uso de encuestas y cuestionarios internos para lograr la recolección de datos	

En el estudio de Behnia, Rashid, & Chaudhry indica que la metodología OCTAVE se centra en actividades, amenazas y vulnerabilidades. Además, uno de los conceptos principales de OCTAVE es la autodirección; es decir, que las personas dentro de la organización deben practicar la seguridad de la información evaluación de riesgos (Bornman & Labuschagne, 2004). En dicho estudio concluye que, si una organización se preocupa por la simplicidad en lugar de la precisión, OCTAVE es un buen ajuste.

En el estudio de Shukla & Kumar, se comparan diferentes metodologías de gestión de riesgos para la seguridad de información. En dicha investigación, describe las metodologías de OCTAVE, CORAS, CRAMM.

Según los autores Stolen, Brader, Lund, & Aagedal (2002), indican en su estudio que uno de los principales objetivos de CORAS es desarrollar una estructura que utilice los métodos de análisis de riesgos, los métodos semi-formales para el modelado orientado a objetos y las herramientas informáticas para una evaluación precisa y no ambigua del riesgo y sistemas críticos eficientes de seguridad (Fredriksen, y otros). La metodología CORAS se basa en UML (Unified Modeling Language), un lenguaje que utiliza diagramas para ilustrar las relaciones y las dependencias entre los usuarios y el entorno en el que trabajan. El marco tiene cuatro pilares principales, de los cuales la gestión de riesgos es uno.

$$Perdida = Impacto \times Probalidad$$

El Método de Análisis y Gestión de Riesgos (CRAMM) (2012), es una herramienta cualitativa de análisis y gestión de riesgos desarrollada por la Agencia Central de Informática y Telecomunicaciones en 1985 para proporcionar a los departamentos gubernamentales un método para revisar la seguridad de los sistemas de información. CRAMM, también se puede utilizar para todo tipo de organizaciones. Los aspectos cruciales de la recolección de datos, el análisis y los resultados de producción que deben estar presentes en una herramienta de

análisis de riesgo programada se cubren en las tres etapas de una revisión CRAMM, las cuales son las siguientes:

- Reconocimiento y valoración de activos.
- Reconocimiento de amenazas y vulnerabilidades, riesgos informáticos.
- Reconocer y priorizar las contramedidas.

CRAMM a diferencia de OCTAVE y CORAS que calculan el riesgo en un intervalo del 1 al 3 (2012), esta calcula el riesgo para cada grupo de activos frente a las amenazas a las que es vulnerable en una escala de 1 a 7 utilizando una matriz de riesgo con los valores por defecto comparándolo con el nivel de actividad de amenaza y vulnerabilidad. En esta escala, 1 implica un requisito fundamental de seguridad y 7 muestra un requisito de seguridad muy alto (Yazar, 2011).

Tabla 8

Marco de comparación de metodologías de análisis de riesgo

CRITERIA	QUALITATIVE		
	OCTAVE	CORAS	CRAMM
Method/Tools	Method/Tools	Tools	Method/Tools
Method/Tool Name	OCTAVEv2.0 OCTAVE – S v1.0	CORAS Editor v.1.1	CCTA Risk Analysis and Management Method
Vendor Name	Carnegie Mellon University, SEI(Software Engineering Institute)	European Commission	Insight Consulting
Country of Origin	USA	Intracom(Greece) Solinet(Germany) Telenor(Norway)	United Kingdom
Date of First Release	Version 0.9 1999	January 2001	1985
Languages	English	English	English, Dutch, Czech
Price	Free	Free	Unknown
Compliance to IT Standards	N/A	ISO 31000 ISO/IEC17799 AS/NZS 4360	ISO/IEC17799
Skills Needed	Standard	Standard	Specialist
Availability	Trial version available, registration required	Trial version available, registration required	Registration required
Tools Supporting the Method	Commercial Tools - Licensed materials - Trainings	An XML Mark-up for exchange of risk assessment data -A UML based specification language targeting security risk assessment	Commercial Tools -CRAMM Expert (Insight) -CRAMM Express(Insight)

Fuente: Elaborado por Shukla & Kumar, 2012

En el artículo de Hoffman, Kiedrowicz, & Stanik señalan que la gestión de riesgos se convierte en un elemento importante de la gestión estratégica de las empresas y, en muchos casos, son cruciales para racionalizar las actividades comerciales y continuar las operaciones. Además, indican que para gestionar correctamente el riesgo de la organización es necesario conocer el papel de la gestión de riesgos (Hoffman, Kiedrowicz, & Stanik, 2016).

Caelli en su libro *Information Security for Managers* indica que la gestión de riesgos tiene como objetivo "identificar, medir y controlar eventos inciertos" con el fin de minimizar las pérdidas y optimizar el rendimiento del dinero invertido para fines de seguridad. En la investigación de Shukla & Kumar (2012) define a la gestión de riesgos como un proceso de políticas en el que se pesan estrategias alternativas para hacer frente al riesgo y se toman decisiones sobre riesgos aceptables. Las estrategias consisten en opciones de política que tienen diversos efectos sobre el riesgo, incluyendo la reducción, remoción o reasignación del riesgo. Un marco de riesgo formal puede ser una herramienta útil para descomponer el problema de la gestión de riesgos (Shukla & Kumar, 2012).

Desde hace una década, las empresas que tienen muchos intercambios de datos con otras empresas (nacionales o internacionales) o con muchos socios y clientes, han experimentado la necesidad de acordar normas para asegurar la información y los procesos de intercambio. Es precisamente establecer una marca de confianza para la seguridad general de la información dentro de las empresas lo que condujo a la creación de la norma ISO / IEC 27005 (Lalanne, Munier, & Gabillon, 2013).

Asimismo, Lalanne, Munier y Gabillon, mencionan que para implementar de manera efectiva esta norma, se puede integrar con las metodologías de gestión de riesgo como CRAMM5, OCTAVE o EBIOS6.

Giri y Prasetyo muestran una tabla comparativa con algunos marcos de gestión de riesgo de seguridad de la información como NIST SP 800-300, OCTAVE e ISO/IEC 27005.

Tabla 9

Comparativo de marcos de referencia de gestión de riesgos de seguridad de la información

Framework	ISO 27005	OCTAVE	NIST SP-800-30
Description	Complete proses in generic manner	Self directed approach	Very detailed guidance and identification
Trget Organization	Goverment, Large Companies SME.	SME	Goverment, Large Companies SME.
Target Level Organization	Management, Operational	Management, Operational	Management, Operational

Fuente: Elaborado por Prasetyo & Giri Sucahyo, 2014

Para concluir, la gestión de riesgos permitirá crear valor para las empresas Pymes a través de la optimización del nivel del riesgo contribuyendo al logro de los objetivos organizacionales; además de fortalecer la cultura e imagen institucional a través de la generación de confianza de los grupos de interés, quienes podrán sentirse seguros de que su información está siendo adecuadamente protegida.

De los enfoques mencionados tomamos como base el híbrido, debido a la evaluación sencilla y rápida del enfoque cualitativo y aprovechar los valores identificados para los activos del enfoque cuantitativo. Así también, tomamos como base la norma ISO/IEC 27005 debido a que cumple con los estándares internacionales en gestión de riesgos de seguridad de la información, y como esta no cuenta con una metodología, nos basaremos en OCTAVE, ya que es tiene un análisis más detallado y puede ser aplicado a pequeñas y medianas empresas utilizando el método OCTAVE-S.

4 CAPÍTULO 4: MARCO TEÓRICO

En el presente capítulo se definen los conceptos principales relacionados con el proyecto, conceptos relacionados a la gestión de riesgo y el enfoque de la seguridad de la información. En este caso, la metodología de gestión de riesgos utilizada es OCTAVE-S, la cual también será definida. Como el proyecto se enfoca en la seguridad de la información, se definen

conceptos relacionados. Este proyecto integra la metodología OCTAVE-S con la norma ISO/IEC 27005, donde se definen conceptos esenciales relacionados a la metodología y a la norma para poder comprender el desarrollo del proyecto, en el cual se realiza un análisis de riesgos de seguridad de la información en una empresa de productos de arcilla cerámica sobre el proceso de ventas.

4.1 Seguridad de la información

La información es un activo valioso para la institución, y en consecuencia requiere una protección adecuada (INDECOPI).

El activo es algo que tiene valor para la empresa. Los activos de tecnología de la información son la combinación de activos lógicos y físicos y se agrupan en clases específicas. Las categorías de activos:

- Información (documentada o electrónica) documentada o propiedad intelectual utilizada para cumplir con la misión de una organización o área o proceso escogido.
- Sistemas: una combinación de recursos de información, software y hardware que procesan y almacenan información.
- Servicios y aplicaciones: aplicaciones y servicios de software (sistemas operativos, aplicaciones de bases de datos, software de redes, aplicaciones de oficina, aplicaciones personalizadas, etc.) que procesan, almacenan o transmiten información.
- Personas: las personas de una organización que poseen habilidades, conocimientos y experiencia únicos que son difíciles de reemplazar (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

En una evaluación del riesgo de seguridad de la información, los activos deben estar ligados a la información de alguna manera (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

A continuación, se mencionan los principios de seguridad de la información:

- Confidencialidad: la necesidad de mantener información privada, confidencial o personal privada e inaccesible para cualquier persona que no esté autorizada a verla
- Integridad: autenticidad, exactitud e integridad de un activo.

- Disponibilidad: cuándo o con qué frecuencia un activo debe estar presente o listo para su uso (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

Se puede incluir también otras propiedades como la autenticidad, responsabilidad, no-repudio y confidencialidad (ISO/IEC, 2015).

La seguridad de la información protege a la información de un amplio rango de amenazas para asegurar la continuidad de las actividades de la institución y minimizar daños (INDECOPI).

4.2 Gestión de riesgos

Actividades coordinadas para dirigir y controlar una organización con relación al riesgo (ISO/IEC, 2002).

El proceso de la gestión de riesgos es identificar, analizar y responder a factores de riesgo. Una gestión de riesgos adecuada implica el control de posibles eventos futuros que puedan causar un daño a la organización o las personas relacionadas a ella.

Existen diferentes enfoques propuestos para el proceso de gestión de riesgos (Kasap & Murat, 2007):

1. Planificación de la gestión de riesgos: se asegura que los objetivos están claramente definidos y entendidos. Es necesario definir las funciones y responsabilidades, la metodología y el enfoque, la frecuencia de la revisión y la presentación de informes, etc.
2. Identificación del riesgo: se determina qué podría afectar y cómo podría suceder, se identifican amenazas y vulnerabilidades. Al final se obtendrá una lista de posibles riesgos.
3. Análisis de riesgos: los riesgos se deben analizar en términos de probabilidad de ocurrencia e impacto. Se debe evaluar la probabilidad y asignarle un criterio ya sea alto, medio o bajo, el mismo caso para el impacto. Con esta información se podrá determinar la clasificación actual para cada riesgo proporcionando una medida de exposición de riesgo.
4. Respuesta al riesgo: se desarrollan respuestas a los riesgos identificados que son apropiados, alcanzables y asequibles o para reducir el riesgo de alguno de ellos. Estas respuestas pueden ser:

- Evitar: busca la eliminación de la incertidumbre, lo que hará imposible que se produzca el riesgo, o que se ejecute de una manera diferente que pueda lograr los mismos objetivos pero que aisle el efecto del riesgo.
 - Transferir: identificar a una parte interesada que pueda gestionar el riesgo, tendrá la responsabilidad e identificará las acciones posibles.
 - Mitigar: se reducen los riesgos para hacerlos más aceptables para la organización, se reduce la probabilidad y el impacto.
 - Aceptar: se aceptan los riesgos y se responde de manera activa mediante la asignación de la contingencia adecuada, o en todo caso no se realiza ninguna acción, excepto el seguimiento de la situación de riesgo.
5. Seguimiento y control de riesgos: se monitorearán los riesgos de forma continua, ya sea semanalmente, mensualmente o trimestralmente. Los riesgos serán reevaluados por su probabilidad de ocurrencia e impacto. Se identificarán nuevos riesgos y los existentes se podrán retirar una vez que se alcance una solución para ellos.

Existen tantas metodologías y normas de gestión de riesgo disponibles que muchas de las empresas no saben cuál de estos deben de utilizar o se adaptaría mejor a su organización. Algunas de las metodologías más conocidas son: OCTAVE, MAGERIT, MEHARI, CRAMM, sp800-30 NIST, etc; así como las normas ISO/IEC 27005 y ISO/IEC 31000.

4.2.1 Metodología OCTAVE

OCTAVE significa “Operationally Critical Threat, Asset and Vulnerability Evaluation”, publicado por SEI, en la Universidad Carnegie Mellon en 1999. OCTAVE es una evaluación estratégica basada en riesgos y una técnica de planificación para la seguridad. 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 C. , Dorofee, Stevens, & Woody, Introduction to the OCTAVE Approach, 2003). Cuando se aplica OCTAVE, un pequeño equipo de personas de las unidades operativas (o de negocios) y el departamento de tecnología de la información (TI) trabajan juntos para satisfacer las necesidades de seguridad de la organización, equilibrando los tres aspectos clave: riesgo operacional, tecnología y prácticas de seguridad (Figura 2).

Figura 2. OCTAVE equilibra tres aspectos

Elaborado por Alberts C., Dorofee, Stevens, & Woody, Introduction to the OCTAVE Approach, 2003

OCTAVE tiene tres métodos:

1. OCTAVE: el enfoque de OCTAVE se basa en dos aspectos el riesgo operacional y las prácticas de seguridad. La tecnología se examina sólo en relación con las prácticas de seguridad, lo que permite a una organización perfeccionar la visión de sus prácticas actuales de seguridad. Mediante el uso de este enfoque, 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, lo que permite a una organización combinar una estrategia de protección basada en prácticas con sus riesgos de seguridad. Es auto dirigido, requiere una organización para administrar el proceso de evaluación y tomar decisiones de protección de la información.

Los aspectos organizativos, tecnológicos y de análisis de una evaluación del riesgo de seguridad de la información se complementan con un enfoque en tres fases (Figura 3).

- Fase 1: Generación de perfiles de amenazas basados en activos, evaluación organizacional.
- Fase 2: Identificar Vulnerabilidades de Infraestructura, una evaluación de la infraestructura de información.

- Fase 3: Desarrollo de estrategias y planes de seguridad, se identifican los riesgos para los activos críticos de la organización y decide qué hacer con ellos (Alberts C. , Dorofee, Stevens, & Woody, Introduction to the OCTAVE Approach, 2003).

Figura 3. Fases de OCTAVE.

Elaborado por El arte de gestionar la información, 2016

2. OCTAVE-S: es una variación del enfoque OCTAVE adaptado a los medios limitados y las limitaciones únicas típicamente encontradas en las pequeñas organizaciones. OCTAVE-S está dirigido por un pequeño equipo interdisciplinario (de tres a cinco personas) de personal 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. Para llevar a cabo OCTAVE-S de manera efectiva, el equipo debe tener un amplio conocimiento de los procesos de negocios y seguridad de la organización, por lo que será capaz de llevar a cabo todas las actividades por sí mismo. Esta metodología pone énfasis en las prácticas de riesgo operacional y seguridad. Además, OCTAVE-S se basa en las tres fases descritas en OCTAVE, aunque el número y la secuencia de actividades difieren de los utilizados en el Método OCTAVE (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

- Fase 1: generación de perfiles de amenazas basados en activos. La Tabla 10 ilustra los procesos y actividades de esta fase.

Tabla 10
OCTAVE-S – Procesos y actividades de la fase 1

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

Fuente: Elaborado por Alberts C., Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005.

- Fase 2: Identificar vulnerabilidades de Infraestructura, el equipo de análisis lleva a cabo una revisión de alto nivel de la infraestructura de computación de la organización, se centra en el grado en que la seguridad es considerada por los mantenedores de la infraestructura. La Tabla 11 ilustra los procesos y actividades de esta fase.

Tabla 11
OCTAVE-S – Procesos y actividades de la fase 2

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

Fuente: Elaborado por Alberts C., Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005.

- Fase 3: Desarrollar estrategias y planes de seguridad, el equipo de análisis identifica los riesgos para los activos críticos de la organización y decide qué hacer con ellos. Se basan en un análisis de la información recopilada, el equipo crea una estrategia de protección para la organización y planes de mitigación para abordar los riesgos de los activos críticos. Las hojas de trabajo de OCTAVE-S utilizadas durante la Fase 3 están altamente estructuradas y estrechamente vinculadas al catálogo de prácticas de OCTAVE, lo que permite al equipo relacionar sus recomendaciones de mejora con una referencia aceptada de la práctica de seguridad. La Tabla 12 describe los procesos y actividades de la Fase 3.

Tabla 12
OCTAVE-S – Procesos y actividades de la fase 3

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 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

Fuente: Elaborado por Alberts C., Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005.

3. OCTAVE ALLEGRO: El enfoque de OCTAVE Allegro 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. Este enfoque difiere de los enfoques anteriores de OCTAVE centrándose principalmente en los activos de información en el contexto de cómo se utilizan, donde se almacenan, transportan y procesan, y cómo se exponen a amenazas, vulnerabilidades e interrupciones como resultado. OCTAVE Allegro puede realizarse en un entorno de colaboración y colaboración, y está respaldado por guías, hojas de trabajo y cuestionarios. Sin embargo, OCTAVE Allegro 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).

OCTAVE Allegro consta de ocho pasos que se organizan en cuatro fases, como se ilustra en la Figura 4. En la fase 1, la organización desarrolla criterios de medición de riesgo

consistentes con los impulsores de la organización. Durante la segunda fase, se perfilan los activos de información que se determinan críticos. Este proceso de establecimiento de perfiles establece límites claros para el activo, identifica sus requisitos de seguridad e identifica todos los lugares donde se almacena, transporta o procesa el activo. En la fase 3, las amenazas al activo de información se identifican en el contexto de las ubicaciones donde se almacena, transporta o procesa el activo. En la fase final, se identifican y analizan los riesgos de los activos de información y se inicia el desarrollo de los enfoques de mitigación (Caralli, Stevens, Young, & Wilson, 2007).

Figura 4. Roadmap OCTAVE Allegro.

Elaborado por Caralli, Stevens, Young, & Wilson, 2007

4.2.2 ISO/IEC 27005

Para comenzar debemos entender el significado de ISO y IEC:

- ISO: International Standardization Organization, es una organización internacional independiente, no gubernamental. Se encargan de dar las especificaciones de clase mundial de productos, servicios y sistemas, para garantizar la calidad, seguridad y eficiencia. Son fundamentales para facilitar el comercio internacional (ISO).
- IEC: International Electrotechnical Commission, es una organización cuasi-gubernamental sin ánimo de lucro, fundada en 1906. Organización global líder que publica estándares internacionales basados en el consenso y gestiona sistemas de evaluación de la

conformidad para productos, sistemas y servicios eléctricos y electrónicos, conocidos colectivamente como electrotécnica (IEC).

La ISO/IEC 27005 es una norma Internacional que proporciona directrices para la gestión del riesgo de seguridad de la información en una organización, apoyando en particular los requisitos de una gestión de la seguridad de la información (SGSI) de acuerdo con ISO / IEC 27001. Sin embargo, ésta no proporciona ningún método específico para la gestión de riesgos de seguridad, es por ello que, corresponde a la organización definir su enfoque de la gestión de riesgos. Esta Norma Internacional es pertinente para los administradores y el personal que se ocupan de la gestión del riesgo de seguridad de la información dentro de una organización y, cuando proceda, de las partes externas que apoyan dichas actividades (ISO/IEC, 2011).

Es necesario un enfoque sistemático de la gestión del riesgo de la seguridad de la información para identificar las necesidades de la organización en relación con los requisitos y crear un sistema eficaz de gestión de la seguridad de la información. Este enfoque debe ser adecuado para el entorno de la organización y, debe estar alineado con la gestión general del riesgo empresarial. Los esfuerzos de seguridad deben abordar los riesgos de manera efectiva y oportuna donde y cuando se necesiten. La gestión del riesgo de seguridad de la información debe ser una parte integral de todas las actividades de gestión de la seguridad de la información y debe aplicarse tanto a la implementación como al funcionamiento en curso de un SGSI. La gestión de riesgos de seguridad de la información debe ser un proceso continuo. El proceso debe establecer el contexto externo e interno, evaluar y tratar los riesgos utilizando un plan de tratamiento de riesgos para implementar las recomendaciones y decisiones. La gestión de riesgos analiza lo que puede suceder y cuáles pueden ser las posibles consecuencias, antes de decidir qué debe hacerse y cuándo, reducir el riesgo a un nivel aceptable (ISO/IEC, 2011). La Figura 5 muestra cómo esta Norma Internacional aplica el proceso de gestión de riesgos.

Figura 5. Proceso de gestión de riesgos de seguridad de la información.

Elaborado por Segura, 2009

El proceso de gestión del riesgo de seguridad de la información puede ser iterativo para la evaluación de riesgos y actividades de tratamiento de riesgos. El enfoque iterativo proporciona un buen equilibrio entre minimizar el tiempo y el esfuerzo dedicado a identificar los controles, al tiempo que se asegura que los riesgos altos se evalúan adecuadamente (ISO/IEC, 2011).

4.3 Conceptos relacionados a la integración

4.3.1 Activo crítico

Son los activos más importantes para una organización. La organización sufrirá un gran impacto adverso si

- Un activo crítico es revelado a personas no autorizadas.
- Un activo crítico se modifica sin autorización.
- Se pierde o se destruye un activo crítico.
- El acceso a un activo crítico se interrumpe (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

4.3.2 Amenaza

Indicación de un posible evento indeseable. Una amenaza se refiere a una situación en la que una persona podría hacer algo indeseable (un atacante que inicia un ataque de denegación de servicio contra el servidor de correo electrónico de una organización) o una ocurrencia natural podría causar un resultado indeseable (un incendio dañando el hardware de tecnología de información de una organización) (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

4.3.3 Catálogo de prácticas

Colección de buenas prácticas estratégicas y operativas de seguridad que una organización puede utilizar para administrar su seguridad (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

4.3.4 Clases de componentes

Categorías de dispositivos y redes utilizadas para acceder a un sistema de interés. Estos dispositivos y redes son parte o relacionados con un sistema de interés. Cuando los usuarios legítimos acceden a un activo crítico, acceden a los componentes de estas clases. Los actores de amenaza también tienen acceso a componentes de estas clases cuando los actores deliberadamente apuntan a un activo crítico (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

4.3.5 Criterios de evaluación de impacto

Criterios de evaluación de impacto: conjunto de medidas cualitativas en las que se evalúa el efecto de cada riesgo sobre la misión y los objetivos empresariales de una organización. Los criterios de evaluación de impacto definen rangos de impactos altos, medios y bajos para una organización (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

4.3.6 Criterios de evaluación de probabilidad

Criterios de evaluación de la probabilidad: un conjunto de medidas cualitativas utilizadas para estimar la probabilidad de que ocurra una amenaza. Los criterios de evaluación de probabilidad definen los rangos de frecuencias para probabilidades altas, medias y bajas; Indican la frecuencia con la que se producen las amenazas durante un período de tiempo común (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

4.3.7 Estado del semáforo

Qué tan bien está realizando una organización en un área o qué tan bien se encuentra en una valorización. Los colores siguientes se asignan a un área basada en el rendimiento percibido en esa área:

- Verde: La organización está llevando a cabo las prácticas de seguridad en el área muy bien o la valoración está muy bien; No hay necesidad real de mejora.
- Amarillo: La organización está realizando las prácticas de seguridad hasta cierto punto o la valoración está bien hasta cierto punto. Hay posibilidad de mejora.
- Rojo: La organización no está realizando las prácticas de seguridad en el área y la valoración no es buena para la empresa. Hay mucho espacio para mejorar (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

4.3.8 Frecuencia anualizada

La probabilidad proyectada de que ocurra una amenaza en un año dado (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

4.3.9 Impacto

Efecto de una amenaza sobre la misión de una organización y los objetivos de negocio (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

4.3.10 Lista de acción

Una lista de los elementos de acción a corto plazo identificados durante. Un elemento de acción es algo que una organización pretende completar en el corto plazo. Los elementos de acción generalmente no requieren entrenamiento especializado, cambios en la política ni cambios en las funciones y responsabilidades (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

4.3.11 Perfil de amenaza

Forma estructurada de presentar una serie de amenazas a un activo crítico. Las amenazas en el perfil se agrupan según la fuente de la amenaza (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

4.3.12 Perfil de amenaza genérico

Catálogo de amenazas que contiene una gama de todas las amenazas potenciales bajo consideración. El perfil de amenaza genérico es un punto de partida para crear un perfil de amenaza único para cada activo crítico. Las amenazas se representan usando las siguientes propiedades:

- Activo: algo de valor para la empresa
- Acceso: cómo un actor accede al activo (acceso a la red, acceso físico). El acceso se aplica sólo a los actores humanos.
- Actor: quién o qué puede violar los requisitos de seguridad (confidencialidad, integridad, disponibilidad) de un activo
- Motivo: la intención de un actor (por ejemplo, deliberada o accidental). El motivo sólo se aplica a los actores humanos.
- Resultado: el resultado inmediato (divulgación, modificación, destrucción, pérdida, interrupción) de la violación de los requisitos de seguridad de un activo (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

4.3.13 Prácticas estratégicas

Son prácticas de seguridad que se centran en cuestiones organizativas a nivel político. Incluyen temas relacionados con negocios, así como asuntos que requieren planes y participación de toda la organización (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

4.3.14 Prácticas operativas

Son prácticas de seguridad que se centran en cuestiones relacionadas con la tecnología. Incluyen temas relacionados con cómo las personas usan, interactúan y protegen la tecnología día a día (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

4.3.15 Prácticas de seguridad

Acciones que ayudan a iniciar, implementar y mantener la seguridad dentro de una empresa (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

4.3.16 Probabilidad

La probabilidad de que ocurra un evento (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

4.3.17 Puntos de acceso

Interfaces que directa o indirectamente permiten el acceso a un sistema de interés. Estas interfaces se agrupan de acuerdo con las siguientes categorías:

- Componentes del sistema de interés.
- Acceso al sistema por personas.
- Puntos de acceso intermedios.
- Otras interfaces y ubicaciones de almacenamiento de datos.
- Otros sistemas (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

4.3.18 Puntos de acceso intermedios

Redes utilizadas para transmitir información y aplicaciones del sistema de interés para las personas (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

4.3.19 Requisitos de seguridad

Declaraciones que describen las cualidades de los activos relacionados con la información que son importantes para una organización.

4.3.20 Riesgo

Posibilidad de sufrir daños o pérdidas. Se refiere a una situación en la que una persona podría hacer algo indeseable o una ocurrencia natural podría causar un resultado indeseable, lo que resulta en un impacto negativo o consecuencia.

Un riesgo se compone de:

- Un evento.
- Incertidumbre.
- Una consecuencia (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

4.3.21 Rutas de acceso a la red

Formas en que se puede acceder a los sistemas, dispositivos, información o servicios a través de la red de una organización (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

4.3.22 Sistema de interés

El sistema o sistemas que están más estrechamente vinculados a un activo crítico, por ejemplo:

- El sistema en el que el activo "vive".
- El sistema al que iría para obtener una copia "oficial" del activo.
- El sistema que proporciona a los usuarios legítimos el acceso a un activo crítico.
- El sistema que permite a un actor amenazador acceder a un activo crítico.

4.3.23 Tiempo entre eventos

Estimación de la frecuencia con la que un evento puede ocurrir (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

4.3.24 Ubicación de almacenamiento de datos

Tipos adicionales de componentes utilizados para almacenar información crítica o proporcionar servicios de soporte de datos relacionados con un sistema de interés (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

4.3.25 Valor de impacto

Medida cualitativa del impacto de un riesgo específico para la organización (alta, media o baja) (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

4.3.26 Valor de probabilidad

Medida cualitativa de la probabilidad de una amenaza (alta, media o baja) (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

4.3.27 Vulnerabilidades

Vulnerabilidades organizacionales: son debilidades en la política o práctica de la organización que pueden resultar en acciones no autorizadas (Alberts C. , Dorofee, Stevens, & Woody, OCTAVE-S Implementation Guide - Introduction to OCTAVE-S, 2005).

5 CAPÍTULO 5: DESARROLLO DEL PROYECTO

El siguiente capítulo describe el diseño y elaboración del Modelo de Gestión de Riesgos de Seguridad de la Información para Pymes en el Perú, el cual comprende la metodología utilizada durante el proyecto, la elección de las metodologías y normas de gestión de riesgos de seguridad de la información a utilizar en el modelo, la elaboración del modelo, así como información básica de la empresa donde se validará el modelo, y la situación actual de esta en seguridad de la información.

5.1 Metodología del proyecto

Para el presente proyecto se utiliza la metodología PMBOK, para definir los documentos de gestión en relación al proyecto. Asimismo, para el diseño del modelo de gestión de riesgos de seguridad de la información se utiliza el comparativo realizado de metodologías y normas de gestión de riesgos enfocadas en tecnologías y seguridad de la información.

5.2 Elección de metodología o norma

A continuación, se presenta un cuadro comparativo de las metodologías y normas investigadas que podrían aplicar al proyecto. Las cuales son:

- MAGERIT - Metodología de análisis y Gestión de Riesgos de IT
- OCTAVE - Operational Critical Threat, Asset and Vulnerability Evaluation
- Mehari
- ISO/IEC 27005 Tecnología de la Información - Técnicas de seguridad - Gestión del riesgo de seguridad de la información
- UNE 71504: 2008 Metodología de análisis y gestión de riesgos para los sistemas de Información
- NIST 800-30 Guía de gestión de riesgos para sistemas de tecnología de la información

- ISO TR 13335: 1997 Tecnología de Información - Guías para la gestión de la seguridad de las TI
- AS/NZS ISO 31000:2009
- BS 7799-3: 2006 Sistemas de Gestión de Seguridad de la Información - Parte 3: Guías para la gestión de riesgos de seguridad de la información
- CRAMM - CCTA Risk Analysis and Management Method
- CORAS - Construct a platform for Risk Analysis of Security critical systems
- FRAP/FRAAP - Facilitated Risk Analysis and Assessment Process
- EBIOS - Et Identification des Objectifs de Sécurité
- ISRAM - Information Security Risk Analysis Method
- ISO/IEC 31010
- COBIT for Risk

Se consideraron los siguientes criterios de evaluación:

Criterio de evaluación	Descripción
País	Lugar donde se creó la metodología o norma.
Responsable	Quien creó la metodología o norma.
Enfoque	Principal tema a tratar de la metodología o norma.
Métodos	Métodos dentro de una metodología o norma.
Procesos	Procesos principales dentro de la metodología o norma.
Apoyo	Si la metodología o norma cuenta con guías de apoyo para facilitar su uso.
Herramienta de Soporte	Si la metodología o norma utiliza alguna herramienta ya sea free o premium.
Acceso	Tipo de acceso público o privado.
Elementos	Procesos, Activos, Recursos, Vulnerabilidades, Amenazas y controles.
Tipo de empresas	Pequeña, mediana, grande.
Tipo de análisis	Cualitativo, cuantitativo.
Ayuda a la implementación	Plan de proyecto, Técnicas, Roles, Comparativas, Cuestionarios.
Complejidad	Complejidad baja, media y alta.

Figura 6. Criterios de evaluación.

Elaborado por jefes de proyecto

A cada criterio de evaluación se le asignó una valorización para poder obtener qué metodología o norma se podría elegir:

Criterio de evaluación	Valorización							
País	3	-	2	-	1	Todas las metodologías o normas que son en idioma español.	0	Todas las metodologías o normas que no son en idioma español.
Responsable								
Enfoque	3	-	2	Centrado en seguridad de la información y tecnologías de TI.	1	En relación general.	0	
Métodos								
Procesos	3	-	2	Cuenta con la mayoría procesos principales de la gestión de riesgos.	1	No cuenta con la mayoría de los procesos principales de la gestión de riesgos.	0	
Apoyo	3	-	2	-	1	Cuenta con apoyo.	0	No cuenta con apoyo.
Herramienta de Soporte	3	-	2	-	1	No cuenta con herramienta.	0	Cuenta con herramienta.
Acceso	3	-	2	Acceso Público	1	Acceso Privado	0	-
Elementos	3	-	2	Cuenta con la mayoría de elementos.	1	No cuenta con la mayoría de elementos, tiene alguno de ellos.	0	-
Tipo de empresas	3	-	2	Aplica para la mayoría de empresas.	1	No aplica para la mayoría de tipos de empresa.	0	-
Tipo de análisis	3	-	2	Cuenta con ambos tipo de análisis.	1	Cuenta con alguno de los tipos de análisis.	0	-
Ayuda a la implementación	3	-	2	Cuenta con la mayoría de elementos.	1	No cuenta con la mayoría de elementos, tiene alguno de ellos.	0	-
Complejidad	3	Baja	2	Media	1	Alta	0	-

Figura 7. Valorización de criterios de evaluación.

