UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

FACULTAD DE INGENIERÍA

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

**Modelo de referencia para la protección de datos personales en el sector
microfinanciero peruano**

TESIS

Para optar el título profesional de Ingeniero de Sistemas de Información

AUTOR(ES)

Alejo Alarcón, Claudio Alfredo Aarón (0000-0001-7885-4119)

Navarro Ruíz, Alan Jesús (0000-0002-6869-0947)

ASESOR

Mansilla López, Juan Pablo Jesus (0000-0003-0039-6044)

Lima, 30 de Noviembre del 2020

DEDICATORIA

A Dios, mis abuelos, padres, tíos, hermano y primos, quienes estuvieron siempre conmigo, dándome la fortaleza y apoyo incondicional para concluir este proceso. Por su inmenso esfuerzo, amor y cariño. Los quiero.

Claudio Alejo Alarcón

A la vida, por darme la oportunidad de demostrarle a las personas que con esfuerzo todo es posible. De igual manera, a mi mamá, quiero agradecerle la paciencia, buena voluntad, amor incondicional y su fe en mí. Este título profesional no se hubiera logrado sin ti, ya puedes decir que tienes un hijo ingeniero. ¡Gracias!

Alan Navarro Ruíz

AGRADECIMIENTOS

Este proyecto es el resultado un constante apoyo de las personas y entidades quienes nos ayudaron para concluir con este trabajo. Principalmente, agradecer a la Universidad Peruana de Ciencias Aplicadas (UPC) que nos formaron profesionalmente a lo largo de nuestra carrera y nos brindó las herramientas necesarias para llevar a cabo este proyecto. Un agradecimiento especial a nuestro profesor y asesor, Pedro Acuña, quien nos guio durante todo el desarrollo de la tesis y se convirtió en un amigo para nosotros. A María del Carmen Laguna Arce, gerente general de la Cooperativa de Ahorros y Créditos “Vale un Perú”, quien nos brindó su gran ayuda y confianza en el momento que más necesitábamos para poder validar nuestra propuesta. De igual manera, agradecerle al Ingeniero de Sistemas Christian Díaz Zamora, quién brindó sus conocimientos especializados en Seguridad de la Información y Protección de Datos Personales, dichos conocimientos permitieron optimizar nuestro modelo de referencia y sección de controles internos. Por último, a la abogada Carolina Ormeño Flores por brindar sus conocimientos y ajustar los controles legales que incluyen la Ley de Protección de Datos Personales – Ley 29733.

RESUMEN

La protección de datos personales consiste en resguardar la información de las personas en todo su ciclo de vida dentro de una entidad y emplearla únicamente para los fines por los cuales fueron proporcionados. Todas las empresas se convierten en titulares de bancos de datos personales al poseer información de sus clientes, colaboradores y/o proveedores, ya sea empleando tecnologías de información para su tratamiento, o documentos y almacenes físicos. La aplicación de las medidas de seguridad adecuadas para la protección de datos personales es de gran importancia en las organizaciones, en especial, en uno de los sectores de mayor crecimiento como es el microfinanciero. De lo contrario, pone en riesgo los derechos y libertades de las personas, además de recibir costosas sanciones económicas.

En la presente tesis, se propone un modelo de referencia que brinda un conjunto de medidas legales, organizativas y técnicas para proteger los datos personales custodiados por una entidad microfinanciera, garantizando su adecuado tratamiento a lo largo de su ciclo de vida. Estas medidas están basadas en la Ley 29733 y su reglamento, ISO 27001, COBIT 5, NIST 800-53 y CIS CSC.

El modelo de referencia fue implementado en una Cooperativa peruana de ahorro y créditos donde se recopiló información relacionada al tratamiento de datos personales, se evaluó el nivel de protección de datos personales y se implementó un plan de mejora. El resultado de la implementación fue un incremento del 57% en el nivel de protección de datos personales, alcanzando así un 74%.

Palabras clave: datos personales; ISO 27001; seguridad de información; sector microfinanciero.

ABSTRACT

The protection of personal data consists of safeguarding the information of people throughout its life cycle within an entity and using it only for the purposes for which it was provided. All companies become owners of personal data banks by having information on their clients, collaborators and / or suppliers, either by using information technologies for their treatment, or documents and physical warehouses. The application of adequate security measures for the protection of personal data is of great importance in organizations, especially in one of the fastest growing sectors such as microfinance. Otherwise, it puts the rights and freedoms of people at risk, in addition to receiving costly financial penalties.

In this thesis, a reference model is proposed that provides a set of legal, organizational and technical measures to protect the personal data kept by a microfinance entity, guaranteeing its adequate treatment throughout its life cycle. These measures are based on Law 29733 and its regulations, ISO 27001, COBIT 5, NIST 800-53 and CIS CSC.

The reference model was implemented in a Peruvian savings and loan cooperative where information related to the processing of personal data was collected, the level of protection of personal data was evaluated and an improvement plan was implemented. The result of the implementation was a 57% increase in the level of protection of personal data, thus reaching 74%.

Keywords: personal data; ISO 27001; information security; microfinance.

TABLA DE CONTENIDOS

1	INTRODUCCIÓN.....	1
2	CAPÍTULO 1: DEFINICIÓN DEL PROYECTO	2
2.1	OBJETIVO DE ESTUDIO	2
2.2	DOMINIO DEL PROBLEMA.....	2
2.3	PLANTEAMIENTO DE LA SOLUCIÓN	4
2.4	OBJETIVOS DEL PROYECTO	5
2.4.1	Objetivo general	5
2.4.2	Objetivos específicos.....	5
2.5	INDICADORES DE ÉXITO	5
2.6	PLANIFICACIÓN DEL PROYECTO	6
2.6.1	Alcance del proyecto	6
2.6.2	Restricciones.....	7
2.6.3	Plan de gestión de tiempo.....	7
2.6.4	Plan de gestión de recursos humanos	9
2.6.5	Plan de gestión de las comunicaciones.....	13
2.6.6	Plan de gestión de riesgos.....	13
3	CAPÍTULO 2: LOGROS DE LOS STUDENT OUTCOMES	15
3.1	STUDENT OUTCOME A.....	15
3.2	STUDENT OUTCOME B.....	16
3.3	STUDENT OUTCOME C.....	19
3.4	STUDENT OUTCOME D.....	20
3.5	STUDENT OUTCOME E	20
3.6	STUDENT OUTCOME F	21
3.7	STUDENT OUTCOME G.....	22
4	CAPÍTULO 3: MARCO TEÓRICO	23
4.1	MODELO DE REFERENCIA.....	23
4.2	SECTOR MICROFINANCIERO PERUANO	24
4.3	LEY N° 29733 – LEY DE PROTECCIÓN DE DATOS PERSONALES.....	27
4.4	DIRECTIVA DE SEGURIDAD – AUTORIDAD NACIONAL DE PROTECCIÓN DE DATOS PERSONALES.....	31

4.5	CIRCULAR G-140.....	37
4.6	ISO/IEC 27001:2014 - SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 39	
4.7	PROJECT MANAGEMENT BODY OF KNOWLEDGE – PMBOK	40
5	CAPÍTULO 4: DESARROLLO DEL PROYECTO	44
5.1	ANÁLISIS DE LOS ESTÁNDARES INTERNACIONALES, MARCOS DE TRABAJO Y BUENAS PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN	44
5.1.1	Análisis de los macroprocesos de las microfinancieras.....	44
5.1.2	Elección de las medidas de seguridad	56
5.1.3	Análisis de los estándares y marcos de trabajo de seguridad de la información 57	
5.1.4	Conclusiones del análisis.....	68
5.2	DISEÑO DEL MODELO DE REFERENCIA PARA LA PROTECCIÓN DE DATOS PERSONALES EN EL SECTOR MICROFINANCIERO PERUANO	70
5.2.1	Modelo de referencia para la protección de datos personales en el sector microfinanciero peruano.....	70
5.2.2	Entradas	72
5.2.3	Ciclo de vida del dato personal.....	74
5.2.4	Medidas legales	76
5.2.5	Medidas organizativas	76
5.2.6	Medidas técnicas.....	76
5.2.7	Soporte.....	77
5.2.8	Salidas.....	77
5.2.9	Herramientas del modelo de referencia.....	78
6	CAPÍTULO 5: RESULTADOS DEL PROYECTO	138
6.1	VALIDACIÓN DE LAS MEDIDAS LEGALES, ORGANIZATIVAS Y TÉCNICAS DEL MODELO PROPUESTO EN UNA ENTIDAD MICROFINANCIERA.....	138
6.1.1	Presentación de la microfinanciera.....	138
6.1.2	Proceso de validación	140
6.1.3	Resultados de la validación	184
6.2	PLAN DE CONTINUIDAD PARA LA ACTUALIZACIÓN DE LAS MEDIDAS LEGALES, ORGANIZATIVAS Y TÉCNICAS DEL MODELO DE REFERENCIA	190

6.2.1	Actualización del marco legal, estándar, marco de trabajo o buenas prácticas de seguridad de información	191
6.2.2	Adquisición de nuevas tecnologías:	193
6.3	COSTOS Y PRESUPUESTOS	195
6.3.1	Apoyo interno	195
6.3.2	Enfoque de gestión de costes.....	197
7	CAPÍTULO 6: GESTIÓN DEL PROYECTO	202
7.1	GESTIÓN DE RECURSOS HUMANOS	203
7.1.1	Descripción de roles	203
7.1.2	Adquisición de personal	204
7.1.3	Requerimientos de personal para el proyecto.....	205
7.1.4	Horarios definidos para el proyecto	205
7.1.5	Criterios de liberación del personal contratado	205
7.1.6	Planes de formación para recursos TDP	205
7.1.7	Personal de expertos requeridos para el proyecto	205
7.2	ROLES Y RESPONSABILIDADES	207
7.2.1	Roles	207
7.2.2	Características del rol requerido e identificación del recurso humano de la organización.....	207
7.2.3	Recursos humanos requeridos en el tiempo	209
7.3	GESTIÓN DE LAS COMUNICACIONES.....	210
7.4	MATRIZ DE ASIGNACIÓN DE RESPONSABILIDADES	212
8	CONCLUSIONES.....	214
9	RECOMENDACIONES	214
10	GLOSARIO	216
11	REFERENCIAS	218
12	ANEXOS	222

ÍNDICE DE TABLAS

Tabla 1: Problema principal y causas	3
Tabla 2: Relación de los indicadores de éxito y los objetivos específicos	6
Tabla 3: Restricciones del proyecto	7
Tabla 4: Tabla de fases e hitos.....	9
Tabla 5: Descripción de los roles del proyecto.....	13
Tabla 6: Lista de riesgos	14
Tabla 7: Tabla de análisis de procesos de negocio de microfinancieras	17
Tabla 8: Tabla de análisis de estándares y marcos de trabajo de seguridad de la información	19
Tabla 9: Tabla de descripción de los derechos fundamentales.....	29
Tabla 10: Descripción de las categorías de la Directiva de seguridad de banco de datos personales	33
Tabla 12: Descripción de medidas de contraseña.....	35
Tabla 13: Descripción de resguardo de información por categoría.....	36
Tabla 14: Definición de conceptos generales del PMBOK.....	41
Tabla 15: Descripción de grupos de procesos	42
Tabla 16: Definición de áreas de conocimiento	43
Tabla 17: Macroprocesos vs Criticidad del tratamiento de datos personales.....	55
Tabla 18: Controles para usar según el estándar de seguridad de la información y/o seguridad informática.....	61
Tabla 19: Comparación del estándar internacional de seguridad de la información y/o seguridad informática	67
Tabla 20: Matriz de evaluación de las medidas legales.....	82
Tabla 21: Matriz de evaluación de las medidas organizativas	98
Tabla 22: Matriz de evaluación de las medidas técnicas.....	123
Tabla 23: Detalle del ciclo de vida del dato personal de la Cooperativa de Ahorro y Crédito "Vale un Perú"	155
Tabla 24: Matriz de evaluación de las medidas legales del estado actual de la Cooperativa de Ahorro y Crédito "Vale un Perú"	158
Tabla 25: Resultados de la evaluación de las medidas legales.....	159
Tabla 26: Matriz de evaluación de las medidas organizativas del estado actual de la Cooperativa de Ahorro y Crédito "Vale un Perú"	164

Tabla 27: Matriz de evaluación de las medidas técnicas del estado actual de la Cooperativa de Ahorro y Crédito “Vale un Perú”	168
Tabla 28: Resultados de la evaluación de las medidas técnicas	169
Tabla 29: Evaluación del curso de capacitación sobre seguridad de la información	173
Tabla 30: Nueva evaluación de las medidas legales posterior a la implementación.....	176
Tabla 31: Nueva evaluación de las medidas organizativas posterior a la implementación	180
Tabla 32: Nueva evaluación de las medidas técnicas posterior a la implementación	183
Tabla 34: Costo por fase (no incluye la implementación).....	196
Tabla 35: Costo por personal (no incluye la implementación).....	196
Tabla 36: Costo por fase (incluye la implementación).....	197
Tabla 37: Costo por personal (incluye la implementación).....	197
Tabla 38: Costos de Materiales	197
Tabla 39: Posibles infracciones impuestas por incumplimiento de las medidas legales....	199
Tabla 40: ROSI para aspectos legales	199
Tabla 41: Posibles infracciones impuestas por incumplimiento de las medidas organizativas	199
Tabla 42: ROSI para aspectos organizativos.....	200
Tabla 43: Posibles infracciones impuestas por incumplimiento de las medidas técnicas .	200
Tabla 44: ROSI para aspectos técnicos	201
Tabla 45: Posibles infracciones impuestas por incumplimiento de las medidas legales, organizativas y técnicas	201
Tabla 46: ROSI del proyecto	202
Tabla 47: Matriz de características de roles	209
Tabla 48: Matriz de la gestión de las comunicaciones	212
Tabla 49: Matriz de asignación de responsabilidades	213

ÍNDICE DE FIGURAS

Figura 1: Organigrama del proyecto.....	10
Figura 2: Matriz de medidas organizativas.....	16
Figura 3: Gráfica representativa de las Cajas Municipales en el Perú	25
Figura 4: Gráfica representativa de las Cajas Municipales en el Perú	26
Figura 5: Gráfica número de datos vs Volumen de información	34
Figura 6: Gráfica de periodo de finalidad vs Volumen de información.....	34
Figura 7: Gráfica tipo de persona vs Volumen de información	35
Figura 8: Flujo para implementar la Ley 29733	37
Figura 9: Modelo de referencia para la protección de datos personales en el sector microfinanciero peruano.....	71
Figura 10: Sección de entradas del modelo de referencia propuesto	72
Figura 11: Sección del ciclo de vida del dato personal del modelo propuesto.....	74
Figura 12: Sección de medidas legales del modelo de referencia propuesto	76
Figura 13: Sección de las medidas organizativas del modelo propuesto	76
Figura 14: Sección de las medidas técnicas del modelo de referencia propuesto	77
Figura 15: Sección de soporte del modelo de referencia propuesta	77
Figura 16: Sección de salidas del modelo de referencia propuesta	78
Figura 17: Sede de la Cooperativa de Ahorro y Crédito "Vale un Perú"	140
Figura 18: Proceso de validación del modelo.....	140
Figura 19: Hoja de cálculo de la matriz de evaluación de las medidas legales.....	142
Figura 20: Hoja de cálculo de la matriz de evaluación de las medidas organizativas.....	143
Figura 21: Hoja de cálculo de la matriz de evaluación de las medidas técnicas	143
Figura 22: Hoja de cálculo con los indicadores del nivel de cumplimiento por cada medida del modelo de referencia y el nivel total de protección de datos personales.....	143
Figura 23: Organigrama de la Cooperativa de Ahorro y Crédito "Vale un Perú"	146
Figura 24: Interfaz gráfica 1 de la ventana "Expediente de créditos" del sistema VITEC	148
Figura 25: Interfaz gráfica 2 de la ventana "Expediente de créditos" del sistema VITEC	148
Figura 26: Servidor de archivos y servidor aplicaciones y base de datos de la Cooperativa de Ahorro y Crédito "Vale un Perú"	150
Figura 27: Computadora de escritorio de la Cooperativa de Ahorro y Crédito "Vale un Perú"	150

Figura 28: Armario de expedientes de la Cooperativa de Ahorro y Crédito "Vale un Perú"	151
Figura 29: Mapa del ciclo de vida del dato personal de la Cooperativa de Ahorro y Crédito "Vale un Perú". Parte 1	153
Figura 30: Mapa del ciclo de vida del dato personal de la Cooperativa de Ahorro y Crédito "Vale un Perú". Parte 2	154
Figura 31: Registro de los bancos de datos de la Cooperativa de Ahorro y Crédito "Vale un Perú"	173
Figura 32: Resultado aprobados de la evaluación del curso de capacitación sobre seguridad de la información en la Cooperativa de Ahorro y Crédito "Vale un Perú"	174
Figura 33: Nivel de cumplimiento inicial por cada medida organizativa	185
Figura 34: Nivel de cumplimiento inicial por cada medida legal	185
Figura 35: Nivel de cumplimiento inicial por cada medida técnica	186
Figura 36: Nivel inicial total del porcentaje de protección de datos personales en el sector microfinanciero peruano	186
Figura 37: Nivel de cumplimiento final de las medidas organizativas	187
Figura 38: Nivel de cumplimiento final de las medidas legales	188
Figura 39: Nivel de cumplimiento final de las medidas técnicas	189
Figura 40: Nivel de total final de la protección de datos personales	189
Figura 41: Comparación del nivel de protección de datos personales antes y actual	189
Figura 42: Comparación del monto de inversión vs el gasto del proyecto	202

1 INTRODUCCIÓN

La presente tesis propone un modelo de referencia que permite proteger los datos personales custodiados y tratados por las microfinancieras en el Perú. Este documento explica el procedimiento que se llevó a cabo para su desarrollo y las teorías han sido empleadas. Para ello, se organizó el documento en 6 capítulos.

En el capítulo 1 se describe el problema principal de las microfinancieras relacionado a la protección de los datos personales y sus respectivas causas. Además, se explicará el objetivo general y los objetivos específicos que se han planteado para llevar a cabo el proyecto de tesis. Por último, se detallará la planificación del proyecto basado en el PMBOK.

En el capítulo 2 se describe detalladamente la manera en que el desarrollo del proyecto logró cumplir con los 7 Student Outcomes definidos por la acreditadora internacional ABET.

En el capítulo 3 se presenta el marco teórico que contiene la recopilación de todos los conceptos que comprende el proyecto. En él se explica la composición del sector microfinanciero, el marco legal y normativo peruano correspondiente a la protección de datos personales, los estándares de seguridad de la información y las metodologías que se emplearon para el desarrollo de la tesis.

En el capítulo 4 se presenta el análisis de los estándares, marcos de trabajo y buenas prácticas de seguridad de la información empleados para el diseño del modelo. Asimismo, se presenta el Modelo de referencia para la protección de datos personales y se explica cada uno de sus componentes y artefactos.

En el capítulo 5 se explica detalladamente el procedimiento que se realizó para implementar el modelo de referencia en una microfinanciera peruana y los resultados obtenidos. Además, se explica el plan de continuidad y los costos de la implementación del proyecto.

Finalmente, en el capítulo 6, se presentan los entregables de la gestión de proyectos. En ellos dan a conocer indican los roles involucrados, la asignación de responsabilidades y el manejo de las comunicaciones como parte del desarrollo de la tesis.

2 CAPÍTULO 1: DEFINICIÓN DEL PROYECTO

El capítulo 1 consiste en describir el problema que tienen las microfinancieras en términos de protección de datos personales. Además, se describirá el objetivo general y los objetivos específicos que se han planteado para lograr una adecuada solución. Por último, se formarán entregables basados en la guía de proyectos PMBOK

2.1 Objetivo de estudio

El proyecto se basa en la gestión de los datos personales por parte del sector microfinanciero peruano, el cual está constituido por Cajas Municipales, Edpymes. Cooperativas de Ahorro y Crédito, Bancos especializados en microfinanzas y ONG especializadas. En consecuencia, vectores como la Seguridad de la Información, Ciberseguridad y el marco normativo peruano permiten proteger el adecuado tratamiento de los datos personales y sensibles de clientes, proveedores, prospectos, entre otros.

2.2 Dominio del problema

El sistema financiero se ha visto afectado por los constantes ataques informáticos y fraudes por robo de identidad. Un reporte realizado por Radio Programas del Perú muestra la forma en que los delincuentes ofrecen las bases de datos de empresas de telefonía y de bancos, ya sea actualizada o antigua, a los transeúntes por un valor de 200 soles (RPP, 2017). Estos registros pueden contener desde DNI, nombres completos y correos electrónicos, hasta cuentas de ahorros, líneas de créditos y código del sistema privado de pensiones. Este es un claro ejemplo de la facilidad en obtener datos privados y sensibles de las personas. Otro caso donde se ve involucrada la información privada nos informa el Diario Gestión, en el cual Melanie Gagné, directora de Desarrollo de Negocio Internacional de Fraude de EQUIFAX, detalla la manera en que las mafias roban datos personales para obtener préstamos y celulares. Ella menciona lo siguiente: "En el mundo, el fraude está en aumento. Hoy, las personas quieren tener un acceso más rápido a los servicios y las empresas compiten entre ellas ofreciendo servicios por teléfono, online y otros; de eso se aprovechan los defraudadores para acceder a los fondos y a información de los consumidores." (Gestion, 2016).

Además, menciona que la finalidad de los delincuentes en usurpar la identidad de las personas es obtener préstamos. Este delito lo realizan comprando bases de datos robadas o infiltrando miembros de la mafia en las empresas financieras para adquirirlas y con la información de alguien hacerse pasar por dicha persona. En adición a lo anterior, a diario se

registran cientos de ataques informáticos producidos por malwares, especialmente a entidades financieras. Algunos de estos se realizan a través de la violación de las barreras de seguridad en las computadoras de terceros a la empresa, porque estos no tienen los mismos mecanismos de seguridad que entidades financieras más robustas, como los bancos, y una vez que acceden al sistema, pueden ingresar al de la financiera. Es por ello por lo que el 2017, solo en Perú, estos cibercrímenes generaron pérdidas mayores a US\$4,782 millones (Gestión, 2017). Inclusive, en el ámbito internacional, un reporte realizado por un portal de pymes español, basándose en el informe “The State of Cybersecurity and Digital Trust 2016”, destaca que el 48% de los ejecutivos de seguridad encuestados, se encuentran preocupados por el robo interno de datos y 42% en los ataques de malware (Cepymenews España, 2017). Estos son algunos de los muchos casos donde la identidad de los clientes de las empresas privadas se afectada, pese a la existencia de la Ley N° 29733 - Ley de Protección de Datos Personales, la cual tiene como finalidad garantizar el adecuado tratamiento, conservación y transferencia de la información sensible y privada (Congreso de la República del Perú, 2011). Sin embargo, entidades gubernamentales como el Instituto Nacional de Estadísticas e Informática - INEI, quien en el último censo, incumplió esta ley al firmar un convenio con más de 80 organizaciones privadas, con el fin de entregar los registros obtenidos, pero sin antes haberlos inscritos y declarados ante la Autoridad Nacional de Protección de Datos Personales (ANPDP), órgano fiscalizador del resguardo de los datos personales designado por el Ministerio de Justicia y Derechos Humanos - MINJUS (RRP, 2017).