Elaborado por jefes de proyecto

A continuación, se muestra el cuadro comparativo realizado por cada metodología y norma de gestión de riesgos de seguridad de la información:

	ISO TR 13335: 1997 Tecnología de Información - Guías para la gestión de la seguridad de las TI	AS/NZS ISO 31000:2009	ISO/IEC 31010	ISO/IEC 27005 Tecnología de la Información - Técnicas de seguridad - Gestión del riesgo de seguridad de la información	UNE 71504: 2008 Metodología de análisis y gestión de riesgos para los sistemas de Información	BS 7799-3: 2006 Sistemas de Gestión de Seguridad de la Información - Parte 3: Guías para la gestión de riesgos de seguridad de la información	MAGERIT - Metodología de análisis y Gestión de Riesgos de IT
País	Suiza	Suiza	Suiza	Suiza	España	Reino Unido	España
Responsable	International Organization for Standardization	International Organization for Standardization	International Organization for Standardization - The International Electrotechnical Commission	International Organization for Standardization - The International Electrotechnical Commission	AENOR, Asociación Española de Normalización y Certificación	BSI, British Standards Institution	Ministerio de Administraciones Públicas
Enfoque	Relación entre Gestión de la seguridad de las tecnologías de la Información y la gestión de las propias Tecnologías de la Información.	Gama de actividades, operaciones, procesos, funciones, proyectos, productos, servicios, activos.	Técnicas de Evaluación de Riesgos	Seguridad de la Información	Tecnologías de Información	Gestión de Seguridad de la Información	Tecnologías de Información
Métodos	-	-	-	-	-	-	-
Procesos	<ul style="list-style-type: none"> - Política, estrategia y objetivos de seguridad de TI. - Opciones de estrategia corporativa de Análisis de riesgos. - Implantación de plan de seguridad TI. - Seguimiento. 	<ul style="list-style-type: none"> - Establecer el contexto - Identificar riesgos - Analizar riesgos - Evaluar riesgos - Tratar riesgos - Monitorear y revisar - Comunicar y consultar 	<ul style="list-style-type: none"> - Métodos de consulta - Métodos de soporte - Análisis de escenarios - Análisis de función - Evaluación de controles - Métodos estadísticos 	<ul style="list-style-type: none"> - Establecimiento del contexto. - Valoración del riesgos (Identificación, Estimación y evaluación) - Tratamiento de riesgos. - Aceptación de riesgos. - Comunicación de riesgos. - Monitorización y revisión de riesgos. 	<ul style="list-style-type: none"> - Determinar el contexto - Identificar riesgos - Analizar riesgos - Evaluar riesgos - Tratamiento de los riesgos - Administración de la gestión del riesgo - Comunicación y consulta 	<ul style="list-style-type: none"> - Análisis de riesgos. - Evaluación de riesgos. - Tratamiento de riesgos y decisiones de la dirección. - Actividades de gestión continuo del riesgo. 	<ul style="list-style-type: none"> - Principios. - Diseño del marco de trabajo. - Implementación de la gestión de riesgos. - Seguimiento y revisión del marco. - Mejora continua del marco.
Apoyo	-	-	Guía técnica	-	-	-	Guía técnica
Herramienta de Soporte	-	-	-	-	-	-	PILAR II (Proceso Informático - Lógico)
Acceso	Privado	Privado	Privado	Privado	Privado	Privado	Público
Elementos	Activos, Recursos, Vulnerabilidades, Amenazas y controles.	Activos, Recursos, Vulnerabilidades, Amenazas y controles.	Procesos, Recursos, vulnerabilidades, Controles	Activos, Recursos, Vulnerabilidades, Amenazas y controles.	Activos, Amenazas y controles.	Procesos, Activos, Recursos, Vulnerabilidades, Amenazas y controles.	Activos, Amenazas y controles.
Tipo de empresas	Grande / Mediana / Pequeña	Grande / Mediana / Pequeña	Grande / Mediana / Pequeña	Grande / Mediana / Pequeña	Grande / Mediana / Pequeña	Grande / Mediana / Pequeña	Grande / Mediana / Pequeña
Tipo de análisis	Cualitativo y cuantitativo	Cualitativo y cuantitativo	Cualitativo y cuantitativo	Cualitativo y cuantitativo	Cualitativo y cuantitativo	Cualitativa	Cualitativo y cuantitativo
Ayuda a la implementación	Plan de proyecto y Técnicas	Plan de proyecto y Roles	Plan de proyecto y Roles	Plan de proyecto y Roles	Plan de proyecto y Roles	Plan de proyecto y Roles	Plan de proyecto, Técnicas, Roles, Comparativas
Complejidad	Medio	Medio	Medio	Medio	Medio	Medio	Medio

Figura 8. Comparativo de metodologías - 1

Elaborado por jefes de proyecto

OCTAVE - Operational Critical Threat, Asset and Vulnerability Evaluation	CRAMM - CCTA Risk Analysis and Management Method	NIST 800-30 Guía de gestión de riesgos para sistemas de tecnología de la información	CORAS - Construct a platform for Risk Analysis of Security critical systems	FRAP/FRAAP - Facilitated Risk Analysis and Assessment Process	EBIOS - Et Identification des Objectifs de Sécurité	Mehari	ISRAM - Information Security Risk Analysis Method	COBIT 5 for Risk
Estados Unidos	Reino Unido	Estados Unidos	Europeo (Noruega)	Canadá	Francia	Francia	Turquia	Estados Unidos
Universidad de Carnegie Mellon	Agencia Central de Cómputo y Telecomunicaciones (CCTA)	National Institute of Standards and Technology (NIST)	SINTEF	Peltier Associates	Central Information Systems Security Division	Comisión de métodos de Clusif (Club Francés de la Seguridad de la Información)	CNR Institute of Electronics and Cryptology and Gebze Institute of Technology	ISACA
Análisis y gestión de riesgo de seguridad	Tecnologías de Información	Tecnologías de Información	Seguridad de la Información	Tecnologías de Información	Seguridad de Sistemas de Información	Seguridad de la Información	Seguridad de la información	Riesgos TI
OCTAVE, OCTAVE-S, OCTAVE Allegro	-	-	-	-	-	-	-	-
- Visión organizativa - Visión tecnológica - Estrategia y desarrollo del plan	- Establecimiento de objetivos de seguridad - Evaluación de riesgos - Identificación y selección de contramedidas	- Caracterización de sistemas - Identificación de amenazas - Identificación de vulnerabilidades - Análisis de controles - Determinación de probabilidades - Análisis de impacto - Determinación del riesgo - Recomendación de controles - Documentación de resultados	- Presentación - Análisis de alto nivel - Aprobación - Identificación de riesgos - Estimación de riesgo - Evaluación de riesgo - Tratamiento del riesgo	- Identificar roles e introducción - Revisar el enfoque - Identificar Amenazas - Establecer niveles de riesgo - Priorizar Amenazas - Identificar controles	- Fase 1. Análisis del contexto - Fases 2 y 3, Análisis de las necesidades de seguridad y de las amenazas - Fases 4 y 5, Resolución del conflicto con pruebas de su cumplimiento	- Analizar los principales problemas - Analizar las vulnerabilidades - Disminuir y controlar los riesgos - Supervisar la seguridad de la información	- Conciencia del problema de seguridad de la información - Factores que afectan la probabilidad y las consecuencias - Convertir los factores en preguntas de encuesta - Preparar la tabla de riesgo para la probabilidad y las consecuencias - Realizar la encuesta para determinar la probabilidad y las consecuencias. - Valor de riesgo - Evaluación de los resultados	- Evaluación del riesgo - Gobierno del riesgo - Respuesta al riesgo
Hojas de trabajo	-	-	-	-	Guía de herramienta	Guía análisis, evaluación, referencia, base de datos y de la herramienta.	-	-
-	OCCTA Risk Analysis	-	Coras Editor	FRAP	DCSSI - EBIOS	RISCARE	-	-
Público	Privado	Público	Público	Público	Público	Público	Público	Privado
Procesos, Activos, Recursos, Vulnerabilidades, Amenazas y controles.	Activos, Recursos, Vulnerabilidades, Amenazas y controles.	Recursos, Vulnerabilidades, Amenazas y controles.	Activos, Recursos, Vulnerabilidades, Amenazas y Controles.	Activo, Amenazas y Controles.	Activo, amenazas, vulnerabilidades.	Activo, amenazas, vulnerabilidades y controles.	Recursos, procesos	Activo, amenazas, vulnerabilidades y controles.
Grande / Mediana / Pequeña	Grande / Mediana / Pequeña	Grande / Mediana	Grande / Mediana / Pequeña	Grande / Mediana / Pequeña	Grande / Mediana / Pequeña	Grande / Mediana / Pequeña	Grande / Mediana / Pequeña	Pequeña / Grande / Mediana
Cualitativo	Cualitativo	Cualitativo	Cualitativo	Cualitativo	Cuantitativo	Cualitativa	Cuantitativo	Cualitativo y Cuantitativo
Plan de proyecto, Técnicas, Roles, Cuestionarios	Plan de proyecto, Roles, Comparativas, Cuestionarios	Roles	Plan de proyecto, Comparativas	Plan de proyecto, Técnicas, Roles, Cuestionarios	Plan de proyecto, Técnicas	Plan de proyecto, Técnicas, Roles, Cuestionarios	Plan de proyecto, Roles, Cuestionarios	Plan de proyecto, Roles
Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio

Figura 9. Comparativo de metodologías - 2

Elaborado por jefes de proyecto

Según la valorización mostrada anteriormente, se obtuvieron los siguientes resultados:

Metodología	Puntaje
MAGERIT - Metodología de análisis y Gestión de Riesgos de IT	17
OCTAVE - Operational Critical Threat, Asset and Vulnerability Evaluation	17
Mehari	17
ISO/IEC 27005 Tecnología de la Información - Técnicas de seguridad - Gestión del riesgo de seguridad de la información	17
UNE 71504: 2008 Metodología de análisis y gestión de riesgos para los sistemas de Información	15
NIST 800-30 Guía de gestión de riesgos para sistemas de tecnología de la información	15
COBIT 5 for risk	15
ISO TR 13335: 1997 Tecnología de Información - Guías para la gestión de la seguridad de las TI	14
AS/NZS ISO 31000:2009	14
BS 7799-3: 2006 Sistemas de Gestión de Seguridad de la Información - Parte 3: Guías para la gestión de riesgos de seguridad de la información	14
CRAMM - CCTA Risk Analysis and Management Method	14
CORAS - Construct a platform for Risk Analysis of Security critical systems	14
FRAP/FRAAP - Facilitated Risk Analysis and Assessment Process	14
EBIOS - Et Identification des Objectifs de Sécurité	14
ISRAM - Information Security Risk Analysis Method	14
ISO/IEC 31010	13

Figura 10. Valoración.

Elaborado por jefes de proyecto

Se define que el puntaje no debía ser menor de 16, por lo que se evalúan las metodologías o normas mayores o iguales a este valor.

Como se puede observar en la tabla las metodologías con más puntaje fueron MAGERIT, OCTAVE, Mehari y la norma ISO/IEC 27005:2008. A continuación, se evalúa cada una de ellas para poder encontrar la más idónea:

Para comenzar, la norma ISO/IEC 27005, es una norma internacional, estándar a nivel mundial, relacionada exclusivamente a la seguridad de la información, por lo que para el proyecto tiene un mayor peso, es decir, consideraremos esta norma como principal eje. Según esta norma, nos menciona que se debe de escoger la metodología a utilizar ya que no está definida. Aquí es donde empieza la evaluación para las metodologías MAGERIT, OCTAVE y Mehari.

La metodología Mehari usa de una herramienta para su implementación, por este lado como se quiere desarrollar el proyecto para Pymes donde aún el tema de gestión de riesgos y seguridad de la información no está maduro, vemos que esta herramienta podría dificultar la

aceptación, ya que algunas empresas se rehúsan al cambio. En este punto, se descarta la metodología Mehari.

Para el caso de las metodologías MAGERIT y OCTAVE, tomando en cuenta la gestión de riesgos, se debe de contemplar con todos los elementos principales para la evaluación, en este caso, MAGERIT, no cuenta con la evaluación de vulnerabilidades, que OCTAVE, si cuenta. Asimismo, OCTAVE cuenta con 3 métodos entre los cuales se puede elegir para poder enfocarnos en las pequeñas y medianas empresas como es el alcance de este proyecto, en este caso el método a escoger sería OCTAVE-S, ya que también puede realizarse con un pequeño equipo de trabajo. Un punto adicional a tratar es que OCTAVE contempla procesos y personas dentro de su evaluación, considerar a las personas es un punto importante, ya que es considerada un agente que podría afectar indirecta o directamente a la empresa.

En conclusión, como mencionamos, el proyecto estará basado en seguridad de la información utilizando la norma ISO/IEC 27005 junto con la metodología OCTAVE, específicamente con el método OCTAVE-S.

5.3 Modelo de gestión de riesgos

Basados en la metodología OCTAVE-S y la norma ISO/IEC 27005 se ha diseñado el modelo de gestión de riesgos de seguridad de la información para empresas Pymes, donde se podrá apreciar cada proceso y actividad a ejecutar.

Los requerimientos para ejecutar el modelo en una empresa son los siguientes:

- Empresa catalogada como pequeña o mediana empresa. Aplicable también para un proceso específico, si este cumple que el número de trabajadores es menor a 250.
- Situación actual en gestión de seguridad de la información sea de nivel bajo.
- Pérdidas monetarias por sufrir delitos informáticos.
- Recomendaciones de auditoría pendientes de atender o no se haya realizado alguna auditoría.
- Contar con un área de TI, ya sea interna o con servicios externos contratados.

El modelo cuenta con las siguientes entradas y salidas:

Entradas

- Información de la empresa: información general referida a la empresa como visión, misión, valores, áreas, procesos, etc.
- Situación actual de la empresa: se utiliza el Anexo A de la ISO/IEC 27001, donde se identifica si los controles se cumplen o no. A partir de ello se genera un porcentaje para poder observar en qué nivel de seguridad nos encontramos.
- Información de políticas: información sobre qué políticas tiene la empresa, si se realiza en un proceso, identificar cuales afectan a este. Esta información también ayuda para el punto anterior de identificar la situación actual de la empresa.
- Información TI: información básica de los activos y procesos de TI.
- Informes de pérdidas: información de pérdidas de dinero que haya tenido la empresa referidos a delitos informáticos.

Salidas:

- Estrategia de protección: cómo la organización/proceso se encuentra respecto a las áreas de prácticas actualmente y cómo la evaluación cambiaría dicha situación.
- Plan de mitigación: acciones concretas a realizar sobre lo identificado durante la gestión de riesgos.
- Riesgos: lista de riesgos identificados con su respectiva valorización.
- Controles: lista de controles identificados para implementar a futuro.

Figura 11. Modelo de gestión de riesgos de seguridad de la información para pymes.

Adaptado de la metodología OCTAVE-S y la norma ISO/IEC 27005, elaborado por jefes de proyecto

5.3.1 Selección de equipo de trabajo

Para empezar con el modelo de gestión de riesgos en la empresa, se necesita, como menciona la metodología OCTAVE-S y la Norma ISO/IEC 27005, seleccionar un equipo de trabajo para poder ejecutar cada proceso, ya que es importante que se cuente con las habilidades y conocimientos suficientes. Para ello, se ha creado una lista de requerimientos que deberían de cumplir los miembros del equipo, así como un formato para poder escoger a dichos miembros.

Los requerimientos para formar el equipo son los siguientes:

- El equipo debe estar conformado entre tres a cinco personas.
- El equipo incluye a personas de toda la organización o relacionadas al proceso que se escoja.
- El equipo debe tener conocimiento de los procesos y capacidades de la empresa, así como conocimientos de tecnología de la información y negocios.

Conocimientos requeridos: sistemas utilizados, infraestructura TI, información utilizada, políticas, seguridad de la información, gestión de riesgos, gestión de proyectos e información general de la empresa.

Habilidades requeridas: habilidad para gestionar un equipo de trabajo, buena comunicación, habilidades analíticas y habilidades blandas.

Para seleccionar el equipo de trabajo se debe enfocar en encontrar miembros que puedan desenvolverse en las tres siguientes áreas: área relacionada al negocio, departamento de tecnología de información y áreas operativas.

- Los miembros a elegir según del área relacionada al negocio deben tener un conocimiento general de cómo los sistemas y la información apoya a los procesos de la empresa, así mismo deberán tener conocimiento de las políticas.
- Los miembros a elegir según el departamento de tecnología de información deben tener conocimiento de la infraestructura de TI de la empresa, si este servicio es externo se deberá seleccionar a un responsable para poder apoyar en la ejecución del modelo de gestión de riesgos.
- Los miembros a elegir según las áreas operativas deben tener conocimiento del área escogida donde se realizará la ejecución.

A continuación, se presenta un formato para la selección del equipo de trabajo:

Selección de
equipo.xlsx

SELECCIÓN DE EQUIPO DE TRABAJO			
Áreas relacionadas al negocio			
¿Quién tiene conocimiento de cómo se utilizan los sistemas y la información para apoyar los procesos de la empresa?			
Nombre	Rol	Habilidades y conocimientos	Área
¿Quién tiene conocimiento sobre las políticas y de los procesos de la empresa?			
Nombre	Rol	Habilidades y conocimientos	Área

Figura 12. Formato de selección de equipo de trabajo – Negocio.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Departamento de Tecnologías de Información			
¿Quién tiene conocimiento sobre los sistemas de la empresa (configuración, mantenimiento, etc)?			
Nombre	Rol	Habilidades y conocimientos	Área
¿Quién tiene conocimiento de la infraestructura de TI?			
Nombre	Rol	Habilidades y conocimientos	Área
Si el servicio de TI es externo, ¿Quién tiene conocimiento sobre cómo se configuran y mantienen los sistemas y redes?			
Nombre	Rol	Habilidades y conocimientos	Área

Figura 13. Formato de selección de equipo de trabajo – TI.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Áreas operativas		
¿Qué áreas operacionales de la empresa son más críticas para lograr su misión?		
Área	Key User/Encargado	
¿Qué áreas operacionales afectarían el funcionamiento de la empresa si esas áreas no funcionaran?		
Área	Key User/Encargado	
¿En qué áreas operacionales cree que la información o los sistemas están en mayor riesgo?		
Área	Key User/Encargado	
Equipo de Trabajo		
A partir de las personas identificadas, seleccionar las más convenientes para poder ejecutar el modelo de gestión de riesgos.		
Nombre	Cargo	Área

Figura 14. Formato de selección de equipo de trabajo – Operativas.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Al final del formato se puede escoger a los miembros más convenientes quienes brindan el apoyo para ejecutar el modelo de gestión de riesgos. Usted se encuentra en la decisión si ejecuta los procesos en toda la empresa o en un área o en un proceso crítico encontrado en

el formato antes mostrado. Asimismo, debe asegurar que al menos uno de los miembros tenga conocimiento de este modelo.

A continuación, se explica cada proceso y actividad de las tres fases mostradas en el modelo, asimismo se muestra la relación encontrada de la metodología OCTAVE-S con la Norma ISO/IEC 27005.

5.3.2 Fase 1: Construcción de perfil de amenazas

5.3.2.1 Proceso 1: Identificar información Organizacional (OCTAVE-S) – Establecimiento del contexto (ISO/IEC 27005)

Para comenzar, se debe desarrollar el alcance y los límites del proceso de gestión de riesgos en la seguridad de la información. Se debe considerar los siguientes puntos:

- Propósito de la organización/proceso: Campo de actividad de la organización/proceso, el segmento del mercado en el que realiza sus actividades y sus objetivos.
- Negocio: Rubro en el que se desenvuelve la organización y los servicios que brinda.
- Misión: Motivo, razón de ser de la existencia de una organización.
- Visión: Camino por el cual se dirige la organización a largo plazo.
- Valores: Son los principios más importantes bien definidos que se aplican al ejercicio de un negocio.
- Estructura de la organización: Define una jerarquía dentro de una organización, identifica puestos, funciones y donde se reportará dentro de la organización. (*)
- Estrategias de la organización: Determina la dirección y el desarrollo necesario con el fin de obtener aspectos en juego y de los cambios importantes que se planifican.
- Restricciones: Es aquello que limita alcanzar los objetivos de la organización.
- Requisitos reglamentarios: Pueden ser leyes, decretos, reglamentos específicos en el campo de la organización o reglamentos internos/externos. Esto también involucra contratos, acuerdos y todas las obligaciones de naturaleza legal o reglamentaria.

(*) Si el contexto se está desarrollando solo para un proceso o un área se deberá agregar la estructura de dicha área.

5.3.2.1.1 Actividad P1-1: Establecer criterio de impacto (OCTAVE-S) – Establecimiento del contexto y Comunicación del riesgo (ISO/IEC 27005)

Según la metodología OCTAVE-S y la ISO/IEC 27005, es recomendable identificar los criterios de impacto y especificarlos en grados de daño. Para esta actividad, se deberá definir un conjunto de medidas cualitativas (Alto, Medio, Bajo) con las que se podrá evaluar el efecto de un riesgo sobre la misión y los objetivos empresariales. Como mínimo se deben considerar las siguientes áreas de impacto:

- Reputación/confianza del cliente
- Finanzas
- Productividad
- Vida / salud de los clientes
- Multas / sanciones legales

Se define una escala para cada área de impacto:

- Impacto Alto (Valor = 3)
- Impacto Medio (Valor = 2)
- Impacto Bajo (Valor = 1)

Si desea puede añadir otros criterios de impacto. Para establecer el criterio de evaluación de impacto utiliza la hoja de trabajo “HT-Criterio de Evaluación de Impacto”. Debe dar clic en cada uno de ellos para poder visualizar la información correspondiente.

HT-Criterio de
Evaluación de Impacto

Figura 15. Hoja de trabajo de evaluación de impacto – Inicio.

Elaborado por jefes de proyecto

Dentro de la hoja de trabajo puede apreciar las áreas de impacto mencionadas. Si considera que el área de impacto no aplica, no complete esa parte del cuadro.

En el área de impacto de “Reputación/Confianza Cliente”, podrá observar dos tipos de impacto, para “Reputación” deberá tener en cuenta los niveles de impacto para actividades que se realizará más adelante, en “Pérdida de clientes” debe completar los rangos en porcentaje de pérdida de clientes sobre cada nivel de impacto. Asimismo, se encuentran los tipos de impacto “Otros” por si se quisiera agregar uno que no está mencionado en el cuadro.

←

HT- CRITERIO DE EVALUACIÓN DE IMPACTO

Reputación / Confianza del cliente

Tipo Impacto	Impacto bajo	Impacto medio	Impacto alto
Reputación	La reputación es minimamente afectada, poco o ningún esfuerzo o gastos es requerido para recuperarse.	La reputación es dañada, poco esfuerzo y gastos es requerido para recuperarse.	La reputación es destruida o dañada irrevocablemente.
Pérdida de cliente	Menos de ____% de reducción de clientes debido a la pérdida de confianza.	____% a ____% reducción en clientes debido a la pérdida de confianza.	Más de ____% reducción de clientes debido a la pérdida de confianza.
Otros			
Otros			

Figura 16. Hoja de trabajo de evaluación de impacto – Reputación/Confianza del cliente.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Para el área de impacto de “Finanzas”, para el tipo de impacto “Costos operativos” y “Pérdida de ingresos” debe completar el porcentaje correspondiente a cada nivel de impacto. Para el tipo de impacto “Pérdida financiera a tiempo” debe colocar cuánto es el impacto en dólares o soles, según como usted lo defina, según cada nivel de impacto. Asimismo, se encuentra el tipo de impacto “Otros” por si se quisiera agregar uno que no está mencionado.

HT- CRITERIO DE EVALUACIÓN DE IMPACTO			
Finanzas			
Tipo Impacto	Impacto bajo	Impacto medio	Impacto alto
Costos operativos	Incremento menos de ___% en costos operativos anuales.	Costos operativos anuales aumentan de ___% a ___%.	Costos operativos anuales aumentan por más de ___%.
Pérdida de ingresos	Menos de ___% en pérdidas de ganancias anuales.	___% a ___% de pérdida de ganancias anuales.	Mayor a ___% de pérdida de ganancias anuales.
Pérdida financiera a tiempo	Costo financiero en tiempo menor de \$____.	Costo financiero en tiempo de \$____ a \$____.	Costo financiero en tiempo mayor a \$____.
Otros			

Figura 17. Hoja de trabajo de evaluación de impacto – Finanzas.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Para el área de impacto “Productividad”, debe completar el porcentaje de horas de trabajo incrementadas y los días que eso significa según cada nivel de impacto. Asimismo, se encuentran los tipos de impacto “Otros” por si se quisiera agregar uno que no está mencionado.

HT- CRITERIO DE EVALUACIÓN DE IMPACTO			
Productividad			
Tipo Impacto	Impacto bajo	Impacto medio	Impacto alto
Horas de trabajo	Horas de trabajo son incrementadas por menos de ___% por ___ a ___ días.	Horas de trabajo son incrementadas entre ___% y ___% por ___ a ___ días.	Horas de trabajo son incrementadas por encima de ___% por ___ a ___ días.
Otros			
Otros			
Otros			

Figura 18. Hoja de trabajo de evaluación de impacto – Productividad.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Para el área de impacto “Vida / Salud de los clientes”, debe tener en cuenta los niveles de impacto proporcionados. Si desea cambiar el valor en “Salud”, realizarlo en la celda correspondiente. Asimismo, se encuentra el tipo de impacto “Otros” por si se quisiera agregar uno que no está mencionado.

HT- CRITERIO DE EVALUACIÓN DE IMPACTO			
Vida / Salud de los clientes			
Tipo Impacto	Impacto bajo	Impacto medio	Impacto alto
Vida	Ninguna pérdida o amenaza significativa a la vida del cliente o personal.	La vida del cliente o personal están amenazadas pero se recuperarán después de recibir tratamiento médico.	Pérdida de la vida de clientes o personal.
Salud	Degradación mínima, inmediatamente tratable en la salud del cliente o personal con recuperación dentro de 4 días.	Discapacidad temporal o recuperable de la salud de los clientes o personal.	Discapacidad permanente de aspectos significativos de la salud de clientes o personal.
Seguridad	Seguridad cuestionada.	Seguridad afectada.	Seguridad violada.
Otros			

Figura 19. Hoja de trabajo de evaluación de impacto – Vida/Salud de los clientes.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Para el área de impacto “Multas / Sanciones legales”, debe completar el monto de las multas según cada nivel de impacto, el mismo caso para el tipo de impacto de demandas. Para el caso de la investigación también tener en cuenta el nivel de impacto proporcionado para futuras actividades. Asimismo, se encuentra el tipo de impacto “Otros” por si se quisiera agregar uno que no está mencionado.

HT- CRITERIO DE EVALUACIÓN DE IMPACTO			
Multas / Sanciones Legales			
Tipo Impacto	Impacto bajo	Impacto medio	Impacto alto
Multas	Multas menos de \$ ____ son cobradas.	Multas entre \$ ____ y \$ ____ son cobradas.	Multas mayores de \$ ____ son cobradas.
Demandas	Demandas no frívolas menores a \$ ____ son presentadas en contra de la organización, o demandas frívolas son presentadas en contra	Demandas no frívolas entre \$ ____ y \$ ____ son presentadas en contra de la organización.	Demandas no frívolas mayores a \$ ____ son presentadas en contra de la organización.
Investigación	No existen consultas del gobierno u otra organización de investigación.	El gobierno u otra organización de investigación requiere información o records (bajo perfil).	El gobierno u otra organización de investigación inicia un alto perfil, investigación a profundidad de las prácticas organizacionales.
Otros			

Figura 20. Hoja de trabajo de evaluación de impacto – Multas.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Los valores completados en la “HT-Criterio de evaluación de impacto”, sirven para completar los niveles de impacto en otras hojas de trabajo.

Como menciona la ISO/IEC 27005, la comunicación eficaz entre las partes involucradas es importante, ya que tiene un impacto significativo en las decisiones que se deben tomar, la

información recolectada en esta primera actividad como los puntos definidos en establecimiento del contexto y los valores de impacto identificados, se debe de informar y compartir entre las personas las involucradas según lo definido para la ejecución del modelo.

5.3.2.1.2 Actividad P1-2: Identificar activos organizacionales (OCTAVE-S) – Identificación del riesgo (Identificación de los activos) y Comunicación del riesgo (ISO/IEC 27005)

La identificación de activos se debe llevar acabo con un nivel adecuado de detalles, el cual proporcione información suficiente para la valoración del riesgo. En este punto se decidió utilizar la clasificación de los activos definidos por OCTAVE-S:

- Información (documentada o electrónica) documentada o propiedad intelectual utilizada para cumplir con la misión de una organización o área o proceso escogido.
- Sistemas: una combinación de recursos de información, software y hardware que procesan y almacenan información.
- Servicios y aplicaciones: aplicaciones y servicios de software (sistemas operativos, aplicaciones de bases de datos, software de redes, aplicaciones de oficina, aplicaciones personalizadas, etc.) que procesan, almacenan o transmiten información.
- Personas: las personas de una organización que poseen habilidades, conocimientos y experiencia únicos que son difíciles de reemplazar.

En esta actividad se debe utilizar la hoja de trabajo “HT-Identificación de activos”, la cual se enfoca en los activos anteriormente mencionados.

HT-Identificación
de activos.xlsx

5.3.2.1.3 Actividad P1-3: Evaluar prácticas organizacionales (OCTAVE-S) – Identificación del riesgo (Identificación de vulnerabilidades) y Comunicación del riesgo (ISO/IEC 27005)

En esta actividad se utiliza la hoja de trabajo “HT-Evaluación prácticas organizacionales” según cada área de práctica de seguridad.

HT-Evaluación de prácticas organizacionales

HT- EVALUACIÓN DE PRÁCTICAS ORGANIZACIONALES					Resultados
 <u>Concientización de la seguridad y capacitación</u>	 <u>Estrategia de seguridad</u>	 <u>Administración de la seguridad</u>	 <u>Políticas de seguridad y regulaciones</u>	 <u>Administración de Seguridad Colaborativa</u>	
 <u>Plan de Contingencia / Recuperación ante desastres</u>	 <u>Control de acceso físico</u>	 <u>Monitoreo y Auditoría de seguridad física</u>	 <u>Administración de sistema y red</u>	 <u>Monitoreo y Auditoría de la seguridad TI</u>	
 <u></u>	 <u></u>	 <u></u>	 <u></u>	 <u></u>	

Figura 24. Hoja de trabajo Evaluación de prácticas organizacionales.

Elaborado por jefes de proyecto

Debe completar hasta qué punto se está cumpliendo con las prácticas de seguridad en cada área de seguridad.

En este caso, debe marcar con una “X” bajo cada respuesta que escoja según cada área de seguridad:

- Mucho: El enunciado representa la actual práctica en la organización (Valor = 1).
- Algo: El enunciado representa parcialmente la actual práctica en la organización (Valor = 2).
- Nada: El enunciado no representa la actual práctica en la organización (Valor = 3).
- No sabe: Si no se conoce información del enunciado (Valor = 4).

Tener en cuenta que si la práctica de seguridad se está cumpliendo completamente tendrá el menor puntaje, es decir, mientras mayor sea el puntaje, la práctica de seguridad es escaso.

←

HT- EVALUACIÓN DE PRÁCTICAS ORGANIZACIONALES

Concientización de la seguridad y capacitación

Afirmación	¿Hasta qué punto la afirmación es reflejada?				¿Qué hace bien tu organización actualmente en esta área?	¿Qué no hace bien tu organización actualmente en esta área?	Valorización de práctica de seguridad
	Mucho	Algo	Nada	No sabe			
Los miembros del personal entienden sus roles y responsabilidades de seguridad. Se encuentra documentado y verificado.							
Existe dentro de su organización los conocimientos adecuados para todos los servicios de apoyo, mecanismo y tecnologías, incluyendo su operación segura. Se encuentra documentado y verificado.							
Concientización de la seguridad, capacitación, y avisos periódicos son proporcionados a todo el personal. La comprensión del personal está documentada y su conformidad es verificada periódicamente.							
Los miembros del personal siguen buenas prácticas de seguridad.							

Figura 25. Hoja de trabajo Evaluación de prácticas organizacionales – Concientización de la seguridad y capacitación.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Completada esta información debe continuar y responder las preguntas referentes a lo que actualmente se está haciendo bien en estas prácticas de seguridad y lo que su no, que en este caso lo veríamos como vulnerabilidades.

←

HT- EVALUACIÓN DE PRÁCTICAS ORGANIZACIONALES

Concientización de la seguridad y capacitación

Afirmación	¿Hasta qué punto la afirmación es reflejada?				¿Qué hace bien tu organización actualmente en esta área?	¿Qué no hace bien tu organización actualmente en esta área?	Valorización de práctica de seguridad
	Mucho	Algo	Nada	No sabe			
Los miembros del personal entienden sus roles y responsabilidades de seguridad. Se encuentra documentado y verificado.							
Existe dentro de su organización los conocimientos adecuados para todos los servicios de apoyo, mecanismo y tecnologías, incluyendo su operación segura. Se encuentra documentado y verificado.							
Concientización de la seguridad, capacitación, y avisos periódicos son proporcionados a todo el personal. La comprensión del personal está documentada y su conformidad es verificada periódicamente.							
Los miembros del personal siguen buenas prácticas de seguridad.							

Figura 26. Hoja de trabajo Evaluación de prácticas organizacionales – Concientización de la seguridad y capacitación.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Finalmente, luego de haber marcado cómo se encuentran las prácticas de seguridad, en el campo de “Valorización de práctica de seguridad” aparecerá el valor cuantitativo de dicha marca, asimismo aparece el promedio de estas y mostrará un icono de color rojo, amarillo o verde donde puede verificar que los controles existentes están funcionando correctamente o no. Es color plomo es debido a que estas celdas no se completan, solo se generan automáticamente.

Se ha definido los colores de la siguiente manera

- Color Rojo: Mayor igual a 2.5.

- Color Amarillo: Menor a 2.5 y mayor a 1.5.
- Color Verde: Menor igual a 1.5.

←

HT- EVALUACIÓN DE PRÁCTICAS ORGANIZACIONALES						
Concientización de la seguridad y capacitación						
Afirmación	¿Hasta qué punto la afirmación es reflejada?				¿Qué hace bien tu organización actualmente en esta área?	¿Qué no hace bien tu organización actualmente en esta área?
	Mucho	Algo	Nada	No sabe		
Los miembros del personal entienden sus roles y responsabilidades de seguridad. Se encuentra documentado y verificado.						
Existe dentro de su organización los conocimientos adecuados para todos los servicios de apoyo, mecanismo y tecnologías, incluyendo su operación segura. Se encuentra documentado y verificado.						
Concientización de la seguridad, capacitación, y avisos periódicos son proporcionados a todo el personal. La comprensión del personal está documentada y su conformidad es verificada periódicamente.						
Los miembros del personal siguen buenas prácticas de seguridad.						

Valorización de práctica de seguridad	

Figura 27. Hoja de trabajo Evaluación de prácticas organizacionales – Valorización de prácticas de seguridad.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Luego de completar la información de cada área de prácticas, según lo que no se hace bien debe identificar las vulnerabilidades y debe de colocarlas en una lista de vulnerabilidades como especifica la ISO/IEC 27005, la cual debe estar relacionada con los activos o en este caso con las áreas de prácticas (“Lista de vulnerabilidades”).

La ISO/IEC 27005 menciona que las vulnerabilidades deben ser identificadas dentro de las siguientes áreas: organización, procesos y procedimientos, rutinas de gestión, personal, ambiente físico, configuración del sistema de información, Hardware, software o equipo de comunicaciones y dependencia de partes externas.

Lista de vulnerabilidades.xls:

LISTA DE VULNERABILIDADES			
ID Activo	Nombre Activo / Área de práctica organizacional	ID Vulnerabilidad	Descripción Vulnerabilidad

Figura 28. Lista de vulnerabilidades.

Elaborado por jefes de proyecto

Luego de haber completado todas las áreas, puede seleccionar el botón “Resultado”, y se observa el resumen de todas las áreas con su valor promedio y el semáforo correspondiente, estos se generan automáticamente.

HT- EVALUACIÓN DE PRÁCTICAS ORGANIZACIONALES		
Resultados		
Áreas	Valor promedio	Semáforo
Concientización de la seguridad y capacitación		
Estrategia de seguridad		
Administración de la seguridad		
Políticas de seguridad y regulaciones		
Administración de Seguridad Colaborativa		
Plan de Contingencia / Recuperación ante desastres		
Control de acceso físico		
Monitoreo y Auditoría de seguridad física		
Administración de sistema y red		
Monitoreo y Auditoría de la seguridad TI		
Autenticación y autorización		
Gestión de vulnerabilidad		
Cifrado		
Arquitectura y diseño de seguridad		
Gestión de incidentes		

Figura 29. Hoja de trabajo Evaluación de prácticas organizacionales – Resultados.

Elaborado por jefes de proyecto

Documentar los puntos de acción a tomar identificados en la hoja de trabajo “HT-Lista de acciones”, así mismo documentar notas relevantes y recomendaciones del proceso 1: Identificar Información Organizacional en la hoja de trabajo “HT-Notas y recomendaciones”.

HT-Lista de
acciones.xlsx

HT-Notas y
Recomendaciones.xl

Lista de Acciones			
Elemento de Acción ¿Qué medidas piensa tomar?		¿Para qué actividad es relevante este elemento de acción?	
Asigne un número de identificación a cada elemento de acción.		¿Quién es responsable de completar el elemento de acción?	
Responsabilidad:		¿Cuándo se debe completar el elemento de acción?	
Fecha de Terminación:		¿Qué apoyo adicional se requiere para completar el elemento de acción?	
Soporte adicional:			

Figura 30. Hoja de trabajo Lista de acciones.

Elaborado por jefes de proyecto, basado en OCTAVE-S

HT- Notas y Recomendaciones			
Nota ¿Qué notas desea grabar?			
¿Hay alguna recomendación asociada con esta nota? Si la respuesta es afirmativa, guárdela en el cuadro de recomendaciones correspondiente.		¿Para qué actividad es relevante esta nota?	
¿Qué recomendaciones desea registrar?		¿Para qué actividad es pertinente esta recomendación?	

Figura 31. Hoja de trabajo Notas y recomendaciones.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Como se mencionó anteriormente, todo punto desarrollado se debe comunicar a las partes interesadas, como menciona la ISO/IEC 27005. En este caso, se debe comunicar la información recolectada de las vulnerabilidades, así como las áreas de prácticas de seguridad críticas.

5.3.2.2 Proceso 2: Crear perfil de amenaza (OCTAVE-S)

5.3.2.2.1 Actividad P2-1: Seleccionar activos críticos (OCTAVE-S) – Identificación del riesgo (Identificación de los activos) y Comunicación del riesgo (ISO/IEC 27005)

Revisar los activos relacionados con la información que se identificó durante la Actividad P1- 2 y seleccionar los activos que aparecen con mayor promedio y en rojo en la “Lista de activos” y colocarlos en la hoja de trabajo “HT- Información de Activos Críticos”. Si considera algún activo más, también colocarlo en la hoja de trabajo.

HT-Información de
activos críticos.xlsx

HT- INFORMACIÓN DE ACTIVOS CRÍTICOS							
Lista de activos críticos							
Propietario de activo	Responsabilidad sobre el activo	Información que maneja el activo	Valoración del activo			Valor promedio	Requisito de seguridad más importante
			Disponibilidad	Integridad	Confidencialidad		

Figura 32. Hoja de trabajo Información de activos críticos.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Tener en cuenta la información recolectada en la “Lista de activos”, usando como base la planteada por la ISO/IEC 27005, y completar la información, dejar en blanco el campo de requisito más importante que se completa en el siguiente punto. Completar la justificación de por qué se escoge como activo crítico si es que no fuera porque el promedio fue uno de los mayores. También, registrar los activos que están relacionados con cada activo crítico en la hoja de trabajo “HT- Información de Activos Críticos”.

OS CRÍTICOS					
Valoración del activo		Valor promedio	Requisito de seguridad más importante	Justificación de selección como activo crítico	Activos relacionados
Integridad	Confidencialidad				

Figura 33. Hoja de trabajo Información de activos críticos - Justificación, activos relacionados.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Como se mencionó anteriormente, todo punto desarrollado se debe comunicar a las partes interesadas, como menciona la ISO/IEC 27005. En este caso, la información recolectada de los activos críticos y las justificaciones correspondientes se deben de informar.

5.3.2.2.2 Actividad P2-2: Identificar requerimientos de seguridad para activos críticos (OCTAVE-S) – Identificación del riesgo (Identificación de los activos) y Comunicación de los activos (ISO/IEC 27005)

Luego de completar las hojas de trabajo en la anterior actividad (Actividad P2-1), se debe seleccionar el requisito de seguridad más importante por cada activo crítico en la hoja de trabajo “HT- Información de Activos Críticos”.

INFORMACIÓN DE ACTIVOS CRÍTICOS					
Lista de activos críticos					
Valoración del activo			Valor promedio	Requisito de seguridad más importante	Justificación de selección como activo crítico
Disponibilidad	Integridad	Confidencialidad			

Figura 34. Hoja de trabajo Información de activos críticos - Requisito de seguridad más importante.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Como se mencionó anteriormente, todo punto desarrollado se debe comunicar a las partes interesadas, como menciona la ISO/IEC 27005. En este caso, la información recolectada de los activos críticos y sus respectivos requisitos de seguridad más importantes se deben informar.