En base a lo descrito, podemos concluir que el problema de las organizaciones, especialmente de las microfinancieras, es un inadecuado tratamiento de los datos personales. Las principales causas que se han detectado son las siguientes:

Problema	Causas
Inadecuado tratamiento de los datos personales.	Deficiente control de acceso a la información.
	Presupuesto limitado en herramientas de seguridad de TI.
	Capacitaciones ineficientes en formación y concientización sobre Seguridad de Información.
	Déficit en políticas de protección de datos personales.

Tabla 1: Problema principal y causas

Las causas principales son las siguientes:

- 1) Según la encuesta global de seguridad de la información, realizada por la compañía Ernst & Young el 2015, muestra que el 25% de los empleados cuenta con más accesos de los que necesita para realizar sus funciones adecuadamente. Además, solo el 55% de las entidades cumple correctamente con brindar los privilegios necesarios a sus empleados (Ernst & Young, 2015).
- 2) Según el informe anual de la empresa Deloitte, elaborado en el 2016 indica que el 92% de los CTOs solicitan aumentar en un 50% el presupuesto asignado a seguridad de la información (Deloitte, 2016).
- 3) Según la encuesta global de seguridad de la información, realizada por Ernst & Young en el 2017, el 33% de las empresas cuenta con Políticas de Seguridad de la Información Ad-hoc o no tienen Políticas. En el Perú, la cifra llega al 35% (Ernst & Young, 2017).
- 4) Según el informe anual del 2017, elaborado por Kaspersky Lab, empresa dedicada a brindar soluciones de seguridad tecnológica. Dio como resultado que de todas las empresas que consumen algún servicio de la compañía, el 49% ha sufrido algún incidente de seguridad, de este porcentaje el 53% tiene como causante empleados descuidados o mal informados en términos de seguridad de la información (Kaspersky Lab, 2017).

En conclusión, se han identificado 04 causas principales, de las cuales se puede inferir que las empresas no tienen como prioridad invertir en seguridad de la información, por ello no se pueden adquirir herramientas de seguridad TI adecuadas, capacitaciones a sus empleados, entre otros. Dando como resultado que las microfinancieras no puedan brindar un adecuado tratamiento a los datos personales de sus clientes, proveedores, empleados y prospectos.

2.3 Planteamiento de la solución

El modelo que se va a desarrollar a lo largo de la tesis va a permitir que las microfinancieras peruanas puedan brindarles a sus clientes, proveedores, prospectos y empleados un adecuado tratamiento de sus datos personales. Para ello, debe realizarse un estudio de los componentes

que intervienen en dicho tratamiento, tales como los aspectos de negocio y tecnológico. Además, se considera la Ley 29733 – Ley de Protección de Datos Personales. El modelo no solo beneficiará a la compañía en términos de resguardo de información, sino también en términos económicos. Esto se debe a que la multa por incumplimiento de la Ley 29733 puede llegar a costar 100 UIT (S/. 420,000.00).

2.4 Objetivos del proyecto

Los objetivos del proyecto deben desarrollarse adecuadamente, con el fin de darle solución al objetivo general. Estas tareas podrán lograrse gestionando adecuadamente los recursos que se tengan a disposición. Tareas como presentar a tiempo los entregables, el presupuesto acordado, gestionar los riesgos, entre otros, Con el fin, de conseguir un modelo de referencia de excelencia.

2.4.1 Objetivo general

Implementar un modelo de referencia para la protección de datos personales en el sector microfinanciero peruano.

2.4.2 Objetivos específicos

OE1: Analizar los estándares internacionales, marco de trabajos y buenas prácticas de seguridad de la información.

OE2: Diseñar un modelo de referencia para la protección de datos personales en el sector microfinanciero peruano.

OE3: Validar las medidas legales, organizativas y técnicas del modelo propuesto en una entidad microfinanciera.

OE4: Elaborar un plan de continuidad para la actualización de las medidas legales, organizativas y técnicas del modelo.

2.5 Indicadores de éxito

A continuación, se detalla los indicadores de éxito para cada uno de los objetivos específicos:

Indicador de éxito		Objetivo
IE1	Acta de aprobación del análisis de los estándares internacionales, marco de trabajos y buenas prácticas de seguridad de la información por el asesor cliente.	OE1

IE2	Acta de aprobación del diseño del modelo de referencia por especialistas en marco legal de protección de datos personales y seguridad de la información.	OE2
IE3	Acta de aprobación de la validación del nivel de cumplimiento de los aspectos legales, organizativos y técnicos propuestos en el modelo por el responsable de la microfinanciera y especialista de seguridad de la información.	OE3
IE4	Acta de aprobación del plan de continuidad para la actualización de las medidas legales, organizativas y técnicas del modelo por el asesor cliente.	OE4

Tabla 2: Relación de los indicadores de éxito y los objetivos específicos

2.6 Planificación del proyecto

2.6.1 Alcance del proyecto

El alcance del proyecto tendrá en consideración los siguientes puntos:

- Análisis de los procesos claves, las políticas de protección de datos y los sistemas del sector microfinanciero peruano.
- Comprender la Ley N° 29733 “Ley de protección de datos personales”, ISO 27001 - “Sistema de Gestión de Seguridad de la Información” y la Directiva de Seguridad brindada por la Autoridad Nacional de Protección de Datos Personales.
- Análisis de documentos legales y normativos adicionales enfocados a la protección de datos personales.
- Análisis de artículos científicos correspondientes a la protección de datos en microfinancieras.
- Documentación de los artefactos de gestión de proyectos basado en la guía PMBOK versión 6.0 (Project Management Body of Knowledge).
- Elaboración de un modelo de referencia enfocado en la protección de datos personales de las empresas del sector microfinanciero en el Perú.

Las exclusiones del proyecto son las siguientes:

- El modelo no se aplica en microfinancieras que estén dentro de la categoría Básico y Simple según la Directiva de seguridad.
- El modelo no incluye la Norma Técnica Peruana NTP-ISO/IEC 17799-2007.
- El modelo no incluye a todas las organizaciones peruanas, solo a las del sector microfinanciero.
- El modelo no incluye procesos del negocio que no procesen información personal de los clientes, colaboradores, proveedores y/o prospectos.

2.6.2 Restricciones

Las restricciones que se han considerado para este proyecto son las siguientes:

Restricciones	Descripción
Tiempo para la implementación	El proyecto tendrá una duración de 1 año comprendido en los ciclos académicos 2018-02 y 2019-01.
Disponibilidad del responsable de la empresa	Las reuniones con el responsable de cada empresa dependen de su disponibilidad y las fechas pactadas pueden tener variaciones.

Tabla 3: Restricciones del proyecto

2.6.3 Plan de gestión de tiempo

El plan para gestionar adecuadamente el tiempo del proyecto consta de hitos y entregables, así como cumplir con determinadas fechas de entrega. A continuación, se presenta el detalle.

Fase	Hito	Fecha estimada	Entregables	Prioridad
Inicio	<i>Project Charter</i> aprobado	23/08/2019	<i>Project Charter</i>	Alta
Planificación	Artefactos de <i>Project</i>	20/09/2018	- Diccionario EDT.	Alta

	<i>Managament</i> aprobados		<ul style="list-style-type: none"> - Matriz de Trazabilidad de Requisitos. - Gestión de RR.HH. - Descripción de roles y responsabilidades. - Matriz RAM. - Matriz de Riesgos. - Matriz de comunicaciones. - Cronograma de Proyecto. 	
Ejecución	Acta del Objetivo 1 del proyecto aprobado	18/10/2018	Documento de análisis de los estándares internacionales, marcos de trabajos y buenas prácticas de seguridad de la información	Alta
	Acta del Objetivo 2 del proyecto aprobado	15/11/2018	Documento del diseño del modelo de referencia para la protección de datos personales en el sector microfinanciero peruano.	Alta
	Acta del Objetivo 3 del proyecto aprobado	02/05/2019	Documento con los resultados de la validación. Documento de las mejoras del modelo.	Alta
	Acta del Objetivo 4 del proyecto aprobado	30/05/2019	Documento del Plan de continuidad para la actualización de las medidas legales,	Alta

			organizativas y técnicas del modelo.	
Cierre	Proyecto aprobado	04/07/2019	<ul style="list-style-type: none"> - Modelo de referencia para la protección de datos personales en el sector microfinanciero peruano. - Memoria - Artículo Científico 	Alta

Tabla 4: Tabla de fases e hitos

2.6.4 Plan de gestión de recursos humanos

Para una correcta gestión de los Recursos Humanos de la organización, se identificaron y describieron los cargos involucrados en el proyecto.

Figura 1: Organigrama del proyecto

El equipo del proyecto estará conformado por:

Rol	Miembro	Responsabilidades
Comité de Proyectos	<ul style="list-style-type: none"> • Rosario Villalta • Jimmy Armas • Daniel Subauste • Pedro Shiguihara 	<ul style="list-style-type: none"> • Dar un veredicto de los proyectos presentados, con respecto a la pertinencia, viabilidad e integridad con la carrera.
		<ul style="list-style-type: none"> • Verificar el cumplimiento de la documentación de cada proyecto.
		<ul style="list-style-type: none"> • Decidir la continuidad de los proyectos.
Director de la PMO	<ul style="list-style-type: none"> • Alfredo Barrientos 	<ul style="list-style-type: none"> • Controla y gestiona los proyectos de TP1 y TP2.
		<ul style="list-style-type: none"> • Coordinar actividades con los Senior Portfolio Manager de las empresas virtuales.
Senior Portfolio Manager	<ul style="list-style-type: none"> • Carlos Díaz 	<ul style="list-style-type: none"> • Supervisar, coordinar y controlar los portafolios de proyectos y las diferentes actividades que tiene asignadas.
		<ul style="list-style-type: none"> • Resolver, adecuadamente, cualquier incidente que esté dentro de su ámbito sin afectar los intereses ni la imagen de la Escuela.
		<ul style="list-style-type: none"> • Realizar cualquier actividad que pudiese ser solicitada por el director de la PMO y por el Comité de proyectos de la Escuela.
		<ul style="list-style-type: none"> • Preservar el cumplimiento de las políticas y procedimientos dentro de los portafolios que tiene asignados.
		<ul style="list-style-type: none"> • Entregar, de forma oportuna, los informes semanales de gestión de los portafolios, que están a su cargo, por cada proyecto profesional.

		<ul style="list-style-type: none"> • Escalar cualquier problema o incidente que no pueda resolver.
Portfolio Manager	<ul style="list-style-type: none"> • Juan Pablo Mansilla 	<ul style="list-style-type: none"> • Supervisar, coordinar y controlar los proyectos, y las diferentes actividades que tiene asignadas dentro de su portafolio.
		<ul style="list-style-type: none"> • Preservar el adecuado cumplimiento de los proyectos sin afectar la calidad esperada de los mismos.
		<ul style="list-style-type: none"> • Resolver, adecuadamente, cualquier incidente que esté dentro de su ámbito sin afectar los intereses ni la imagen de la Escuela.
		<ul style="list-style-type: none"> • Realizar cualquier actividad que pudiera ser solicitada por el director de la PMO y por el Comité de proyectos de la Escuela.
		<ul style="list-style-type: none"> • Facilitar la gestión de los proyectos a cargo apoyando constantemente a los Project Managers.
Asesor Cliente	<ul style="list-style-type: none"> • Pedro Acuña 	<ul style="list-style-type: none"> • Cumplir el rol de Product Manager en los proyectos profesionales que tiene asignados.
		<ul style="list-style-type: none"> • Realizar cualquier actividad que sea solicitada por su Portfolio Manager, el Senior Portfolio Manager, el director de la PMO y por el Comité de Proyectos de la Escuela.
		<ul style="list-style-type: none"> • Proporcionar, los insumos necesarios, al Project Manager y al Portfolio Manager para el desarrollo del Project Charter del proyecto profesional.

Project Manager	<ul style="list-style-type: none"> • Claudio Alejo • Alan Navarro 	<ul style="list-style-type: none"> • Gestionar, según el <i>Project Management Body Of Knowledge</i>, su proyecto profesional, siguiendo los lineamientos de la Dirección de Proyectos durante todos sus procesos: Inicio, Planificación, Ejecución, Seguimiento y Control, y Cierre.
		<ul style="list-style-type: none"> • Administrar, eficientemente, todos los recursos asignados a su cargo.
		<ul style="list-style-type: none"> • Realizar cualquier actividad que pudiese ser solicitada por su Portfolio Manager, por el Senior Portfolio Manager, por el Director de la PMO y por el Comité de Proyectos de la Escuela.
		<ul style="list-style-type: none"> • Elaborar, en conjunto con el Portfolio Manager asignado, el Project Charter de su proyecto profesional siguiendo los lineamientos del Comité de Proyectos para la definición de: la problemática, los objetivos generales y específicos, y los indicadores del proyecto para cada carrera.
		<ul style="list-style-type: none"> • Gestionar, adecuadamente, cada uno de los requerimientos que son solicitados por su asesor/cliente especificando claramente el <i>Definition of Done</i> (DoD).

Tabla 5: Descripción de los roles del proyecto

2.6.5 Plan de gestión de las comunicaciones

Visualizar el detalle en el Anexo 2: Matriz de comunicaciones del Proyecto.

2.6.6 Plan de gestión de riesgos

El plan de gestión de riesgos es un proceso documentado que señala la estrategia en como los riesgos se identificarán y abordarán con el objetivo de disminuir el efecto que podría

causar. De esta manera, se pueden tomar decisiones para mitigarlos, aceptarlos, transferirlos o eliminarlos. A continuación, se detallarán los riesgos del proyecto con sus estrategias de mitigación correspondientes:

#	Riesgo	Probabilidad	Impacto	Estrategia de mitigación
1	Poca disponibilidad del representante de la microfinanciera.	Media	Alto	Elaborar un calendario de las reuniones que se realizará con el representante, tomando como prioridad su disponibilidad. Además, enviar recordatorios y actas de la reunión.
2	Poca disponibilidad del especialista en datos personales para validar el modelo.	Media	Alto	Elaborar un calendario de las reuniones que se realizará con el especialista, tomando como prioridad su disponibilidad. Además, enviar recordatorios y actas de la reunión.
3	Cambios en la Ley de protección de datos personales	Media	Alto	Analizar el impacto de los cambios en el modelo y realizar las modificaciones correspondientes.

Tabla 6: Lista de riesgos

3 CAPÍTULO 2: LOGROS DE LOS STUDENT OUTCOMES

En este capítulo se va a describir detalladamente como el proyecto logró cubrir con cada uno de los *Student Outcomes* definidos por la acreditadora internacional ABET.

3.1 Student Outcome A

La capacidad de identificar, formular y resolver problemas complejos de ingeniería aplicando los principios de ingeniería, ciencia y matemática.

El proyecto “Modelo de referencia para la protección de datos personales en el sector microfinanciero peruano”, como proceso inicial, recopila e identifica información pertinente de las microfinancieras peruanas con el fin de analizar el marco normativo, estructura organizacional y sus componentes tecnológicos, respecto de la protección de datos personales. Al identificar el problema, se formulan 3 medidas generales para darle solución y optimizar el resultado basado en buenas prácticas internacionales de seguridad de la información. Las medidas legales están conformadas en 19 controles y están basadas en la Ley de Protección de Datos Personales – Ley N° 29733. Las medidas organizativas constituyen 39 controles, los cuales están basados en el estándar internacional de seguridad de la información ISO 27001 “Sistema de Gestión de Seguridad de la Información” y el marco de trabajo COBIT en su versión 5. Las medidas técnicas conforman 25 controles basados en el estándar internacional de Ciberseguridad NIST 800-54 y el marco de trabajo CSC CSI en su versión 6. Con el fin, de analizar el cumplimiento de las medidas y sus controles, se complementó la matriz con indicadores de impactos y nivel de cumplimiento. Se asignaron pesos al indicador de impacto y al de cumplimiento en base a la escala Likert. Para cada medida (legal, organizativa y técnica) se realizó una sumatoria de los pesos del nivel de cumplimiento y el impacto y se dividió sobre el total de puntaje esperado. Esto permitió elaborar gráficos para analizar la situación actual de la microfinanciera y tomar acciones correctivas priorizando tareas, según el nivel de cumplimiento.

MATRIZ DE CUMPLIMIENTO DE LAS MEDIDAS ORGANIZATIVAS

MEDIDAS DE ORGANIZATIVAS	REFERENCIA	CONTROLES	APLICA	IMPACTO				CUMPLIMIENTO				PUNTAJE	
				BAJO	MODERADO	ALTO	MUY BAJO	BAJO	ADECUADO	BUENO	EXCELENTE	ESPERADO	LOGRADO (%)
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	ISO 27001 A.5.1.1	Política General de Seguridad	SI		X		X					8	0
	ISO 27001 A.5.1.2	Revisión de la Política General de Seguridad	SI		X		X					8	0
	ISO 27001 A.6.1.1	Roles y Responsabilidades para el Resguardo de la Seguridad	SI			X		X				12	3
	ISO 27001 A.7.2.1	Responsabilidad de la Alta Dirección	SI			X		X				12	3
	ISO 27001 A.7.2.2	Política para la Revisión de los Derechos de Ingreso Lógicos	SI		X			X				8	2
	ISO 27001 A.10.1.1	Política de Validación de Lineamientos Criptográficos	SI		X		X					8	0
	ISO 27001 A.11.2.9	Política de Escritorios Ordenados	SI		X		X					8	0
	ISO 27001 A.6.2.1	Política de Control para los Dispositivos Móviles Internos	SI		X		X					8	0
	ISO 27001 A.7.2.2	Política de entrenamiento al personal en términos de seguridad	SI		X		X					8	0
	ISO 27001 A.8	Política de gestión de activos	SI		X		X					8	0
	ISO 27001 A.8.2.1	Política de Segmentación de la Información	SI		X		X					8	0
	ISO 27001 A.9.1.1	Política de acceso de usuario a la red empresarial	SI		X		X					8	0
	ISO 27001 A.11.1	Política de seguridad física	SI		X		X					8	0

Figura 2: Matriz de medidas organizativas

3.2 Student Outcome B

La capacidad de aplicar el diseño de ingeniería para producir soluciones que satisfagan necesidades específicas considerando la salud pública, seguridad y bienestar, así como factores globales, culturales, sociales, ambientales y económicos.

El proyecto Modelo de Referencia para la Protección de Datos Personales en el Sector Microfinanciero peruano analiza los procesos de negocio y tecnológicos de las microfinancieras. Además, estudia e interpreta el marco legal y normativo, por el cual está sujeta la entidad financiera. El resultado del análisis permite interpretar el contexto, por el cual fluyen los datos personales. Para complementar esta información y poder esquematizar un diseño que permita proteger y brindarles un adecuado tratamiento a los datos personales, se realizó el estudio de artículos científicos, conference papers, informes periodísticos e informes anuales de empresas dedicadas a seguridad de la información. Todo ello, con el fin de poder diseñar el modelo de referencia, el cual dio como resultado identificar el flujo del dato, para ello nos apoyamos en artículos científicos que permitan diagramar un adecuado ciclo de vida del dato. El estudio de artículos científicos nos permitió diagramar de forma adecuada los procesos generales que debería tener el modelo para lograr proteger los datos personales, es decir, las medidas legales, organizativas y técnicas. En el primer caso, nos basamos en el marco legal peruano (Ley 29733 – Ley de Protección de Datos Personales). En el segundo caso, los controles se basaron en la ISO 27001 y COBIT 5 y para las medidas técnicas, se utilizaron estándar de Ciberseguridad como el NIST 800-53 y CIS CSS versión 6.

		CRITERIOS				
MACROPROCESOS		Tratamiento Datos Personales	Tratamiento Datos Sensibles	Transferencia de datos personas	Tratamiento inter-sede	Resultado
ESTRATÉGICOS	G. de Planificación	-	-	-	-	No aplica
	G. de Seguimiento y Control	Clientes	Préstamo	Interna	Agencias	Aplica

	Marketing	Clientes	Sueldo	Interna y Externa	-	Aplica
OPERATIVOS	Inversiones	Clientes	Sueldo	Interna	Agencias	Aplica
	Operaciones	Clientes	-	Externa	Agencias	No aplica
	Colocaciones	Clientes	Sueldo	Interna	Agencias	Aplica
	Recuperaciones	Clientes	Sueldo	-	Agencias	Aplica
	Captaciones	Clientes	Sueldo	Interna	Agencias	Aplica
	Riesgo Operativo	-	-	-	-	No aplica
	Riesgo Crediticio	Clientes	Sueldo	Externa	Agencias	Aplica
	Riesgo Mercado	-	-	-	-	No aplica
APOYO	Logística	-	-	-	-	No aplica
	G. de Recursos Humanos	Empleados	Sueldo	Interna	Agencias	Aplica
	Soporte Tecnológico	Clientes y Empleados	Sueldo	Interna	-	Aplica
	Contabilidad	-	-	-	-	No aplica
	Asesoría Legal	-	-	-	-	No aplica

Tabla 7: Tabla de análisis de procesos de negocio de microfinancieras

MEDIDAS	ISO 27001	COBIT 5	ISA	NIST 800-53	CCS CSI 6
Política Seg. Información	07 procesos con enfoque de Gobierno TI	15 controles para gestionar políticas SDI considerando el marco regulatorio.	08 controles para gestionar políticas de ciberseguridad.	01 control para políticas de Seguridad Cibernética.	N/A
Gestión De Activos	07 procesos con enfoque en 02 componentes (sw y hw).	07 controles para protección de activos de información.	03 controles de protección para los SI industriales.	03 controles básicos para la protección de activos lógicos.	02 controles para inventario de sw y hw.
Gestión Accesos Lógicos	03 procesos sobre la	11 controles gestionar los SI como	17 controles gestión de SI orientados a	08 controles como privilegios mínimos,	05 controles orientados a la

	administración de SI.	inventario y propietario.	sistemas industriales.	autenticación, pero no completos.	estructura lógicos de los SI, para que sean seguros.
Gestión Accesos Físicos	03 procesos para control de la infraestructura TI.	06 controles para los espacios de la empresa donde hay información.	01 control general para resguardo de espacios físicos.	12 controles para casos de emergencia y sitio alternativo de trabajo.	N/A
Gestión De Riesgos	09 procesos dedicadas a las etapas del riesgo en la empresa.	11 controles para riesgos en diferentes escenarios.	14 controles secuenciales para abarcar un riesgo en el ámbito industrial.	09 controles sobre riesgos con enfoque en los proveedores.	03 controles con evaluación de vulnerabilidades y pruebas del equipo rojo.
Gestión Seguridad RR.HH.	07 procesos para evaluar, medir y entrenar al personal respecto de sus funciones.	03 controles para entrenar, normar y educar en SDI a los empleados.	06 controles para capacitar y evaluar al personal en términos de ciberseguridad.	04 controles para entrenar y educar al personal de acuerdo con sus funciones.	N/A
Cifrado	N/A	01 control para gestionar los	N/A	03 controles gestionar las	03 controles

		hashes de la organización.		claves criptográficas respecto del marco legal.	para conexiones inalámbricas y monitoreo de acceso.
Gestión De Incidentes	08 procesos para gestionar los incidentes de la empresa.	07 controles para gestionar incidentes SDI de la empresa.	12 controles para gestionar los incidentes de seguridad cibernética.	04 controles con plan de respuesta, auditorías y procesos para los incidentes.	01 control para dar respuesta a incidentes de seguridad informática.
Gestión Continuidad	07 procesos orientados a la continuidad del negocio.	04 controles orientados a la continuidad de la SDI.	07 controles para clasificar, priorizar SI que deben estar activos.	09 controles para mantener operativos los sistemas pertinentes.	N/A

Tabla 8: Tabla de análisis de estándares y marcos de trabajo de seguridad de la información

3.3 Student Outcome C

La capacidad de funcionar efectivamente en un equipo cuyos miembros juntos proporcionan liderazgo, crean un entorno de colaboración e inclusivo, establecen objetivos, planifican tareas y cumplen objetivos.