5.3.2.2.3 Actividad P2-3: Identificar amenazas de los activos críticos (OCTAVE-S) – Identificación del riesgo (Identificación de las amenazas e Identificación de las consecuencias) y Comunicación del riesgo (ISO/IEC 27005)

Se trabajará con la hoja de trabajo “HT-Perfil de riesgos”.

HT-Perfil de riesgos.xlsx

HT- PERFIL DE RIESGO																
Perfil de riesgos																
Resultado	Motivo			Historia		Valores de impacto					Probabilidad		Estratégico			
	¿Qué tan fuerte es el motivo del actor?			¿Qué tan seguido ha ocurrido esta amenaza en el pasado?		Reputación	Financiera	Productividad	Multas	Seguridad	Total	Valor cualitativo	Valor cuantitativo	Concientización de la seguridad	Estrategia de seguridad	Administración de la seguridad
	Alto	Medio	Bajo													
Revelación				veces en	años.											
Modificación				veces en	años.											
Pérdida, destrucción				veces en	años.											
Interrupción				veces en	años.											
Revelación				veces en	años.											
Modificación				veces en	años.											
Pérdida, destrucción				veces en	años.											
Interrupción				veces en	años.											
Revelación				veces en	años.											
Modificación				veces en	años.											
Pérdida, destrucción				veces en	años.											
Interrupción				veces en	años.											
Revelación				veces en	años.											
Modificación				0 veces en	3 años.											
Pérdida, destrucción				0 veces en	3 años.											
Interrupción				0 veces en	3 años.											
Revelación				0 veces en	3 años.											
Modificación				0 veces en	3 años.											

Figura 35. Hoja de trabajo Perfil de riesgos.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Completar la hoja de trabajo hasta antes de la primera marca amarilla, las siguientes partes son completadas más adelante. Dentro de esta hoja, complete la información según cada

activo crítico seleccionado. Si necesita más campos, debe generar más celdas, y copiar toda la línea del activo crítico anterior para obtener el formato.

Según cada activo crítico, debe marcar con una “X” según cada actor, ya sea interno o externo, y según cada motivo, accidental o intencionado, el resultado que usted cree que corresponda, que es la consecuencia de darse la amenaza.

HT- PERFIL DE RIESGO															
Amenaza				Motivo			Historia			Valores de impacto					Probabilidad
				¿Qué tan fuerte es el motivo del actor?			¿Qué tan seguido ha ocurrido esta amenaza en el pasado?								¿Qué tan probable es que ocurra la amenaza en el futuro?
				Alto	Medio	Bajo				Reputación	Financiera	Productividad	Medias	Seguridad	Total
Activo	Actor	Motivo	Resultado												
	Interno	Accidental	Revelación				veces en	años							
			Modificación				veces en	años							
			Pérdida, destrucción				veces en	años							
		Intencionado	Interrupción				veces en	años							
			Revelación				veces en	años							
			Modificación				veces en	años							
	Externo	Accidental	Pérdida, destrucción				veces en	años							
			Interrupción				veces en	años							
			Revelación				veces en	años							
		Intencionado	Modificación				veces en	años							
			Pérdida, destrucción				veces en	años							
			Interrupción				veces en	años							

Figura 36. Hoja de trabajo Perfil de riesgos – Actor, Motivo y Resultado.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Debe completar qué tan fuerte es el motivo del actor para realizar dicho resultado que se identificó en el paso anterior. Debe marcar con una “X”, según el nivel que escoja.

- Alto: El actor se enfoca en atacar, se dirige específicamente a atacar al activo crítico, y tomará medidas para asegurar su éxito.
- Medio: El actor se enfoca en atacar, dirigido a activos en general, cuenta con una estrategia de salida o abandono del ataque.
- Bajo: El actor se enfoca en atacar, no tiene metas específicas, se dirige a cualquier activo que pueda ser acceder y atacar fácilmente, abandonará el ataque si no le resulta fácil.

No completar los cuadros en color plomo, ya que en estos no aplica.

HT- PERFIL DE RIESGO																
Amenaza				Motivo			Historia		Perfil de riesgos					Probabilidad		Consecuencia en la actividad de la organización
				¿Qué tan fuerte es el motivo del actor?					Valores de impacto				¿Qué tan probable es que ocurra la amenaza en el			
				Alto	Medio	Bajo			Reputación	Financiera	Productividad	Riesgos	Seguridad	Total	Valor cualitativo	
Activo	Actor	Motivo	Resultado													
	Interno	Accidental	Revelación					veces en	años							
			Modificación					veces en	años							
			Pérdida, destrucción					veces en	años							
		Intencionado	Interrupción					veces en	años							
			Revelación					veces en	años							
			Modificación					veces en	años							
	Externo	Accidental	Pérdida, destrucción					veces en	años							
			Interrupción					veces en	años							
			Revelación					veces en	años							
		Intencionado	Modificación					veces en	años							
			Pérdida, destrucción					veces en	años							
			Interrupción					veces en	años							

Figura 37. Hoja de trabajo Perfil de riesgos – Motivo.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Completar el campo de “Historia” y rellenar los espacios en blanco relacionados a qué tan seguido ocurrió la amenaza identificada en pasos anteriores.

HT- PERFIL DE RIESGO																		
Amenaza							Perfil de riesgos											
							Motivo			Historia		Valores de impacto					Probabilidad	
							¿Qué tan fuerte es el motivo del actor?										¿Qué tan probable es que ocurra la amenaza en el	
Activo	Actor	Motivo	Resultado	Alto	Medio	Bajo								Valor cualitativo	Valor cuantitativo	Consecuencia en la seguridad y capacidad		
				¿Qué tan seguido ha ocurrido esta amenaza en el pasado?										Reputación	Financiera	Productividad	Multas	Seguridad
	Interno	Accidental	Revelación					veces en	años									
			Modificación					veces en	años									
			Pérdida, destrucción					veces en	años									
		Intencionado	Interrupción					veces en	años									
			Revelación					veces en	años									
			Modificación					veces en	años									
	Externo	Accidental	Pérdida, destrucción					veces en	años									
			Interrupción					veces en	años									
			Revelación					veces en	años									
		Intencionado	Modificación					veces en	años									
			Pérdida, destrucción					veces en	años									
			Interrupción					veces en	años									
				Revelación				veces en	años									

Figura 38. Hoja de trabajo Perfil de riesgos – Historia.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Si de los puntos anteriores se identificaron vulnerabilidades, actualizar la “Lista de vulnerabilidades”, como menciona la ISO/IEC 27005.

Luego de identificar las amenazas de cada activo crítico, identificar una lista de escenarios de incidentes con las consecuencias relacionadas con los activos y los procesos del negocio que se afecten en la lista “Lista de escenarios de incidente”, como se menciona en la ISO/IEC 27005.

Lista de escenarios de incidentes.xlsx

Se recomienda identificar las consecuencias operativas de los escenarios de incidentes en términos de: tiempo de investigación y reparación, pérdida de tiempo (trabajo), pérdida de

Dentro de la “Lista de escenarios de incidentes”, completar los campos correspondientes a ID Activo, que ya se ha completado anteriormente, el nombre del activo, actor, motivo, resultado, relacionar las vulnerabilidades identificadas con las amenazas para poder identificar un supuesto escenario en el que esta se materializa, y así completar cual sería la consecuencia de esta materialización.

[illegible]

Elaborado por jefes de proyecto

Como se mencionó anteriormente, todo punto desarrollado se debe comunicar a las partes interesadas, como menciona la ISO/IEC 27005. En este caso, la información recolectada de las amenazas y lo posibles escenarios de incidentes se deben informar.

5.3.3.1 Proceso 3: Examinar la infraestructura computacional en relación a los activos claves

En esta actividad debe establecer qué componentes forman parte del sistema de interés crítico que escoja, empezar por completar dentro del primer recuadro de la hoja de trabajo “HT-Rutas de acceso a la red”.

HT-Rutas de acceso
a la red.xlsx

Hoja de Trabajo de rutas de acceso a la red			
Sistema de Interés ¿Qué sistema o sistemas están más estrechamente relacionados con el activo crítico?			
Sistema de interés ¿Cuáles de las siguientes clases de componentes forman parte del sistema de interés?	Puntos de acceso intermedios ¿Cuáles de las siguientes clases de componentes se utilizan para transmitir información y aplicaciones del sistema de interés para las personas? ¿Qué clases de componentes podrían servir como puntos de acceso intermedios?	Acceso al sistema por personas ¿De cuál de las siguientes clases de componentes las personas (por ejemplo, usuarios, atacantes) pueden acceder al sistema de interés? Considere los puntos de acceso tanto internos como externos a las redes de su organización.	Ubicaciones ¿En qué clases de información de para fine
Servidores Redes Internas	Redes Internas Redes Externas	Estaciones de trabajo en sitio Laptops	Dispositivos móviles Otros

Figura 40. Hoja de trabajo de rutas de acceso a la red – Sistema de interés.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Debe marcar con una "X" en cada casilla junto a cada respuesta apropiada según el área que corresponda (Sistema de interés, Puntos de acceso intermedio, acceso al sistema por personas, otros sistemas y componentes).

Para el sistema de interés debe determinar cómo la información y las aplicaciones se transmiten a las personas que acceden a ese sistema, considerando qué tipos de componentes se utilizan para transmitirle dicha información.

Para los puntos de acceso intermedios se debe examinar qué componentes utilizan las personas para acceder al sistema de interés. Al revisar cómo las personas pueden acceder al sistema de interés, debe pensar en los puntos de acceso tanto internos como externos a las redes de su organización.

Sistema de interés	Puntos de acceso intermedios	Acceso al sistema por personas	Ubicaciones
¿Cuáles de las siguientes clases de componentes forman parte del sistema de interés?	¿Cuáles de las siguientes clases de componentes se utilizan para transmitir información y aplicaciones del sistema de interés para las personas? ¿Qué clases de componentes podrían servir como puntos de acceso intermedios?	¿De cuál de las siguientes clases de componentes las personas (por ejemplo, usuarios, atacantes) pueden acceder al sistema de interés? Considere los puntos de acceso tanto internos como externos a las redes de su organización.	¿En qué clases de información de para fine
Servidores Redes Internas Estaciones de trabajo en sitio Otros (Listar)	Redes Internas Redes Externas Otros (Listar)	Estaciones de trabajo en sitio Laptops PDAs / Componentes inalámbricos Hogar / Estaciones de trabajo Otros (Listar)	Dispositivos móviles Otros
Otros	Otros	Otros	Otros

Figura 41. Hoja de trabajo de rutas de acceso a la red.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Si selecciona "Otros", debe enumerar las clases específicas de componentes. Cuando seleccione una clase clave de componentes, deberá documentar cualquier subclase relevante o cite ejemplos específicos cuando sea apropiado.

Finalmente, listar en los activos identificados en la “Lista de activos”, como menciona la ISO/IEC 27005, y si considera que alguno de ellos es crítico, colocarlo en la hoja de trabajo “HT- Información de Activos Críticos”. Luego debe completar el perfil de riesgo para estos, en la hoja de perfil de riesgos que corresponda.

Como se mencionó anteriormente, todo punto desarrollado se debe comunicar a las partes interesadas, como menciona la ISO/IEC 27005. En este caso, la información obtenida luego de esta actividad se debe de informar.

5.3.3.1.2 Actividad P3-2: Analizar procesos relacionados con tecnología (OCTAVE-S) – Identificación del riesgo (Identificación de los activos, Identificación de controles existentes, Identificación de vulnerabilidades, Identificación de las consecuencias) y Comunicación del riesgo (ISO/IEC 27005)

Revisar las clases de componentes que se identificaron para cada activo crítico en el punto anterior en la “HT-Rutas de acceso a la red”. Para cada clase que esté relacionada con uno o más activos críticos, completar dicha información en la Hoja de trabajo “HT-Revisión de infraestructura”.

HT-Revisión de
infraestructura.xlsx

Las clases de componentes están divididas en:

- Servidores
- Redes internas
- Estaciones de trabajo en sitio
- Laptops
- PDA/Componentes inalámbricos
- Otros sistemas
- Dispositivos de almacenamiento

- Redes externas
- Estaciones de trabajo externas
- Otro

Clases	Activos Críticos	Responsabilidad	¿En qué cont
¿Qué clases de componentes están relacionadas con uno o más activos críticos?	¿Qué activos críticos están relacionados con cada clase?	¿Quién es responsable de mantener y asegurar cada clase de componentes?	
			Mucho
Servidores			
Redes internas			

Figura 42. Hoja de trabajo Revisión de infraestructura - Clases.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Anotar qué activos críticos están relacionados con cada clase de componentes, anteriormente se habían seleccionado 5. Para cada clase que se completó en la Hoja de trabajo “HT- Revisión de infraestructura” durante el punto anterior, registrar qué activos críticos están relacionados con esa clase marcando una “X” en los recuadros debajo de los nombres de activos aplicables.

Clases	Activos Críticos	Responsabilidad	¿En qué cont
¿Qué clases de componentes están relacionadas con uno o más activos críticos?	¿Qué activos críticos están relacionados con cada clase?	¿Quién es responsable de mantener y asegurar cada clase de componentes?	
			Mucho
Servidores			
Redes internas			

Figura 43. Hoja de trabajo Revisión de infraestructura – Activos críticos.

Elaborado por jefes de proyecto, basado en OCTAVE-S

A continuación, debe identificar al responsable de mantener y asegurar cada clase de componentes. Si ha identificado más de una subclase para una clase determinada de

componentes, debe identificar a la parte (o partes) responsable de mantener y asegurar cada subclase. Anote el nombre de la parte o partes responsables de mantener y asegurar cada clase (o subclase cuando sea aplicable) del componente en la Hoja de trabajo “HT-Revisión de infraestructura”.

Clases	Activos Críticos	Responsabilidad	¿En qué categoría?
¿Qué clases de componentes están relacionadas con uno o más activos críticos?	¿Qué activos críticos están relacionados con cada clase?	¿Quién es responsable de mantener y asegurar cada clase de componentes?	
Servidores			
Redes internas			

Figura 44. Hoja de trabajo Revisión de infraestructura – Responsabilidad.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Para el campo de protección, determinar qué tan bien cree que cada clase de componentes está siendo protegida actualmente. Si ha identificado más de una subclase para una clase determinada de componentes, debe determinar cuán bien cree que cada subclase está siendo protegida actualmente. Puede haber variaciones en cómo se protegen las subclases dentro de la misma clase, especialmente si una parte diferente es responsable de configurar y mantener cada subclase. Marcar una "X" en la escala en el punto que indica cuánta seguridad se considera al configurar y mantener cada clase de componentes. Las referencias en la escala son:

- Mucho: Se tiene una cantidad considerable de datos objetivos relacionados con su estimación. (Valor = 3)
- Algo: Se tiene una cantidad limitada de datos objetivos relacionados con su estimación (Valor = 2).
- Nada: Se tiene pocos o ningún dato objetivo relacionado con su estimación (Valor = 1).

El campo “Total” se completa automáticamente, muestra el valor cuantitativo según la escala que ha escogido. Este campo no se completa.

Clases ¿Qué clases de componentes están relacionadas con uno o más activos críticos?	Activos Críticos ¿Qué activos críticos están relacionados con cada clase?				Responsabilidad ¿Quién es responsable de mantener y asegurar cada clase de componentes?	Protección ¿En qué medida se considera la seguridad al configurar y mantener cada clase de componentes?			
						Mucho	Algo	Nada	Total
Servidores									
Redes internas									

Figura 45. Hoja de trabajo Revisión de infraestructura – Responsabilidad.

Elaborado por jefes de proyecto, basado en OCTAVE-S

También se debe tener en cuenta las fuentes de los datos que utilizó al determinar la medida en que se considera la seguridad al configurar y mantener cada clase de componentes. Marcar con una "X" en la casilla junto a la mejor respuesta en la Hoja de trabajo “HT-Revisión de infraestructura”.

- Técnica Formal: se emplean técnicas rigurosas de recolección de datos y análisis.
- Medios Informales: se realiza una evaluación superficial de la situación. realizadas por personal inexperto.
- Otros: se utiliza esta categoría para identificar cualquier otro medio utilizado para llegar a su conclusión que no se contemple en ninguna de las categorías anteriores.

Clases ¿Qué clases de componentes están relacionadas con uno o más activos críticos?	Activos Críticos ¿Qué activos críticos están relacionados con cada clase?				Responsabilidad ¿Quién es responsable de mantener y asegurar cada clase de componentes?	Protección ¿En qué medida se considera la seguridad al configurar y mantener cada clase de componentes?				¿Cómo lo sabes?
						Mucho	Algo	Nada	Total	
Servidores										
Redes internas										
Estaciones de trabajo en sitio										

Figura 46. Hoja de trabajo Revisión de infraestructura – Protección.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Proporcionar cualquier información adicional en la columna "Notas / Problemas" cuando corresponda. También documentar cualquier otra nota relevante o asuntos relacionados con

una clase de componente en el espacio provisto en la Hoja de trabajo “HT-Revisión de infraestructura” cuando sea apropiado.

HT-Revisión de infraestructura													
Activos Críticos				Responsabilidad		Protección				Notas / Problemas			
¿Los activos críticos están relacionados con cada clase?				¿Quién es responsable de mantener y asegurar cada clase de componentes?		¿En qué medida se considera la seguridad al configurar y mantener cada clase de componentes?				¿Cómo lo sabes?			¿Qué información adicional desea registrar?
						Mucho	Algo	Nada	Total	Técnicas formales	Medios informales	Otros	

Figura 47. Hoja de trabajo Revisión de infraestructura – Notas/Problemas.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Como se identifican los activos críticos del lado de infraestructura, se puede identificar una lista de vulnerabilidades para dichos activos (“Lista de vulnerabilidades”).

Finalmente, se identifica una lista de escenarios de incidentes con las consecuencias relacionadas en la lista “Lista de escenarios de incidente”, como se menciona en la ISO/IEC 27005.

Documentar los puntos de acción a tomar identificados en la hoja de trabajo “HT-Lista de acciones”, así mismo documentar notas relevantes y recomendaciones relacionadas a la fase 2 en la hoja de trabajo “HT-Notas y recomendaciones”.

Como se mencionó anteriormente, todo punto desarrollado se debe comunicar a las partes interesadas, como menciona la ISO/IEC 27005. En este caso, la información obtenida de la infraestructura se debe informar.

5.3.4 Fase 3: Planes y estrategia de seguridad

5.3.4.1 Proceso 4: Identificar y analizar riesgos

5.3.4.1.1 Actividad P4-1: Evaluar el impacto de las amenazas (OCTAVE-S) –Estimación del riesgo (Evaluación de las consecuencias) y Comunicación del riesgo (ISO/IEC 27005)

El valor del impacto del negocio se puede expresar de manera cualitativa y cuantitativa, pero cualquier método para asignar valor monetario en general puede suministrar más

Como se mencionó anteriormente, todo punto desarrollado se debe comunicar a las partes interesadas, como menciona la ISO/IEC 27005. En este caso, la información sobre el impacto de cada amenaza se debe informar.

5.3.4.1.2 Actividad P4-2: Establecer criterios basados en la frecuencia (OCTAVE-S) – Estimación del riesgo (Evaluación de la probabilidad de incidentes) y Comunicación del riesgo (ISO/IEC 27005)

En este punto es necesario evaluar la probabilidad de cada escenario identificado y el impacto de que ocurra, utilizando técnicas de estimación cualitativas o cuantitativas. Se debe tomar en consideración la frecuencia con la que ocurren las amenazas y la facilidad con que las vulnerabilidades pueden ser explotadas.

Revisar la siguiente información de la “HT-Perfil de riesgo”:

- Los tipos de amenazas para los activos críticos.
- La frecuencia con que cada amenaza ha ocurrido en el pasado (historia).

En la “HT-Criterios de Evaluación de Probabilidad”, podrá observar frecuencias de ocurrencia de las amenazas, luego de acuerdo a su criterio colocar el rango limite alto, medio y bajo. Si considera que el rango establecido debería cambiarse, modificar dicho punto.

HT- Criterios de Evaluación de la Probabilidad											
Rango	Criterios basados en la frecuencia										
	Alto				Medio			Bajo			
Tiempo entre eventos	Diario	Semanal	Mensual	4 veces al año	2 veces al año	1 vez al año	1 vez cada 2 años	1 vez cada 5 años	1 vez cada 10 años	1 vez cada 20 años	1 vez cada 50 años
Frecuencia	365	52	12	4	2	1	0.5	0.2	0.1	0.05	0.02

Figura 49. Hoja de trabajo Criterios de Evaluación de Probabilidad.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Como menciona la ISO/IEC 27005, en algunos casos, se requiere más que un valor numérico para especificar las consecuencias para diferentes eventos, es así que se debe mantener la consistencia en el enfoque cuantitativo o cualitativo.

En este punto, se debe completar el campo de consecuencia y la valorización cualitativa del incidente (alto, medio y bajo), la columna de valorización cuantitativa de incidente se completará automáticamente. Mostrará también un semáforo donde:

- [illegible]

Elaborado por jefes de proyecto

5.3.4.1.3 Actividad P4-3: Evaluar probabilidades de amenazas (OCTAVE-S) – Estimación del riesgo (Nivel de estimación del riesgo) y Comunicación del riesgo (ISO/IEC 27005)

- "Alto" para cada alta probabilidad (Valor = 3).

[illegible]

Figura 52. Lista de escenarios de incidentes - Probabilidad.

Elaborado por jefes de proyecto

Documentar los puntos de acción a tomar describiendo la acción, el responsable, algunas acciones de gestión que puedan ayudar a facilitar que se complete la acción en la hoja de trabajo “HT-Lista de acciones”, así mismo documentar notas relevantes y recomendaciones del proceso en la hoja de trabajo “HT-Notas y recomendaciones”.

Como se mencionó anteriormente, todo punto desarrollado se debe comunicar a las partes interesadas, como menciona la ISO/IEC 27005. En este caso, la información obtenida de la probabilidad identificada se debe informar.

5.3.4.2 Proceso 5: Desarrollar estrategia de protección y planes de mitigación

5.3.4.2.1 Actividad P5-1: Describir estrategia de protección actual (OCTAVE-S) – Evaluación del riesgo y Comunicación del riesgo (ISO/IEC 27005)

Tener en cuenta que se debe revisar algunas notas y recomendaciones de la “HT-Notas y recomendaciones” y las acciones en la “HT-Lista de acciones” que pueden ser relevantes para desarrollar esta actividad.

Revisar la información de la “HT-Evaluación de prácticas organizacionales” y enfocarse en los siguientes puntos:

- El estado del semáforo.
- La medida en cada área de seguridad.
- Lo que la organización está haciendo bien en el área.
- Lo que la organización no está haciendo bien en el área.

Colocar el mismo estado del semáforo de la “HT-Evaluación de prácticas organizacionales” en la “HT-Estrategia de protección” en cada área de seguridad.

HT- Estrategia de protección.xlsx

Tener en cuenta que en esta actividad solo completaremos la hoja hasta antes de la línea marcada con amarillo de cada estrategia de seguridad.

HT- ESTRATEGIA DE PROTECCIÓN				
Concientización de la seguridad y capacitación	Estrategia de seguridad	Administración de la seguridad	Políticas de seguridad y regulaciones	Administración de Seguridad Colaborativa
Plan de Contingencia / Recuperación ante desastres	Control de acceso físico	Monitoreo y Auditoría de seguridad física	Administración de sistema y red	Monitoreo y Auditoría de la seguridad TI

Figura 53. Hoja de trabajo Estrategia de protección.

Elaborado por jefes de proyecto

HT- ESTRATEGIA DE PROTECCIÓN				
Concientización de la seguridad y capacitación				
<div> <div>Semáforo</div> </div>				
Estrategia de Entrenamiento Se cuenta con una estrategia de capacitación documentada que incluye capacitación en seguridad y capacitación relacionada con la seguridad para las tecnologías soportadas. Se tiene una estrategia de capacitación informal e indocumentada. Se tiene un punto intermedio entre las dos primeras opciones		¿Qué tan formal es la estrategia de capacitación?	¿Alguna de las actividades de mitigación cambiará su estrategia de entrenamiento? ¿Desea realizar cambios adicionales en su estrategia de formación?	
		Presente	Cambio	
		Presente	Cambio	
		Presente	Cambio	
Entrenamiento de Concientización de Seguridad Se proporciona capacitación periódica de concientización de seguridad a todos los empleados _____ veces cada _____ años. Se imparte capacitación de sensibilización sobre la seguridad a los nuevos miembros del personal como parte de sus actividades de orientación		¿Con qué frecuencia se imparte capacitación de sensibilización sobre la seguridad?	¿Alguna de las actividades de mitigación cambiará la frecuencia con la que se imparte capacitación de sensibilización sobre la seguridad? ¿Desea realizar cambios adicionales en la frecuencia con la que se proporciona formación sobre seguridad?	
		Presente	Cambio	
		Presente	Cambio	

Figura 54. Hoja de trabajo Estrategia de protección - Semáforo.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Como se menciona en la ISO/IEC 27005, se debe realizar una evaluación según lo puntos ya identificados, en este caso, ya contamos con el semáforo de cada área, por lo que podemos

- Cada área estratégica de seguridad comprende las siguientes características:
- Políticas documentadas
- Gestión de Políticas
- Aplicación de políticas
- Conciencia del personal
- Cumplimiento normativo y reglamentario
- Otros

HT- ESTRATEGIA DE PROTECCIÓN			
Concientización de la seguridad y capacitación			
Semáforo			
Estrategia de Entrenamiento	Se cuenta con una estrategia de capacitación documentada que incluye capacitación en seguridad y capacitación relacionada con la seguridad para las tecnologías soportadas.	¿Tan formal es la estrategia de capacitación?	¿Alguna de las actividades de mitigación cambiará su estrategia de entrenamiento? ¿Desea realizar cambios adicionales en su estrategia de formación?
	Se tiene una estrategia de capacitación informal e indocumentada.	☐ Presente	☐ Cambio
	Se tiene un punto intermedio entre las dos primeras opciones	☐ Presente	☐ Cambio
		☐ Presente	☐ Cambio
Entrenamiento de Concienciación de Seguridad	Se proporciona capacitación periódica de concientización de seguridad a todos los empleados _____ veces cada _____ años.	¿Con qué frecuencia se imparte capacitación de sensibilización sobre la seguridad?	¿Alguna de las actividades de mitigación cambiará la frecuencia con la que se imparte capacitación de sensibilización sobre la seguridad? ¿Desea realizar cambios adicionales en la frecuencia con la que se proporciona formación sobre seguridad?
	Se imparte capacitación de sensibilización sobre la seguridad a los nuevos miembros del personal como parte de sus	☐ Presente	☐ Cambio
		☐ Presente	☐ Cambio

Figura 55. Hoja de trabajo Estrategia de protección - Características.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Cada área de práctica operacional comprende varias características. A continuación, se describe cada característica y cuando necesita abordar esa característica:

- Responsabilidad: define quién tiene la responsabilidad de completar un conjunto de tareas especificadas para un área de práctica operacional de seguridad, si esta recae en personas de su organización, con terceros o con una combinación de personas.

- Procedimientos: la medida en que los procedimientos se definen formalmente para un área de práctica operacional de seguridad.
- Formación: define el enfoque para crear las habilidades de los miembros del personal en un área de práctica.
- Cuestiones de Colaboración: define el grado en que los requisitos para un área de práctica operacional de seguridad se comunican formalmente a cada tercero.
- Verificación: define el grado en que cada tercero cumple con los requisitos para un área de práctica operacional de seguridad.

En la “HT-Estrategia de Protección”, para el caso específico de quién tiene la responsabilidad de cada tarea para un área de práctica operacional de seguridad identificará otro tipo de tabla donde deberá marcar primero con una "X" en la casilla titulada "Presente", si su organización lo contempla.

Responsabilidad	¿Quién es actualmente responsable de la administración del sistema y de la red?			¿Cambiarán las actividades de mitigación la responsabilidad de la administración del sistema y de la red? ¿Desea realizar cambios adicionales que afecten la responsabilidad de la administración del sistema y de la red?		
	Presente			Cambio		
Tarea	Interno	Externo	Combinado	Interno	Externo	Combinado
Configuración de hardware y software de TI.						
Almacenamiento seguro de información confidencial (por ejemplo, copias de seguridad almacenadas fuera del sitio, proceso para descartar información sensible).						
Comprobación de la integridad del software instalado.						
Mantener los sistemas actualizados con respecto a revisiones, parches y recomendaciones en avisos de seguridad.						
Realización y seguimiento de cambios en el hardware y software de TI.						
Administración de contraseñas, cuentas y privilegios.						
Selección de herramientas de gestión de sistemas y redes.						

Figura 56. Hoja de trabajo Estrategia de protección - Responsabilidad.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Como se observa, la tabla de responsabilidad enumera tres opciones para cada tarea:

- Interno: las personas de la organización son responsables de completar la tarea.
- Externo: Uno o más terceros son responsables de completar la tarea.
- Combinado: Una combinación de personas en su organización y uno o más terceros son responsables de completar la tarea.

Marcar con una "X" en la casilla correspondiente para cada tarea. Puede cambiar las palabras proporcionadas para una tarea o agregar palabras adicionales según sea necesario.

Si tiene tareas que no figuran en la estrategia de protección para un área de práctica de seguridad operacional, registre esas tareas en los espacios en blanco proporcionados y marcar con una "X" en el cuadro apropiado que designe quién es responsable de cada tarea.

Si las personas de su organización tienen la responsabilidad de algunas o todas las tareas de un área de práctica operacional de seguridad, debe designar un enfoque para las características de Procedimientos y Formación.

Si una de las opciones coincide con la situación actual de su organización, marcar con una "X" en la casilla "Presente" junto a esa opción. Asegúrese de rellenar los espacios en blanco proporcionados para la opción que seleccione. Puede cambiar las palabras proporcionadas o agregar palabras adicionales según sea necesario.

Procedimientos	¿Hasta qué punto los procedimientos para esta área están formalmente documentados?		¿Alguna de las actividades de mitigación cambiará el grado en que los procedimientos están formalmente documentados para esta área? ¿Desea realizar cambios adicionales en la documentación de los procedimientos para esta área?	
Si el personal de su organización es parcial o totalmente responsable de esta área:				
Se ha documentado formalmente planes y procedimientos para controlar el acceso físico al edificio y a las instalaciones, áreas de trabajo, hardware de TI y medios de software.		Presente		Cambio
Se tiene políticas y procedimientos formalmente documentados para controlar el acceso físico al edificio y a las instalaciones, áreas de trabajo, hardware de TI y medios de software. Algunas políticas y procedimientos en esta área son informales e indocumentados.		Presente		Cambio
Se tiene planes y procedimientos informales e indocumentados para controlar el acceso físico al edificio y a los locales, áreas de trabajo, hardware de TI y medios de software.		Presente		Cambio
		Presente		Cambio

Figura 57. Hoja de trabajo Estrategia de protección - Procedimientos.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Formación	¿Hasta qué punto se requiere que los empleados asistan a la capacitación en esta área?		¿Alguna de las actividades de mitigación cambiará el requisito para asistir a la capacitación en esta área? ¿Desea hacer algún cambio adicional en el requisito de asistir a la capacitación en esta área?	
Si el personal de su organización es parcial o totalmente responsable de esta área:				
Los miembros del personal de tecnología de la información deben asistir a la capacitación para administrar sistemas y redes y utilizar herramientas de administración de sistemas y redes.		Presente		Cambio
Los miembros del personal de tecnología de la información pueden asistir a la capacitación para administrar sistemas y redes y usar herramientas de administración de sistemas y redes si lo solicitan.		Presente		Cambio
Por lo general, no se ofrece oportunidades para que los miembros del personal de tecnología de la información asistan a la capacitación para administrar sistemas y redes y utilizar herramientas de administración de sistemas y redes. Los miembros del personal de tecnología de la información aprenden sobre la gestión de sistemas y redes por su cuenta.		Presente		Cambio
		Presente		Cambio

Figura 58. Hoja de trabajo Estrategia de protección - Formación.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Si quisiera registrar como su organización aborda esta característica se le brinda líneas en blanco bajo cada cuadro o si tuviera alguna característica que añadir se puede colocar en dichas líneas.

Si el tercero tiene la responsabilidad de algunas o todas las tareas de un área de práctica operacional de seguridad, debe designar un enfoque para las características de Colaboración y Verificación. Anote el nombre del tercero arriba del cuadro.

Cuestiones de Colaboración		¿En qué medida su organización comunica formalmente sus requerimientos en esta área a este tercero?		¿Cambiarán las actividades de mitigación cómo su organización comunica sus requerimientos a este tercero? ¿Desea realizar cambios adicionales a cómo comunica los requisitos a este tercero?	
Si el personal de un tercero es parcial o totalmente responsable de esta área:					
El sistema de seguridad y los requisitos de gestión de red se comunican formalmente a todos los contratistas y proveedores de servicios que mantienen sistemas y redes.		Presente			Cambio
El sistema de seguridad y los requisitos de gestión de red se comunican informalmente a todos los contratistas y proveedores de servicios que mantienen sistemas y redes.		Presente			Cambio
El sistema de seguridad y los requisitos de gestión de red no se comunican a todos los contratistas y proveedores de servicios que mantienen sistemas y redes.		Presente			Cambio
					Cambio

Figura 59. Hoja de trabajo Estrategia de protección - Cuestiones de colaboración.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Verificación		¿En qué medida su organización verifica que este tercero está respondiendo a los requisitos en esta área?		¿Cambiará alguna de las actividades de mitigación cómo verifica que este tercero está respondiendo a los requisitos en esta área? ¿Desea realizar cambios adicionales en la forma de verificar que se cumplan los requisitos?	
Si el personal de un tercero es parcial o totalmente responsable de esta área:					
Se verifica formalmente que los contratistas y los proveedores de servicios han cumplido con los requisitos para el sistema de seguridad y la gestión de la red.		Presente			Cambio
Se verifica de manera informal que los contratistas y los proveedores de servicios han cumplido con los requisitos para la gestión del sistema y la red relacionados con la seguridad.		Presente			Cambio
No se verifica que los contratistas y los proveedores de servicios cumplan con los requisitos para la gestión del sistema y la red relacionados con la seguridad.		Presente			Cambio
		Presente			Cambio

Figura 60. Hoja de trabajo Estrategia de protección - Verificación.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Si tiene más de un tercero, rellenar esta información tantas veces como la cantidad de terceros que tenga.

Deberá completar la “HT-Estrategia de Protección” para todas las áreas de práctica operacional de seguridad.

Como se mencionó anteriormente, todo punto desarrollado se debe comunicar a las partes interesadas, como menciona la ISO/IEC 27005. En este caso, la información obtenida luego de esta actividad se debe informar.

5.3.4.2.2 Actividad P5-2: Seleccionar enfoques de mitigación (OCTAVE-S) y calcular riesgo – Evaluación, Tratamiento, Aceptación y Comunicación del riesgo (ISO/IEC 27005)

Completar las "Áreas de Práctica de Seguridad" de la hoja de trabajo “HT-Perfil de Riesgo” de cada activo crítico.

- Bajo, estrategia de seguridad baja (Valor = 3)
- Medio, estrategia de seguridad media (Valor =2)
- Alto, estrategia de seguridad alta (Valor = 1)

HT- PERFIL DE RIESGO																					
Perfil de riesgos																					
Historia ¿fue esta amenaza en el pasado?		Valores de impacto					Probabilidad		Áreas de prácticas de seguridad												
							¿Qué tan probable es que ocurra la amenaza en el futuro?		Estratégico						Operacional						
							Valor cualitativo	Valor cuantitativo	Concientización de la seguridad y capacitación	Estrategia de seguridad	Administración de la seguridad	Políticas de seguridad y regulaciones	Administración de Seguridad Colaborativa	Plan de Contingencia / Recuperación ante desastres	Control de acceso físico	Monitoreo y Auditoría de seguridad física	Administración de sistema y red	Monitoreo y Auditoría de seguridad TI	Auditorías y autorizaciones	Calificación de vulnerabilidad	Cifrado
	años.																				
	años.																				
	años.																				
	años.																				
	años.																				
	años.																				
	años.																				
	años.																				
	años.																				
	años.																				
	años.																				
	años.																				
	años.																				
	años.																				

Figura 61. Hoja de trabajo Perfil de Riesgo – Áreas de prácticas de seguridad.

Elaborado por jefes de proyecto, basado en OCTAVE-S

El campo “Total” se completa automáticamente, y muestra un semáforo donde se puede observar que tan crítica se encuentra dicha área de seguridad, sumando cada criterio.

- Rojo, mayor a 30.
- Amarillo, menor igual a 30 y menor a 15.
- Verde, menor igual a 15.

Como menciona la ISO/IEC 27005, se debe realizar la evaluación del riesgo, los criterios de evaluación del riesgo utilizados para tomar decisiones deberían ser consistentes con el contexto definido para la gestión del riesgo en la seguridad de la información externa e interna y se debe tomar en consideración los objetivos de la organización, los puntos de vista de las partes interesadas, etc. Las decisiones, tal como se toman en la actividad de evaluación del riesgo, se basan principalmente en el nivel aceptable de riesgo. Sin embargo, también es recomendable considerar las consecuencias, la probabilidad y el grado de confianza en la identificación y el análisis del riesgo.