Para lograr comunicar adecuadamente el proyecto Modelo de Referencia para la Protección de Datos Personales en el Sector Microfinanciero peruano, se realizaron exposiciones de prueba, con la finalidad de optimizar la forma (entonación, postura, léxico académico y señas) en que se presentará el problema, la solución, implementación del modelo y sus características. Para lograr darle mayor fluidez a la presentación, se realizó un estudio de la

mejor forma de realizar la presentación, es decir, utilizando un proyector, herramienta de software y un adaptador de cable VGA. Además, en las exposiciones de prueba, se optó por juntar compañeros de estudio, con el fin de recibir una retroalimentación y mejorar. Por otro lado, todo lo que se exponga debe estar escrito y descrito en documentos formales, los cuales han sido revisados y aprobados con anterioridad. Se utilizó la metodología PMBOK (*Project Management Body of Knowledge*) para gestionar el proyecto, se realizó el estudio de diversas fuentes de información para lograr extraer la información más relevante y veras. De tal modo, que pueda ser sintetizado y traspasado en los documentos.

3.4 Student Outcome D

La capacidad de reconocer responsabilidades éticas y profesionales en situaciones de ingeniería y hacer juicios informados, que deben considerar el impacto de las soluciones de ingeniería en contextos globales, económicos, ambientales y sociales.

Para llevar a cabo la implementación del proyecto Modelo de Referencia para la Protección de Datos Personales en el Sector Microfinanciero peruano se consideraron diversos aspectos, como el hecho de generar un Acuerdo de Confidencialidad con la entidad financiera, con el fin de brindarle la seguridad a la empresa, es decir, su información confidencial no será expuesta. Además, para la especificación del modelo de referencia en los documentos / entregables pertinentes, se citaron a los autores de las fuentes de información, los cuales fueron recopilados de repositorios como IEEE Computer Society, ACM y SCOPUS. Por último, el modelo comprende el entorno normativo del país, es decir, propone que la información personal de sus clientes. Colaboradores, prospectos, clientes potenciales y proveedores sea tratada con responsabilidad, es decir, contemplando los 3 pilares de seguridad de la información: confidencialidad, integridad y disponibilidad. Asimismo, las 03 matrices de cumplimiento están unidas a las sanciones administrativas que derivan del incumplimiento de la Ley de Protección de Datos Personales – Ley N° 29733.

3.5 Student Outcome E

La capacidad de funcionar efectivamente en un equipo cuyos miembros juntos proporcionan liderazgo, crean un entorno de colaboración e inclusivo, establecen objetivos, planifican tareas y cumplen objetivos.

Para llevar a cabo el proyecto Modelo de Referencia para la Protección de Datos Personales en el Sector Microfinanciero peruano, se trabajó con diversos profesionales, los cuales

brindaron diversos puntos de vistas, con la finalidad de optimizar el modelo. Los rubros involucrados fueron de cumplimiento normativo (legal), Auditoría Interna, Metodologías Ágiles, Seguridad de la Información, Redes e Infraestructura TI. Liderar adecuadamente el proyecto fue un desafío, pero se pudo lograr gracias al adecuado uso de la comunicación oral y escrita. Además, se optimizaron las tareas y se segregaron funciones de acuerdo con los pendientes utilizando la metodología KANBAN y la herramienta de software TRELLO. Por otro lado, para obtener información de cómo está estructurada una microfinanciera y cuáles eran sus componentes se tuvo una entrevista con personal de la Superintendencia de Banca y Seguros del Perú – SBS y se realizó el estudio de diversas fuentes (Tesis, Artículos Científicos e Informes Periodísticos), con el fin de detallar el flujo de información modelo de una entidad financiera de este tipo.

3.6 Student Outcome F

La capacidad de desarrollar y llevar a cabo la experimentación adecuada, analizar e interpretar datos, y usar el juicio de ingeniería para sacar conclusiones.

Se realizó un cronograma de actividades para desplegar e implementar adecuadamente el proyecto Modelo de Referencia para la Protección de Datos Personales en el Sector Microfinanciero peruano. El diagrama de tiempo consta de 04 fases, las cuales son recopilación de información, diagnóstico, plan de mejora e implementación de las medidas correctivas.

El modelo de referencia propuesto consta de tres artefactos: Matriz de evaluación para las medidas legales, organizativas y técnicas. Estos artefactos permiten medir el nivel de cumplimiento de cada medida, basándose en el impacto de los controles en la microfinanciera y el cumplimiento de estos. Las medidas legales tienen 19 controles, las medidas organizativas tienen 39 controles y las medidas técnicas tienen 25 controles. Durante la validación, se recopiló documentos sobre los procesos de negocio, políticas de seguridad, procedimientos, organigrama y funciones, fichas de empleados, antecedentes sobre implementación de protección de datos personales, expedientes de clientes, información acerca de los servidores, softwares, entre otros. Los datos recopilados sirvieron para que, en base a los criterios de cumplimiento que contiene cada control de la matriz, establecer el nivel de cumplimiento de la microfinanciera. En base a ello, se calculó el nivel de protección de datos personales, permitiendo saber las categorías donde hay mayor incumplimiento y con ello priorizar las acciones de mejora.

Para el plan de mejora se definió un cronograma con los puntos más críticos de atender. Cuando las acciones definidas en el plan se implementaron se realizó una evaluación nuevamente, de las cuales el nivel de protección se incrementó de un 17% a 74%.

3.7 Student Outcome G

La capacidad de adquirir y aplicar nuevos conocimientos según sea necesario, utilizando estrategias de aprendizaje apropiadas.

El proyecto Modelo de Referencia para la Protección de Datos Personales en el Sector Microfinanciero peruano, se basa principalmente en 03 pilares, los cuales son: Medidas Legales, Medidas Organizativas y Medidas Técnicas. Para realizar la implementación de las medidas técnicas, se aplicaron 25 controles basados en 02 marcos internacionales de trabajo de Ciberseguridad (NIST 800-53 y CCS CSI v6). Implementar dichos controles permitió a la organización madurar en términos de gestión de incidentes, gestión de accesos lógicos, gestión de accesos físicos, seguridad interna y perimetral. Para la gestión de incidente se implementó una herramienta open source (iTop), para la gestión de accesos lógicos se ejecutó la revisión de accesos del sistema VITEC a nivel de usuarios, perfiles y privilegios asociados. Para robustecer la seguridad perimetral e interna se realizaron actividad de aseguramiento del entorno, como la implementación y/o actualización de software antivirus, configuración del firewall local, segregación de carpetas compartidas y bloqueo de puerto USB mediante el BIOS del sistema operativo. Por último, gracias a todas las actividades estudiadas y elaboradas, se aprendieron y reforzaron una serie de conocimientos de seguridad de la información y todas las expectativas para incursionar en este rubro de una forma adecuada. El modelo de referencia consta de un lenguaje formal y común para el entendimiento de los distintos niveles jerárquicos del proyecto y de la entidad microfinanciera. Además, durante la exposición se expone la manera en que el modelo cumple la necesidad del cliente, basándose en datos estadísticos por organizaciones dedicadas al estudio del tema. Por otra parte, para mantener la buena comunicación, posterior a cada reunión se enviará un acta donde se detallará los temas tratados y acuerdos por ambas partes.

4 CAPÍTULO 3: MARCO TEÓRICO

En el capítulo 3 se presentan las definiciones de todos los conceptos fundamentales relacionados al proyecto, conceptos relacionados directamente a las microfinancieras, el marco legal peruano, marco normativo peruano, estándares de seguridad de la información y la metodología que se utilizará para desarrollar el proyecto en sí.

4.1 Modelo de referencia

Según Vojislav y León (Vojislav B. & J. Leon, 2000), el término 'arquitectura del sistema' denota la descripción de la estructura (o estructuras) de un sistema de información basado en computadora; las estructuras en cuestión comprenden componentes de software, las propiedades visibles externamente de esos componentes y las relaciones entre ellos. Un modelo de referencia, por otro lado, describe una descomposición estándar de un dominio de problema conocido en una colección de partes interrelacionadas, o componentes, que resuelven el problema de manera cooperativa. También describe la manera en que los componentes interactúan para proporcionar las funciones requeridas. En resumen, un modelo de referencia es un marco conceptual para describir la arquitectura del sistema, proporcionando así una especificación de alto nivel para una clase de sistemas.

Una vez desarrollado, un modelo de referencia para un dominio de problema particular se puede utilizar de diferentes maneras:

- 1) Un modelo de referencia puede proporcionar el marco para la identificación, el desarrollo y la coordinación de estándares relacionados. (La existencia de modelos y estándares ampliamente aceptados es la base necesaria para el desarrollo descendente de aplicaciones y sistemas flexibles, interoperables y coherentes). Ciertamente facilita la comunicación entre las partes interesadas.
- 2) Se puede usar un modelo de referencia para desarrollar modelos más especializados para soportar requisitos y escenarios específicos.
- 3) Se puede mapear un modelo de referencia en una colección de componentes de software y flujos de datos entre esos componentes, para obtener una denominada arquitectura de referencia. La arquitectura de referencia puede, entonces, refinarse aún más -agregando suficientes detalles de implementación- para llegar a la arquitectura del sistema.
- 4) Finalmente, un modelo de referencia ampliamente aceptado permite el uso de un proceso de desarrollo basado en la arquitectura. El desarrollo basado en la

arquitectura se caracteriza por componer o ensamblar componentes desarrollados por separado en una entidad funcional, respetando las restricciones y la estructura organizacional impuesta por la arquitectura del sistema (y, en última instancia, el modelo de referencia subyacente). En general, se considera que dicho desarrollo conduce a una mayor calidad y / o ahorro de costes, tanto durante el desarrollo del sistema como en la vida operativa normal (Vojislav B. & J. Leon, 2000).

4.2 Sector microfinanciero peruano

- **Institución Financiera (IMF)**

Se define como toda entidad, banco comercial pequeño, unión de crédito, organización no gubernamental financiera, o cooperativa de crédito, las cuales, proveen servicios financieros a las personas de menos recursos.

- **Sistema Microfinanciero peruano**

En el 2017, según ComexPerú las Mypes (Micro y pequeña empresa) representan el 96.5% del total de empresas peruanas. Este grupo suma 5,7 millones aproximadamente y genera trabajo para 8,13 millones de personas. Aun así, el 80% de este universo son empresas informales, lo cual limita su desarrollo. El sistema microfinanciero peruano está conformado por 208 empresas, donde 38 de ellas son empresas reguladas y supervisadas por la Superintendencia de Banca, Seguros y AFP - SBS (18.3%), 158 son Cooperativas de Ahorro y Crédito reguladas por la SBS, pero supervisadas por la Federación Nacional de Cooperativas de Ahorro y Crédito – FERNACREP (76.0%) y 12 corresponden a entidades no reguladas (5.8%).