La evaluación del riesgo utiliza la comprensión del riesgo que se obtiene mediante el análisis del riesgo para tomar decisiones sobre acciones futuras. Las decisiones deben incluir si se debe realizar una actividad y prioridades para el tratamiento de los riesgos considerando los valores estimado. A partir de este análisis se podrá obtener la lista de riesgos priorizada.

Tomando en cuenta el Anexo E de la ISO/IEC 27005 creamos la siguiente tabla para el impacto de las amenazas:

- Valor bajo = 1
- Valor medio = 2
- Valor alto = 3

Se ha considerado los criterios de impacto de Reputación, Financiero, Productividad, Multas y Seguridad, los cuales, si su valor es bajo en todo, el mínimo valor es 5 y el máximo 15, si su valor es alto para todos.

Generamos la tabla de riesgo, multiplicando la probabilidad por el impacto.

	Amenaza	5	6	7	8	9	10	11	12	13	14	15
Probabilidad	1	5	6	7	8	9	10	11	12	13	14	15
	2	10	12	14	16	18	20	22	24	26	28	30
	3	15	18	21	24	27	30	33	36	39	42	45

Figura 62. Impacto por probabilidad.

Elaborado por jefes de proyecto

Para obtener el valor mínimo y máximo de riesgo, se debe realizar lo siguiente:

Para el perfil de riesgo:

- Como mínimo se puede completar 1 amenaza y como máximo 16.
- Si solo se completa una amenaza, este se multiplica por el mínimo valor obtenido de la tabla de impacto por probabilidad ($1 \times 5 = 5$). Por lo que el valor de impacto mínimo de riesgo sería 5. Si se completa todos los tipos de amenaza solo se deberá cambiar el número de amenazas, por lo que el valor de impacto de riesgo sería 96 ($16 \times 6 = 96$). En este caso, se tiene que considerar el mínimo de amenazas completadas.
- El valor máximo de impacto de riesgo sería completando todos los tipos de amenaza y multiplicándolo por el mayor número de la tabla de impacto por probabilidad, por lo que el valor máximo de impacto de riesgo sería 864 ($16 \times 54 = 864$).

En este punto, la organización debe establecer el nivel correspondiente de valor de riesgo bajo, medio y alto, según sea su criterio. Asimismo, debe identificar el nivel de tolerancia de riesgo. Debe contemplar una matriz de riesgo para poder mostrar los valores de riesgo según

el color verde, para riesgo bajo; color amarillo, para riesgo medio; y color rojo, para riesgo alto. Es decisión de cada empresa cómo realizar su matriz de riesgo.

A partir de esta evaluación, se puede realizar una priorización de riesgos, que como menciona la ISO/IEC 27005 (“Lista de riesgos con prioridad”) se debe de hacer, esta lista puede ser desarrollada por los propios miembros del equipo de análisis.

Lista de riesgos con prioridad.xlsx

Lista riesgos con prioridad				
Cod. Activo	Activo	Riesgo	Nivel de riesgo	Prioridad

Figura 63. Lista riesgos con prioridad.

Elaborado por jefes de proyecto

Comenzar a pensar en cómo abordar cada riesgo. Es necesario comenzar a pensar en los riesgos que se pretenden mitigar, que se pretende aceptar y que se pretende monitorear y reevaluar en algún momento en el futuro. Marcar con una “X” el enfoque que se tendrá frente a cada riesgo identificado en la “HT-Perfil de Riesgos”.

Como se menciona en la ISO/IEC 27005, considerar qué riesgos va a mitigar, aceptar, transferir o evitar, pensando en el impacto de estos. Marcar con una “X” la decisión que tome al respecto.

- Mitigar: abordar un riesgo mediante la implementación de actividades diseñadas para contrarrestar la amenaza subyacente. Los riesgos que se mitigan normalmente tienen un alto impacto en una organización.
- Aceptar: Si el nivel del riesgo satisface los criterios para su aceptación, no es necesario implementar controles adicionales y el riesgo se puede retener.

Lista riesgos aceptados				
Cod. Activo	Activo	Riesgo	Riesgo Residual	Justificación de aceptación del riesgo

Figura 65. Lista de riesgos aceptados.

Elaborado por jefes de proyecto

Como se mencionó anteriormente, todo punto desarrollado se debe comunicar a las partes interesadas, como menciona la ISO/IEC 27005. En este caso, la información de los enfoques y los posibles riesgos a aceptar se debe informar.

5.3.4.2.3 Actividad P5-3: Desarrollar plan de mitigación (OCTAVE-S) – Tratamiento, Aceptación y Comunicación del riesgo (ISO/IEC 27005)

Revisar toda la información que ha registrado durante toda la evaluación en las “HT-Notas y Recomendaciones”, se debe prestar atención específica a cualquier recomendación que se haya hecho con respecto a posibles actividades de mitigación.

Crear planes de mitigación para cada área de práctica de seguridad. Si identifica riesgos para mitigar puede guiarse de la “Guía de Actividades de Mitigación” para identificar las posibles acciones a realizar. La guía proporciona posibles actividades de mitigación, pero no una lista exhaustiva. No debe limitarse a las actividades enumeradas en tal guía, también, como menciona la ISO/IEC 27005 puede basarse en los controles mencionados en la ISO/IEC 27002, ya que están bien detallados.

HT-Guía de Mitigación.xlsx

HT-ACTIVIDADES DE MITIGACIÓN

Concientización de la seguridad y capacitación	Estrategia de seguridad	Administración de la seguridad	Políticas de seguridad y regulaciones	Administración de Seguridad Colaborativa

Plan de Continencia / Recuperación ante desastres	Control de acceso físico	Monitoreo y Auditoría de seguridad física	Administración de sistema y red	Monitoreo y Auditoría de la seguridad TI

Autenticación y autorización	Gestión de vulnerabilidad	Cifrado	Arquitectura y diseño de seguridad	Gestión de incidentes

Figura 66. Guía de Mitigación - Inicio.

Elaborado por jefes de proyecto

Como se menciona en la ISO/IEC 27005, los controles pueden brindar uno o más de los siguientes tipos de protección: corrección, eliminación, prevención, minimización del impacto, disuasión, detección, recuperación, monitoreo y concienciación. Es importante considerar que el costo de implementar un control no puede ser más que el costo del impacto del riesgo.

Buscar instancias en las que se anticipe que una actividad provocará un cambio en la protección. Utilizar la hoja de trabajo “HT-Plan de mitigación”.

HT-Plan de mitigación.xlsx

HT- Plan de mitigación				
Área de Mitigación	Actividad de Mitigación ¿Qué actividades de mitigación va a implementar en este área de protección de seguridad?	Razón fundamental ¿Por qué seleccionó cada actividad?	Responsabilidad de Mitigación ¿Quién necesita participar en la implementación de cada actividad? ¿Por qué?	Soporte adicional ¿Qué apoyo adicional será necesario al implementar cada actividad (por ejemplo, financiamiento, conocimientos del personal, patrocinio)?

Figura 67. Hoja de trabajo – Plan de mitigación.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Como se mencionó anteriormente, todo punto desarrollado se deberá comunicar a las partes interesadas, como menciona la ISO/IEC 27005. En este caso, la información obtenida para el plan de mitigación se deberá informar.

Aquí, deberá tomar en cuenta los controles completados en las amenazas identificadas y las vulnerabilidades relacionadas a ellas, contemplando esta información podrá completar la “Lista de controles” identificando los posibles controles para lo identificado.

Elaborado por jefes de proyecto

- Preventivo: Si el control se aplica antes de un proceso (Valor = 4).
- Correctivo: Si el control se aplica durante el proceso y permite corregir las deficiencias (Valor = 3).

Completar el valor de riesgo para cada activo según lo explicado anteriormente.

Para hallar el riesgo residual de cada activo debemos aplicar la siguiente formula: “Valor riesgo del activo/Valor promedio del valor de la eficacia del activo”.

A partir de los riesgos residuales identificados, se podrá identificar una lista de riesgos que se podrán aceptar (“Lista de riesgos aceptados”) que se menciona en la ISO/IEC 27005, que la podrán realizar los miembros del equipo de análisis al terminar este punto, junto con su respectiva justificación.

Con la información recolectada hasta este punto, se puede generar la matriz de riesgo residual de los activos, la cual será definida con la organización.

Como se mencionó anteriormente, todo punto desarrollado se debe comunicar a las partes interesadas, como menciona la ISO/IEC 27005. En este caso, la información obtenida sobre los controles identificados se debe informar.

5.3.4.2.5 Actividad P5-5: Identificar cambios a la estrategia de protección (OCTAVE-S) – Comunicación del riesgo (ISO/IEC 27005)

Si determina que una actividad de mitigación afecta a una de las características de un área de práctica de seguridad, marcar con una "X" en el recuadro "Cambio" después del nuevo enfoque en la “HT-Estrategia de Protección”. Asegúrese de rellenar los espacios en blanco proporcionados para la opción que seleccione. Puede cambiar las palabras proporcionadas o agregar palabras adicionales según sea necesario.

HT- ESTRATEGIA DE PROTECCIÓN			
Políticas de seguridad y regulaciones			
Semáforo			
Políticas documentadas	¿Hasta qué punto están formalmente documentadas las políticas relacionadas con la seguridad de su organización?	¿Las actividades de mitigación cambiarán el grado en que sus políticas relacionadas con la seguridad están formalmente documentadas? ¿Desea realizar cambios adicionales a la formalidad y documentación de sus políticas relacionadas con la seguridad?	
La organización tiene un conjunto completo de políticas formalmente documentadas relacionadas con la seguridad.	Presente		Cambio
La organización tiene un conjunto parcial de políticas formalmente documentadas relacionadas con la seguridad.	Presente		Cambio
Algunas políticas relacionadas con la seguridad son informales e indocumentadas.	Presente		Cambio
Las políticas relacionadas con la seguridad de la organización son informales e indocumentadas.	Presente		Cambio

Figura 70. Hoja de Estrategia de Protección – Políticas de seguridad y regulaciones.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Monitoreo y Auditoría de la seguridad TI							
Semáforo							
Responsabilidad	Tarea	¿Quién es actualmente el responsable de monitorear y auditar la seguridad de TI?			¿Cambiarán las actividades de mitigación la responsabilidad de monitorear y auditar la seguridad de TI? ¿Desea realizar cambios adicionales que afecten a la responsabilidad de supervisar y auditar la seguridad de TI?		
		Interno	Externo	Combinado	Interno	Externo	Cambio
	Uso de herramientas de supervisión del sistema y la red para realizar un seguimiento de la actividad del sistema y de la red.						
	Auditar periódicamente el firewall y otros componentes de seguridad para verificar el cumplimiento de la política.						
	Investigar y abordar cualquier actividad inusual que se identifique.						

Figura 71. Hoja de Estrategia de Protección – Monitoreo y Auditoría de la seguridad TI.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Monitoreo y Auditoría de la seguridad TI							
Semáforo							
Responsabilidad	Tarea	¿Quién es actualmente el responsable de monitorear y auditar la seguridad de TI?			¿Cambiarán las actividades de mitigación la responsabilidad de monitorear y auditar la seguridad de TI? ¿Desea realizar cambios adicionales que afecten a la responsabilidad de supervisar y auditar la seguridad de TI?		
		Interno	Externo	Combinado	Interno	Externo	Cambio
	Uso de herramientas de supervisión del sistema y la red para realizar un seguimiento de la actividad del sistema y de la red.						
	Auditar periódicamente el firewall y otros componentes de seguridad para verificar el cumplimiento de la política.						
	Investigar y abordar cualquier actividad inusual que se identifique.						

Figura 72. Hoja de Estrategia de Protección – Monitoreo y Auditoría de la seguridad TI – Cambiar.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Documentar los puntos de acción a tomar describiendo la acción, el responsable, algunas acciones de gestión que puedan ayudar a facilitar que se complete la acción en la hoja de trabajo “HT-Lista de acciones”, así mismo documentar notas relevantes y recomendaciones del proceso en la hoja de trabajo “HT-Notas y recomendaciones”.

Como se mencionó anteriormente, todo punto desarrollado se debe comunicar a las partes interesadas, como menciona la ISO/IEC 27005. En este caso, la información obtenida de los cambios a la estrategia de protección se debe informar.

5.3.4.2.6 Actividad P5-6: Identificar siguientes pasos (OCTAVE-S) – Comunicación del riesgo (ISO/IEC 27005)

Determinar qué pasos debe tomar su organización para implementar los resultados de esta evaluación según las acciones, notas y recomendaciones identificadas. Registrar los pasos en la “HT-Pasos siguientes”.

HT-Siguientes pasos			
Patrocinio de la gerencia para la mejora	Implementación de monitoreo	Ampliación de la evaluación actual del riesgo	Próxima información de Evaluación del riesgo de
¿Qué debe hacer la administración para apoyar la implementación de los resultados?	¿Qué hará la organización para seguir el progreso y asegurar que se implementan los resultados de esta evaluación?	¿Ampliará la actual evaluación de para incluir activos críticos adicionales? ¿Cuáles?	¿Cuándo realizará la organización su próxima evaluación?

Figura 73. Hoja de Siguientes pasos.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Asimismo, se decide añadir en esta sección que se presenten indicadores para el debido monitoreo de los controles propuestos.

Como se mencionó anteriormente, todo punto desarrollado se debe comunicar a las partes interesadas, como menciona la ISO/IEC 27005. En este caso, la información de los siguientes pasos a seguir se debe informar.

A este punto, ya se ha completado la evaluación de OCTAVE-S integrado con la ISO/IEC 27005. Asegurarse de documentar formalmente los resultados de esta evaluación. Se puede distinguir en qué áreas se encuentra bien o mal, y sobre todo los activos considerados dentro de su organización. Asimismo, se tiene conocimiento de las acciones a tomar para poder reducir el riesgo sobre su organización, ya tendrá conocimiento sobre qué procesos, activos o áreas poner énfasis.

Para que la siguiente vez que realice el análisis se puede utilizar el formato macro “MGRSIPP Principal”, en el cual debe completar la casilla de “Dirección carpeta” con las plantillas del modelo, luego como ya cuenta con el conocimiento de la primera

implementación podrá seguir los pasos descritos según cada fase del modelo. Para poder abrir y completar cada plantilla debe hacer clic en los botones al lado de cada nombre de la plantilla, es preferible no cambiar dichos nombres, ya que si esto ocurriera también deberían cambiarse los nombres de las plantillas en esta macro, por lo que se sugiere mantener los nombres de las plantillas para que esta macro pueda funcionar correctamente.

Figura 74. Formato "MGRSIPP Principal".

Elaborado por jefes de proyecto

5.4 Validación de expertos

Para validar el modelo de gestión de riesgos de seguridad de la información se contacta con expertos de seguridad de la información para que puedan dar sus puntos de vista acerca del modelo y si este cumple con los requerimientos de una gestión de riesgos.

Se contacta con tres expertos en seguridad de la información, a quienes se les explica debidamente cada uno de los procesos dentro del modelo. Asimismo, se responden las preguntas relacionadas y se aceptan las recomendaciones otorgadas por cada uno de ellos.

Experto	Conocimientos	Cargo	Imagen
Alfonso Farje	CISM, CRISC, CISA (Isaca); CRMA (IIA)	Auditor
Eduardo Padilla	CISO	Ciberseguridad
Jorge Arévalo	ISO 27001 ISO 2000-1 ISO 22301	Consultor y auditor

Figura 75. Expertos en seguridad.

Elaborado por jefes de proyecto

Al finalizar la presentación del modelo se realiza una encuesta a cada uno de ellos donde se realizaron las siguientes preguntas:

- ¿El modelo contempla los principales componentes para una adecuada gestión de riesgos?
- ¿Los procesos del modelo tienen concordancia y siguen los lineamientos de la gestión de riesgos y la seguridad de la información?
- ¿El modelo contempla el proceso de identificación de controles a aplicar sobre los riesgos identificados, y así contemplar el riesgo residual?
- El modelo cuenta con una guía adecuada para su implementación en las Pymes.

Cada una de las preguntas esta valorizadas entre 1 y 5, donde 1 significada “En desacuerdo” y 5, “Completamente de acuerdo”.

Los tres expertos entregan un puntaje a cada una de las preguntas realizadas respecto al modelo, donde se puede obtener un promedio respectivamente. De esta manera, el modelo diseñado en este proyecto se validada, ya que los resultados son mayores o iguales a 4, que es un buen puntaje.

P1: El modelo contempla los principales componentes para una adecuada gestión de riesgos.
P2: Los procesos del modelo tienen concordancia y siguen los lineamientos de la gestión de riesgos y la seguridad de la información.
P3: El modelo contempla el proceso de identificación de controles a aplicar sobre los riesgos identificados, y así contemplar el riesgo residual.
P4: El modelo cuenta con una guía adecuada para su implementación en las Pymes.

Figura 76. Expertos en seguridad.

Elaborado por jefes de proyecto

Un punto importante a resaltar es relacionado a la última pregunta, el proyecto sí cuenta con una guía sobre cómo implementar cada uno de los procesos, pero los expertos mencionan que, por más de ello, las Pymes por su falta de cultura no siguen paso a paso lo que deben hacer, es por ello que se le otorgaba un menor puntaje. Se menciona que, las Pymes poco a poco están tomando conciencia de lo importante que es enfocarse en la seguridad de los activos de información debido a los distintos ataques que han ocurrido alrededor del mundo.

5.5 Impacto económico del proyecto

Para el presente proyecto, se realiza un estudio de impacto económico, ya que esto ayuda a validar que el proyecto es viable para la empresa de producto de arcilla cerámica. El estudio se basa en el beneficio que traería a la empresa implementar este proyecto, estos datos se han basado en estimaciones.

5.5.1 Costo del proyecto

En esta sección, se presenta el costo del proyecto según las horas de trabajo a realizar por los involucrados en la implementación del mismo.

Tabla 13
Costo del proyecto

	Cantidad	Horas	Costo por horas	S./
Norma ISO/EIC 27005	1			S/. 594.35
Analista de seguridad	2	230	S/. 34.38	S/. 15,812.50
Analista de procesos	1	91	S/. 28.13	S/. 2,559.38
Jefe de Proyecto	1	50	S/. 50.00	S/. 2,500.00
Total				S/. 21,466.23

Fuente: Elaborado por jefes de proyecto

Como se puede observar, el costo total del proyecto sería 21,466.23 soles.

5.5.2 Beneficios del proyecto y recuperación por parte de la empresa

En esta sección, se presenta los beneficios obtenidos si se implementa el proyecto dentro de la empresa.

Tabla 14
Beneficios

Pedidos que no se realizan	Cantidad	Costo por horas	Costo mensual	Costo anual
Cientes perdidos	1	-	S/. 1,800.00	S/. 1,800.00
Reducción de costos de operación	Cantidad	Costo por horas	Costo mensual	Costo anual
Digitadores	2	-	S/. 161.67	S/. 1,940.00
Analista de procesos en horas	15	S/. 28.00	S/. 35.00	S/. 420.00
Consultor	1	-	S/. 666.67	S/. 8,000.00
		Total	S/. 2,663.33	S/. 12,160.00

Fuente: Elaborado por jefes de proyecto

Como se observa, anualmente se obtendrá un retorno de 12,160.00 soles. Para obtener de manera exacta el tiempo en que la empresa de productos de arcilla cerámica recuperaría la inversión por el proyecto se calculó el Retorno de inversión.

Tabla 15
Retorno de inversión y tiempo de recuperación

		ROI Mensual	ROI Anual
Total inversión	S/. 21,466.23	12%	57%
Meses a recuperar la inversión		8.1	

Fuente: Elaborado por jefes de proyecto

Como se puede observar, el Retorno de inversión obtenido mensual es de 12%, con lo que se obtiene que la empresa de producto de arcilla cerámica podrá recuperar lo invertido en 8.1 meses.

5.6 Información básica de la empresa

El presente proyecto es desarrollado para empresas del tipo Pyme. La empresa escogida de productos de arcilla cerámica se encuentra ubicada en Puente Piedra, se encarga de la producción y venta de estos productos, ya sea a clientes naturales o clientes corporativos. Específicamente llega a través de tres sectores; el retail, el tipo depósito y las constructoras.

Visión: Operar con calidad un sistema de negocios que permita identificar y servir a aquellos segmentos del mercado que pueden ser satisfechos con productos cerámicos, ofreciendo a los clientes productos de inmejorable calidad y precio.

Misión: Satisfacer las necesidades del sector construcción, con una actitud de liderazgo en el servicio y atención al cliente; respeto por el medio ambiente y la salud de nuestros trabajadores. Ser considerados por los clientes como un socio estratégico para su crecimiento. Ser una compañía en la cual los empleados estén orgullosos de pertenecer, por lo cual la armonía en el trabajo debe ser un estándar.

La empresa considera que sus procesos son limpios, como trabajan con arcilla que extraen de canteras locales, es decir, no usan tierra agrícola, de esta manera es como participan en el cuidado del medio ambiente.

La empresa tiene alrededor de 24 productos en cartera que abarcan todas las necesidades de vivienda que puedan existir desde los ladrillos que puedan soportar carga, ladrillos para muro, para techo y ladrillos que conforman la tabiquería, como son panderetas, ladrillos de decoración, ladrillos que protegen de las lluvias y ladrillos que permiten métodos de

construcción muy rápidos para grandes estructuras como son centros comerciales o edificios que requieren alta mano de obra, facilitamos ladrillos que hacen que este proceso se haga mucho más rápido.

A continuación, se presenta los procesos para la producción de los productos de arcilla cerámica:

Figura 77. Proceso de producción.

Elaborado por jefes de proyecto

5.7 Modelo a implementar en proceso de ventas

En esta sección, se verifica si la empresa cumple con los requisitos para implementar el modelo y se seleccionará el equipo de trabajo para la gestión de riesgos de seguridad de la información dentro de la empresa de productos de arcilla cerámica.

La empresa cumple con los requisitos:

- En el proceso de ventas son menos de 250 trabajadores.
- Según el análisis realizado la empresa tiene un nivel de 43% de cumplimiento en seguridad de la información, el cual es considerado un nivel bajo.
- Hace unos años la empresa perdió una suma importante de dinero por delitos informáticos.
- La empresa cuenta con recomendaciones de auditoría pendientes, las cuales aún no han sido implementadas o controladas.
- La empresa cuenta con un área de TI, y también cuenta con servicios externos contratados.

5.8 Plan de Continuidad

5.8.1 Post Implementación del modelo

Luego de realizada la implementación del modelo de gestión de riesgos de seguridad de la información, será necesario analizar y monitorear los controles según los resultados obtenidos.

La empresa puede comparar los resultados y determinar las acciones a realizar para mejorar en la gestión de riesgos de seguridad de la información.

Para este punto, nos basamos en el ciclo PDCA (Plan, Do, Check, Act):

Tabla 16

Ciclo PDCA - Post Implementación del modelo

Planear	Hacer	Verificar	Actuar
Analizar los controles que solucionan las vulnerabilidades encontradas en el proceso, definir las tareas para su implementación. Se debe tener prioridad en los activos críticos.	Implementar los controles identificados en la fase de planificación.	Monitorear que los controles y cambios aplicados para verificar que se reduzca el riesgo de los activos.	Si los controles no muestran los resultados esperados, se debe volver a la primera fase: planear, para evaluar nuevas mejoras.

Fuente: Elaborado por jefes de proyecto

5.8.2 Método de adaptabilidad

Al tener las distintas propuestas de mejora para el modelo propuesto es necesario realizar el mantenimiento del mismo para que siga siendo efectivo y sobre todo este tenga continuidad a través del tiempo. Para poder generar la adaptabilidad del modelo se ve necesario el uso de la norma ISO 31000: Gestión del riesgo. Esta norma proporciona principios y directrices de carácter genérico sobre la gestión de riesgos. El diseño y ejecución de planes de gestión de riesgos y marcos tendrá que tomar en cuenta las diferentes necesidades de una organización específica, sus objetivos particulares, contexto, estructura, operaciones,

procesos, funciones, proyectos, productos, servicios o activos específicos y prácticas empleadas (Organización Internacional de Normalización, 2009).

La ISO 31000:2018 está basada tres componentes: principios, un marco de referencia y el proceso.

Los principios proporcionan orientación sobre las características de una gestión de riesgos eficaz y eficiente, comunicando valor y explicando su intención y propósito (Asociación Española de Normalización, 2018). Los principios son que la gestión de riesgos debe ser integrada, estructurada y exhaustiva, adaptada, inclusiva, dinámica, mejor información disponible, factores humanos y culturales y la mejora continua.

El marco de referencia asiste a la organización en integrar la gestión de riesgo en todas las actividades y funciones significativas (Asociación Española de Normalización, 2018). En dicho marco se observa la modificación del tradicional ciclo PHVA (Planificar-Hacer-Verificar-Actuar), ya que se ve ampliado a cinco pasos: Integración, Diseño, Implementación, Evaluación y Mejora.

A continuación, describiremos cada una de las etapas del marco de referencia:

- Integración: todos los miembros de una organización tienen la responsabilidad de gestionar el riesgo. Asimismo, se determinan los roles para la rendición y cuentas y la supervisión de la gestión del riesgo.
- Diseño: se analiza y comprende el contexto interno e externo de la organización, se fija un propósito para la gestión del riesgo, se asignan recursos y roles, autoridades y responsabilidades, así como se establece la comunicación y la consulta.
- Implementación: implementar los procesos del marco de referencia de gestión de riesgos. La implementación exitosa depende del compromiso y la toma de conciencia de las partes interesadas.
- Valoración: se mide periódicamente el desempeño del marco de referencia con relación al propósito, los planes de implementación, indicadores y el compromiso esperado. Se determina si permanece idóneo para apoyar el logro de los objetivos de la organización.
- Mejora: se debe realizar el seguimiento continuo y adaptar el marco de referencia en función de los cambios externos e internos, así mismo, la organización debe mejorar

continuamente la idoneidad, adecuación y eficacia del marco de referencia y la manera en la que se integra al proceso de gestión del riesgo (Asociación Española de Normalización, 2018).

El proceso de gestión de riesgo implica la aplicación de políticas, procedimientos y practicas a las actividades de comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registro e informe del riesgo.

Figura 78. Marco de referencia y proceso ISO 31000.

Elaborado por Asociación Española de Normalización, 2018

A continuación, mostramos los puntos a tener en cuenta enfocados según el presente proyecto para poder continuar con el mismo a través del tiempo, centrándonos en el marco de referencia proporcionado por la ISO 31000: 2018.

Integración

La gerencia debe ser responsable de la gestión, debe determinar los roles que participaran frente a esta gestión, a quienes se debe de rendir cuentas sobre cualquier acontecimiento y quién designar un supervisor de la gestión del riesgo. Se define que para la rendición de

cuentas el responsable debe recopilar la información, presentar un informe, y la gerencia verificará el contenido del mismo.

Se planifica los objetivos de la gestión de riesgos mediante indicadores, asimismo debe mantener la integridad del modelo de gestión de riesgos. En todo momento la gerencia debe de estar comprometida con el proceso, y velar por integrar la política de gestión de riesgo y su monitoreo constante.

Diseño

Se debe tener en cuenta el análisis interno y externo de la empresa, puede ayudarse del establecimiento del contexto del modelo propuesto. La gerencia designa las responsabilidades de cada autoridad y participante de la gestión del riesgo y genera la debida comunicación al respecto del proceso.

Si se realiza alguna revisión de la gerencia para mantener la adecuación y la eficacia continua del sistema de gestión de riesgos, se debe registrar los cambios realizados. También, la gerencia debe tener en cuenta los recursos necesarios para la implementación del modelo de gestión de riesgos, respecto de los recursos humanos, estos deben tener las competencias necesarias para realizar este proceso, si fuera el caso debe elaborar un presupuesto para la realización de esta gestión. En este punto, se puede ayudar de la selección de equipo de trabajo del modelo, ya que se identifica el personal idóneo, capacitado y con habilidades que se necesita para poder desempeñar las labores necesarias dentro de este proceso.

Implementación

En este punto se implementa cada proceso del modelo de gestión de riesgos que se esté adaptando para poder analizar los resultados obtenidos, dar propuestas de control y gestionar la validación del mismo tomando en cuenta lo planificado para poder asegurar que los resultados han cumplido con los requisitos. Si se diera el caso de tener cambios dentro del proceso, estos deben de ser debidamente registrados.

Valoración

En este punto la gerencia debe de tener en cuenta realizar monitoreo de indicadores y auditorías internas respecto a la implementación del modelo en determinado tiempo para poder verificar los procesos, determinar si se satisfacen los requisitos y si la implementación y mantenimiento se desarrolla correctamente. Asimismo, debe de realizarse el debido

seguimiento de los resultados que genere el modelo para verificar la veracidad de los mismos y el cumplimiento de los requisitos planificados. Se debe tener en cuenta que todo debe de estar debidamente evidenciado.

Mejora

A partir de los resultados obtenidos en la revisión, la empresa debe de mejorar la eficacia del modelo implementado, teniendo en cuenta los objetivos, los resultados, el monitoreo, las auditorías y las revisiones de gerencia. A partir de ello, la gerencia tomará ciertas acciones, ya sean correctivas, las cuales contemplan las no conformidades, daños, resultados erróneos; o acciones preventivas, las cuales contemplan la prevención de cualquier tipo de problema dentro de la implementación del modelo. Asimismo, contribuye con la una mejor gestión de riesgo la comunicación continua con las partes interesadas dentro del proceso.

5.8.3 Certificaciones

Realizando la evaluación de riesgo dentro de la empresa y cumpliendo las observaciones de auditoría, la empresa podrá considerar aplicar a la certificación de la ISO/IEC 27001. La empresa debe considerar los requisitos que incluye la certificación, no necesariamente todos están contemplados en el modelo, debe tener en cuenta también si cuenta con el presupuesto necesario para dicha certificación.

5.9 Hoja de ruta

La Hoja de Ruta presenta los posibles proyectos a desarrollar basados en el proyecto “Modelo de Gestión de Riesgos de Seguridad de la Información para Pymes en el Perú”.

Tabla 17
Lista de proyectos

Nombre del proyecto	Descripción	Dependencias entre proyectos
Herramienta automatizada para usar modelo	La herramienta permitirá que las hojas de trabajo que estén integradas en un solo sistema.	Modelo de Gestión de Riesgos de Seguridad de la Información para Pymes en el Perú

Monitoreo de controles implementados en Pymes	La implementación del proyecto “Modelo de Gestión de Riesgos de Seguridad de la Información para Pymes en el Perú” identificó controles a implementar en una empresa para ayudar a reducir el riesgo, por lo que este nuevo proyecto verificará el cumplimiento de estos.	Herramienta automatizada para usar modelo
Tablero de control de activos, vulnerabilidades, amenazas, riesgos y controles implementados para Pymes	El tablero de control que permitirá tener una vista más gerencial y que ayudará a la toma de decisiones frente a los riesgos, este tablero se realizará por medio de la herramienta MicroStrategy.	Monitoreo de controles implementados en Pymes
Implementación de un chat box basado en gestión de riesgos de seguridad de la información para Pymes	Implementar un chat box que permita al usuario saber qué riesgos se pueden presentar por realizar ciertas acciones que exploten vulnerabilidades, donde solo se necesite alimentar una base de datos con los posibles riesgos frente a ciertas situaciones.	
Implementar una herramienta de gestión de riesgos para Pymes	Implementar una herramienta de gestión de riesgos que permita realizar en menos tiempo la evaluación y el análisis de gestión de riesgos.	
Diseño de aplicación móvil de uso interno basado en un tablero de control de gestión de riesgos	Aplicación de uso interno para gerentes y personal de seguridad de la información para mostrar las amenazas en tiempo real y entre en contacto con el equipo responsable para poder resolver	Tablero de control de activos, vulnerabilidades, amenazas, riesgos y controles

	dicha situación si es que esta es una amenaza crítica.	implementados para Pymes
--	--	--------------------------

Fuente: Elaborado por jefes de proyecto

Figura 79. Hoja de ruta.

Elaborado por jefes de proyecto

5.9.1 Objetivo de los proyectos

Herramienta automatizada para usar modelo.

- Hojas de trabajo integradas

Monitoreo de controles implementados en Pymes.

- Generación de indicadores.
- Monitorear el cumplimiento de controles propuestos.

Tablero de control de activos, vulnerabilidades, amenazas, riesgos y controles implementados para Pymes.

- Mejorar la visualización de la gestión de riesgos.
- Tomar mejores decisiones frente al riesgo.

Implementación de un chat box basado en gestión de riesgos de seguridad de la información para Pymes.

- Crear un modelo de chat box para el personal de la empresa.
- Generación de respuestas automáticas.

- Conocer las posibles consecuencias de acciones que generen riesgo.

Implementar una herramienta de gestión de riesgos para Pymes.

- Implementar una herramienta de gestión de riesgos que permita facilitar la evaluación de riesgos.
- Generar reportes según la evaluación realizada por la herramienta.

Diseño de aplicación móvil de uso interno basado en un tablero de control de gestión de riesgos.

- Diseñar una aplicación móvil para visualizar las amenazas que se presenten en la empresa.
- Mejorar el contacto con el equipo responsable ante emergencias.

5.9.2 Beneficios

Herramienta automatizada para usar modelo de Gestión de Riesgos.

- Disminuir el tiempo de trabajo al llenar las Hojas de Trabajo.
- Contar con la información en un solo sistema

Monitoreo de controles implementados en Pymes.

- Validar la reducción del riesgo identificado en la empresa.
- Información en tiempo real sobre los controles implementados.
- Garantizar la seguridad de la información.

Tablero de control de activos, vulnerabilidades, amenazas, riesgos y controles implementados para Pymes.

- Información en tiempo real sobre activos, vulnerabilidades, amenazas, riesgos y controles implementados.
- Rapidez en toma de decisiones.

Implementación de un chat box basado en gestión de riesgos de seguridad de la información para Pymes.

- Rápida respuesta frente a situaciones de riesgo.

- Reducir costos de personal de seguridad de información capacitado.
- Garantizar la seguridad de la información.

Implementar una herramienta de gestión de riesgos para Pymes.

- Automatización en la evaluación y análisis de riesgos.
- Rapidez en la evaluación y análisis de riesgos.
- Garantizar la seguridad de la información.

Diseño de aplicación móvil de uso interno basado en un tablero de control de gestión de riesgos.

- Disponibilidad de información y facilidad de acceso.
- Localizar en cualquier momento a los responsables de equipo para solucionar situaciones de riesgo.

5.9.3 Lista de prioridad de implementación del proyecto

Tabla 18

Lista de prioridad de implementación del proyecto

Nombre del Proyecto	Prioridad	Razón
Herramienta automatizada para usar modelo de Gestión de Riesgos	Alta	Permite completar las hojas de trabajo en menor tiempo, por lo que se podría usar el análisis de riesgo más seguido
Monitoreo de controles implementados en Pymes	Alta	Permite validar la implementación de controles. Es indispensable que los controles se estén cumpliendo para poder reducir el riesgo identificado en la empresa.
Tablero de control de activos, vulnerabilidades, amenazas, riesgos y controles implementados para Pymes	Alta	Permite la visualización en tiempo real de activos, vulnerabilidades, amenazas, riesgos y controles implementados en la empresa y así poder tomar mejores decisiones sobre lo que

		se quiere abarcar según la seguridad de la información.
Implementación de un chat box basado en gestión de riesgos de seguridad de la información para Pymes	Media	El automatizar las respuestas frente a situaciones de riesgo puede ayudar a reducir más rápido el riesgo, pero tomando la situación actual de la empresa en presupuesto, este no sería un proyecto de gran necesidad.
Implementar una herramienta de gestión de riesgos para Pymes	Alta	Permite la automatización de la evaluación y análisis de riesgo de una empresa y a su vez generará rapidez en dicho proceso, por lo que es importante que se pueda implementar este tipo de herramienta.
Diseño de aplicación móvil de uso interno basado en un tablero de control de gestión de riesgos	Media	Permite a los gerentes y personal de seguridad de la información estar pendientes de las amenazas presentadas en una empresa y poder contactar con los responsables para que dicha situación no se agrave, pero debido al poco presupuesto de empresas en seguridad de la información no es un proyecto tan necesario.

Fuente: Elaborado por jefes de proyecto

5.9.4.3 Costo estimado de la migración

- Herramienta automatizada para usar Modelo de Gestión de Riesgos

Tabla 19

Tabla de costo estimado de herramienta automatizada

Personal de Programador	
Costo x mes(S/.)	Costo x 6 meses
5.000	30.000

Personal de QA	
Costo x mes(S/.)	Costo x 6 meses
4.000	24.000

Total (2)	108.000
------------------	---------

Fuente: Elaborado por jefes de proyecto

- Monitoreo de controles implementados en Pymes

Implementar los controles no cuenta con un precio, sin embargo, para el monitoreo se necesita a un personal de seguridad de la información.