Figura 3: Gráfica representativa de las Cajas Municipales en el Perú

Fuente: Equilibrium

- **Caja Municipal**

Las cajas municipales aportan de forma considerable en el crecimiento económico de las microempresas mediante financiamientos que ofrecen. Estas cajas son supervisadas y reguladas por la Superintendencia de Banca y Seguros (SBS) y están formadas parte del Fondo de Seguros de Depósitos (FSD). Además, se les permite trabajar en todas las regiones del Perú. Los propietarios son las municipalidades provinciales, debido a que tienen economía y finanzas independientes, asimismo, capacidad administrativa propia (Microfinanzas, 2016).

Figura 4: Gráfica representativa de las Cajas Municipales en el Perú

Elaboración: Federación Peruana de Cajas Municipales de Ahorro y Crédito

- **Caja Metropolitana**

Es una empresa que realiza operaciones múltiples. Su función principal es ofrecer créditos pignoratícios al público en general y realizar préstamos a las micros y pequeñas empresas. Además, lleva a cabo operaciones activas y pasivas con los concejos provinciales y distritales, y con las empresas municipales dependientes (Municipalidad de Lima, s.f.).

- **EDPYME - Entidades de Desarrollo para la Pequeña y Microempresa**

Son entidades encargadas de brindar préstamos a personas naturales y jurídicas, cuyas actividades sean calificadas como de pequeñas y microempresas. Para satisfacer la demanda de los servicios crediticios, emplea sus propios recursos económicos y a aquellos provenientes de donaciones (Capillo, 2015).

- **Cajas Rurales de Ahorro y Crédito**

Las Cajas Rurales de Ahorro y Créditos (CRAC) son instituciones autorizadas para ofrecer créditos y captar los depósitos del público en general. Están reguladas por la Superintendencia de Banca, Seguros y AFP (SBS) y forman parte del grupo de empresas cuyas operaciones son no bancarias. En el 2017, las CRACs generaron el 0.18% de los créditos a nivel nacional y el 0.21% de los depósitos del Sistema Financiero Nacional. Sin embargo, en los últimos años su participación se redujo debido al retiro varias instituciones del sector, convirtiéndose en el más pequeño del sistema microfinanciero (Arana , Núñez, Ore, & Velazco, 2017).

- **Entidades Financieras**

Una entidad financiera es aquella que ofrecer servicios financieros tales como el asesoramiento para la inversión en el mercado de seguros o brindar prestamos crediticios. Puede estar compuesto por una o más entidades que tengan el mismo propósito. La regulación vigente clasifica a las entidades financieras según el servicio que ofrece al público en general (Economipedia, s.f.).

4.3 Ley N° 29733 – Ley de Protección de Datos Personales

- **Antecedentes**

Antes de promulgarse la Ley N° 29733 el 03 de julio del 2011, era muy común que alguna empresa con la cual nunca se haya tenido contacto llame para ofrecer sus productos o servicios. Este proceso, se ejecutaba constantemente sin tener alguna regulación que lo impida, afectando la privacidad de las personas. (Gestión, 2015).

- **Objetivo**

El objetivo de la vigente Ley 29733 - Ley de Protección de Datos Personales es garantizar el derecho fundamental de la protección de datos personales a través de un tratamiento proporcional, informado y seguro, y alineados a los derechos fundamentales a los cuales se relaciona.

- **Obligaciones**

A continuación, se detalla las principales obligaciones que las empresas deberán cumplir para proteger los datos personales que tratan:

Inscribir ante la Autoridad Nacional de Protección de Datos Personales (ANPDP) los Bancos de Datos Personales (BDP) y/o Códigos de conductas que posean: La Ley define a los bancos de datos personales como un conjunto

organizado de información de las personas naturales, tales como nombres, domicilio, teléfonos, sueldo, DNI, correo electrónico, sexo, orientación política o religiosa, entre otros, independiente de su alojamiento. Es de suma importancia considerar que, para lograr cumplir de forma efectiva con esta obligación, es necesario revisar y analizar en todas las áreas de la organización a fin de identificar los datos personales que se tratan y los procesos que los emplean. El objetivo es conocer todos los BDP que gestiona la organización. Aun así, en la práctica, muchas empresas solo inscriben ante el Registro Nacional de Datos Personales, los BDP de clientes, empleados y proveedores, sin considerar los BDP con propósitos no operativos de la organización. Algunos de ellos son los datos personales que se registran y guardan en el control de visitas, grabaciones de video como parte de la vigilancia, grabaciones telefónicas, registros biométricos, entre otros.

Obtener el consentimiento: Este documento es una autorización que permite a la organización tratar los datos personales de su titular. Este consentimiento debe cumplir con lo siguiente: Ser libre en oponerse a lo condicionado, informado previamente, expreso e inequívoco. La mayoría de las organizaciones suelen cometer errores cuando tratan de cumplir esta obligación y traer como consecuencias sanciones económicas. Los consentimientos deben ser específicos y concretos en el tratamiento que se realizará con los datos personales. Por ejemplo, se debe informar que datos se recopilará, el tiempo de tratamiento, la finalidad por la cual se solicita, si los datos serán transferidos a terceros, quien es el titular del banco de datos personales y encargado del tratamiento, etc. Por otra parte, si la empresa requiere realizar algún tratamiento de los datos personales con la finalidad de cumplir con las obligaciones que dispone la ley, entonces no necesita solicitar el consentimiento al titular.

Definir y ejecutar medidas idóneas y eficaces para garantizar la seguridad: Las organizaciones deberán definir y aplicar medidas legales, organizativas y técnicas para evitar que personas no permitidas puedan infiltrarse a los bancos de datos personales y obtener información a la que no deberían tener acceso. Estas medidas podrían consistir en elaborar políticas de seguridad, manuales para el manejo y cuidado durante el tratamiento de datos personales, documentos de confidencialidad,

protocolos de seguridad para la gestión de archivos almacenados en soporte digital o físico y cláusulas contractuales.

Establecer procedimientos para la aplicación y el respeto de los derechos de los titulares de los datos personales: Las organizaciones que administren bancos de datos personales, deberán garantizar que los titulares de los datos puedan ejercer sus derechos que la Ley define. A continuación, se describen los derechos del titular:

Tipo de derecho	Descripción del derecho
Acceso	Toda persona que haya brindado sus datos personales a una empresa y su consentimiento para el tratamiento tiene derecho a solicitar lo siguiente: el acceso a su información, la finalidad por la que fueron recopilados, las transferencias que se hayan realizado o aquellas que estén próximas a realizarse y las razones que incentivaron la recopilación.
Rectificación	Toda persona está en su derecho de solicitar la modificación de sus datos personales contenidos en el banco de datos personales de la empresa, siempre y cuando, haya evidencias de los errores, inexactitud o falsedad en los registros.
Cancelación	Cuando los datos personales del titular ya sean necesarios para el motivo por el cual se obtuvieron, o hayan cumplido la duración del tratamiento, el titular podrá solicitar la eliminación de sus datos del BDP.
Oposición	Toda persona puede solicitar la eliminación de sus datos personales cuando hayan sido recopilados sin su previo consentimiento.

Tabla 9: Tabla de descripción de los derechos fundamentales

Fuente: Ley N° 29733 - Ley de Protección de Datos Personales

Comunicar el flujo transfronterizo:

En caso la organización transfiera bancos de datos personales a una entidad ubicada en un país diferente al del origen, se deberá comunicar al titular de los datos personales, indicando el nombre del receptor y su ubicación. Algunas de las transferencias se realizan a empresas pertenecientes al mismo grupo o empresas

terceras que brindan servicios informáticos, tales como host o almacenamiento (Gestión, 2017).

- **Infracciones y sanciones tributarias**

Las infracciones sancionables son por omisiones o acciones que estén en contra o incumplan lo dispuesto en la Ley 29733 o su reglamento. La clasificación de las infracciones es: leve, graves y muy graves. A continuación, los detalles:

Por infracciones leves se consideran:

- Tratar datos personales sin solicitar el consentimiento de los titulares como lo dispone la Ley.
- No atender, impedir u obstaculizar el ejercicio de los derechos del titular de datos personales reconocidos en el título III “Derechos del Titular de Datos Personales”, cuando legalmente proceda.
- Obstaculizar la función fiscalizadora de la ANPDP.

Por infracciones graves se consideran:

- Tratar los datos personales actuando en contra de los principios o disposiciones establecidos en la presente Ley o de su reglamento.
- Incumplir la obligación de confidencialidad establecida en el artículo 17 “Confidencialidad de Datos Personales”.
- No atender, impedir u obstaculizar, en forma sistemática el ejercicio de los derechos del titular de datos personales.
- Obstaculizar de forma sistemática la función fiscalizadora de la ANPDP.
- No inscribir el banco de datos personales en el Registro Nacional de Protección de Datos Personales.

Por infracciones muy graves se consideran:

- Dar tratamiento a los datos personales de manera que incumpla los principios o disposiciones definidos en la Ley o de su reglamento, cuando ello se limite o vulnere los derechos fundamentales.
- Crear, modificar, cancelar o mantener bancos de datos personales incumpliendo las disposiciones de la Ley o su reglamento.

- Proporcionar documentos con información errónea o incompleta a la ANPDP.
- No detener el tratamiento ilícito de datos personales, pese a un previo aviso de la ANPDP.
- No inscribir el banco de datos personales en el Registro Nacional de Protección de Datos Personales, pese a un previo aviso de la ANPDP.

- **Sanciones administrativas**

En caso de incumplimiento de las disposiciones de la Ley o de su reglamento, la ANPDP puede aplicar las siguientes multas:

- Las infracciones leves recibirán una multa mínima desde 0.5 hasta 50 unidades impositivas tributarias (UIT).
- Las infracciones graves recibirán una multa desde más de 5 hasta 50 unidades impositivas tributarias (UIT).
- Las infracciones muy graves recibirán una multa desde más de 50 hasta 100 unidades impositivas tributarias (UIT).

En ningún caso, la multa impuesta puede sobrepasar el 10% de los ingresos brutos anuales del infractor durante el ejercicio anterior.

4.4 Directiva de Seguridad – Autoridad Nacional de Protección de Datos Personales

- **Presentación**

La Autoridad Nacional de Protección de Datos Personales – ANPDP –Ministerio de Justicia y Derechos Humanos, la cual proviene de la segunda disposición complementaria final de la Ley N° 29733, se encargó de elaborar la directiva de seguridad para facilitar el cumplimiento de la Ley a los titulares de los bancos de datos personales.

- **Estructura**

La Directiva de Seguridad se divide en 05 categorías para clasificar a las organizaciones, las cuales son: básico, simple, intermedio, complejo y crítico.

- **Objetivo**

El objetivo principal de la cartilla de seguridad es servir como guía para la implementación de las disposiciones de seguridad indicadas en la Ley N° 29733 y su reglamento.

- **Alcance**

La directiva se aplica a los bancos de datos personales de administración pública o privada conforme a lo establecido en la Ley N° 29733 y su reglamento.

- **Responsabilidades**

Las responsabilidades son asumidas por personas o instituciones que participan en la protección de los datos personales. Estas son las siguientes: Titular de datos personales, titular del banco de datos personales y Autoridad Nacional de Protección de Datos Personales. Sus atribuciones se deberán mantener coherentes y en concordancia con su actuación.

- **Medidas generales**

Para cumplir con lo requerido por el principio de proporcionalidad ubicado en el artículo 7 de la Ley N° 29733, se tienen los siguientes criterios para clasificar el tratamiento de datos personales.

Categoría	Condición de la categoría
Básico	No contiene datos de más de 50 personas.
	Tiene como máximo 5 datos personales (campos).
	No incluye datos sensibles.
	El titular del banco de datos personales es una persona natural.
Simple	No contiene información de más de 100 personas.
	El periodo de tiempo de tratamiento para cumplir con la finalidad es menor a un año.
	No incluye datos sensibles.
	El titular del banco de datos personales es una persona natural o jurídica.
Intermedio	No contiene datos de más de 1000 personas.
	El periodo de tiempo de tratamiento para cumplir con la finalidad es indeterminado o mayor a un año.
	Puede incluir datos sensibles.
	El titular del banco de datos personales es una persona natural o jurídica.