Tabla 20

Tabla de costo estimado de Monitoreo de controles

Personal de Seguridad de la Información	
Costo x mes(S/.)	Costo x año(S/.)
5.500	66.000

Cantidad:	2
Costo Anual Total:	132.000

Fuente: Elaborado por jefes de proyecto

- Tablero de control de activos, vulnerabilidades, amenazas, riesgos y controles implementados para Pymes

En las siguientes tablas se muestran propuestas de diferentes proveedores, el cual la empresa tendrá que escoger a uno de ellos.

Tabla 21

Tabla de costo estimado del tablero

Tipo de Cambio	3,26
-----------------------	------

Tableau		
Costo mensual (\$)	Costo anual (\$)	Soles
35	420	1369,2

Power BI		
Costo mensual (\$)	Costo anual (\$)	Soles
9,5	114	371,64

Qlik		
Costo mensual (\$)	Costo anual (\$)	Soles
25	300	978

MicroStrategy		
Costo mensual (\$)	Costo anual (\$)	Soles
0	0	0

Fuente: Elaborado por jefes de proyecto

- Implementación de un chatbox basado en gestión de riesgos de seguridad de la información para Pymes

En las siguientes tablas se muestran propuestas de diferentes proveedores, el cual la empresa tendrá que escoger a uno de ellos.

Tabla 22

Tabla de costo estimado de chat box

Tipo de Cambio	3,26	
IBM	(*) Por usuario	
Costo mensual (\$)	Costo anual (\$)	Soles
0,0025	0,03	0,0978
Zendesk Chat	(*) Usuarios Ilimitados	
Costo mensual (\$)	Costo anual (\$)	Soles
14	168	547,68
LiveChat	(*) Usuarios Ilimitados	
Costo mensual (\$)	Costo anual (\$)	Soles
16	192	625,92

Fuente: Elaborado por jefes de proyecto

- Implementar una herramienta de gestión de riesgos para Pymes

En las siguientes tablas se muestran propuestas de diferentes proveedores, el cual la empresa tendrá que escoger a uno de ellos.

Tabla 23

Tabla de costo estimado de herramienta de gestión de riesgos

Tipo de Cambio	3,26
Nessus	(*) 256 computadoras
Costo Mensual	Costo anual
1.392,16	16.706
Microsoft Baseline Security Analyzer 2.3	
Costo Mensual	Costo Anual
-	-

Retina CS		(*) 256 computadora
Costo Mensual (\$)	Costo Anual (\$)	Costo Anual (S/.)
6.656,00	79.872,00	260.383

Fuente: Elaborado por jefes de proyecto

- Diseño de aplicación móvil de uso interno basado en un tablero de control de gestión de riesgos

En las siguientes tablas se muestran propuestas de diferentes proveedores, el cual la empresa tendrá que escoger a uno de ellos.

Tabla 24

Tabla de costo estimado de aplicación móvil

Personal de Diseño Gráfico	
Costo x mes(S/.)	Costo x 2 meses
4.000	8.000

Personal de Programador	
Costo x mes(S/.)	Costo x 6 meses
5.000	30.000

Total	38.000
-------	--------

Fuente: Elaborado por jefes de proyecto

5.9.5 Recomendaciones en la implementación

5.9.5.1 Criterios de efectividad de los proyectos

- El éxito del proyecto se mide por que los costos no sobrepasen el límite de presupuesto estimado.
- El éxito del proyecto se mide por que no sobrepasen la fecha estimada de implementación.
- La medición del avance de los proyectos será medida por indicadores que serán supervisados cada semana.

5.9.5.2 Riesgos y problemas

- No contar con suficiente presupuesto para realizar los proyectos es considerado un riesgo para los proyectos, ya que no permitirá el desarrollo de los mismos.
- Que los proveedores no cumplan con el cronograma estimado y sobrepasen las fechas de entrega, esto ocasionaría un retraso en los demás proyectos.
- El que los empleados de la empresa no cuenten con el tiempo para poder explicarles el funcionamiento de cada proyecto.
- La falta de interés de la gerencia por la implementación de los proyectos.
- Resistencia al cambio.

6 CAPÍTULO 6: RESULTADOS DEL PROYECTO

En el siguiente capítulo se presenta los resultados del proyecto respecto a las hojas y listas de trabajo utilizadas según el modelo de gestión de riesgos de seguridad de la información, validado en una empresa de productos de arcilla cerámica.

6.1 Resultados del proyecto 2017

6.1.1 Selección de equipo de trabajo

Se realiza la entrevista respectiva al responsable asignado de la empresa, para poder completar el formato de “Selección equipo de trabajo”. Dentro de este formato se identifica qué personas se iban a relacionar al proyecto para poder brindar la información correspondiente. En este caso, las áreas críticas para evaluar identificados fueron ventas y producción. Considerando que el área de venta es un proceso Core de la empresa, y se tiene que proteger toda la información relacionada al proceso, se decide implementar el modelo en este proceso.

6.1.2 Fase 1: Construcción perfiles de amenaza

En esta sección, se presenta los resultados más resaltantes obtenidos durante el desarrollo de la fase 1 del proyecto.

En el caso del establecimiento del contexto, algunos puntos ya han sido identificados en la información básica de la empresa por lo que solo se definirán los faltantes.

- Valores: Respeto, compromiso, equidad y creatividad.

- Estructura de la organización:

Figura 81. Estructura organizativa.

Elaborado por empresa de productos de arcilla cerámica

- Estrategias de la organización: Ser considerados por los clientes como un socio estratégico para el crecimiento. Asimismo, quiere que sus empleados estén orgullosos de pertenecer a la empresa, por lo que tiene como estándar la armonía en el trabajo.
- Restricciones: facturación electrónica, bancos, cultura, presupuesto
- Requisitos reglamentarios: legislación referente a ladrilleras en el Perú, MINAM, ONG y contratos con los clientes.

Información adicional:

Combustible utilizado en el sector ladrillero: El manual de manual de capacitación sector ladrillero en América Latina nos indica qué combustible se utiliza en el Perú (CCAC, 2016):

Figura 82. Combustible utilizado por productores ladrilleros.

Elaborado por CCAC, 2016.

Asimismo, el manual otorga unas buenas prácticas de producción, que contribuye a un proceso más eficiente:

Figura 83. Buenas prácticas de producción.

Elaborado por CCAC, 2016.

El límite de emisión de partículas en mg/m^3 para Perú es 100 (combustible líquido) y 150 (combustible sólido). A continuación, se muestran los compromisos para la mitigación del cambio climático:

Pais	Reducción de deforestación	Diversificación de matriz energética	Meta de reducción de emisiones	Producción de biocombustibles	Socio de la CCAC
ARGENTINA

BOLIVIA

BRASIL

COLOMBIA					BC
COSTA RICA

CUBA

CHILE					BC
ECUADOR

EL SALVADOR

GUATEMALA

HONDURAS

MÉXICO					BC
PANAMÁ

PARAGUAY					BC
PERÚ					BC
REP. DOMINICANA					BC
URUGUAY					BC
VENEZUELA

Figura 84. Compromisos para la mitigación de cambios climáticos.

Elaborado por CCAC, 2016.

El Ministerio del Ambiente (MINAM) está a cargo de la reglamentación de los límites de emisiones del sector y de promover la implementación de Acciones Nacionales Apropriadas de Mitigación (CCAC, 2016).

Los objetivos de la coalición para hacer frente a los contaminantes climáticos de vida corta son (CCAC, 2016):

- Concientización sobre los impactos y estrategias de mitigación de CCVC
- Promoción y desarrollo de nuevas acciones nacionales y regionales que incluyan la identificación y superación de barreras, aumenten capacidades y movilicen apoyos.
- Promoción de buenas prácticas y casos de éxito.
- Mejora del conocimiento científico en los impactos de los CCVC y estrategias de mitigación.

La dirección general de calidad ambiental indica los estándares de calidad ambiental para el aire y los límites máximos permisibles de emisiones atmosféricas para las actividades de producción de ladrillos (MINAM, 2014):

Tabla 25
Estándares de calidad ambiental para el aire

Contaminante	Periodo	ECA ($\mu\text{g}/\text{m}^3$)
Dióxido de Azufre* (SO_2)	24 h	80 / 20
Material Particulado (PM_{10})	Anual	50
	24 h	150
Material Particulado ($\text{PM}_{2,5}$)	24 h	25
Monóxido de Carbono (CO)	8 h	10000
	1 h	30000
Dióxido de Nitrógeno (NO_2)	Anual	100
	1 h	200
Ozono (O_3)	8 h	120
Plomo (Pb)	Anual	0.5
	Mensual	1.5
Benceno	Anual	2
HT (Hexano)	24 h	100 mg/m^3
Hidrógeno Sulfurado (H_2S)	24 h	150

Fuente: Elaborado por MINAM, 2014

Tabla 26
Límite máximos permisibles de emisiones atmosféricas

Contaminante	Concentración 1/ (mg/Nm³)			Método de Medición 2/
	Tipo de Combustible			
	Gas	Líquido	Sólido	
Material Particulado (MP)	--	100	150	2002, NTP. 900.005 (EPA 5)
Óxidos de nitrógeno (NO _x)	320	460	650	2002, NTP. 900.007 (EPA 7)
Dióxido de Azufre (SO ₂)	—	750	500	2002, NTP. 900.006 (EPA 6)
Monóxido de carbono (CO)	300	700	1000	2002, NTP. 900.010 (EPA 10)

Fuente: Elaborado por MINAM, 2014

- Alcance: La implementación del modelo de gestión de riesgos se desarrolla en el proceso de ventas como se explicó anteriormente, ya que es un proceso crítico. A continuación, se explica en qué consiste dicho proceso:

La venta puede generarse por el cliente que va directo a planta a comprar o por medio de vendedores, quienes son los que visitan las ferreterías y los retail. Los ladrillos se venden a granel y son puestos en parihuelas.

Cuentas por cobrar valida si se atiende al cliente con crédito o no, ya que ellos se encargan de cobrar las deudas de los clientes al crédito o morosos. Revisa si tiene deudas con la empresa o si está en INFOCORP, si es así no se le otorga el crédito. Al validar el crédito, el cliente o vendedor genera la solicitud de pedido de venta. Acorde al pedido de ventas, se asigna un camión. En este caso, la empresa cuenta con 3 camiones. Los compradores pueden enviar su propio camión.

El camión llega a planta con la solicitud de pedido, va a balanza y se pesa vacío, esta información se almacena en SAP. El camión se dirige a ventanilla (Atención al cliente) con el pedido. En ventanilla se le genera un picking, documento que hace la reserva de ladrillos en los almacenes.

Cuando el camionero cuenta con el picking se dirige al área de despacho y se le indica la zona del almacén donde se va a cargar los ladrillos. El camión se dirige nuevamente a balanza y se pesa el camión lleno. SAP hace un cálculo con el peso y las unidades para observar la diferencia si lleva más ladrillo de los que debe ($\pm 5\%$). Si el peso fuera más, el camión es retenido y se recuentan los ladrillos, si es que hubiera más, se descarga. Luego de que el balancero pesa el camión, se genera la guía de remisión y la factura o boleta, si es que se verificó antes el peso.

Si el cliente paga al contado, el camión procede a dejar el pedido. Si paga al crédito, la factura se envía al área de cuentas por cobrar para que se realice el seguimiento correspondiente.

Al entregar pedido, el cliente lo valida, si no está correcto debe presentar un reclamo, el cual se envía a atención al cliente, que tiene una sub área de reclamo, si se aprueba, se le reconoce entregando ladrillos, si el cliente ya no desea los ladrillos, se le regresa su dinero según el número de ladrillos. Finalmente, si el camión es de la empresa regresa a la empresa. Solo para los retails, el camión regresa las parihuelas, ya que son alquiladas para ellos, si se rompen o se pierden se cobra al retail.

Figura 85. Proceso de venta de empresa de productos de arcilla cerámica.

Elaborado por jefes de proyecto

Asimismo, se identifica la relación de cada actividad de este proceso con las diferentes áreas de la empresa y también con las entidades externas, como se puede observar, el proceso de ventas es un proceso muy importante dentro de la empresa, es por ello que se decidió implementar el modelo en este proceso.

Figura 86. Relación de ventas con procesos internos y entidades externas.

Elaborado por jefes de proyecto

En esta sección del establecimiento del contexto, también se debe definir los criterios de evaluación de impacto utilizando la hoja de trabajo de “HT - Criterios de Evaluación de impacto” para la empresa de productos de arcilla cerámica. Los criterios están divididos en cinco tipos: reputación / confianza del cliente, finanzas, productividad, vida / salud clientes y multas / sanciones legales. Para este proyecto, el criterio de evaluación de impacto de productividad no aplica. A continuación, se muestra los valores identificados para cada nivel de impacto según cada tipo de criterio de evaluación.

Tipo Impacto	Impacto bajo	Impacto medio	Impacto alto
Reputación	La reputación es mínimamente afectada, poco o ningún esfuerzo o gastos es requerido para recuperarse.	La reputación es dañada, poco esfuerzo y gastos es requerido para recuperarse.	La reputación es destruida o dañada irrevocablemente.
Pérdida de cliente	Menos de 0.1% de reducción de clientes debido a la pérdida de confianza.	0.1% a 10% reducción en clientes debido a la pérdida de confianza.	Más de 10% reducción de clientes debido a la pérdida de confianza.

Figura 87. HT-Criterio de evaluación de impacto - Reputación / Confianza cliente.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Tipo Impacto	Impacto bajo	Impacto medio	Impacto alto
Costos operativos	Incremento menos de 5% en costos operativos anuales.	Costos operativos anuales aumentan de 5% a 15%.	Costos operativos anuales aumentan por más de 15%.
Pérdida de ingresos	Menos de 5% en pérdidas de ganancias anuales.	5% a 15% de pérdida de ganancias anuales.	Mayor a 15% de pérdidas de ganancias anuales.
Pérdida financiera a tiempo	Costo financiero en tiempo menor de S./20,588.	Costo financiero en tiempo de S./20,588 a S./41,176.	Costo financiero en tiempo mayor a S./41,176.

Figura 88. HT-Criterio de evaluación de impacto - Finanzas.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Tipo Impacto	Impacto bajo	Impacto medio	Impacto alto
Vida	Ninguna pérdida o amenaza significativa a la vida del cliente o personal.	La vida del cliente o personal están amenazadas pero se recuperarán después de recibir tratamiento médico.	Pérdida de la vida de clientes o personal.
Salud	Degradación mínima, inmediatamente tratable en la salud del cliente o personal con recuperación dentro de 4 días.	Discapacidad temporal o recuperable de la salud de los clientes o personal.	Discapacidad permanente de aspectos significativos de la salud de clientes o personal.
Seguridad	Seguridad cuestionada.	Seguridad afectada.	Seguridad violada.

Figura 89. HT-Criterio de evaluación de impacto - Productividad.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Tipo Impacto	Impacto bajo	Impacto medio	Impacto alto
Multas	Multas menos de S./200 son cobradas.	Multas entre S./200 y S./500 son cobradas.	Multas mayores de S./500 son cobradas.
Demandas	Demandas no frívolas menores a S./10 son presentadas en contra de la organización, o demandas frívolas son presentadas en contra	Demandas no frívolas entre S./10 y S./600 son presentadas en contra de la organización.	Demandas no frívolas mayores a S./600 son presentadas en contra de la organización.
Investigación	No existen consultas del gobierno u otra organización de investigación.	El gobierno u otra organización de investigación requiere información o records (bajo perfil).	El gobierno u otra organización de investigación inicia un alto perfil, investigación a profundidad de las prácticas organizacionales.

Figura 90. HT-Criterio de evaluación de impacto - Multas / Sanciones Legales.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Se identifican 22 activos más relevantes relacionados al proceso de ventas de la empresa de productos de arcilla cerámica.

ID Activo	Nombre Activo	Descripción de Activo	Tipo de activo
AC-001	Línea de Crédito	Tope de Línea de Credito	Información
AC-002	Lista de precios	Listado de precios por producto	Información
AC-003	Canal	Canal al que pertenece un cliente	Información
AC-004	Tipo de precios	Clasificación de precios por canal	Información
AC-005	SAP	Sistema ERP	Sistemas
AC-006	Office	Utilitario de oficina	Servicios y aplicaciones
AC-007	Outlook	Cliente de correo	Servicios y aplicaciones
AC-008	VMWare	Administrador de Servidores virtuales	Servicios y aplicaciones
AC-009	Sistema Operativo	Sistema Operativo	Servicios y aplicaciones
AC-010	Computadoras / Laptops	Equipo de usuario finales	Sistemas
AC-011	Impresoras	Servicio	Servicios y aplicaciones
AC-012	Scanners	Servicio	Servicios y aplicaciones
AC-013	Servicio de impresión	Servicio	Servicios y aplicaciones
AC-014	Internet	Servicio	Servicios y aplicaciones
AC-015	Telefonía móvil	Servicio	Servicios y aplicaciones
AC-016	Telefonía fija	Servicio	Servicios y aplicaciones
AC-017	INFOCORP	Central de Riesgo	Servicios y aplicaciones
AC-018	SUNAT	Superintendencia Nacional de Adm Tributaria	Servicios y aplicaciones
AC-019	Asistente de ventas (Key user)	Registro de Pedidos	Personas
AC-020	Personal de ventas	Personal de ventas	Personas
AC-021	Certificados electrónicos	Componente de Seguridad de la Facturación	Información
AC-022	Licencia de Antivirus	Bit Defender	Servicios y aplicaciones

Figura 91. Lista de activos.

Elaborado por jefes de proyecto

Asimismo, se evalúan las prácticas organizacionales encontrando que la mayoría de ellas no están totalmente formalizadas y documentadas, la empresa de productos cerámicos debe tomar mayor énfasis en cada área de práctica de seguridad. La evaluación arrojó la siguiente información:

Áreas	Valor promedio	Semáforo
Concientización de la seguridad y capacitación	1.50	●
Estrategia de seguridad	2.00	●
Administración de la seguridad	2.29	●
Políticas de seguridad y regulaciones	2.00	●
Administración de Seguridad Colaborativa	1.50	●
Plan de Contingencia / Recuperación ante desastres	2.25	●
Control de acceso físico	2.00	●
Monitoreo y Auditoría de seguridad física	2.00	●
Administración de sistema y red	2.00	●
Monitoreo y Auditoría de la seguridad TI	2.00	●
Autenticación y autorización	2.00	●
Gestión de vulnerabilidad	1.67	●
Cifrado	1.00	●
Arquitectura y diseño de seguridad	1.50	●
Gestión de incidentes	1.67	●

Figura 92. Evaluación de prácticas organizacionales.

Elaborado por jefes de proyecto

Debido a las actividades que no se desarrollan correctamente se encuentran vulnerabilidades correspondientes a cada área de práctica organizacional.

Nombre Activo / Área de práctica organizacional	ID Vulnerabilidad	Descripción Vulnerabilidad
Concientización de la seguridad y capacitación	VUL-001	Falta de concientización y capacitación formal.
	VUL-002	Falta de aprobación de documentos de políticas por gerente.
	VUL-003	Falta de validación de concientización en empleados.
Estrategia de seguridad	VUL-004	Falta de monitoreo de políticas.
	VUL-005	Falta de revisión periódica y comunicación de documentos.
Políticas de seguridad y regulaciones	VUL-006	Falta de documentación formal.
	VUL-001	Falta de concientización y capacitación formal.
Administración de la seguridad	VUL-007	Falta de presupuesto para actividades de seguridad.
	VUL-006	Falta de documentación formal.
	VUL-001	Falta de concientización y capacitación formal.
Administración de Seguridad Colaborativa	VUL-008	Falta de proceso formal de gestión de riesgos.
	VUL-002	Falta de aprobación de documentos de políticas por gerente.
	VUL-006	Falta de documentación formal.
Plan de Contingencia / Plan de Recuperación ante desastres	VUL-001	Falta de concientización y capacitación formal.
	VUL-009	Falta realizar pruebas periódicas correspondientes a los planes.
	VUL-006	Falta de documentación formal.
Control de acceso físico	VUL-001	Falta de concientización y capacitación formal.
	VUL-010	Falta de gestión adecuada sobre el control de acceso.
Monitoreo y Auditoría de seguridad física	VUL-001	Falta de concientización y capacitación formal.
	VUL-005	Falta de revisión periódica y comunicación de documentos.
	VUL-006	Falta de documentación formal.
Administración de sistema y red	VUL-001	Falta de concientización y capacitación formal.
	VUL-005	Falta de revisión periódica y comunicación de documentos.
	VUL-006	Falta de documentación formal.
Monitoreo y Auditoría de la seguridad TI	VUL-001	Falta de concientización y capacitación formal.
	VUL-005	Falta de revisión periódica y comunicación de documentos.
	VUL-011	Falta de formalización en verificación de los requisitos.
Autenticación y autorización	VUL-006	Falta de documentación formal.
	VUL-001	Falta de concientización y capacitación formal.
	VUL-005	Falta de revisión periódica y comunicación de documentos.
Gestión de vulnerabilidad	VUL-006	Falta de documentación formal.
	VUL-001	Falta de concientización y capacitación formal.
Cifrado	VUL-006	Falta de documentación formal.
	VUL-001	Falta de concientización y capacitación formal.
Arquitectura y diseño de seguridad	VUL-006	Falta de documentación formal.
	VUL-001	Falta de concientización y capacitación formal.
Gestión de incidentes	VUL-006	Falta de documentación formal.

Figura 93. Lista de vulnerabilidades de prácticas de seguridad.

Elaborado por jefes de proyecto

De los 22 activos identificados, según la valorización de cada uno de ellos, se identifican los activos más críticos (9).

ID Activo	Nombre Activo	Descripción de Activo	Tipo de activo
AC-001	Línea de Crédito	Tope de línea de crédito	Información
AC-002	Lista de precios	Listado de precios por producto	Información
AC-004	Tipo de precios	Clasificación de precios por canal	Información
AC-005	SAP	Sistema ERP	Sistemas
AC-007	Outlook	Cliente de correo	Servicios y aplicaciones
AC-008	VMWare	Administrador de Servidores virtuales	Servicios y aplicaciones
AC-009	Sistema Operativo	Sistema Operativo	Servicios y aplicaciones
AC-010	Computadoras	Equipo de usuario finales	Sistemas
AC-021	Certificados electrónicos	Componente de Seguridad de la Facturación	Información

Figura 94. Lista de activos críticos.

Elaborado por jefes de proyecto

De dichos activos críticos se identifican las vulnerabilidades y amenazas relacionadas.

Nombre Activo / Área de práctica organizacional	ID Vulnerabilidad	Descripción Vulnerabilidad
Línea de Crédito	VUL-002	Falta de aprobación de documentos de políticas por gerente.
	VUL-020	Falta de control por divulgación de información (sanción).
	VUL-001	Falta de concientización y capacitación formal.
	VUL-003	Falta de validación de concienciación en empleados.
Lista de precios	VUL-002	Falta de aprobación de documentos de políticas por gerente.
	VUL-020	Falta de control por divulgación de información (sanción).
	VUL-001	Falta de concientización y capacitación formal.
	VUL-003	Falta de validación de concienciación en empleados.
Tipo de precios	VUL-002	Falta de aprobación de documentos de políticas por gerente.
	VUL-020	Falta de control por divulgación de información (sanción).
	VUL-001	Falta de concientización y capacitación formal.
	VUL-003	Falta de validación de concienciación en empleados.
SAP	VUL-001	Falta de concientización y capacitación formal.
	VUL-002	Falta de aprobación de documentos de políticas por gerente.
	VUL-003	Falta de validación de concienciación en empleados.
	VUL-004	Falta de monitoreo de políticas.
	VUL-005	Falta de revisión periódica y comunicación de documentos.
	VUL-006	Falta de documentación formal.
	VUL-007	Falta de presupuesto para actividades de seguridad.
	VUL-008	Falta de proceso formal de gestión de riesgos.
	VUL-009	Falta realizar pruebas periódicas correspondientes a los planes.
	VUL-010	Falta de gestión adecuada sobre el control de acceso.
	VUL-012	Falta de capacitación sobre el sistema.
	VUL-013	Falta de control en la red interna.
Outlook	VUL-020	Falta de control por divulgación de información (sanción).
	VUL-001	Falta de concientización y capacitación formal.
	VUL-003	Falta de validación de concienciación en empleados.
	VUL-004	Falta de monitoreo de políticas.
	VUL-005	Falta de revisión periódica y comunicación de documentos.
	VUL-006	Falta de documentación formal.
	VUL-007	Falta de presupuesto para actividades de seguridad.
	VUL-008	Falta de proceso formal de gestión de riesgos.
	VUL-013	Falta de control en la red interna.
	VUL-014	Falta de control de filtros de correo electrónico.
	VUL-020	Falta de control por divulgación de información (sanción).
	VUL-002	Falta de aprobación de documentos de políticas por gerente.
VMWare	VUL-003	Falta de validación de concienciación en empleados.
	VUL-004	Falta de monitoreo de políticas.
	VUL-006	Falta de documentación formal.
	VUL-007	Falta de presupuesto para actividades de seguridad.
	VUL-008	Falta de proceso formal de gestión de riesgos.
	VUL-009	Falta realizar pruebas periódicas correspondientes a los planes.
	VUL-010	Falta de gestión adecuada sobre el control de acceso.
	VUL-015	Falta de configuración con recomendaciones de seguridad.
	VUL-020	Falta de control por divulgación de información (sanción).
	VUL-002	Falta de aprobación de documentos de políticas por gerente.
Sistema Operativo	VUL-003	Falta de validación de concienciación en empleados.
	VUL-004	Falta de monitoreo de políticas.
	VUL-005	Falta de revisión periódica y comunicación de documentos.
	VUL-006	Falta de documentación formal.
	VUL-007	Falta de presupuesto para actividades de seguridad.
	VUL-008	Falta de proceso formal de gestión de riesgos.
	VUL-016	Falta de actualización de parches.
	VUL-001	Falta de concientización y capacitación formal.
Computadoras / Laptops	VUL-002	Falta de aprobación de documentos de políticas por gerente.
	VUL-003	Falta de validación de concienciación en empleados.
	VUL-004	Falta de monitoreo de políticas.
	VUL-005	Falta de revisión periódica y comunicación de documentos.
	VUL-006	Falta de documentación formal.
	VUL-007	Falta de presupuesto para actividades de seguridad.
	VUL-010	Falta de gestión adecuada sobre el control de acceso.
	VUL-017	Falta de control en medios de almacenamiento.
	VUL-018	Falta de control en instalación no autorizada.
Certificado electrónico	VUL-019	Falta de control sobre vencimiento de certificado electrónico.

Figura 95. Lista de vulnerabilidades de activos críticos.

Elaborado por jefes de proyecto

Cod. Activo	Activo	Actor	Motivo	Resultado
AC-001	Línea de crédito	Interno	Intencionado	Revelación
				Modificación
AC-002	Lista de precios	Interno	Intencionado	Revelación
				Modificación
AC-004	Tipo de precios	Interno	Intencionado	Revelación
				Modificación
AC-005	SAP	Interno	Accidental	Revelación
				Pérdida, destrucción
				Interrupción
			Intencionado	Revelación
				Pérdida, destrucción
				Interrupción
		Externo	Accidental	Revelación
				Pérdida, destrucción
				Interrupción
			Intencionado	Revelación
				Pérdida, destrucción
				Interrupción
AC-007	Outlook	Interno	Accidental	Revelación
			Intencionado	Revelación
		Externo	Accidental	Revelación
			Intencionado	Revelación
AC-008	VMware	Interno	Accidental	Revelación
				Pérdida, destrucción
				Interrupción
			Intencionado	Revelación
				Pérdida, destrucción
				Interrupción
		Externo	Accidental	Revelación
				Pérdida, destrucción
				Interrupción
			Intencionado	Revelación
				Pérdida, destrucción
				Interrupción
AC-009	Sistemas operativos	Interno	Accidental	Pérdida, destrucción
			Intencionado	Interrupción
		Externo	Intencionado	Pérdida, destrucción
				Interrupción
				Pérdida, destrucción
AC-010	Computadoras / Laptops	Interno	Accidental	Pérdida, destrucción
			Intencionado	Interrupción
		Externo	Accidental	Pérdida, destrucción
				Interrupción
			Intencionado	Pérdida, destrucción
				Interrupción
AC-021	Certificados electrónicos	Externo	Accidental	Pérdida, destrucción
			Intencionado	Interrupción
				Pérdida, destrucción
AC-023	Producción	Interno	Accidental	Pérdida, destrucción
			Intencionado	Interrupción
		Externo	Accidental	Pérdida, destrucción
				Interrupción
			Intencionado	Pérdida, destrucción
				Interrupción

Figura 96. Amenazas relacionadas a activos críticos.

Elaborado por jefes de proyecto

De cada amenaza identificada, se identifican escenarios de incidentes que podrían ocurrir si se presentara la amenaza. Se identifican un total de 43 escenarios, los cuales tienen consecuencias en pérdida tiempo operacional, pérdida de tiempo en investigación, reputación de la empresa y tiempo invertido en recuperación de cambios. Dichos escenarios se encuentran en la “Lista de escenarios de incidentes”.

6.1.3 Fase 2: Identificar vulnerabilidades de infraestructura

El sistema de interés elegido para evaluar las rutas de acceso fue SAP, ya que es el activo más crítico dentro de la empresa. Se identifica lo siguiente:

Sistema de Interés		
¿Qué sistema o sistemas están más estrechamente relacionados con el activo crítico?		
SAP (Sistema de interés de la empresa)		

Sistema de interés		
¿Cuáles de las siguientes clases de componentes forman parte del sistema de interés?	Especificar componentes (Nombres)	
X Servidores		
X Redes Internas		
X Estaciones de trabajo en sitio		
Otros (Listar)		

Puntos de acceso intermedios		
¿Cuáles de las siguientes clases de componentes se utilizan para transmitir información y aplicaciones del sistema de interés para las personas? ¿Qué clases de componentes podrían servir como puntos de acceso intermedios?	Especificar componentes (Nombres)	
X Redes Internas		
Redes Externas		
Otros (Listar)		

Acceso al sistema por personas		
¿En cuál de las siguientes clases de componentes las personas pueden acceder al sistema de interés?	Especificar componentes (Nombres)	
X Estaciones de trabajo en sitio		
X Laptops		
PDAs / Componentes inalámbricos		
X Hogar / Estaciones de trabajo externas		
Otros (Listar)		

Figura 97. HT-Rutas de acceso.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Ubicaciones de almacenamiento de datos		
¿En qué clases de componentes se encuentra la información del sistema de interés almacenada para fines de copia de seguridad?	Especificar componentes (Nombres)	
X Dispositivos de almacenamiento		
Otros (Listar)		

Otros sistemas y componentes		
¿Qué otros sistemas tienen acceso a información o aplicaciones del sistema de interés?	Especificar componentes (Nombres)	
¿Qué otras clases de componentes se pueden utilizar para acceder a información crítica o aplicaciones del sistema de interés?		
Ninguno		

Figura 98. HT-Rutas de acceso.

Elaborado por jefes de proyecto, basado en OCTAVE-S

En la hoja de trabajo “HT-Revisión de infraestructura”, se identifica la relación de cada componente con cada activo crítico, la responsabilidad sobre cada componente y la protección actual sobre este.

Clases	Activos Críticos									
¿Qué clases de componentes están relacionadas con uno o más activos críticos?	¿Qué activos críticos están relacionados con cada clase?									
	Línea de Crédito	Lista de precios	Tipo de precios	SAP	Outlook	VMWare	Sistema Operativo	Computadoras	Certificados electrónicos	Producción
Servidores										
Producción	X	X	X	X		X	X	X		X
QA/desarrollo				X		X	X	X		
Repositorios antiguos				X		X	X	X		
SAP Priori				X		X	X	X		
Controladores de dominio				X		X	X	X		
Facturación Electrónica				X		X	X	X		
Professional Manager				X		X	X	X		
Bussiness Intelligence				X		X	X	X		
Servidor HP1						X	X	X		
Servidor HP1						X	X	X		
Servidor HP1						X	X	X		
Redes internas										
Red interna	X	X	X	X	X	X	X	X	X	X
Estaciones de trabajo en sitio										
PC	X	X	X	X	X	X	X	X	X	X
Laptops										
Laptops	X	X	X	X	X	X	X	X	X	X

Figura 99. HT-Revisión de Infraestructura-Relación activos críticos.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Como se identifican componentes relacionados, estos se agregan a la lista de activos. Se identifica un servidor crítico, y este se coloca en la hoja de trabajo “HT-Información de activos críticos”, el servidor de Producción.

ID Activo	Nombre Activo	Descripción de Activo	Tipo de activo
AC-001	Línea de Crédito	Tope de Línea de Credito	Información
AC-002	Lista de precios	Listado de precios por producto	Información
AC-003	Canal	Canal al que pertenece un cliente	Información
AC-004	Tipo de precios	Clasificación de precios por canal	Información
AC-005	SAP	Sistema ERP	Sistemas
AC-006	Office	Utilitario de oficina	Servicios y aplicaciones
AC-007	Outlook	Cliente de correo	Servicios y aplicaciones
AC-008	VMWare	Administrador de Servidores virtuales	Servicios y aplicaciones
AC-009	Sistema Operativo	Sistema Operativo	Servicios y aplicaciones
AC-010	Computadoras / Laptops	Equipo de usuario finales	Sistemas
AC-011	Impresoras	Servicio	Servicios y aplicaciones
AC-012	Scanners	Servicio	Servicios y aplicaciones
AC-013	Servicio de impresión	Servicio	Servicios y aplicaciones
AC-014	Internet	Servicio	Servicios y aplicaciones
AC-015	Telefonía móvil	Servicio	Servicios y aplicaciones
AC-016	Telefonía fija	Servicio	Servicios y aplicaciones
AC-017	INFOCORP	Central de Riesgo	Servicios y aplicaciones
AC-018	SUNAT	Superintendencia Nacional de Adm Tributaria	Servicios y aplicaciones
AC-019	Asistente de ventas (Key user)	Registro de Pedidos	Personas
AC-020	Personal de ventas	Personal de ventas	Personas
AC-021	Certificados electrónicos	Componente de Seguridad de la Facturación	Información
AC-022	Licencia de Antivirus	Bit Defender	Servicios y aplicaciones
AC-023	Producción	Servidor	Servicios y aplicaciones
AC-024	QA/desarrollo	Servidor	Sistemas
AC-025	Repositorios antiguos	Servidor	Sistemas
AC-026	SAP Priori	Servidor	Sistemas
AC-027	Controladores de dominio	Servidor	Sistemas
AC-028	Facturación Electrónica	Servidor	Sistemas
AC-029	Professional Manager	Servidor	Sistemas
AC-030	Business Intelligence	Servidor	Sistemas
AC-031	Servidor HP1	Servidor	Sistemas
AC-032	Servidor HP1	Servidor	Sistemas
AC-033	Servidor HP1	Servidor	Sistemas
AC-034	Red interna	Red interna	Servicios y aplicaciones
AC-035	File Server	Almacenamiento de backups	Sistemas

Figura 100. Lista de activos.

Elaborado por jefes de proyecto

ID Activo	Nombre Activo	Descripción de Activo	Tipo de activo
AC-001	Línea de Crédito	Tope de línea de crédito	Información
AC-002	Lista de precios	Listado de precios por producto	Información
AC-004	Tipo de precios	Clasificación de precios por canal	Información
AC-005	SAP	Sistema ERP	Sistemas
AC-007	Outlook	Cliente de correo	Servicios y aplicaciones
AC-008	VMWare	Administrador de Servidores virtuales	Servicios y aplicaciones
AC-009	Sistema Operativo	Sistema Operativo	Servicios y aplicaciones
AC-010	Computadoras	Equipo de usuario finales	Sistemas
AC-021	Certificados electrónicos	Componente de Seguridad de la Facturación	Información
AC-023	Producción	Servidor	Servicios y aplicaciones

Figura 101. Información de activos críticos.

Elaborado por jefes de proyecto

Asimismo, se identifican las vulnerabilidades relacionadas a este nuevo activo crítico y los posibles escenarios en los que se harían presentes las amenazas.

Nombre Activo / Área de práctica organizacional	ID Vulnerabilidad	Descripción Vulnerabilidad
Producción	VUL-001	Falta de concientización y capacitación formal.
	VUL-002	Falta de aprobación de documentos de políticas por gerente.
	VUL-003	Falta de validación de concienciación en empleados.
	VUL-004	Falta de monitoreo de políticas.
	VUL-006	Falta de documentación formal.
	VUL-007	Falta de presupuesto para actividades de seguridad.
	VUL-008	Falta de proceso formal de gestión de riesgos.
	VUL-009	Falta realizar pruebas periódicas correspondientes a los planes.
	VUL-010	Falta de gestión adecuada sobre el control de acceso.
	VUL-013	Falta de control en la red interna.

Figura 102. Lista de vulnerabilidades.

Elaborado por jefes de proyecto

6.1.4 Fase 3: Desarrollar estrategias y planes de seguridad

En esta sección, se evalúa el impacto sobre cada amenaza identificada de cada activo crítico, en la hoja de trabajo “HT-Perfil de Riesgos”, donde se aprecia el nivel de impacto según:

- Rojo: mayor a 10 y menor a igual 15.
- Amarillo: mayor a 5 y menor igual a 10.
- Verde: mayor a 0 y menor igual a 5.

Amenaza						Motivo			Historia		Valores de impacto					
						¿Qué tan fuerte es el motivo del actor?			¿Qué tan seguido ha ocurrido esta amenaza en el pasado?							
						Alto	Medio	Bajo								
Activo	Actor		Motivo	Resultado												
Línea de Crédito	X	Interno	Accidental		Revelación			0	veces en	3 años.						
					Modificación			0	veces en	3 años.						
					Pérdida, destrucción			0	veces en	3 años.						
					Interrupción			0	veces en	3 años.						
		X	Intencionado	X	Revelación		X	3	veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
				X	Modificación		X	12	veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
					Pérdida, destrucción			0	veces en	3 años.						
					Interrupción			0	veces en	3 años.						
			Accidental		Revelación			0	veces en	3 años.						
					Modificación			0	veces en	3 años.						
					Pérdida, destrucción			0	veces en	3 años.						
					Interrupción			0	veces en	3 años.						
			Intencionado		Revelación			0	veces en	3 años.						
					Modificación			0	veces en	3 años.						
					Pérdida, destrucción			0	veces en	3 años.						
					Interrupción			0	veces en	3 años.						
Lista de precios	X	Interno	Accidental		Revelación			0	veces en	3 años.						
					Modificación			0	veces en	3 años.						
					Pérdida, destrucción			0	veces en	3 años.						
					Interrupción			0	veces en	3 años.						
		X	Intencionado	X	Revelación		X	15	veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
				X	Modificación		X	25	veces en	3 años.	Medio	Medio	Medio	Alto	Bajo	10
					Pérdida, destrucción			0	veces en	3 años.						
					Interrupción			0	veces en	3 años.						
			Accidental		Revelación			0	veces en	3 años.						
					Modificación			0	veces en	3 años.						
					Pérdida, destrucción			0	veces en	3 años.						
					Interrupción			0	veces en	3 años.						
			Intencionado		Revelación			0	veces en	3 años.						
					Modificación			0	veces en	3 años.						
					Pérdida, destrucción			0	veces en	3 años.						
					Interrupción			0	veces en	3 años.						
Tipo de precios	X	Interno	Accidental		Revelación			0	veces en	3 años.						
					Modificación			0	veces en	3 años.						
					Pérdida, destrucción			0	veces en	3 años.						
					Interrupción			0	veces en	3 años.						
		X	Intencionado	X	Revelación		X	3	veces en	3 años.	Medio	Bajo	Bajo	Alto	Bajo	8
				X	Modificación		X	3	veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
					Pérdida, destrucción			0	veces en	3 años.						
					Interrupción			0	veces en	3 años.						
			Accidental		Revelación			0	veces en	3 años.						
					Modificación			0	veces en	3 años.						
					Pérdida, destrucción			0	veces en	3 años.						
					Interrupción			0	veces en	3 años.						
			Intencionado		Revelación			0	veces en	3 años.						
					Modificación			0	veces en	3 años.						
					Pérdida, destrucción			0	veces en	3 años.						
					Interrupción			0	veces en	3 años.						
SAP	X	Interno	Accidental	X	Revelación			1	veces en	3 años.	Medio	Bajo	Bajo	Alto	Bajo	8
					Modificación			0	veces en	3 años.						
				X	Pérdida, destrucción			1	veces en	3 años.	Medio	Medio	Medio	Alto	Bajo	10
				X	Interrupción			1	veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
		X	Intencionado	X	Revelación	X		36	veces en	3 años.	Medio	Bajo	Bajo	Alto	Bajo	8
					Modificación			0	veces en	3 años.						
				X	Pérdida, destrucción	X		1	veces en	3 años.	Medio	Medio	Medio	Alto	Bajo	10
				X	Interrupción	X		1	veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
			Accidental	X	Revelación			0	veces en	3 años.	Bajo	Medio	Medio	Alto	Bajo	9
				X	Pérdida, destrucción			0	veces en	3 años.						
					Interrupción			1	veces en	3 años.	Medio	Medio	Medio	Alto	Bajo	10
		X	Intencionado	X	Revelación	X		1	veces en	3 años.	Bajo	Medio	Bajo	Alto	Bajo	9
					Modificación			0	veces en	3 años.						
				X	Pérdida, destrucción	X		0	veces en	3 años.	Medio	Medio	Medio	Alto	Bajo	10
				X	Interrupción	X		1	veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9

Figura 103. HT-Perfil de riesgos.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Outlook	X	Interno	X	Accidental	X	Revelación				1 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
						Modificación				0 veces en	3 años.						0
						Pérdida, destrucción				0 veces en	3 años.						0
			X	Intencionado	X	Revelación		X		0 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
						Modificación				0 veces en	3 años.						0
						Pérdida, destrucción				0 veces en	3 años.						0
	X	Externo	X	Accidental	X	Revelación				1 veces en	3 años.	Bajo	Medio	Bajo	Alto	Bajo	8
						Modificación				0 veces en	3 años.						0
						Pérdida, destrucción				0 veces en	3 años.						0
			X	Intencionado	X	Revelación		X		0 veces en	3 años.	Bajo	Medio	Bajo	Alto	Bajo	8
						Modificación				0 veces en	3 años.						0
						Pérdida, destrucción				0 veces en	3 años.						0
VMware	X	Interno	X	Accidental	X	Revelación				1 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
						Modificación				0 veces en	3 años.						0
						Pérdida, destrucción				1 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
			X	Intencionado	X	Revelación		X		1 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
						Modificación				0 veces en	3 años.						0
						Pérdida, destrucción		X		1 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
	X	Externo	X	Accidental	X	Revelación				1 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
						Modificación				0 veces en	3 años.						0
						Pérdida, destrucción				1 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
			X	Intencionado	X	Revelación		X		1 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
						Modificación		X		0 veces en	3 años.						0
						Pérdida, destrucción		X		1 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
Sistema Operativo	X	Interno	X	Accidental	X	Revelación				1 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
						Modificación				0 veces en	3 años.						0
						Pérdida, destrucción				1 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
			X	Intencionado	X	Revelación		X		1 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
						Modificación				0 veces en	3 años.						0
						Pérdida, destrucción		X		1 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
	X	Externo	X	Accidental	X	Revelación				1 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
						Modificación				0 veces en	3 años.						0
						Pérdida, destrucción				1 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
			X	Intencionado	X	Revelación		X		1 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
						Modificación		X		0 veces en	3 años.						0
						Pérdida, destrucción		X		1 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
Computadoras / Laptops	X	Interno	X	Accidental	X	Revelación				1 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
						Modificación				0 veces en	3 años.						0
						Pérdida, destrucción				1 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
			X	Intencionado	X	Revelación				1 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
						Modificación				0 veces en	3 años.						0
						Pérdida, destrucción		X		36 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	10
	X	Externo	X	Accidental	X	Revelación				1 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	8
						Modificación				0 veces en	3 años.						0
						Pérdida, destrucción				1 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
			X	Intencionado	X	Revelación				0 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
						Modificación				0 veces en	3 años.						0
						Pérdida, destrucción		X		1 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	10
Certificados electrónicos	X	Interno	X	Accidental	X	Revelación				0 veces en	3 años.						0
						Modificación				0 veces en	3 años.						0
						Pérdida, destrucción				0 veces en	3 años.						0
			X	Intencionado	X	Revelación				0 veces en	3 años.						0
						Modificación				0 veces en	3 años.						0
						Pérdida, destrucción		X		1 veces en	3 años.	Medio	Bajo	Bajo	Alto	Bajo	8
	X	Externo		Accidental		Revelación				0 veces en	3 años.						0
						Modificación				0 veces en	3 años.						0
						Pérdida, destrucción				1 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
				Intencionado		Revelación				0 veces en	3 años.						0
						Modificación				0 veces en	3 años.						0
						Pérdida, destrucción				0 veces en	3 años.						0
Producción	X	Interno	X	Accidental		Revelación				0 veces en	3 años.						0
						Modificación				0 veces en	3 años.						0
						Pérdida, destrucción				0 veces en	3 años.	Alto	Alto	Bajo	Bajo	Bajo	9
			X	Intencionado		Revelación				0 veces en	3 años.						0
						Modificación				0 veces en	3 años.						0
						Pérdida, destrucción		X		0 veces en	3 años.	Alto	Alto	Bajo	Bajo	Bajo	9
	X	Externo	X	Accidental		Revelación				0 veces en	3 años.						0
						Modificación				0 veces en	3 años.						0
						Pérdida, destrucción				0 veces en	3 años.	Alto	Alto	Bajo	Bajo	Bajo	9
			X	Intencionado		Revelación				0 veces en	3 años.						0
						Modificación				0 veces en	3 años.						0
						Pérdida, destrucción		X		0 veces en	3 años.	Alto	Alto	Bajo	Bajo	Bajo	9

Figura 104. HT-Perfil de riesgos.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Se procede a identificar la probabilidad de cada amenaza de cada activo crítico.

Amenaza						Probabilidad	
						¿Qué tan probable es que ocurra la amenaza en el futuro?	
Activo		Actor		Motivo	Resultado	Valor cualitativo	Valor cuantitativo
Línea de Crédito	X	Interno		Accidental	Revelación		
					Modificación		
					Pérdida, destrucción		
					Interrupción		
			X	Intencionado	X Revelación	Medio	2
					X Modificación	Medio	2
		Externo		Accidental	Pérdida, destrucción		
					Interrupción		
					Revelación		
					Modificación		
					Pérdida, destrucción		
					Interrupción		
				Intencionado	Revelación		
					Modificación		
					Pérdida, destrucción		
					Interrupción		
					Revelación		
					Modificación		
Lista de precios	X	Interno		Accidental	Revelación		
					Modificación		
					Pérdida, destrucción		
					Interrupción		
			X	Intencionado	X Revelación	Medio	2
					X Modificación	Medio	2
		Externo		Accidental	Pérdida, destrucción		
					Interrupción		
					Revelación		
					Modificación		
					Pérdida, destrucción		
					Interrupción		
				Intencionado	Revelación		
					Modificación		
					Pérdida, destrucción		
					Interrupción		
					Revelación		
					Modificación		
Tipo de precios	X	Interno		Accidental	Revelación		
					Modificación		
					Pérdida, destrucción		
					Interrupción		
			X	Intencionado	X Revelación	Medio	2
					X Modificación	Medio	2
		Externo		Accidental	Pérdida, destrucción		
					Interrupción		
					Revelación		
					Modificación		
					Pérdida, destrucción		
					Interrupción		
				Intencionado	Revelación		
					Modificación		
					Pérdida, destrucción		
					Interrupción		
					Revelación		
					Modificación		
SAP	X	Interno	X	Accidental	X Revelación	Medio	2
					X Modificación		
					X Pérdida, destrucción	Medio	2
					X Interrupción	Medio	2
			X	Intencionado	X Revelación	Alto	3
					X Modificación		
		Externo		Accidental	X Pérdida, destrucción	Medio	2
					X Interrupción	Medio	2
					X Revelación	Medio	2
					X Modificación		
					X Pérdida, destrucción	Bajo	1
					X Interrupción	Medio	2
				Intencionado	X Revelación	Medio	2
					X Modificación		
					X Pérdida, destrucción	Bajo	1
					X Interrupción	Medio	2
					X Revelación		
					X Modificación		

Figura 105. HT-Perfil de riesgos – Probabilidad.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Outlook	X	Interno	X	Accidental	X	Revelación	Medio	2
						Modificación		
						Pérdida, destrucción		
						Interrupción		
		X	X	Intencionado	X	Revelación	Bajo	1
						Modificación		
						Pérdida, destrucción		
	X	Externo	X	Accidental		Interrupción		
					X	Revelación	Medio	2
						Modificación		
		X	X	Intencionado	X	Revelación	Medio	2
						Modificación		
						Pérdida, destrucción		
VMware	X	Interno	X	Accidental	X	Revelación	Medio	2
						Modificación		
					X	Pérdida, destrucción	Medio	2
		X	X	Intencionado	X	Interrupción	Medio	2
					X	Revelación	Medio	2
						Modificación		
	X	Externo	X	Accidental	X	Pérdida, destrucción	Medio	2
					X	Interrupción	Medio	2
					X	Revelación	Medio	2
		X	X	Intencionado		Modificación		
					X	Pérdida, destrucción	Medio	2
					X	Interrupción	Medio	2
Sistema Operativo	X	Interno	X	Accidental		Revelación		
						Modificación		
					X	Pérdida, destrucción	Bajo	1
		X	X	Intencionado	X	Interrupción	Medio	2
						Revelación		
						Modificación		
	X	Externo	X	Accidental	X	Pérdida, destrucción	Bajo	1
					X	Interrupción	Medio	2
					X	Revelación	Medio	2
		X	X	Intencionado		Modificación		
					X	Pérdida, destrucción	Medio	2
					X	Interrupción	Medio	2
Computadoras / Laptops	X	Interno	X	Accidental		Revelación		
						Modificación		
					X	Pérdida, destrucción	Medio	2
		X	X	Intencionado	X	Interrupción	Medio	2
						Revelación		
						Modificación		
	X	Externo	X	Accidental	X	Pérdida, destrucción	Medio	2
					X	Interrupción	Bajo	1
						Revelación		
		X	X	Intencionado		Modificación		
					X	Pérdida, destrucción	Medio	2
					X	Interrupción	Bajo	1
Certificados electrónicos	X	Interno	X	Accidental		Revelación		
						Modificación		
					X	Pérdida, destrucción		
		X	X	Intencionado	X	Interrupción		
						Revelación		
					X	Pérdida, destrucción	Medio	2
	X	Externo	X	Accidental	X	Interrupción	Medio	2
						Revelación		
						Modificación		
		X	X	Intencionado		Pérdida, destrucción	Medio	2
						Interrupción	Medio	2
						Revelación		
Producción	X	Interno	X	Accidental		Revelación		
						Modificación		
					X	Pérdida, destrucción	Bajo	1
		X	X	Intencionado	X	Interrupción	Bajo	1
						Revelación		
						Modificación		
	X	Externo	X	Accidental	X	Pérdida, destrucción	Bajo	1
					X	Interrupción	Bajo	1
						Revelación		
		X	X	Intencionado		Modificación		
					X	Pérdida, destrucción	Bajo	1
					X	Interrupción	Bajo	1

Figura 106. HT-Perfil de riesgos – Probabilidad.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Dicha probabilidad también se completa en la lista de escenarios de incidentes. Asimismo, se completa la hoja de trabajo “HT-Estrategia de Protección” observando cómo se cumplen las características de responsabilidad, procedimientos, formación, cuestiones de Colaboración y verificación. Dicha información se puede apreciar en la hoja de trabajo.

Luego de ello, se completa cómo se encuentra la protección en las áreas de práctica de seguridad de la hoja de trabajo “HT-Perfil de Riesgo” de cada activo crítico.

Amenaza				Áreas de prácticas de seguridad																			
				Estratégico									Operacional										Total
				Concientización de la seguridad y capacitación	Estrategia de seguridad	Administración de la seguridad	Políticas de seguridad y regulaciones	Administración de Seguridad Colaborativa	Plan de Contingencia / Recuperación ante desastres	Control de acceso físico	Monitoreo y Auditoría de seguridad física	Administración de sistema y red	Monitoreo y Auditoría de la seguridad TI	Autenticación y autorización	Gestión de vulnerabilidad	Cifrado	Arquitectura y diseño de seguridad	Gestión de incidentes					
Activo	Actor	Motivo	Resultado																				
Línea de Crédito	X	Interno	Accidental	Revelación																			
				Modificación																			
				Pérdida, destrucción																			
		X	Intencionado	Interrupción																			
				Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	25		
				Modificación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	Alto	25	
				Pérdida, destrucción																			
				Interrupción																			
			Accidental	Revelación																			
				Modificación																			
				Pérdida, destrucción																			
		X	Interno	Intencionado	Interrupción																		
Revelación																							
Modificación																							
X	Intencionado		Pérdida, destrucción																				
			Interrupción																				
			Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	Alto	25		
Lista de precios	X	Interno	Intencionado	Modificación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	Alto	25		
				Pérdida, destrucción																			
				Interrupción																			
			Accidental	Revelación																			
				Modificación																			
				Pérdida, destrucción																			
			Intencionado	Interrupción																			
				Revelación																			
				Modificación																			
			Accidental	Pérdida, destrucción																			
				Interrupción																			
		Tipo de precios	X	Interno	Accidental	Revelación																	
Modificación																							
Pérdida, destrucción																							
X	Intencionado			Interrupción																			
				Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	Alto	25		
				Modificación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	Alto	25		
			Accidental	Pérdida, destrucción																			
				Interrupción																			
				Revelación																			
			Intencionado	Modificación																			
				Pérdida, destrucción																			
	SAP		X	Interno	Accidental	Interrupción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	25	
Modificación																							
Pérdida, destrucción		Medio				Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	25		
X		Intencionado		Interrupción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	Alto	25		
				Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	Alto	25		
				Modificación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	Alto	25		
		X	Accidental	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	Alto	25		
				Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	Alto	25		
				Interrupción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	Alto	25		
		X	Intencionado	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	Alto	25		
				Modificación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	Alto	25		
				Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	Alto	25		

Figura 107. HT-Perfil de riesgos – Área de práctica de seguridad.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Amenaza						Áreas de prácticas de seguridad															
						Estratégico							Operacional								Total
						Concientización de la seguridad y capacitación	Estrategia de seguridad	Administración de la seguridad	Políticas de seguridad y regulaciones	Administración de Seguridad Colaborativa	Plan de Contingencia / Recuperación ante desastres	Control de acceso físico	Monitoreo y auditoría de seguridad física	Administración de sistema y red	Monitoreo y Auditoría de la seguridad TI	Autenticación y autorización	Gestión de vulnerabilidad	Cifrado	Arquitectura y diseño de seguridad	Gestión de incidentes	
Activo	Actor	Motivo	Resultado																		
Outlook	X	Interno	Accidental	X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25	
					Modificación																
					Pérdida, destrucción																
		X	Intencionado	X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25	
					Modificación																
					Pérdida, destrucción																
	X	Externo	Accidental	X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25	
					Modificación																
					Pérdida, destrucción																
		X	Intencionado	X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25	
					Modificación																
					Pérdida, destrucción																
VMware	X	Interno	Accidental	X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	25		
					Modificación																
				X	Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	25		
		X	Intencionado	X	Interrupción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	25		
					Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	25			
					Modificación																
	X	Externo	Accidental	X	Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	25		
					Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	25			
					Modificación																
		X	Intencionado	X	Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	25		
					Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	25			
					Modificación																
Sistema Operativo	X	Interno	Accidental	X	Revelación																
					Modificación																
				X	Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	25		
		X	Intencionado	X	Interrupción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	25		
					Revelación																
					Modificación																
	X	Externo	Accidental	X	Pérdida, destrucción																
					Revelación																
					Modificación																
		X	Intencionado	X	Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	25		
					Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	25			
					Modificación																

Figura 108. HT-Perfil de riesgos – Área de práctica de seguridad.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Amenaza				Áreas de prácticas de seguridad																
				Estratégico							Operacional									
				Concientización de la seguridad y capacitación	Estrategia de seguridad	Administración de la seguridad	Políticas de seguridad y regulaciones	Administración de seguridad	Colaborativa	Plan de Contingencia / Recuperación ante desastres	Control de acceso físico	Monitoreo y Auditoría de seguridad física	Administración de sistema y red	Monitoreo y Auditoría de seguridad TI	Autenticación y autorización	Gestión de vulnerabilidad	Cifrado	Arquitectura y diseño de seguridad	Gestión de incidentes	Total
Activo	Autor	Motivo	Resultado																	
Computadoras / Laptops	X	X	Accidental	Revelación																
				Modificación																
				X Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
		X	Intencionado	X Interrupción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
				Revelación																
				Modificación																
	X	X	Accidental	X Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
				X Interrupción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
				Revelación																
		X	Intencionado	Modificación																
				X Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
				X Interrupción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
Certificados electrónicos	X	X	Accidental	Revelación																
				X Pérdida, destrucción																
				X Interrupción																
		X	Intencionado	Modificación																
				X Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
				X Interrupción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
			Accidental	Revelación																
				Modificación																
				X Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
			Intencionado	X Interrupción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
				Revelación																
				Modificación																
Producción	X	X	Accidental	Revelación																
				Modificación																
				X Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
		X	Intencionado	X Interrupción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
				Revelación																
				Modificación																
	X	X	Accidental	X Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
				X Interrupción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
				Revelación																
		X	Intencionado	Modificación																
				X Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
				X Interrupción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25

Figura 109. HT-Perfil de riesgos – Área de práctica de seguridad.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Para obtener el nivel de tolerancia de riesgo, podemos observar que el mínimo de amenazas identificadas es 1, por lo que el nivel mínimo de riesgo sería 5, y el máximo de amenazas completadas ha sido 12, por lo que el nivel máximo de riesgo sería 540. La empresa de productos de arcilla cerámica decidió los siguientes niveles:

Bajo	5	100
Medio	101	199
Alto	200	540

Figura 110. Nivel de riesgo.

Elaborado por jefes de proyecto

A continuación, se calcula el riesgo para cada activo crítico, tomando en cuenta el impacto y la probabilidad identificada.

Cod. Activo	Activo	Actor		Motivo		Resultado		Amenaza	Probabilidad	Amen. * Prob.	Riesgo	Nivel de riesgo
AC-001	Línea de crédito	x	Interno	X	Intencionado	X	Revelación	9	2	18	36	Bajo
						X	Modificación	9	2	18		
AC-002	Lista de precios	x	Interno	X	Intencionado	X	Revelación	9	2	18	38	Bajo
						X	Modificación	10	2	20		
AC-004	Tipo de precios	x	Interno	X	Intencionado	X	Revelación	8	2	16	34	Bajo
						X	Modificación	9	2	18		
AC-005	SAP	X	Interno	X	Accidental	X	Revelación	8	2	16	208	Alto
						X	Pérdida, destrucción	10	2	20		
						X	Interrupción	9	2	18		
				X	Intencionado	X	Revelación	8	3	24		
						X	Pérdida, destrucción	10	2	20		
						X	Interrupción	9	2	18		
		X	Externo	X	Accidental	X	Revelación	9	2	18		
						X	Pérdida, destrucción	10	1	10		
						X	Interrupción	9	2	18		
				X	Intencionado	X	Revelación	9	2	18		
						X	Pérdida, destrucción	10	1	10		
						X	Interrupción	9	2	18		
AC-007	Outlook	X	Interno	X	Accidental	X	Revelación	9	2	18	59	Bajo
				X	Intencionado	X	Revelación	9	1	9		
		X	Externo	X	Accidental	X	Revelación	8	2	16		
				X	Intencionado	X	Revelación	8	2	16		
AC-008	VMware	X	Interno	X	Accidental	X	Revelación	9	2	18	216	Alto
						X	Pérdida, destrucción	9	2	18		
						X	Interrupción	9	2	18		
				X	Intencionado	X	Revelación	9	2	18		
						X	Pérdida, destrucción	9	2	18		
						X	Interrupción	9	2	18		
		X	Externo	X	Accidental	X	Revelación	10	2	20		
						X	Pérdida, destrucción	9	2	18		
						X	Interrupción	8	2	16		
				X	Intencionado	X	Revelación	10	2	20		
						X	Pérdida, destrucción	9	2	18		
						X	Interrupción	8	2	16		
AC-009	Sistemas operativos	X	Interno	X	Accidental	X	Pérdida, destrucción	9	1	9	85	Bajo
				X	Intencionado	X	Interrupción	10	2	20		
		X	Externo	X	Intencionado	X	Pérdida, destrucción	10	1	10		
				X	Intencionado	X	Interrupción	9	2	18		
AC-010	Computadoras / Laptops	X	Interno	X	Accidental	X	Pérdida, destrucción	10	2	20	139	Medio
				X	Intencionado	X	Interrupción	8	2	16		
				X	Intencionado	X	Pérdida, destrucción	10	3	30		
		X	Externo	X	Accidental	X	Interrupción	8	2	16		
				X	Intencionado	X	Pérdida, destrucción	10	2	20		
				X	Intencionado	X	Interrupción	9	1	9		
AC-021	Certificados electrónicos	X	Externo	X	Accidental	X	Pérdida, destrucción	10	2	20	68	Bajo
				X	Intencionado	X	Interrupción	9	2	18		
				X	Intencionado	X	Pérdida, destrucción	8	2	16		
				X	Intencionado	X	Interrupción	8	2	16		
AC-023	Producción	X	Interno	X	Accidental	X	Pérdida, destrucción	9	1	9	72	Bajo
				X	Intencionado	X	Interrupción	9	1	9		
				X	Intencionado	X	Pérdida, destrucción	9	1	9		
				X	Intencionado	X	Interrupción	9	1	9		
		X	Externo	X	Accidental	X	Pérdida, destrucción	9	1	9		
				X	Intencionado	X	Interrupción	9	1	9		
				X	Intencionado	X	Pérdida, destrucción	9	1	9		
				X	Intencionado	X	Interrupción	9	1	9		

Figura 111. Cálculo del riesgo de activos críticos.

Elaborado por jefes de proyecto

Se procede a listar los riesgos según su prioridad por el valor calculado.

Lista riesgos con prioridad

Cod. Activo	Activo	Riesgo	Nivel de riesgo	Prioridad
AC-001	Línea de crédito	36	Bajo	9
AC-002	Lista de precios	38	Bajo	8
AC-004	Tipo de precios	34	Bajo	10
AC-005	SAP	208	Alto	2
AC-007	Outlook	59	Bajo	7
AC-008	VMware	216	Alto	1
AC-009	Sistemas operativos	85	Bajo	4
AC-010	Computadoras / Laptops	139	Medio	3
AC-021	Certificados electrónicos	68	Bajo	6
AC-023	Producción	72	Bajo	5

Figura 112. Lista riesgos con prioridad.

Elaborado por jefes de proyecto

Con la información del riesgo, se procede a evaluar el enfoque a elegir, si sería mitigar, aceptar, eliminar o transferir. Junta a la empresa de productos de arcilla cerámica se deciden los siguientes enfoques:

Amenaza						Enfoque			
						¿Cuál es su enfoque para abordar cada riesgo?			
						Mitigar	Aceptar	Transferir	Evitar
Activo	Actor		Motivo		Resultado				
Línea de Crédito	X	Interno		Accidental	Revelación				
					Modificación				
					Pérdida, destrucción				
		X	Intencionado		Interrupción				
					Revelación	x			
					Modificación	x			
		Externo		Accidental	Pérdida, destrucción				
					Interrupción				
					Revelación				
				Intencionado	Modificación				
					Pérdida, destrucción				
					Interrupción				
Lista de precios	X	Interno		Accidental	Revelación				
					Modificación				
					Pérdida, destrucción				
		X	Intencionado		Interrupción				
					Revelación	x			
					Modificación	x			
		Externo		Accidental	Pérdida, destrucción				
					Interrupción				
					Revelación				
				Intencionado	Modificación				
					Pérdida, destrucción				
					Interrupción				
Tipo de precios	X	Interno		Accidental	Revelación				
					Modificación				
					Pérdida, destrucción				
		X	Intencionado		Interrupción				
					Revelación	x			
					Modificación	x			
		Externo		Accidental	Pérdida, destrucción				
					Interrupción				
					Revelación				
				Intencionado	Modificación				
					Pérdida, destrucción				
					Interrupción				
SAP	X	Interno	X	Accidental	Revelación	x			
					Modificación				
					Pérdida, destrucción	x			
		X	Intencionado		Interrupción	x			
					Revelación	x			
					Modificación				
	X	Externo	X	Accidental	Pérdida, destrucción	x			
					Interrupción	x			
					Revelación	x			
		X	Intencionado		Modificación				
					Pérdida, destrucción	x			
					Interrupción	x			

Figura 113. Enfoques.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Amenaza						Enfoque			
						¿Cuál es su enfoque para abordar cada riesgo?			
Activo	Acor	Motivo	Resultado			Mitigar	Acopiar	Transferir	Evitar
Outlook	X	X	Accidental	X	Revelación	x			
					Modificación				
					Pérdida, destrucción				
					Interrupción				
		X	Intencionado	X	Revelación	x			
					Modificación				
					Pérdida, destrucción				
	X	X	Accidental	X	Revelación	x			
					Modificación				
					Pérdida, destrucción				
		X	Intencionado	X	Revelación	x			
					Modificación				
					Pérdida, destrucción				
VMware	X	X	Accidental	X	Revelación	x			
					Modificación				
				X	Pérdida, destrucción	x			
		X	Intencionado	X	Revelación	x			
					Modificación				
				X	Pérdida, destrucción	x			
	X	X	Accidental	X	Revelación	x			
					Modificación				
				X	Pérdida, destrucción	x			
		X	Intencionado	X	Revelación	x			
					Modificación				
				X	Pérdida, destrucción	x			
Sistema Operativo	X	X	Accidental	X	Revelación				
					Modificación				
				X	Pérdida, destrucción	x			
		X	Intencionado	X	Revelación	x			
					Modificación				
				X	Pérdida, destrucción	x			
	X	X	Accidental	X	Revelación	x			
					Modificación				
				X	Pérdida, destrucción	x			
		X	Intencionado	X	Revelación	x			
					Modificación				
				X	Pérdida, destrucción	x			
Computadoras / Laptops	X	X	Accidental	X	Revelación				
					Modificación				
				X	Pérdida, destrucción	x			
		X	Intencionado	X	Revelación				
					Modificación				
				X	Pérdida, destrucción	x			
	X	X	Accidental	X	Revelación				
					Modificación				
				X	Pérdida, destrucción	x			
		X	Intencionado	X	Revelación				
					Modificación				
				X	Pérdida, destrucción	x			
Certificados electrónicos	X	X	Accidental	X	Revelación				
					Modificación				
				X	Pérdida, destrucción	x			
		X	Intencionado	X	Revelación				
					Modificación				
				X	Pérdida, destrucción	x			
	X	X	Accidental	X	Revelación				
					Modificación				
				X	Pérdida, destrucción	x			
		X	Intencionado	X	Revelación				
					Modificación				
				X	Pérdida, destrucción	x			
Producción	X	X	Accidental	X	Revelación				
					Modificación				
				X	Pérdida, destrucción	x			
		X	Intencionado	X	Revelación				
					Modificación				
				X	Pérdida, destrucción	x			
	X	X	Accidental	X	Revelación				
					Modificación				
				X	Pérdida, destrucción	x			
		X	Intencionado	X	Revelación				
					Modificación				
				X	Pérdida, destrucción	x			

Figura 114. Enfoques.

Elaborado por jefes de proyecto, basado en OCTAVE-S

A continuación, se procede a completar la hoja de trabajo “HT-Plan de mitigación”, en el que se puede observar qué actividades debe de realizar la empresa para poder contrarrestar el posible impacto si se llegaran a presentar las amenazas.

La empresa de productos de arcilla cerámica decide mitigar los riesgos, por lo que se procedió a identificar controles para cada uno de ellos, todos los controles se pueden observar en la “Lista de controles”. Se valoriza cada uno de ellos para poder encontrar el riesgo residual de cada uno de los activos críticos, donde se obtiene lo siguiente:

Cod. Activo	Activo	Riesgo	Riesgo Residual
AC-001	Línea de crédito	36	15
AC-002	Lista de precios	38	18
AC-004	Tipo de precios	34	14
AC-005	SAP	208	101
AC-007	Outlook	59	28
AC-008	VMware	216	109
AC-009	Sistemas operativos	85	51
AC-010	Computadoras / Laptops	139	60
AC-021	Certificados electrónicos	68	23
AC-023	Producción	72	35

Figura 115. Riesgo Residual.

Elaborado por jefes de proyecto

A partir de ello, la empresa decide aceptar el nivel de cada riesgo residual por esta evaluación y se coloca la justificación en la “Lista de riesgos aceptados”. Se calcula que el porcentaje promedio de reducción de riesgo es 54% teóricamente, es superior al nivel que se acordó con la empresa al aplicar este modelo, por lo que validamos nuestro modelo.

Se procede a terminar de completar la “HT-Estrategia de protección”, identificando qué cambios ocurrirían luego de aplicado los controles.

Finalmente, se identifica qué pasos realizar luego de la evaluación, y como adición se identifican qué indicadores la empresa podría utilizar para monitorear los controles propuestos, y así ayudarlos a que esta etapa pueda ser más rápida. Dichos indicadores se pueden observar en el documento “Indicadores”.

A continuación, se muestran gráficas resumen de lo anteriormente explicado según las amenazas, vulnerabilidades, riesgo inherente, controles y riesgo residual.

Las amenazas identificadas fueron agrupadas según su resultado: revelación, modificación, pérdida, destrucción e interrupción.

Figura 116. Agrupación de Amenazas.

Elaborado por jefes de proyecto

Las vulnerabilidades identificadas fueron agrupadas según: concientización, monitoreo, capacitación, documentación formal y presupuesto.

Figura 117. Agrupación de Vulnerabilidades.

Elaborado por jefes de proyecto

El riesgo inherente por activo se muestra en la siguiente ilustración radial, donde se puede observar que para los de color rojo son los de riesgo algo, los de amarillo, riesgo medio y los de verde, riesgo bajo.

Figura 118. Riesgo inherente por activo.

Elaborado por jefes de proyecto

Los controles identificados también fueron agrupados según monitoreo, formalización de documentos, acuerdos de confidencialidad, concientización y presupuesto.

Figura 119. Agrupación de controles.

Elaborado por jefes de proyecto

Si los controles propuestos se implementaran dentro de la empresa de productos de arcilla cerámica, el riesgo de cada activo reduciría en un promedio del 54%, el riesgo residual se muestra en la siguiente ilustración radial.

Figura 120. Riesgo residual por activo.

Elaborado por jefes de proyecto

A continuación, se muestra la matriz de probabilidad e impacto del riesgo inherente y del riesgo residual para los activos críticos, donde se puede apreciar gráficamente cómo se reduce el riesgo.

Figura 121. Riesgo por activo.

Elaborado por jefes de proyecto

Figura 122. Riesgo residual por activo.

Elaborado por jefes de proyecto

Se proponen 17 indicadores para poder monitorear el avance que tiene la Pyme en la implementación de medidas de seguridad según los controles propuestos.

6.2 Resultados del proyecto 2018

6.2.1 Selección de equipo de trabajo

El equipo designado es el mismo que realizó la primera implementación del modelo en la empresa, quienes brindaron la información correspondiente. Las áreas críticas para evaluar identificadas fueron ventas y producción. Se sigue considerando el área de venta como proceso Core de la empresa, y se tiene que proteger toda la información relacionada al proceso.

6.2.2 Fase 1: Construcción perfiles de amenaza

En esta sección, se presenta los resultados más resaltantes obtenidos durante el desarrollo de la fase 1 del proyecto.

En el caso del establecimiento del contexto, algunos puntos ya han sido identificados en la información básica de la empresa y en la Fase 1 realizada en el año 2017 (Punto 6.1.2). Asimismo, se mantuvo los niveles para los criterios de evaluación de impacto.

Se identifican 40 activos más relevantes relacionados al proceso de ventas de la empresa de productos de arcilla cerámica.

ID Activo	Nombre Activo	Descripción de Activo	Tipo de activo
AC-001	Línea de Crédito	Tope de Línea de Credito	Información
AC-002	Lista de precios	Listado de precios por producto	Información
AC-003	Canal	Canal al que pertenece un cliente	Información
AC-004	Tipo de precios	Clasificación de precios por canal	Información
AC-005	SAP	Sistema ERP	Sistemas
AC-006	Office	Utilitario de oficina	Servicios y aplicaciones
AC-007	Outlook	Cliente de correo	Servicios y aplicaciones
AC-008	VMWare	Administrador de Servidores virtuales	Servicios y aplicaciones
AC-009	Sistema Operativo	Sistema Operativo	Servicios y aplicaciones
AC-010	Computadoras / Laptops	Equipo de usuario finales	Sistemas
AC-011	Impresoras	Servicio	Servicios y aplicaciones
AC-012	Scanners	Servicio	Servicios y aplicaciones
AC-013	Servicio de impresión	Servicio	Servicios y aplicaciones
AC-014	Internet	Servicio	Servicios y aplicaciones
AC-015	Telefonía móvil	Servicio	Servicios y aplicaciones
AC-016	Telefonía fija	Servicio	Servicios y aplicaciones
AC-017	INFOCORP	Central de Riesgo	Servicios y aplicaciones
AC-018	SUNAT	Superintendencia Nacional de Adm Tributaria	Servicios y aplicaciones
AC-019	Asistente de ventas (Key user)	Registro de Pedidos	Personas
AC-020	Personal de ventas	Personal de ventas	Personas
AC-021	Certificados electrónicos	Componente de Seguridad de la Facturación	Información
AC-022	Licencia de Antivirus	Bit Defender	Servicios y aplicaciones
AC-023	Producción	Servidor	Servicios y aplicaciones
AC-024	QA/desarrollo	Servidor	Sistemas
AC-025	Repositorios antiguos	Servidor	Sistemas
AC-026	SAP Fiori	Servidor	Sistemas
AC-027	Controladores de dominio	Servidor	Sistemas
AC-028	Facturación Electrónica	Servidor	Sistemas
AC-029	Professional Manager	Servidor	Sistemas
AC-030	Business Intelligence	Servidor	Sistemas
AC-031	Servidor HP1	Servidor	Sistemas
AC-032	Servidor HP1	Servidor	Sistemas
AC-033	Servidor HP1	Servidor	Sistemas
AC-034	Red interna	Red interna	Servicios y aplicaciones
AC-035	File Server	Almacenamiento de backups	Sistemas
AC-036	Visual ASIS	Sistema de control de asistencia	Sistemas
AC-037	PAYROLL	Sistema de planillas	Sistemas
AC-038	SISCON	Sistema contable (antiguo)	Sistemas
AC-039	Responsable de planillas	Responsable de planillas	Personas
AC-040	Asistentes contables	Asistentes contables	Personas

Figura 123. Lista de activos.