Complejo	El periodo de tiempo de tratamiento para cumplir con la finalidad es indeterminado o mayor a un año.
	El tratamiento es realizado en múltiples localizaciones.
	Puede incluir datos sensibles.
	El titular del banco de datos personales es una persona natural o jurídica.
Crítico	Su finalidad del tratamiento está respaldado por una norma legal.
	El periodo de tiempo de tratamiento para cumplir con la finalidad es indeterminado o mayor a un año.
	El tratamiento es realizado en múltiples localizaciones.
	Puede incluir datos sensibles.
	El titular del banco de datos personales es una persona natural o jurídica.

Tabla 10: Descripción de las categorías de la Directiva de seguridad de banco de datos personales

Fuente: Ministerio de Justicia y Derechos Humanos

- **Criterios de clasificación**

La Directiva de Seguridad establece los siguientes criterios para categorizar los bancos de datos:

- Volumen de registros.
- Número de campos de datos personales.
- Periodo de tiempo para la finalidad del tratamiento de datos personales.
- La titularidad del banco de datos personales (Las entidades públicas están en la categoría Crítico, ya que por Resolución Ministerial 129-2012-PCM está obligada a implementar un SGSI).
- Finalidad del tratamiento de datos personales respaldada por normal legal.
- Múltiples localizaciones.
- Tratamiento de datos sensible.

Figura 5: Gráfica número de datos vs Volumen de información
Elaboración: Directiva de Seguridad

Figura 6: Gráfica de periodo de finalidad vs Volumen de información
Elaboración: Directiva de Seguridad

Figura 7: Gráfica tipo de persona vs Volumen de información

Elaboración: Directiva de Seguridad

- **Medidas de seguridad técnicas**

- Verificar la asignación y monitorear el uso de las credenciales de los usuarios que tengan accesos a los sistemas de información que hacen el tratamiento de los datos personales. Se deberán incorporar las siguientes medidas:

Item	Descripción de medidas por contraseña
1	Pedir a los usuarios mantengan la confidencialidad de las credenciales asignadas.
2	En caso se emplee un servidor de autenticador, se debe verificar la encriptación de las contraseñas.
3	Permitir a los usuarios modificar la contraseña asignada cuando crea conveniente.
4	Las contraseñas deberán tener 8 dígitos entre caracteres alfanuméricos y tener, al menos, un carácter especial.
5	Cuando sea público el acceso al sistema, se debe bloquear al usuario después de 05 intentos incorrectos de autenticación de forma consecutiva.

Tabla 11: Descripción de medidas de contraseña

Fuente: Directiva de Seguridad

- Se debe verificar periódicamente que los accesos a los datos personales sean asignados al personal autorizado. El periodo de revisión deberá realizar de forma semestral, como frecuencia mínima.
- Asegurar el banco de datos personales con accesos físicos con algún mecanismo que solo permita ingresar a personas autorizadas.

Aplica a la categoría de tratamiento				
Básico	Simple	Intermedio	Complejo	Crítico
Ubicar el banco de datos personales en un mueble o similar, con su respectiva cerradura y brindando la llave o similar al operador responsable de su cuidado.	Ubicar el banco de datos personales en un mueble o similar, con su respectiva cerradura y brindando la llave o similar al operador responsable de su cuidado.	En el caso que almacenen datos sensibles, se debe situar el banco de datos personales en un ambiente donde solo pueda ser accedido por el titular del banco o alguna persona autorizado, mediante algún mecanismo de seguridad.	En el caso que almacenen datos sensibles, se debe situar el banco de datos personales en un ambiente donde solo pueda ser accedido por el titular del banco o alguna persona autorizado, mediante algún mecanismo de seguridad.	En el caso que almacenen datos sensibles, se debe situar el banco de datos personales en un ambiente donde solo pueda ser accedido por el titular del banco o alguna persona autorizado, mediante algún mecanismo de seguridad.

Tabla 12: Descripción de resguardo de información por categoría

Fuente: Directiva de Seguridad

- **Flujograma**

Figura 8: Flujo para implementar la Ley 29733

Fuente: Directiva de Seguridad

4.5 Circular G-140

- **Objetivo**

Establecer criterios mínimos para realizar una gestión adecuada de la seguridad de la información, tomando como referencia estándares internacionales como la ISO 27001.

- **Alcance**

La Circular será aplicada a las organizaciones indicadas en los artículos 16° y 17° de la Ley General, así como a las Administradoras Privadas de Fondos de Pensiones (AFP), en adelante empresas. Asimismo, se aplicará al Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI), Cajas Municipales de Ahorro y Crédito (CMAC), Cajas Municipales de Crédito Popular, Corporación Financiera de Desarrollo (COFIDE), Derramas, Banco de la Nación, Banco Agropecuario, Fondo MIVIVIENDA S.A., y Cajas de Beneficios bajo control de la Superintendencia, Fondo de Cajas Municipales de

Ahorro y Crédito (FOCMAC) y la Federación Peruana de Cajas Municipales de Ahorro y Crédito (FEPCMAC).

- **Sistema de Gestión de Seguridad de la Información – SGSI**

La circular impone que las organizaciones establezcan, mantengan y documenten un sistema de gestión de seguridad de la información (SGSI). Las actividades mínimas para desarrollar son las siguientes: definir una política de seguridad de la información aprobada por el Directorio; definir e implementar una metodología de gestión de riesgos mantener los registros a fin de cumplir con las normas, políticas, estándares, procedimientos y otros definidos por la empresa; y contar con pistas de auditoría.

- **Estructura organizacional**

Las empresas deben establecer una estructura organizacional que les permita implementar y mantener un sistema de gestión de la seguridad de la información (SGSI). Además, mediante una unidad especializada o alguna área de la empresa, se pueda velar el cumplimiento de las siguientes funciones:

- Asegurar y comprobar el cumplimiento de Los documentos internos de seguridad.
- Coordinar y monitorear la implementación y entrenamiento de las medidas de seguridad de la información en la organización.
- Llevar a cabo actividades de concientización sobre la seguridad de la información.
- Evaluar los incidentes de seguridad de información y proponer acciones correctivas y preventivas.

La Superintendencia podrá solicitar a la organización la creación de una unidad especializada en seguridad de la información cuando se categorice como Compleja, según la Directiva de seguridad. De igual forma, cuando compruebe el incumplimiento de los criterios previstos en la normativa vigente.

- **Seguridad en operaciones de transferencia de fondos por canales electrónicos**

Las empresas deben implementar un esquema de autenticación para las operaciones de transferencia de fondos por medio de los canales electrónicos. Este consiste en que el cliente se autentique empleando como mínimo dos factores. En el caso de canales

electrónicos por internet, uno de los factores deberá generarse y asignarse de forma dinámica.

- **Subcontratación**

Las organizaciones deberán hacerse responsables de mantener las características de seguridad de la información indicadas en la presente norma, inclusive si todas o algunas de las funciones o procesos son realizadas por terceros, a través de una subcontratación. Se debe considerar lo dispuesto en el Reglamento de la Gestión Integral de Riesgos. Asimismo, las empresas subcontratadas deben tener la información adecuadamente aislada en todo momento (SBS, 2009).

4.6 ISO/IEC 27001:2014 - Sistema de Gestión de Seguridad de la Información

- **Objetivo**

Esta norma detalla los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información en una organización.

- **Referencia normativa**

La norma internacional en la cual está basada es la ISO/IEC 2700, Information Technology. Security Technology Techniques. Information Security Management Systems. Overview and Vocabulary.

- **Contexto de la organización**

Se requiere entender el contexto de la organización, las necesidades y expectativas de las partes interesadas, así como los aspectos internos y externos que afectan el propósito y la capacidad de lograr los resultados deseados de la implementación del sistema de gestión de seguridad de la información, según el alcance que se le haya definido.

- **Liderazgo**

La alta dirección debe liderar y comprometerse a la aplicación y cumplimiento del SGSI. Ello implica establecer una política de seguridad de la información que corresponda al propósito de la organización incluyendo en ella los objetivos de seguridad de la información o proporcionando el marco de referencia para definirlo. Además, la política debe incorporar el compromiso de satisfacción de los requisitos aplicables de seguridad de la información o el de la mejora continua. Asimismo, la política deberá ser

documentada, comunicada y disponible para los miembros de la organización y las partes interesadas, según sea apropiado.

Por último, la alta dirección debe asignar y comunicar las responsabilidades y la autoridad para los roles de seguridad de la información.

- **Planificación**

Para planificar asuntos correspondientes al sistema de gestión de seguridad de la información, la organización deberá acudir a los asuntos referidos en el punto 6.3.1 de la presente norma y los requisitos del numeral 6.3.2, y determinar los riesgos y oportunidades que necesitan ser tratados.

- **Soporte**

La organización debe contar con recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI.

Las personas encargadas de la seguridad de la información en la organización deberán estar preparados sobre la base de educación y experiencia. En caso no cumpla con lo anterior, la organización deberá contratar personas preparadas y evaluar su efectividad, asimismo, solicitar información documentada como evidencia de competencia.

Por otra parte, las personas de seguridad de la información que sean parten de una organización, deben ser conscientes de la política de seguridad de información y su beneficio a la efectividad del SGSI.

Para las comunicaciones internas y externas, las organizaciones deben definir el contenido que se comunicará, el tiempo en que se realizará, los receptores, el emisor y los procesos por los cuales la comunicación debe ser efectuada.

4.7 Project Management Body of Knowledge – PMBOK

- **Definiciones generales**

Nº	Áreas	Proyecto	Programa	Portafolio
1	Alcance	Poseen un alcance reducido y entregables específicos	Poseen un alcance más amplio que podría cambiar para satisfacer las	Poseen un alcance que cambia de acuerdo con los objetivos

			expectativas de beneficios de la organización.	estratégicos de la organización.
2	Cambios	El director de proyecto mantiene los cambios a un mínimo.	El director del programa debe esperar cambios y aceptarlos.	El director de portafolio monitorea continuamente los cambios en el entorno organizacional.
3	Criterios de éxito	El éxito se mide si el proyecto está dentro del presupuesto establecido, entregado dentro del tiempo establecido y los productos entregados de acuerdo con las especificaciones.	El éxito es medido en términos de retorno de la inversión (ROI), las nuevas capacidades creadas y los beneficios obtenidos.	El éxito se mide en términos del rendimiento global de los componentes del portafolio.
4	Administración	El director del proyecto administra especialistas, técnicos, etc.	El director del programa administra a otros directores de proyectos.	El director del portafolio puede administrar y coordinar todo el personal de la cartera de proyectos.

Tabla 13: Definición de conceptos generales del PMBOK

Fuente: Project Management Institute - PMI

- **Marco general**

Es una guía para la dirección de proyectos y describe el conocimiento y prácticas aplicables a la mayoría de los proyectos desde que se inicia hasta su finalización. Esta guía brinda normas, métodos, procesos y prácticas establecidas. Además, de un vocabulario propio para la dirección de proyectos. Debemos entender por proyecto, según la definición del PMBOK en su sexta edición, al esfuerzo temporal que se lleva a

cabo para crear un producto, servicio o resultado único. Por su naturaleza, un proyecto tiene un principio y un final definidos. Esta guía ha sido desarrollada por Project Management Institute, una organización que tiene por socios a profesionales interesados y relacionados con la Gestión de Proyectos.