Elaborado por jefes de proyecto

Asimismo, se evalúa las prácticas organizacionales encontrando que la mayoría de ellas no están totalmente formalizadas y documentadas, la empresa de productos cerámicos debe tomar mayor énfasis en cada área de práctica de seguridad. La evaluación arrojó la siguiente información:

Áreas	Valor promedio	Semáforo
Concientización de la seguridad y capacitación	1.50	●
Estrategia de seguridad	1.00	●
Administración de la seguridad	1.86	●
Políticas de seguridad y regulaciones	1.75	●
Administración de Seguridad Colaborativa	1.50	●
Plan de Contingencia / Recuperación ante desastres	1.50	●
Control de acceso físico	1.50	●
Monitoreo y Auditoría de seguridad física	1.83	●
Administración de sistema y red	2.00	●
Monitoreo y Auditoría de la seguridad TI	2.00	●
Autenticación y autorización	2.00	●
Gestión de vulnerabilidad	1.67	●
Cifrado	1.00	●
Arquitectura y diseño de seguridad	1.50	●
Gestión de incidentes	1.67	●

Figura 124. Evaluación de prácticas organizacionales.

Elaborado por jefes de proyecto

Debido a las actividades que no se desarrollan correctamente se encontraron vulnerabilidades correspondientes a cada área de práctica organizacional.

Nombre Activo / Área de práctica organizacional	ID Vulnerabilidad	Descripción Vulnerabilidad
Concientización de la seguridad y capacitación	VUL-001	Falta de concientización y capacitación formal.
	VUL-002	Falta de aprobación de documentos de políticas por gerente.
	VUL-003	Falta de validación de concientización en empleados.
Estrategia de seguridad	VUL-004	Falta de monitoreo de políticas.
	VUL-005	Falta de revisión periódica y comunicación de documentos.
Políticas de seguridad y regulaciones	VUL-006	Falta de documentación formal.
	VUL-001	Falta de concientización y capacitación formal.
Administración de la seguridad	VUL-007	Falta de presupuesto para actividades de seguridad.
	VUL-006	Falta de documentación formal.
	VUL-001	Falta de concientización y capacitación formal.
	VUL-008	Falta de proceso formal de gestión de riesgos.
Administración de Seguridad Colaborativa	VUL-002	Falta de aprobación de documentos de políticas por gerente.
	VUL-006	Falta de documentación formal.
	VUL-001	Falta de concientización y capacitación formal.
Plan de Contingencia / Plan de Recuperación ante desastres	VUL-009	Falta realizar pruebas periódicas correspondientes a los planes.
	VUL-006	Falta de documentación formal.
Control de acceso físico	VUL-001	Falta de concientización y capacitación formal.
	VUL-010	Falta de gestión adecuada sobre el control de acceso.
	VUL-001	Falta de concientización y capacitación formal.
Monitoreo y Auditoría de seguridad física	VUL-005	Falta de revisión periódica y comunicación de documentos.
	VUL-006	Falta de documentación formal.
	VUL-001	Falta de concientización y capacitación formal.
Administración de sistema y red	VUL-005	Falta de revisión periódica y comunicación de documentos.
	VUL-006	Falta de documentación formal.
	VUL-001	Falta de concientización y capacitación formal.
Monitoreo y Auditoría de la seguridad TI	VUL-005	Falta de revisión periódica y comunicación de documentos.
	VUL-011	Falta de formalización en verificación de los requisitos.
	VUL-006	Falta de documentación formal.
	VUL-001	Falta de concientización y capacitación formal.
Autenticación y autorización	VUL-005	Falta de revisión periódica y comunicación de documentos.
	VUL-006	Falta de documentación formal.
	VUL-001	Falta de concientización y capacitación formal.
Gestión de vulnerabilidad	VUL-006	Falta de documentación formal.
	VUL-001	Falta de concientización y capacitación formal.
	VUL-006	Falta de documentación formal.
Cifrado	VUL-006	Falta de documentación formal.
	VUL-001	Falta de concientización y capacitación formal.
Arquitectura y diseño de seguridad	VUL-006	Falta de documentación formal.
	VUL-001	Falta de concientización y capacitación formal.
Gestión de incidentes	VUL-006	Falta de documentación formal.

Figura 125: Lista de vulnerabilidades de prácticas de seguridad.

Elaborado por jefes de proyecto

De los 40 activos identificados, según la valorización de cada uno de ellos, se identifican los activos más críticos (13).

ID Activo	Nombre Activo	Descripción de Activo	Tipo de activo
AC-001	Línea de Crédito	Tope de línea de crédito	Información
AC-002	Lista de precios	Listado de precios por producto	Información
AC-004	Tipo de precios	Clasificación de precios por canal	Información
AC-005	SAP	Sistema ERP	Sistemas
AC-007	Outlook	Cliente de correo	Servicios y aplicaciones
AC-008	VMWare	Administrador de Servidores virtuales	Servicios y aplicaciones
AC-009	Sistema Operativo	Sistema Operativo	Servicios y aplicaciones
AC-010	Computadoras	Equipo de usuario finales	Sistemas
AC-021	Certificados electrónicos	Componente de Seguridad de la Facturación	Información
AC-023	Producción	Servidor	Servicios y aplicaciones
AC-036	Visual ASIS	Sistema de control de asistencia	Sistemas
AC-037	PAYROLL	Sistema de planillas	Sistemas
AC-038	SISCON	Sistema contable (antiguo)	Sistemas

Figura 126: Lista activos críticos.

Elaborado por jefes de proyecto

De dichos activos críticos se identifican las vulnerabilidades y amenazas relacionadas.

ID Activo	Nombre Activo / Área de práctica organizacional	ID Vulnerabilidad	Descripción Vulnerabilidad
AC-001	Línea de Crédito	VUL-002	Falta de aprobación de documentos de políticas por gerente.
		VUL-020	Falta de control por divulgación de información (sanción).
		VUL-001	Falta de concientización y capacitación formal.
AC-002	Lista de precios	VUL-003	Falta de validación de concientización en empleados.
		VUL-002	Falta de aprobación de documentos de políticas por gerente.
		VUL-020	Falta de control por divulgación de información (sanción).
AC-004	Tipo de precios	VUL-001	Falta de concientización y capacitación formal.
		VUL-003	Falta de validación de concientización en empleados.
		VUL-002	Falta de aprobación de documentos de políticas por gerente.
AC-005	SAP	VUL-020	Falta de control por divulgación de información (sanción).
		VUL-001	Falta de concientización y capacitación formal.
		VUL-003	Falta de validación de concientización en empleados.
		VUL-002	Falta de aprobación de documentos de políticas por gerente.
		VUL-003	Falta de validación de concientización en empleados.
		VUL-004	Falta de monitoreo de políticas.
		VUL-005	Falta de revisión periódica y comunicación de documentos.
		VUL-006	Falta de documentación formal.
		VUL-007	Falta de presupuesto para actividades de seguridad.
		VUL-008	Falta de proceso formal de gestión de riesgos.
		VUL-009	Falta realizar pruebas periódicas correspondientes a los planes.
		VUL-010	Falta de gestión adecuada sobre el control de acceso.
		VUL-012	Falta de capacitación sobre el sistema.
		VUL-013	Falta de control en la red interna.
		VUL-020	Falta de control por divulgación de información (sanción).
AC-008	Outlook	VUL-001	Falta de concientización y capacitación formal.
		VUL-003	Falta de validación de concientización en empleados.
		VUL-004	Falta de monitoreo de políticas.
		VUL-005	Falta de revisión periódica y comunicación de documentos.
		VUL-006	Falta de documentación formal.
		VUL-007	Falta de presupuesto para actividades de seguridad.
		VUL-008	Falta de proceso formal de gestión de riesgos.
		VUL-013	Falta de control en la red interna.
		VUL-014	Falta de control de filtros de correo electrónico.
		VUL-020	Falta de control por divulgación de información (sanción).
		VUL-002	Falta de aprobación de documentos de políticas por gerente.
		VUL-003	Falta de validación de concientización en empleados.
		VUL-004	Falta de monitoreo de políticas.
		VUL-006	Falta de documentación formal.
		VUL-007	Falta de presupuesto para actividades de seguridad.
AC-007	VMWare	VUL-008	Falta de proceso formal de gestión de riesgos.
		VUL-009	Falta realizar pruebas periódicas correspondientes a los planes.
		VUL-010	Falta de gestión adecuada sobre el control de acceso.
		VUL-015	Falta de configuración con recomendaciones de seguridad.
		VUL-020	Falta de control por divulgación de información (sanción).
		VUL-002	Falta de aprobación de documentos de políticas por gerente.
		VUL-003	Falta de validación de concientización en empleados.
		VUL-004	Falta de monitoreo de políticas.
		VUL-006	Falta de documentación formal.
		VUL-007	Falta de presupuesto para actividades de seguridad.
		VUL-008	Falta de proceso formal de gestión de riesgos.
		VUL-009	Falta realizar pruebas periódicas correspondientes a los planes.
		VUL-010	Falta de gestión adecuada sobre el control de acceso.
		VUL-015	Falta de configuración con recomendaciones de seguridad.
		VUL-020	Falta de control por divulgación de información (sanción).
AC-009	Sistema Operativo	VUL-002	Falta de aprobación de documentos de políticas por gerente.
		VUL-003	Falta de validación de concientización en empleados.
		VUL-004	Falta de monitoreo de políticas.
		VUL-005	Falta de revisión periódica y comunicación de documentos.
		VUL-006	Falta de documentación formal.
		VUL-007	Falta de presupuesto para actividades de seguridad.
		VUL-008	Falta de proceso formal de gestión de riesgos.
		VUL-016	Falta de actualización de parches.
		VUL-001	Falta de concientización y capacitación formal.
		VUL-002	Falta de aprobación de documentos de políticas por gerente.
		VUL-003	Falta de validación de concientización en empleados.
		VUL-004	Falta de monitoreo de políticas.
		VUL-005	Falta de revisión periódica y comunicación de documentos.
		VUL-006	Falta de documentación formal.
		VUL-007	Falta de presupuesto para actividades de seguridad.
AC-010	Computadoras / Laptops	VUL-008	Falta de proceso formal de gestión de riesgos.
		VUL-017	Falta de control en medios de almacenamiento.
		VUL-018	Falta de control en instalación no autorizada.
		VUL-019	Falta de control sobre vencimiento de certificado electrónico.
		VUL-001	Falta de concientización y capacitación formal.
		VUL-002	Falta de aprobación de documentos de políticas por gerente.
		VUL-003	Falta de validación de concientización en empleados.
		VUL-004	Falta de monitoreo de políticas.
		VUL-005	Falta de revisión periódica y comunicación de documentos.
		VUL-006	Falta de documentación formal.
		VUL-007	Falta de presupuesto para actividades de seguridad.
		VUL-010	Falta de gestión adecuada sobre el control de acceso.
		VUL-017	Falta de control en medios de almacenamiento.
		VUL-018	Falta de control en instalación no autorizada.
		VUL-019	Falta de control sobre vencimiento de certificado electrónico.
AC-021	Certificado electrónico	VUL-001	Falta de concientización y capacitación formal.
AC-023	Producción	VUL-002	Falta de aprobación de documentos de políticas por gerente.
		VUL-003	Falta de validación de concientización en empleados.
		VUL-004	Falta de monitoreo de políticas.
		VUL-006	Falta de documentación formal.
		VUL-007	Falta de presupuesto para actividades de seguridad.
		VUL-008	Falta de proceso formal de gestión de riesgos.
		VUL-009	Falta realizar pruebas periódicas correspondientes a los planes.
		VUL-010	Falta de gestión adecuada sobre el control de acceso.
		VUL-013	Falta de control en la red interna.
		VUL-003	Falta de validación de concientización en empleados.
		VUL-006	Falta de documentación formal.
		VUL-020	Falta de control por divulgación de información (sanción).
		VUL-021	Falta de respaldo de la información
		VUL-003	Falta de validación de concientización en empleados.
		VUL-006	Falta de documentación formal.
AC-036	Visual ASIS	VUL-020	Falta de control por divulgación de información (sanción).
AC-037	PAYROLL	VUL-021	Falta de respaldo de la información
		VUL-003	Falta de validación de concientización en empleados.
		VUL-006	Falta de documentación formal.
AC-038	SISCON	VUL-020	Falta de control por divulgación de información (sanción).
		VUL-021	Falta de respaldo de la información
		VUL-003	Falta de validación de concientización en empleados.
		VUL-006	Falta de documentación formal.
		VUL-020	Falta de control por divulgación de información (sanción).

Figura 127: Lista de vulnerabilidades de activos críticos.

Elaborado por jefes de proyecto

Cod. Activo	Activo	Actor	Motivo	Resultado
AC-001	Línea de crédito	Interno	Intencionado	Revelación
				Modificación
AC-002	Lista de precios	Interno	Intencionado	Revelación
				Modificación
AC-004	Tipo de precios	Interno	Intencionado	Revelación
				Modificación
AC-005	SAP	Interno	Accidental	Revelación
				Pérdida, destrucción
				Interrupción
			Intencionado	Revelación
				Pérdida, destrucción
				Interrupción
		Externo	Accidental	Revelación
				Pérdida, destrucción
				Interrupción
			Intencionado	Revelación
				Pérdida, destrucción
				Interrupción
AC-007	Outlook	Interno	Accidental	Revelación
			Intencionado	Revelación
		Externo	Accidental	Revelación
			Intencionado	Revelación
AC-008	VMware	Interno	Accidental	Revelación
				Pérdida, destrucción
				Interrupción
			Intencionado	Revelación
				Pérdida, destrucción
				Interrupción
		Externo	Accidental	Revelación
				Pérdida, destrucción
				Interrupción
			Intencionado	Revelación
				Pérdida, destrucción
				Interrupción
AC-009	Sistemas operativos	Interno	Accidental	Pérdida, destrucción
			Intencionado	Interrupción
				Pérdida, destrucción
		Externo	Intencionado	Interrupción
				Pérdida, destrucción
			Intencionado	Interrupción
AC-010	Computadoras / Laptops	Interno	Accidental	Pérdida, destrucción
			Intencionado	Interrupción
				Pérdida, destrucción
		Externo	Accidental	Interrupción
			Intencionado	Pérdida, destrucción
				Interrupción
AC-021	Certificados electrónicos	Externo	Accidental	Pérdida, destrucción
			Intencionado	Interrupción
				Pérdida, destrucción
AC-023	Producción	Interno	Accidental	Pérdida, destrucción
			Intencionado	Interrupción
				Pérdida, destrucción
		Externo	Accidental	Interrupción
			Intencionado	Pérdida, destrucción
				Interrupción
AC-036	Visual ASIS	Interno	Accidental	Pérdida, destrucción
			Intencionado	Pérdida, destrucción
AC-037	PAYROLL	Interno	Accidental	Pérdida, destrucción
			Intencionado	Pérdida, destrucción
AC-038	SISCON	Interno	Accidental	Pérdida, destrucción
			Intencionado	Pérdida, destrucción

Figura 128: Amenazas relacionadas a activos críticos.

Elaborado por jefes de proyecto, basado en OCTAVE-S

De cada amenaza identificada, se identifican los escenarios de incidentes que podrían ocurrir si se presentara la amenaza, los cuales tienen consecuencias en pérdida tiempo operacional, pérdida de tiempo en investigación, reputación de la empresa y tiempo invertido en recuperación de cambios. Dichos escenarios se encuentran en la “Lista de escenarios de incidentes”.

6.2.3 Fase 2: Identificar vulnerabilidades de infraestructura

El sistema de interés elegido para evaluar las rutas de acceso fue SAP, SISCON, Visual ASIS y PayRoll, ya que estos son activos críticos dentro de la empresa. Se identifica lo siguiente:

Sistema de Interés		
¿Qué sistema o sistemas están más estrechamente relacionados con el activo crítico?		
SAP (Sistema de interés de la empresa), SISCON, Visual ASIS, PayRoll		

Sistema de interés		Puntos de acceso intermedios		Acceso al sistema por personas	
¿Cuáles de las siguientes clases de componentes forman parte del sistema de interés?	Especificar componentes (Nombres)	¿Cuáles de las siguientes clases de componentes se utilizan para transmitir información y aplicaciones del sistema de interés para las personas? ¿Qué clases de componentes podrían servir como puntos de acceso intermedios?	Especificar componentes (Nombres)	¿En cuál de las siguientes clases de componentes las personas pueden acceder al sistema de interés?	Especificar componentes (Nombres)
X Servidores		X Redes Internas		X Estaciones de trabajo en sitio	
X Redes Internas		Redes Externas		X Laptops	
X Estaciones de trabajo en sitio		Otros (Listar)		PDAs / Componentes Inalámbricos	
Otros (Listar)				X Hogar / Estaciones de trabajo externas	
				Otros (Listar)	

Figura 129: HT-Rutas de acceso.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Ubicaciones de almacenamiento de datos		Otros sistemas y componentes	
¿En qué clases de componentes se encuentra la información del sistema de interés almacenada para fines de copia de seguridad?	Especificar componentes (Nombres)	¿Qué otros sistemas tienen acceso a información o aplicaciones del sistema de interés?	Especificar componentes (Nombres)
X Dispositivos de almacenamiento		¿Qué otras clases de componentes se pueden utilizar para acceder a información crítica o aplicaciones del sistema de interés?	
Otros (Listar)		Ninguno	

Figura 130: HT-Rutas de acceso.

Elaborado por jefes de proyecto, basado en OCTAVE-S

En la hoja de trabajo “HT-Revisión de infraestructura”, se identifica la relación de cada componente con cada activo crítico, la responsabilidad sobre cada componente y la protección actual sobre este.

Clases	Activos Críticos												
¿Qué clases de componentes están relacionadas con uno o más activos críticos?	¿Qué activos críticos están relacionados con cada clase?												
	Línea de Crédito	Lista de precios	Tipo de precios	SAP	Outlook	VMWare	Sistema Operativo	Computadoras	Certificados electrónicos	Producción	Visual ASIS	PayRoll	SISCON
Servidores													
Producción	X	X	X	X		X	X	X		X			
QA/desarrollo				X		X	X	X					
Repositorios antiguos				X		X	X	X					
SAP Priori				X		X	X	X					
Controladores de dominio				X		X	X	X					
Facturación Electrónica				X		X	X	X					
Professional Manager				X		X	X	X					
Bussiness Intelligence				X		X	X	X					
Servidor HP1						X	X	X					
Servidor HP1						X	X	X					
Servidor HP1						X	X	X					
Servidor Visual ASIS											X		
Servidor Payroll												X	
Servidor SISCON													X
Redes internas													
Red interna	X	X	X	X	X	X	X	X	X	X	X	X	X
Estaciones de trabajo en sitio													
PC	X	X	X	X	X	X	X	X	X	X	X	X	X
Laptops													
Laptops	X	X	X	X	X	X	X	X	X	X	X	X	X
PDAs / Componentes inalámbricos													
No hay													
Otros sistemas													
Dispositivos de almacenamiento													
File Server				X		X	X						
Redes externas													
No hay													
Hogar / Estaciones de trabajo externas													
No hay													

Figura 131: HT-Revisión de Infraestructura-Relación activos críticos.

Elaborado por jefes de proyecto, basado en OCTAVE-S

En este caso no se detecta un componente crítico así que se continua con la fase 3.

6.2.4 Fase 3: Desarrollar estrategias y planes de seguridad

En esta sección, se evalúa el impacto sobre cada amenaza identificada de cada activo crítico, en la hoja de trabajo “HT-Perfil de Riesgos”, donde se aprecia el nivel de impacto según:

- Rojo: mayor a 10 y menor a igual 15.
- Amarillo: mayor a 5 y menor igual a 10.

- Verde: mayor a 0 y menor igual a 5.

Amenaza						Motivo			Historia		Valores de impacto					
						¿Qué tan fuerte es el motivo del actor?			¿Qué tan seguido ha ocurrido esta amenaza en el pasado?							
						Alto	Medio	Bajo			Reputación	Financiera	Productividad	Multas	Seguridad	Total
Activo	Actor		Motivo	Resultado												
Línea de Crédito	X	Interno	Accidental		Revelación				0 veces en	3 años.						
					Modificación			0 veces en	3 años.							
					Pérdida, destrucción			0 veces en	3 años.							
			Intencionado		Interrupción			0 veces en	3 años.							
				X	Revelación		X	3 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9	
				X	Modificación		X	12 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9	
	Lista de precios	X	Interno	Accidental		Pérdida, destrucción			0 veces en	3 años.						
						Interrupción			0 veces en	3 años.						
						Revelación			0 veces en	3 años.						
				Intencionado		Modificación			0 veces en	3 años.						
						Pérdida, destrucción			0 veces en	3 años.						
						Interrupción			0 veces en	3 años.						
Tipo de precios		X	Interno	Accidental		Revelación			15 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
						Modificación		X	25 veces en	3 años.	Medio	Medio	Medio	Alto	Bajo	10
						Pérdida, destrucción			0 veces en	3 años.						
				Intencionado		Interrupción			0 veces en	3 años.						
						Revelación			0 veces en	3 años.						
						Modificación			0 veces en	3 años.						
	SAP	X	Interno	Accidental		Pérdida, destrucción			0 veces en	3 años.						
						Interrupción			0 veces en	3 años.						
						Revelación		X	3 veces en	3 años.	Medio	Bajo	Bajo	Alto	Bajo	8
				Intencionado		Modificación		X	3 veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
						Pérdida, destrucción			0 veces en	3 años.						
						Interrupción			0 veces en	3 años.						
X		Externo	Accidental		Revelación			0 veces en	3 años.							
					Modificación			0 veces en	3 años.							
					Pérdida, destrucción			0 veces en	3 años.							
			Intencionado		Interrupción			0 veces en	3 años.							
					Revelación			0 veces en	3 años.							
					Modificación			0 veces en	3 años.							

Figura 132: HT-Perfil de riesgos.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Outlook	X	Interno	X	Accidental	X	Revelación				0	veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
						Modificación				0	veces en	3 años.						
						Pérdida, destrucción				0	veces en	3 años.						
		X		Intencionado	X	Revelación		X		1	veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
						Modificación				0	veces en	3 años.						
						Pérdida, destrucción				0	veces en	3 años.						
	X	Externo	X	Accidental	X	Revelación				0	veces en	3 años.	Bajo	Medio	Bajo	Alto	Bajo	8
						Modificación				0	veces en	3 años.						
						Pérdida, destrucción				0	veces en	3 años.						
		X		Intencionado	X	Revelación		X		1	veces en	3 años.	Bajo	Medio	Bajo	Alto	Bajo	8
						Modificación				0	veces en	3 años.						
						Pérdida, destrucción				0	veces en	3 años.						
VMware	X	Interno	X	Accidental	X	Revelación				0	veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
						Modificación				0	veces en	3 años.						
					X	Pérdida, destrucción				0	veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
		X		Intencionado	X	Revelación		X		1	veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
						Modificación				0	veces en	3 años.						
					X	Pérdida, destrucción	X			1	veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
	X	Externo	X	Accidental	X	Revelación				0	veces en	3 años.	Medio	Medio	Medio	Alto	Bajo	10
						Modificación				0	veces en	3 años.						
					X	Pérdida, destrucción				0	veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
		X		Intencionado	X	Revelación		X		1	veces en	3 años.	Medio	Medio	Medio	Alto	Bajo	10
						Modificación				0	veces en	3 años.						
					X	Pérdida, destrucción	X			1	veces en	3 años.	Medio	Bajo	Bajo	Alto	Bajo	9
Sistema Operativo	X	Interno	X	Accidental	X	Revelación				0	veces en	3 años.						
						Modificación				0	veces en	3 años.	Bajo	Medio	Medio	Alto	Bajo	9
					X	Pérdida, destrucción				0	veces en	3 años.	Medio	Medio	Medio	Alto	Bajo	10
		X		Intencionado	X	Revelación				0	veces en	3 años.						
						Modificación				0	veces en	3 años.						
					X	Pérdida, destrucción		X		1	veces en	3 años.	Bajo	Medio	Bajo	Alto	Bajo	8
	X	Externo	X	Accidental	X	Revelación				0	veces en	3 años.						
						Modificación				0	veces en	3 años.						
					X	Pérdida, destrucción				0	veces en	3 años.						
		X		Intencionado	X	Revelación		X		1	veces en	3 años.	Medio	Medio	Medio	Alto	Bajo	10
						Modificación				0	veces en	3 años.						
					X	Pérdida, destrucción		X		1	veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
Computadoras / Laptops	X	Interno	X	Accidental	X	Revelación				0	veces en	3 años.						
						Modificación				0	veces en	3 años.						
					X	Pérdida, destrucción				0	veces en	3 años.	Medio	Medio	Medio	Alto	Bajo	10
		X		Intencionado	X	Revelación				0	veces en	3 años.	Medio	Bajo	Bajo	Alto	Bajo	8
						Modificación				0	veces en	3 años.						
					X	Pérdida, destrucción		X		1	veces en	3 años.	Medio	Medio	Medio	Alto	Bajo	10
	X	Externo	X	Accidental	X	Revelación				0	veces en	3 años.						
						Modificación				0	veces en	3 años.						
					X	Pérdida, destrucción				0	veces en	3 años.	Medio	Medio	Medio	Alto	Bajo	10
		X		Intencionado	X	Revelación				0	veces en	3 años.						
						Modificación				0	veces en	3 años.						
					X	Pérdida, destrucción		X		1	veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
Certificados electrónicos	X	Interno	X	Accidental	X	Revelación				0	veces en	3 años.						
						Modificación				0	veces en	3 años.						
					X	Pérdida, destrucción				0	veces en	3 años.						
		X		Intencionado	X	Revelación				0	veces en	3 años.						
						Modificación				0	veces en	3 años.						
					X	Pérdida, destrucción		X		1	veces en	3 años.	Medio	Bajo	Bajo	Alto	Bajo	8
	X	Externo	X	Accidental	X	Revelación		X		1	veces en	3 años.	Medio	Bajo	Bajo	Alto	Bajo	8
						Modificación				0	veces en	3 años.						
						Pérdida, destrucción				0	veces en	3 años.	Medio	Medio	Bajo	Alto	Bajo	9
		X		Intencionado	X	Revelación				0	veces en	3 años.						
						Modificación				0	veces en	3 años.						
					X	Pérdida, destrucción				0	veces en	3 años.						

Figura 133: HT-Perfil de riesgos.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Amenaza						Probabilidad	
						¿Qué tan probable es que ocurra la amenaza en el futuro?	
Activo		Actor		Motivo	Resultado	Valor cualitativo	Valor cuantitativo
Línea de Crédito	X	Interno		Accidental	Revelación		
					Modificación		
					Pérdida, destrucción		
					Interrupción		
			X	Intencionado	X Revelación	Medio	2
					X Modificación	Medio	2
		Externo		Accidental	Pérdida, destrucción		
					Interrupción		
					Revelación		
					Modificación		
				Intencionado	Pérdida, destrucción		
					Interrupción		
Lista de precios	X	Interno		Accidental	Revelación		
					Modificación		
					Pérdida, destrucción		
					Interrupción		
			X	Intencionado	X Revelación	Medio	2
					X Modificación	Medio	2
		Externo		Accidental	Pérdida, destrucción		
					Interrupción		
					Revelación		
					Modificación		
				Intencionado	Pérdida, destrucción		
					Interrupción		
Tipo de precios	X	Interno		Accidental	Revelación		
					Modificación		
					Pérdida, destrucción		
					Interrupción		
			X	Intencionado	X Revelación	Medio	2
					X Modificación	Medio	2
		Externo		Accidental	Pérdida, destrucción		
					Interrupción		
					Revelación		
					Modificación		
				Intencionado	Pérdida, destrucción		
					Interrupción		
SAP	X	Interno	X	Accidental	X Revelación	Bajo	1
					Modificación		
					X Pérdida, destrucción	Bajo	1
					X Interrupción	Bajo	1
			X	Intencionado	X Revelación	Bajo	1
					Modificación		
		Externo	X	Accidental	X Pérdida, destrucción	Bajo	1
					X Interrupción	Bajo	1
					X Revelación	Bajo	1
					Modificación		
			X	Intencionado	X Pérdida, destrucción	Bajo	1
					X Interrupción	Bajo	1

Figura 135: HT-Perfil de riesgos - Probabilidad.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Outlook	X	Interno	X	Accidental	X	Revelación	Bajo	●	1
						Modificación			
						Pérdida, destrucción			
						Interrupción			
		X	X	Intencionado	X	Revelación	Bajo	●	1
						Modificación			
						Pérdida, destrucción			
	X	Externo	X	Accidental		Interrupción			
					X	Revelación	Bajo	●	1
						Modificación			
		X	X	Intencionado		Pérdida, destrucción			
						Interrupción			
VMware	X	Interno	X	Accidental	X	Revelación	Bajo	●	1
						Modificación			
					X	Pérdida, destrucción	Bajo	●	1
					X	Interrupción	Bajo	●	1
		X	X	Intencionado	X	Revelación	Bajo	●	1
						Modificación			
					X	Pérdida, destrucción	Bajo	●	1
	X	Externo	X	Accidental	X	Interrupción	Bajo	●	1
						Revelación			
					X	Modificación			
		X	X	Intencionado	X	Pérdida, destrucción	Bajo	●	1
					X	Interrupción	Bajo	●	1
					X	Revelación	Bajo	●	1
Sistema Operativo	X	Interno	X	Accidental		Modificación			
					X	Pérdida, destrucción	Bajo	●	1
					X	Interrupción	Bajo	●	1
		X	X	Intencionado		Revelación			
						Modificación			
					X	Pérdida, destrucción	Bajo	●	1
	X	Externo		Accidental		Interrupción	Bajo	●	1
						Revelación			
						Modificación			
		X	X	Intencionado	X	Pérdida, destrucción	Bajo	●	1
					X	Interrupción	Bajo	●	1
						Revelación			
Computadoras / Laptops	X	Interno	X	Accidental		Modificación			
					X	Pérdida, destrucción	Bajo	●	1
					X	Interrupción	Bajo	●	1
		X	X	Intencionado		Revelación			
						Modificación			
					X	Pérdida, destrucción	Bajo	●	1
	X	Externo	X	Accidental	X	Interrupción	Bajo	●	1
						Revelación			
					X	Modificación			
		X	X	Intencionado	X	Pérdida, destrucción	Bajo	●	1
					X	Interrupción	Bajo	●	1
						Revelación			
Certificados electrónicos	X	Interno	X	Accidental		Modificación			
					X	Pérdida, destrucción			
					X	Interrupción			
		X	X	Intencionado		Revelación			
						Modificación			
					X	Pérdida, destrucción	Bajo	●	1
		Externo		Accidental	X	Interrupción	Bajo	●	1
						Revelación			
						Modificación			
				Intencionado		Pérdida, destrucción			
						Interrupción			
						Revelación			

Figura 136: HT-Perfil de riesgos - Probabilidad.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Producción	X	Interno	X	Accidental		Revelación		
						Modificación		
					X	Pérdida, destrucción	Bajo	1
			X	Intencionado	X	Interrupción	Bajo	1
						Revelación		
						Modificación		
	X	Externo	X	Accidental	X	Pérdida, destrucción	Medio	2
					X	Interrupción	Medio	2
						Revelación		
			X	Intencionado		Modificación		
					X	Pérdida, destrucción	Medio	2
					X	Interrupción	Medio	2
Visual ASIS	X	Interno	X	Accidental		Revelación		
					X	Pérdida, destrucción	Bajo	1
						Interrupción		
			X	Intencionado		Revelación		
						Modificación		
					X	Pérdida, destrucción	Bajo	1
		Externo		Accidental		Revelación		
						Modificación		
						Pérdida, destrucción		
				Intencionado		Revelación		
						Modificación		
						Pérdida, destrucción		
PAYROLL	X	Interno	X	Accidental		Revelación		
					X	Pérdida, destrucción	Bajo	1
						Interrupción		
			X	Intencionado		Revelación		
						Modificación		
					X	Pérdida, destrucción	Bajo	1
		Externo		Accidental		Revelación		
						Modificación		
						Pérdida, destrucción		
				Intencionado		Revelación		
						Modificación		
						Pérdida, destrucción		
SISCON	X	Interno	X	Accidental		Revelación		
					X	Pérdida, destrucción	Bajo	1
						Interrupción		
			X	Intencionado		Revelación		
						Modificación		
					X	Pérdida, destrucción	Bajo	1
		Externo		Accidental		Revelación		
						Modificación		
						Pérdida, destrucción		
				Intencionado		Revelación		
						Modificación		
						Pérdida, destrucción		

Figura 137: HT-Perfil de riesgos - Probabilidad.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Dicha probabilidad también se completa en la lista de escenarios de incidentes. Asimismo, se completa la hoja de trabajo “HT-Estrategia de Protección” observando cómo se cumplen las características de responsabilidad, procedimientos, formación, cuestiones de Colaboración y verificación. Dicha información se puede apreciar en la hoja de trabajo.

Luego de ello, se completa cómo se encuentra la protección en las áreas de práctica de seguridad de la hoja de trabajo “HT-Perfil de Riesgo” de cada activo crítico.

Amenaza				Áreas de prácticas de seguridad																			
				Estratégico									Operacional										Total
				Concientización de la seguridad y capacitación	Estrategia de seguridad	Administración de la seguridad	Política de seguridad y regulaciones	Administración de seguridad Colaborativa	Plan de Contingencia / Recuperación ante desastres	Control de acceso físico	Monitoreo y Auditoría de seguridad física	Administración de sistema y red	Monitoreo y Auditoría de la seguridad TI	Autenticación y autorización	Gestión de vulnerabilidad	Cifrado	Arquitectura y diseño de seguridad	Gestión de incidentes					
Activo	Actor		Motivo	Resultado																			
Línea de Crédito	X	Interno	Accidental		Revelación																		
					Modificación																		
					Pérdida, destrucción																		
		X	Intencionado	X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	25		
				X	Modificación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	25		
					Pérdida, destrucción																		
	X	Externo	Accidental		Revelación																		
					Modificación																		
					Pérdida, destrucción																		
		Intencionado		Revelación																			
				Modificación																			
				Pérdida, destrucción																			
Lista de precios	X	Interno	Accidental		Revelación																		
					Modificación																		
					Pérdida, destrucción																		
		X	Intencionado	X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	25		
				X	Modificación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	25		
					Pérdida, destrucción																		
	X	Externo	Accidental		Revelación																		
					Modificación																		
					Pérdida, destrucción																		
		Intencionado		Revelación																			
				Modificación																			
				Pérdida, destrucción																			
Tipo de precios	X	Interno	Accidental		Revelación																		
					Modificación																		
					Pérdida, destrucción																		
		X	Intencionado	X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	25		
				X	Modificación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	25		
					Pérdida, destrucción																		
	X	Externo	Accidental		Revelación																		
					Modificación																		
					Pérdida, destrucción																		
		Intencionado		Revelación																			
				Modificación																			
				Pérdida, destrucción																			
SAP	X	Interno	Accidental	X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	25			
				X	Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	25		
				X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	25		
		X	Intencionado	X	Modificación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	25		
				X	Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	25		
				X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	25		
	X	Externo	Accidental	X	Modificación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	25		
				X	Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	25		
				X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	25		
		X	Intencionado	X	Modificación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	25		
				X	Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	25		
				X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	Alto	25		

Figura 138: HT-Perfil de riesgos – Área de práctica de seguridad.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Outlook	X	Interno	X	Accidental	X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
						Modificación																
						Pérdida, destrucción																
			X	Intencionado	X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
						Modificación																
						Pérdida, destrucción																
	X	Externo	X	Accidental	X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
						Pérdida, destrucción																
						Interrupción																
		X	X	Intencionado	X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
						Modificación																
						Pérdida, destrucción																
VMware	X	Interno	X	Accidental	X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
						Modificación																
						Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
		X	Intencionado	X	X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
						Modificación																
						Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
	X	Externo	X	Accidental	X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
						Modificación																
						Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
		X	Intencionado	X	X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
						Modificación																
						Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
Sistema Operativo	X	Interno	X	Accidental	X	Revelación																
						Modificación																
						Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
		X	Intencionado	X	X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
						Modificación																
						Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
	X	Externo		Accidental		Revelación																
						Modificación																
						Pérdida, destrucción																
		X	Intencionado	X		Revelación																
						Modificación																
						Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
Computadoras / Laptops	X	Interno	X	Accidental	X	Revelación																
						Modificación																
						Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
		X	Intencionado	X	X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
						Modificación																
						Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
	X	Externo	X	Accidental	X	Revelación																
						Modificación																
						Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
		X	Intencionado	X	X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
						Modificación																
						Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
Certificados electrónicos	X	Interno	X	Accidental	X	Revelación																
						Modificación																
						Pérdida, destrucción																
		X	Intencionado	X	X	Revelación																
						Modificación																
						Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
	X	Externo		Accidental		Revelación																
						Modificación																
						Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
		X	Intencionado	X	X	Revelación	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25
						Modificación																
						Pérdida, destrucción	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Alto	25

Figura 139: HT-Perfil de riesgos – Área de práctica de seguridad.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Cod. Activo	Activo	Actor		Motivo		Resultado		Amenaza	Probabilidad	Amen. * Prob.	Riesgo	Nivel de riesgo
AC-001	Línea de crédito	x	Interno	X	Intencionado	X	Revelación	9	2	18	36	Bajo
						X	Modificación	9	2	18		
AC-002	Lista de precios	x	Interno	X	Intencionado	X	Revelación	9	2	18	38	Bajo
						X	Modificación	10	2	20		
AC-004	Tipo de precios	x	Interno	X	Intencionado	X	Revelación	8	2	16	34	Bajo
						X	Modificación	9	2	18		
AC-005	SAP	X	Interno	X	Accidental	X	Revelación	8	1	8	110	Medio
						X	Pérdida, destrucción	10	1	10		
						X	Interrupción	9	1	9		
						X	Revelación	8	1	8		
				X	Intencionado	X	Pérdida, destrucción	10	1	10		
						X	Interrupción	9	1	9		
						X	Revelación	9	1	9		
		X	Externo	X	Accidental	X	Pérdida, destrucción	10	1	10		
						X	Interrupción	9	1	9		
				X	Intencionado	X	Revelación	9	1	9		
						X	Revelación	9	1	9		
						X	Pérdida, destrucción	10	1	10		
						X	Interrupción	9	1	9		
AC-007	Outlook	X	Interno	X	Accidental	X	Revelación	9	1	9	34	Bajo
				X	Intencionado	X	Revelación	9	1	9		
		X	Externo	X	Accidental	X	Revelación	8	1	8		
				X	Intencionado	X	Revelación	8	1	8		
AC-008	VMware	X	Interno	X	Accidental	X	Revelación	9	1	9	108	Medio
						X	Pérdida, destrucción	9	1	9		
						X	Interrupción	9	1	9		
				X	Intencionado	X	Revelación	9	1	9		
						X	Pérdida, destrucción	9	1	9		
						X	Interrupción	9	1	9		
		X	Externo	X	Accidental	X	Revelación	10	1	10		
						X	Pérdida, destrucción	9	1	9		
						X	Interrupción	8	1	8		
				X	Intencionado	X	Revelación	10	1	10		
						X	Pérdida, destrucción	9	1	9		
						X	Interrupción	8	1	8		
AC-009	Sistemas operativos	X	Interno	X	Accidental	X	Pérdida, destrucción	9	1	9	56	Bajo
				X	Intencionado	X	Interrupción	10	1	10		
		X	Externo	X	Intencionado	X	Pérdida, destrucción	10	1	10		
				X	Intencionado	X	Interrupción	9	1	9		
AC-010	Computadoras / Laptops	X	Interno	X	Accidental	X	Pérdida, destrucción	10	1	10	73	Medio
				X	Intencionado	X	Interrupción	8	1	8		
				X	Intencionado	X	Pérdida, destrucción	10	1	10		
		X	Externo	X	Accidental	X	Interrupción	8	1	8		
				X	Intencionado	X	Pérdida, destrucción	10	1	10		
				X	Intencionado	X	Interrupción	8	1	8		
AC-021	Certificados electrónicos	X	Externo	X	Accidental	X	Pérdida, destrucción	9	1	9	34	Bajo
				X	Intencionado	X	Interrupción	9	1	9		
				X	Intencionado	X	Pérdida, destrucción	8	1	8		
				X	Intencionado	X	Interrupción	8	1	8		
AC-023	Producción	X	Interno	X	Accidental	X	Pérdida, destrucción	9	1	9	108	Medio
				X	Intencionado	X	Interrupción	9	1	9		
				X	Intencionado	X	Pérdida, destrucción	9	2	18		
		X	Externo	X	Accidental	X	Interrupción	9	2	18		
				X	Accidental	X	Pérdida, destrucción	9	1	9		
				X	Intencionado	X	Pérdida, destrucción	9	2	18		
AC-036	Visual ASIS	X	Interno	X	Accidental	X	Pérdida, destrucción	10	1	10	20	Bajo
				X	Intencionado	X	Pérdida, destrucción	10	1	10		
AC-037	PAYROLL	X	Interno	X	Accidental	X	Pérdida, destrucción	10	1	10	20	Bajo
				X	Intencionado	X	Pérdida, destrucción	10	1	10		
AC-038	SISCON	X	Interno	X	Accidental	X	Pérdida, destrucción	10	1	10	20	Bajo
				X	Intencionado	X	Pérdida, destrucción	10	1	10		

Figura 142. Cálculo del riesgo de activos críticos.

Elaborado por jefes de proyecto

Se procede a listar los riesgos según su prioridad por el valor calculado.

Cod. Activo	Activo	Riesgo	Nivel de riesgo	Prioridad
AC-001	Línea de crédito	36	Bajo	7
AC-002	Lista de precios	38	Bajo	6
AC-004	Tipo de precios	34	Bajo	10
AC-005	SAP	110	Medio	1
AC-007	Outlook	34	Bajo	9
AC-008	VMware	108	Medio	3
AC-009	Sistemas operativos	56	Bajo	5
AC-010	Computadoras / Laptops	73	Bajo	4
AC-021	Certificados electrónicos	34	Bajo	8
AC-023	Producción	108	Medio	2
AC-036	Visual ASIS	20	Bajo	11
AC-037	PAYROLL	20	Bajo	12
AC-038	SISCON	20	Bajo	13

Figura 143. Lista riesgos con prioridad.

Elaborado por jefes de proyecto

Con la información del riesgo, se procede a evaluar el enfoque a elegir, si sería mitigar, aceptar, eliminar o transferir. Junta a la empresa de productos de arcilla cerámica se decide los siguientes enfoques:

Amenaza							Enfoque			
							¿Cuál es su enfoque para abordar cada riesgo?			
Activo	Actor		Motivo		Resultado		Mitigar	Aceptar	Transferir	Evitar
Línea de Crédito	X	Interno	Accidental		Revelación					
					Modificación					
					Pérdida, destrucción					
			Intencionado	X	Interrupción					
					Revelación	x				
					Modificación	x				
					Pérdida, destrucción					
					Interrupción					
		Externo	Accidental		Revelación					
					Modificación					
					Pérdida, destrucción					
			Intencionado		Interrupción					
					Revelación					
					Modificación					
					Pérdida, destrucción					
					Interrupción					
Lista de precios	X	Interno	Accidental		Revelación					
					Modificación					
					Pérdida, destrucción					
			Intencionado	X	Interrupción					
					Revelación	x				
					Modificación	x				
					Pérdida, destrucción					
					Interrupción					
		Externo	Accidental		Revelación					
					Modificación					
					Pérdida, destrucción					
			Intencionado		Interrupción					
					Revelación					
					Modificación					
					Pérdida, destrucción					
					Interrupción					
Tipo de precios	X	Interno	Accidental		Revelación					
					Modificación					
					Pérdida, destrucción					
			Intencionado	X	Interrupción					
					Revelación	x				
					Modificación	x				
					Pérdida, destrucción					
					Interrupción					
		Externo	Accidental		Revelación					
					Modificación					
					Pérdida, destrucción					
			Intencionado		Interrupción					
					Revelación					
					Modificación					
					Pérdida, destrucción					
					Interrupción					
SAP	X	Interno	Accidental	X	Revelación	x				
					Modificación					
					Pérdida, destrucción	x				
			Intencionado	X	Interrupción	x				
					Revelación	x				
					Modificación					
					Pérdida, destrucción	x				
					Interrupción	x				
		Externo	Accidental	X	Revelación	x				
					Modificación					
					Pérdida, destrucción	x				
			Intencionado	X	Interrupción	x				
					Revelación	x				
					Modificación					
					Pérdida, destrucción	x				
					Interrupción	x				

Figura 144. Enfoques.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Outlook	X	Interno	X	Accidental	X	Revelación	x				
						Modificación					
						Pérdida, destrucción					
			X	Intencionado	X	Revelación	x				
						Modificación					
						Pérdida, destrucción					
	X	Externo	X	Accidental	X	Revelación	x				
						Modificación					
						Pérdida, destrucción					
			X	Intencionado	X	Revelación	x				
						Modificación					
						Pérdida, destrucción					
VMware	X	Interno	X	Accidental	X	Revelación	x				
						Modificación					
					X	Pérdida, destrucción	x				
			X	Intencionado	X	Revelación	x				
						Modificación					
					X	Pérdida, destrucción	x				
	X	Externo	X	Accidental	X	Revelación	x				
						Modificación					
					X	Pérdida, destrucción	x				
			X	Intencionado	X	Revelación	x				
						Modificación					
					X	Pérdida, destrucción	x				
Sistema Operativo	X	Interno	X	Accidental		Revelación					
						Modificación					
					X	Pérdida, destrucción	x				
			X	Intencionado	X	Revelación	x				
						Modificación					
					X	Pérdida, destrucción	x				
	X	Externo		Accidental		Revelación					
						Modificación					
						Pérdida, destrucción					
			X	Intencionado		Revelación					
						Modificación					
					X	Pérdida, destrucción	x				
Computadoras / Laptops	X	Interno	X	Accidental		Revelación					
						Modificación					
					X	Pérdida, destrucción	x				
			X	Intencionado		Revelación					
						Modificación					
					X	Pérdida, destrucción	x				
	X	Externo	X	Accidental		Revelación					
						Modificación					
					X	Pérdida, destrucción	x				
			X	Intencionado		Revelación					
						Modificación					
					X	Pérdida, destrucción	x				
Certificados electrónicos	X	Interno	X	Accidental		Revelación					
						Modificación					
					X	Pérdida, destrucción					
			X	Intencionado		Revelación					
						Modificación					
					X	Pérdida, destrucción	x				
		Externo		Accidental		Revelación					
						Modificación					
						Pérdida, destrucción	x				
				Intencionado		Revelación					
						Modificación					
						Pérdida, destrucción					

Figura 145. Enfoques.

Elaborado por jefes de proyecto, basado en OCTAVE-S

Producción	X	Interno	X	Accidental		Revelación				
						Modificación				
					X	Pérdida, destrucción	x			
			X	Intencionado	X	Interrupción	x			
						Revelación				
						Modificación				
	X	Externo	X	Accidental	X	Pérdida, destrucción	x			
					X	Interrupción	x			
						Revelación				
			X	Intencionado		Modificación				
					X	Pérdida, destrucción	x			
					X	Interrupción	x			
Visual ASIS	X	Interno	X	Accidental		Revelación				
						Modificación				
					X	Pérdida, destrucción				
			X	Intencionado		Interrupción				
						Revelación				
					X	Modificación				
		Externo		Accidental	X	Pérdida, destrucción				
						Interrupción				
						Revelación				
				Intencionado		Modificación				
						Pérdida, destrucción				
						Interrupción				
PAYROLL	X	Interno	X	Accidental		Revelación				
						Modificación				
					X	Pérdida, destrucción	X			
			X	Intencionado		Interrupción				
						Revelación				
					X	Modificación				
		Externo		Accidental	X	Pérdida, destrucción	X			
						Interrupción				
						Revelación				
				Intencionado		Modificación				
						Pérdida, destrucción				
						Interrupción				
SISCON	X	Interno	X	Accidental		Revelación				
						Modificación				
					X	Pérdida, destrucción	X			
			X	Intencionado		Interrupción				
						Revelación				
					X	Modificación				
		Externo		Accidental	X	Pérdida, destrucción	X			
						Interrupción				
						Revelación				
				Intencionado		Modificación				
						Pérdida, destrucción				
						Interrupción				

Figura 146. Enfoques.

Elaborado por jefes de proyecto, basado en OCTAVE-S

A continuación, se procede a completar la hoja de trabajo “HT-Plan de mitigación”, en el que se puede observar qué actividades deber de realizar la empresa para poder contrarrestar el posible impacto si se llegaran a presentar las amenazas.

La empresa de productos de arcilla cerámica decide mitigar los riesgos, por lo que se procedió a identificar controles para cada uno de ellos, todos los controles se podrán observar en la “Lista de controles”. Se valoriza cada uno de ellos para poder encontrar el riesgo residual de cada uno de los activos críticos, donde se obtiene lo siguiente:

Cod. Activo	Activo	Riesgo	Riesgo Residual
AC-001	Línea de crédito	36	15
AC-002	Lista de precios	38	18
AC-004	Tipo de precios	34	14
AC-005	SAP	110	53
AC-007	Outlook	34	16
AC-008	VMware	108	54
AC-009	Sistemas operativos	56	33
AC-010	Computadoras / Laptops	73	32
AC-021	Certificados electrónicos	34	11
AC-023	Producción	108	52
AC-036	Visual ASIS	20	10
AC-037	PAYROLL	20	10
AC-038	SISCON	20	10

Figura 147. Riesgo residual.

Elaborado por jefes de proyecto

A partir de ello, la empresa decide aceptar el nivel de cada riesgo residual por esta evaluación y se coloca la justificación en la “Lista de riesgos aceptados”. Se calcula que el porcentaje promedio de reducción de riesgo es 53%.

Se procede a terminar de completar la “HT-Estrategia de protección”, identificando qué cambios ocurrirían luego de aplicado los controles.

Finalmente, se identifica qué pasos realizar luego de la evaluación, y como adición se identifica qué indicadores la empresa podría utilizar para monitorear los controles propuestos, y así ayudarlos a que esta etapa pueda ser más rápida. Dichos indicadores se

pueden observar en el documento “Indicadores”, para esta evaluación se agregaron tres indicadores a diferencia del año anterior.

A continuación, se muestran gráficas resumen de lo anteriormente explicado según las amenazas, vulnerabilidades, riesgo inherente, controles y riesgo residual.

Las amenazas identificadas fueron agrupadas según su resultado: revelación, modificación, pérdida, destrucción e interrupción.

Figura 148. Agrupación de amenazas.

Elaborado por jefes de proyecto

Las vulnerabilidades identificadas fueron agrupadas según: concientización, monitoreo, capacitación, documentación formal y presupuesto.

Figura 149. Agrupación de vulnerabilidades.

Elaborado por jefes de proyecto

El riesgo inherente por activo se muestra en la siguiente ilustración radial, donde se puede observar que para los de color rojo son los de riesgo algo, los de amarillo, riesgo medio y los de verde, riesgo bajo.

Figura 150. Riesgo por activo.

Elaborado por jefes de proyecto

Los controles identificados (27) también fueron agrupados según monitoreo, formalización de documentos, acuerdos de confidencialidad, concientización y presupuesto.

Figura 151. Agrupación de controles.

Elaborado por jefes de proyecto

Si los controles propuestos se implementaran dentro de la empresa de productos de arcilla cerámica, el riesgo de cada activo reduciría en un promedio del 53%, el riesgo residual se muestra en la siguiente ilustración radial.

Figura 152. Riesgo residual por activo.

Elaborado por jefes de proyecto

A continuación, se muestra la matriz de probabilidad e impacto del riesgo inherente y del riesgo residual para los activos críticos, donde se puede apreciar gráficamente cómo se reduce el riesgo. La Pyme decide modificar las regiones de la matriz, ya que decide aceptar algunos riesgos identificados.

Figura 153. Riesgo por activo.

Elaborado por jefes de proyecto

Figura 154. Riesgo residual por activo.

Elaborado por jefes de proyecto

Dentro de los indicadores propuestos se agregan dos más para que la Pyme pueda monitorear el respaldo de información de cada uno de sus sistemas.

6.3 Comparativa de riesgo según el año 2017 y 2018

Para realizar una comparativa respecto al riesgo según el año 2017 y 2018, tenemos:

Tabla 27

Comparativo de Riesgo 2017 - 2018

Activo	RIESGO 2017	RIESGO 2018	Diferencia
Línea de crédito	● 36	● 36	-
Lista de precios	● 38	● 38	-
Tipo de precios	● 34	● 34	-
SAP	● 208	● 110	↓ 47%
Outlook	● 59	● 34	↓ 42%
VMware	● 216	● 108	↓ 50%
Sistemas operativos	● 85	● 56	↓ 34%
Computadoras / Laptops	● 139	● 73	↓ 47%
Certificados electrónicos	● 68	● 34	↓ 50%
Producción	● 72	● 108	↑ -50%
Visual ASIS		● 20	
PAYROLL		● 20	
SISCON		● 20	

Fuente: Elaborado por jefes de proyecto

En este análisis no consideraremos los tres últimos activos, ya que no se tiene con que comparar, tomaremos los 10 primeros activos, donde podemos observar que de los 10, 6 de

ellos han disminuido en su valor de riesgo, en promedio entre ellos disminuyeron en un aproximado de 55% de valor de riesgo. Asimismo, se puede observar que se logra reducir el riesgo de los dos activos que se encontraban en un nivel alto en el año 2017 según el gráfico radial de los niveles de riesgo identificado por cada activo.

La Pyme se encuentra en proceso de implementación de los controles propuestos, es por ello que solo en algunos de los activos se ha visto reflejada la disminución del valor riesgo, asimismo la empresa decide modificar los niveles de los criterios de evaluación de la probabilidad, en el cual decidieron aceptar un poco más el riesgo, ya que ya estaban contando con más medidas de seguridad debido a la implementación del modelo realizado en el año 2017. La empresa continuará con la implementación de los controles para en una siguiente evaluación poder reducir también el impacto de las amenazas identificadas.

7 CAPÍTULO 7: GESTIÓN DEL PROYECTO

En el siguiente capítulo se describe la gestión del proyecto respecto a los documentos de gestión realizados, asimismo se identifica si se realizaron cambios durante la realización de este. Adicionalmente, se identifican las lecciones aprendidas al culminar con el proyecto.

7.1 Producto final

El producto final de este proyecto es el modelo de gestión de riesgos de seguridad de la información para Pymes en el Perú, integrando la metodología OCTAVE-S y la norma ISO/IEC 27005, el cual se logró gracias al cumplimiento de tiempos y las actividades definidas en los documentos de gestión de proyectos. Así, se pudo validar el modelo en el proceso de ventas de la empresa de productos de arcilla cerámica.

7.2 Gestión del proyecto

7.2.1 Gestión del tiempo

Para la gestión del tiempo, se divide en hitos para TP1 y TP2. A continuación, se muestra la tabla de hitos con un criterio de cumplimiento, con algunas observaciones respecto al hito del proyecto.

Tabla 28
Gestión del Tiempo - Fases e Hitos del Proyecto

Hito del proyecto	Fecha Estimada	Entregables incluidos	Criterio cumplim.	Observaciones
Aprobación del Project Charter	2017-01 Semana 4	Project Charter	Cumplido	Se fueron realizando modificaciones y se aprobaron mediante una solicitud de cambio.
Exposición parcial TP1	2017-01 Semana 6	Project Charter, Plan de Trabajo, Entregables de Gestión	Cumplido	
Aprobación del diseño del Modelo de Gestión de riesgos de SI	2017-01 Semana 15	Diseño del Modelo de Gestión de riesgos de SI	Cumplido	
Exposición final TP1	Semana 16	Modelo de Gestión de riesgos de SI y Memoria	Cumplido	
Validación del Modelo de Gestión de riesgos de SI	2017-02 Semana 21	Modelo de Gestión de riesgos de SI	Cumplido	
Exposición parcial TP2	2017-02 Semana 25	Modelo de Gestión de riesgos de SI, Memoria	Cumplido	
Aprobación Hoja de Ruta y Perfil de proyecto	2017-02 Semana 26	Hoja de Ruta Perfil de proyecto	Cumplido	
Aprobación del Plan de Continuidad	2017-02 Semana 27	Plan de Continuidad	Cumplido	
Aprobación de la Memoria y paper	2017-02 Semana 28	Memoria, Paper	Cumplido	
Exposición final TP2	2017-02 Semana 32	Modelo de Gestión de riesgos de SI, Perfil de Proyecto, Lecciones aprendidas, Plan de Continuidad, Memoria, Paper,	Cumplido	

		Poster		
--	--	--------	--	--

Fuente: Elaborado por jefes de proyecto

No se encontraron inconvenientes graves dentro del desarrollo del proyecto que pudieron retrasar el mismo.

7.2.2 Gestión de los Recursos Humanos

A continuación, se muestran los stakeholders relacionados con el proyecto, los cuales trabajaron en conjunto con los jefes de proyecto y de manera correcta. Asimismo, se incluyen las horas de participación de cada uno.

Tabla 29

Gestión de los Recursos Humanos - Stakeholders

Nivel de Experiencia / Conocimiento	Tipo (Interno/ Externo)	Fase – Entregable del Proyecto requerido	Cantidad personal requerido	Total de Horas de participación en el proyecto	Costo Hora del personal requerido (S/.)
Comité de proyecto	Externo	Planificación, Ejecución, Control y Cierre	4	2 hrs	1
Gerente General	Interno	Control	1	-	1
Profesor Cliente	Externo	Inicio, Planificación, Ejecución, Control y Cierre	1	28.17 hrs	1
Profesor Gerente	Interno	Inicio, Planificación, Ejecución, Control y Cierre	1	43.3 hrs	1
Co-Autor	Externo	Planificación, Ejecución y Cierre	2	44.5 hrs	1
Jefes de proyecto	Interno	Inicio, Planificación, Ejecución, Control y Cierre	2	1287.04 hrs	1
Analista IT Service	Interno	Control	2	192.5 hrs	1
Cliente	Externo	Planificación, Ejecución	1	12 hrs	1

Fuente: Elaborado por jefes de proyecto

7.2.3 Gestión de las Comunicaciones

La gestión de las Comunicaciones se desarrolla adecuadamente como se ha descrito en el plan de las comunicaciones, en el capítulo 1. Durante la primera parte del proyecto, con el primer asesor, se realizaron reuniones vía Skype; con el segundo, las reuniones fueron presenciales.

Reuniones totales con profesor gerente: 27

Reuniones totales con profesor cliente: 26

Reuniones totales con el personal de la empresa: 5

7.2.4 Gestión de los Riesgos

A continuación, se muestran los riesgos definidos en el capítulo 1, los cuales podrían retrasar el proyecto.

Tabla 30

Gestión de los riesgos – Matriz de riesgos

Cód. Riesgo	Descripción del Riesgo	Disparador	Probabilidad	Impacto (HH)	Impacto	Exp al Riesgo (Horas)	Exp al Riesgo (Costo S/.)
ARSIBMGR-R001	Cambios en el proyecto	Correcciones o cambios de gran impacto al proyecto.	30% Baja	1129	5 Muy alta	338.70	338.7
ARSIBMGR-R002	Retraso de proyecto	Incumplimiento de tareas.	10% Muy baja	564	5 Muy alta	56.40	56.4
ARSIBMGR-R003	Desaprobación del profesor cliente o gerente en un documento	Inconformidad de entregables.	30% Baja	117	5 Muy alta	35.10	35.1
ARSIBMGR-R004	Deficiente comunicación entre jefes de proyecto	Conflicto de ideas entre jefes de proyectos.	30% Baja	564	5 Muy alta	169.20	169.2
ARSIBMGR-R005	Falta de información	No encontrar documentos gratuitos del enfoque de la metodología y la ISO.	30% Baja	59	5 Muy alta	17.70	17.7
ARSIBMGR-R006	Cancelación de reuniones	Falta de tiempo de los jefes de proyecto o profesor cliente o gerente.	50% Media	65	5 Muy alta	32.50	32.5
ARSIBMGR-R007	Pérdida de información del proyecto	Eliminación de documentos del proyecto en el Drive o en las laptops de los	30% Baja	408	5 Muy alta	122.40	122.4

		jefes de proyecto.					
ARSIBMGR-R008	Falta de interés por parte de la empresa.	Falta de información brindada por parte de la empresa.	50% Media	17	3 Media	8.50	8.5
ARSIBMGR-R009	Rechazo frente a las recomendaciones brindadas luego de la ejecución del proyecto.	Rechazo de implantar los controles propuestos a la empresa.	30% Baja	12	3 Media	3.60	3.6

Fuente: Elaborado por jefes de proyecto

Durante la ejecución del proyecto se presentó el siguiente riesgo y se presentará la respectiva estrategia de mitigación:

Cambios en el proyecto:

Durante la primera fase del proyecto se presentaron inconvenientes para reunirse con el profesor cliente, el profesor y los jefes de proyecto no concordaban para una reunión presencial, ya que sus horarios eran muy ajustados. Observando lo que ocurría, el profesor cliente manifestó que si se deseaba se podría solicitar el cambio de cliente, ya que no quería que el proyecto se retrase.

Por más que se había definido la estrategia de tener reuniones semanales vía Skype, el trabajo del proyecto no avanzaba mucho, por lo que los jefes de proyecto decidieron consultar con el profesor gerente sobre el cambio y anticipadamente buscaron un nuevo profesor cliente, el cual pueda asesorar en el desarrollo del proyecto relacionado a Seguridad de la Información. El profesor gerente se comunicó con el Gerente General y solicitaron a los jefes de proyecto la solicitud de gestión de cambio para poder cambiar de cliente. Se generó la solicitud y esta se envió al primer profesor cliente para su validación y su firma, igualmente para el nuevo profesor cliente. Los jefes de proyecto presentaron la solicitud al profesor gerente debidamente firmada también por ellos, el profesor gerente envió la solicitud al Gerente General para poder validar el cambio. El cambio se realizó oficialmente una semana antes de la exposición parcial de Taller de Proyectos 1.

Luego de efectuado el cambio, el proyecto se realizó de acuerdo al cronograma y se realizaron reuniones presenciales para poder obtener las observaciones necesarias para poder validar los documentos a presentar para el proyecto.

Al finalizar el curso de Taller de Proyectos 1, se realizaron algunas observaciones respecto al nombre del proyecto y sus objetivos, por dicha razón el proyecto cambio a “Modelo de Gestión de Riesgos de Seguridad de la Información” al empezar el curso de Taller de Proyectos 2. Dichos cambios se reflejaron en los documentos de gestión del proyecto.

Durante el curso de Taller de Proyectos 2, no se realizaron más cambios significativos, solo se realizó cambios en los capítulos de la memoria, se agregó el capítulo 6 referido a los resultados del proyecto.

En la semana 13 del curso, se aumentó un punto más al capítulo 2 de los Student Outcomes, donde se debió agregar las competencias generales designadas por la convalidación WASC referida a comunicación escrita, comunicación oral, ciudadanía, pensamiento innovador, pensamiento crítico, pensamiento cuantitativo y manejo de la información.

7.2.5 Lecciones aprendidas

A continuación, se señalan los puntos a mejorar y tener en cuenta para futuros proyectos:

1. Al empezar el proyecto se define un plan de trabajo, se debe de seguir los tiempos determinados en este plan para que durante el proyecto no se presenten retrasos o se necesite realizar un mayor esfuerzo para poder lograr el objetivo. Si se sigue los tiempos establecidos, el proyecto se desarrollará correctamente y sin apuros.
2. Plantear las reuniones desde un principio para que el profesor cliente pueda gestionar su tiempo y pueda estar presente sin ningún problema.
3. Plantear un horario específico para contactar al equipo responsable de brindar la información de la empresa.
4. Plantear tareas específicas de cambios para cada jefe de proyecto, según el área que más domine.
5. Coordinar con tiempo las reuniones con la alumna de diseño profesional de la universidad para poder modificar el poster del proyecto.

6. Seleccionar más personas que se puedan considerar en el equipo de trabajo por si alguna de ellas decide retirarse de la empresa.
7. Seleccionar a los usuarios correctos dentro del repositorio para los permisos de escritura y lectura.

8 CONCLUSIONES

A continuación, se mencionan las conclusiones sobre el presente proyecto:

1. La implementación del modelo en las Pymes, permite que tengan conocimiento a qué riesgos de seguridad de la información se encuentran expuestas y cuáles son los más críticos, al conocer esto y realizando las acciones necesarias sobre estos, las Pymes pueden reducir el impacto de estos y así mantener protegida su información.
2. Los resultados obtenidos permitieron la reducción del riesgo de seguridad de la información dentro de la Pyme sobre los activos más críticos, se lograron identificar los componentes de una gestión de riesgos, y se propusieron controles e indicadores para que la Pyme pueda mejorar con respecto al riesgo y mantener un constante monitoreo del mismo.
3. Contar con indicadores ayuda a monitorear cómo la Pyme está avanzando respecto al control de temas de seguridad de la información, para que ante alguna amenaza el impacto no sea tan grande.
4. La continua implementación de este modelo en la Pyme, ayuda a comparar cómo la empresa está mejorando respecto a la evaluación anterior, y se pueden tomar mejores decisiones de las ya tomadas para los activos críticos para así seguir reduciendo el riesgo.
5. El empleo de un modelo de gestión de riesgo para Pymes es de mucha ayuda, ya que la mayoría de ellas no cuenta con el presupuesto suficiente para que una empresa externa realice estas evaluaciones, el modelo presenta las fases detalladamente para que quienes lo implementen puedan entender fácilmente cada paso a seguir.

9 RECOMENDACIONES

A continuación, se mencionan las recomendaciones sobre el presente proyecto:

1. Se recomienda que antes de realizar la implementación del modelo en una Pyme, se explique a los encargados que es lo que se va a realizar y explicarles cuáles son los beneficios que conllevaría la implementación, para contar con su apoyo, ya que en estos temas de seguridad y privacidad es complicado el levantamiento de información.
2. Durante la implementación del modelo, se recomendó reducir campos de algunas hojas de trabajo, ya que algunos de ellos son repetitivos en las listas.
3. Se recomienda que las Pymes que implementen este modelo realicen las propuestas finales para poder cumplir con el objetivo de reducir el riesgo.
4. Se recomienda que la Pymes implementen este tipo de modelos, ya que les ayuda a implementar mejoras en su sistema de gestión de seguridad de la información, así podrán tener una mejor protección frente a los ataques malintencionados o robo de información que se puedan presentar.

10 REFERENCIAS

- ABET. (2017). *ABET*. Obtenido de <http://www.abet.org/>
- 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.
- Alireza, S. S., Rouzbeh, A. B., & Mohamed, C. (2015). Taxonomy of Information Security Risk Assessment. *Computers & Security*. doi:dx.doi.org/doi:10.1016/j.cose.2015.11.001
- Asociación Española de Normalización. (2018). *UNE - ISO 31000*. Obtenido de <http://www.foncodes.gob.pe/portal/index.php/convocatorias-a-myperu/archivos-pdf-sci/1387-capacitacion-sistema-gestion-de-riesgos-iso-31000-aenor-franco-gamboni-30-05-a-11-06-2018/file>

- Behnia, A., Rashid, R. A., & Chaudhry, J. A. (Febrero de 2012). A Survey of Information Security Risk Analysis Methods. *Smart Computing Review*, 2, 81-94. doi:10.6029/smartcr.2012.01.007
- Beranek, L. (2012). Risk analysis methodology used by several small and medium enterprises in the Czech Republic. *Information Management & Computer Security*, 19(1), 42-52. doi:10.1108/09685221111115854
- Bornman, G., & Labuschagne, L. (2004). A comparative framework for evaluating information security risk management methods. *Proc. of the Information Security South Africa Conference*.
- Büyüközkan, G., & Ruan, D. (2010). Choquet integral based aggregation approach to software development risk assessment. *Information Sciences*, 180, 441-451. doi:10.1016/j.ins.2009.09.009
- Caralli, R., Stevens, J., Young, L., & Wilson, W. (2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*. Pittsburgh.
- CCAC. (2016). *Manual de capacitación sector ladrillero en américa latina*. Lima.
- Chanchala, J., & Umesh, K. S. (2017). Information security risks management framework – A step towards mitigating security risks in university network. *Journal of Information Security and Applications*, 128-137. doi:http://dx.doi.org/10.1016/j.jisa.2017.06.006
- Faris, S., Ghazouani, M., Medromi, H., & Sayouti, A. (Octubre de 2014). Information Security Risk Assessment — A Practical Approach with a Mathematical Formulation of Risk. *International Journal of Computer Applications*, 103(8), 36-42.
- Feng, N., Harry, J., & Li, M. (2013). A security risk analysis model for information systems. *Information Sciences*.
- Finne, T. (2000). Information Systems Risk Managment : Key Concepts and Business Processes. *Computers & Security*, 19, 234-234.
- Fredriksen, R., Kristiansen, M., Gran, B., Stolen, K., Opperud, T., & Dimitrakos, T. (s.f.). The CORAS framework for a model-based risk management process. *Proceedings of the 21st International Conference. Computer Safety, Reliability and Security*.

- Hakemi, A., Ryul , J. S., Jeong, S. R., Ghani, I., & Sanaei, M. G. (6 de Junio de 2014). Enhancement of VECTOR Method by Adapting OCTAVE for Risk Analysis in Legacy System Migration. *KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS*, 2118-2138. doi:10.3837/tiis.2014.06.018
- Hoffman, R., Kiedrowicz, M., & Stanik, J. (2016). Risk management system as the basic paradigm of the information security management system in an organization. *MATEC Web of Conferences*. doi:10.1051/mateconf/2016760
- IBM Data Security Support Programs. (1984). USA.
- IEC. (s.f.). *International Electrotechnical Commission*. Recuperado el 2017, de International Electrotechnical Commission: <http://www.iec.ch/about/activities/>
- INDECOPI. (s.f.). *INDECOPI*. Recuperado el 2017, de INDECOPI: <https://www.indecopi.gob.pe/principios-de-la-seguridad-de-la-informacion>
- ISO. (s.f.). *International Organization for Standardization*. Recuperado el 2017, de International Organization for Standardization: <https://www.iso.org/about-us.html>
- ISO/IEC. (2002). *Gestión de riesgos - Vocabulario - Directrices*.
- ISO/IEC. (01 de Junio de 2011). Information technology — Security techniques — Information security risk management. Switzerland.
- ISO/IEC. (2015). *Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información*. 15: Junio.
- Kasap, D., & Murat, K. (2007). *Risk Identification Step of the Project Risk Management*. Turquía. doi:10.1109/PICMET.2007.4349543
- Lalanne, V., Munier, M., & Gabillon, A. (2013). Information Security Risk Management in a World of Services. *IEEE*. doi:10.1109/SocialCom.2013.88
- Mana Gonçalves, J., & Neves Fernandes, F. R. (2009). The Impact of Information Security on Latin America. *IEEE*.
- MINAM. (2014). *Gestión de la calidad del aire en el Perú*. Lima.

- Montenegro, C., & Moncayo, D. (2016). Information Security Risk in SMEs: A Hybrid Model Compatible with IFRS. *2016 6th International Conference on Information Communication and Management* (págs. 115-120). IEEE.
- Mouna, J., Latifa, B., & Ridha, K. (2015). A Multidimensional Approach Towards a Quantitative. *Procedia Computer Science*, 507-514.
- Organización Internacional de Normalización. (2009). *ISO 31000*. Obtenido de http://gestion-calidad.com/wp-content/uploads/2016/09/iso_31000_2009_gestion_de_riesgos.pdf
- Pacheco, F. G. (Febrero de 2013). The Need for Formal Education on Information Security. *IEEE LATIN AMERICA TRANSACTIONS*, 668-670. Recuperado el 23 de Junio de 2017
- SENASA. (2010). *Instructivo para identificar, medir, controlar y monitorear los riesgos operacionales*. Instructivo, Costa Rica.
- Shamala, P., Ahmad, R., & Yusoff, M. (2013). A conceptual framework of info structure for information security risk assessment (ISRA). *Information security and applications*, 45-52. doi:dx.doi.org/10.1016/j.jisa.2013.07.002
- Shedden, P., Ahmad, A., Tscherning, H., Smith, W., & Scheepers, R. (Setiembre de 2016). Asset Identification in Information Security Risk Assessment: A Business Practice Approach. *Communications of the Association for Information Systems*, 39, 297-320.
- Shukla, N., & Kumar, S. (2012). A comparative Study on Information Security Risk Analysis Practices. *Intelligence and Computing Technologies*, 29-33.
- The Foundation Coalition. (2005). *The Foundation Coalition*. Obtenido de The Foundation Coalition: http://fc.civil.tamu.edu/home/keycomponents/assessment_eval/ec_outcomes_summaries.html
- UPC Alumni. (2016). *UPC Alumni*. Obtenido de <https://blogs.upc.edu.pe/upc-alumni/sobre-alumni/acreditacion-institucional-internacional-wasc>
- Wangen, G., & Snekenes, E. (2014). A Comparison between Business Process Management and Information Security Management. *IEEE*.

WASC Senior College and University Commission. (s.f.). *WASC Senior College and University Commission*. Recuperado el 08 de Noviembre de 2017, de <https://www.wscuc.org/>

Yazar, Z. (2011). A Qualitative Risk Analysis and Managment Tool - CRAMM. *SANS Institute InfoSec Reading Room*.