- **Grupos de procesos**

El PMBOK se divide en 05 grupos de procesos de gestión, los cuales son:

Grupo de proceso	Descripción del grupo
Inicio	Grupo relacionado a la definición de un proyecto nuevo o una fase en un proyecto existente.
Planificación	En este grupo se establece el alcance, los objetivos y el plan de acción para cumplir los objetivos.
Ejecución	En este grupo se tienen conjuntos de actividades o procesos que deben desarrollarse para cumplir los objetivos.
Monitoreo y Control	En este grupo se rastrea y revisa el desempeño del proyecto.
Cierre	En este grupo se realizan las actividades para realizar el fin del proyecto.

Tabla 14: Descripción de grupos de procesos

Fuente: Project Management Institute – PMI

- **Áreas de conocimientos**

El PMBOK identifica 10 áreas de conocimiento que son (PMI, 2014):

Área de conocimiento	Descripción del área
Gestión de la integración	Consiste en decidir sobre los recursos asignados, gestión de interdependencia entre las áreas de conocimiento y el balance de objetivos.
Gestión del alcance	Define y controlar lo que se incluye y no se incluye en el proyecto. Ello incluye los procesos requeridos para garantizar que el proyecto tenga definido todo el trabajo necesario para completarlo exitosamente.

Gestión del tiempo	Define las actividades y secuencias del proyecto, estima recursos para cada actividad, programa la duración de las actividades, y elaborar y controlar el cronograma para finalizar el proyecto.
Gestión de los costos	Estima, presupuesta y controla los costos con la finalidad de que el presupuesto del proyecto sea aprobado.
Gestión de la calidad	Determina los objetivos, políticas y responsabilidades de calidad para que el proyecto sea ejecutado adecuadamente y conforme a los stakeholders.
Gestión de los recursos humanos	Considera los procesos relacionados con la organización, gestión y conducción del equipo del proyecto. Se les asigna roles y responsabilidades a las personas del equipo para completar el proyecto
Gestión de las comunicaciones	Implementa los procesos para transmitir la información del proyecto a todos los involucrados de forma adecuada y oportuna.
Gestión de los riesgos	Desarrolla los procesos relacionados con la planificación, identificación, análisis y respuesta ante los riesgos. Además, se encarga del monitoreo, control y mitigación en un proyecto.
Gestión de las adquisiciones	Consiste en los procesos de compra o adquisición de insumos, bienes y servicios que se requiere para llevar a cabo el proyecto hasta su finalización.
Gestión de los interesados	Desarrolla los procesos de identificación de las personas, grupos u organizaciones que pueden afectar o ser afectados por el proyecto. Se requiere conocer y evaluar sus expectativas y el impacto en el proyecto.

Tabla 15: Definición de áreas de conocimiento

Fuente: Project Management Institute - PMI

5 CAPÍTULO 4: DESARROLLO DEL PROYECTO

En este capítulo se procederá a describir los puntos específicos que se llevaron a cabo para realizar el proyecto adecuadamente. Asimismo, se describen de forma detallada los objetivos planteados, los cuales van a permitir darle una solución eficaz al problema general.

5.1 Análisis de los estándares internacionales, marcos de trabajo y buenas prácticas de seguridad de la información

Para proteger los datos personales es necesario conocer los procedimientos, métodos, técnicas o tecnologías ya definidas, estudiadas y comprobadas que brinden seguridad a la información, especialmente, a aquellas que corresponden a los clientes, colaboradores y proveedores de las microfinancieras. Por ello, en esta sección se explicará el análisis realizado para determinar los estándares internacionales, marcos de trabajo y buenas prácticas de seguridad de la información con controles más adecuados a la realidad de las entidades microfinancieras.

5.1.1 Análisis de los macroprocesos de las microfinancieras

El proyecto, necesitaba entender cómo funciona una microfinanciera en términos de negocio, por ello se realizó el estudio de 17 proyectos de tesis acerca del sector microfinanciero, con el fin de obtener los macroprocesos referenciales de estas entidades y con esta información poder analizarla desde el punto de vista de los criterios de categorización impuestos por la Directiva de Seguridad.

Categoría	Macroprocesos	Criterios					Resultado
		Titularidad de datos personales	Datos personales	Tratamiento de datos sensibles	Tratamiento en múltiples localizaciones	Transferencia de datos personales	
Estratégico	Gestión de Planificación	-	-	-	- Sede Central, a cargo del área de Planeamiento y Presupuesto	-	No Aplica
	Gestión de Seguimiento y Control	- Clientes - Clientes Potenciales	- Registro de cliente (Nombres, Apellidos, DNI, correo electrónico, teléfono, monto de préstamo)	- Patrimonio	- Agencias a nivel nacional	Interna: Los datos personales del cliente se envían a las personas encargadas de ejecutar el proceso de Recuperaciones cuando el cliente tenga pagos	Aplica

						pendientes de realizar.	
	Marketing	<ul style="list-style-type: none"> - Clientes capturados - Clientes de base de datos adquiridos 	<ul style="list-style-type: none"> - Registro de cliente (Nombres, Apellidos, DNI, correo electrónico, dirección de vivienda, sueldo) 	<ul style="list-style-type: none"> - Sueldos - Cuenta de ahorros 	<ul style="list-style-type: none"> - Sede Central, a cargo de la Gerencia de Marketing 	<p>Externa: Los datos personales llegan a la empresa mediante la compra de base de datos a un proveedor a solicitud del área de Marketing.</p> <p>Interna: Los datos personales se envían al área de Sistemas para que realice su proceso de Gestión de la capacidad y configuración, con la finalidad que los datos estén</p>	Aplica

						disponibles en los sistemas de la microfinanciera.	
Operativos	Inversiones	- Clientes	- Registro de cliente (Nombres, Apellidos, DNI, correo electrónico, teléfono, sueldo, cuenta de ahorros)	- Sueldos - Cuenta de ahorros	- Agencias a nivel nacional	Interna: Los datos personales del cliente quien deposita un monto para la inversión son enviados al área de colocaciones para contabilidad para el registro al balance de la empresa.	Aplica
	Operaciones	- Clientes	- Registro de cliente (Nombres,		- Agencias a nivel nacional	Externa: Los datos personales del cliente se envía a la	No Aplica

			Apellidos, DNI, teléfono, número de cuenta, Monto de inversión ganado)			entidad bancaria donde se depositará el monto de inversión ganado.	
	Colocaciones	- Clientes Potenciales	- Registro de cliente (Nombres, Apellidos, DNI, correo electrónico, teléfono, sueldo, cuenta de ahorros)	- Sueldos - Cuenta de ahorros	- Agencias a nivel nacional	Interna: Los datos personales del cliente quien deposita periódicamente el monto el cual fue prestado, se envían a las áreas de Cobranzas y Recuperaciones para que se realice un seguimiento de los pagos. Además, el área de Crédito	Aplica

						envía las colocaciones del cliente al área de Operaciones para el depósito.	
	Recuperaciones	- Clientes	- Registro de cliente (Nombres, apellidos, N° DNI, Teléfono, Correo, Dirección de vivienda, Sueldo, Cuenta de ahorros, Nombres de aval, Apellidos de aval, N° DNI de aval)	- Sueldos - Cuenta de ahorros del cliente - Cuenta de ahorros del aval	- Agencias a nivel nacional	-	Aplica

	Captaciones	- Clientes	<ul style="list-style-type: none"> - Ficha de inscripción (Nombres, apellidos, N° DNI, Teléfono, Correo, Dirección de vivienda) - Formulario de registro (Nombres, apellidos, N° DNI, Teléfono, Correo, Dirección de vivienda, Sueldo, Nivel crediticio, Nombres de aval, Apellidos 	<ul style="list-style-type: none"> - Sueldo - Cuenta de ahorros 	- Agencias a nivel nacional	<p>Interna: Los datos personales se envían al área de Marketing y al Comité de Riesgo Crediticio. El área de Marketing emplea esta información para la segmentación de los clientes potenciales y actuales, y promoción de ofertas. El comité de riesgo crediticio recibe esta información para la evaluación del cliente mediante el sistema SENTINEL</p>	Aplica
--	-------------	------------	---	---	-----------------------------	--	--------

			de aval, N° DNI de aval)			y provisionar dinero al que la microfinanciera está expuesta.	
	Riesgo Operativo	-	-	-	- Sede Central, a cargo del Comité de Riesgos Operativos	-	No Aplica
	Riesgo Crediticio	- Clientes	Registro de cliente (Nombres, apellidos, N° DNI, Teléfono, Correo, Dirección de vivienda, Sueldo, Cuenta de ahorros)	- Sueldo	- Agencias a nivel nacional	Externa: Los datos personales se le envían a la empresa SENTINEL para emplear el servicio de visualización de deudas de sus clientes.	Aplica

	Riesgo de Mercado	-	-	-	- Sede Central, a cargo del Comité de Riesgos de Mercado	-	No Aplica
Apoyo	Logística	- Proveedores - Videovigilancia	- Ficha de identificación (Nombres, apellidos, N° DNI, Teléfono, Correo, Dirección de vivienda)	-	- Sede Central, a cargo de la Gerencia de Logística	-	No Aplica
	Gestión de Recursos Humanos	- Postulantes - Colaboradores - Proveedores	- Curriculum Vitae (Nombres, apellidos, N° DNI, teléfono, correo, dirección de vivienda)	- Antecedentes policiales - Sueldo - Historial Médico - Historial Financiero	- Sede Central, a cargo de la Gerencia de Recursos Humanos	Interna: Los datos personales del postulante son enviados a la Gerencia solicitante del nuevo colaborador. Asimismo, estos	Aplica

			<ul style="list-style-type: none"> - Copia de DNI (Nombres, apellidos, N° DNI, Dirección de vivienda) - Copia de Antecedentes Policiales (Nombres, apellidos, N° DNI, antecedentes policiales) - Copia de Título profesional (Nombres, apellidos, N° DNI, nivel de educación) 			<p>datos son enviados a la Gerencia de Sistemas para la creación de las cuentas a los sistemas requeridos para su labor. También, los datos son enviados al mismo empleado de forma electrónica presentados en boleta de pago.</p>	
--	--	--	--	--	--	--	--

			- Contrato (Nombres, apellidos, N° DNI, Sueldo)				
	Soporte Tecnológico	- Clientes - Clientes Potenciales - Empleados - Proveedores	- Hoja de cálculo con nuestros usuarios (Nombres, apellidos, N° DNI, teléfono, correo, dirección de vivienda, Sueldo). - Clientes (Nombres,	- Sueldo - Cuenta de ahorros	- Sede Central, a cargo de la Gerencia de Sistemas	Interna: Los datos personales se envían al área de Recursos Humanos y al Comité de Riesgo Crediticio. El área de Recursos Humanos emplea esta información para conocer y notificar las cuentas de los usuarios creados (nuevos	Aplica

			apellidos, N° DNI, teléfono, correo, dirección de vivienda, Sueldo, cuenta de ahorros)			ingresantes a la empresa) en los sistemas. El comité de riesgo crediticio consulta la información para verificar el nivel crediticio del cliente y si es apto para el producto adquirir.	
	Contabilidad	-	-	-	- Sede Central, a cargo de la Gerencia de Contabilidad	-	No Aplica
	Asesoría Legal	-	-	-	- Sede Central, a cargo de la Gerencia de Legal	-	No Aplica

Tabla 16: Macroprocesos vs Criticidad del tratamiento de datos personales

Con esta información, se pudo estructurar cómo circula y se almacenan los datos personales en una microfinanciera. Además, cuáles son los procesos críticos que generan mayores transacciones con los datos.

5.1.2 Elección de las medidas de seguridad

Para poder evaluar los estándares internacionales, marcos de trabajo y buenas prácticas de seguridad de la información, primero, se determinó las medidas en las cuales estará basado el análisis. Estas medidas comprenden los criterios de seguridad de información que deben cumplir las microfinancieras. En base a la literatura estudiada y la Ley 29733 – Ley de protección de datos personales, se determinó las siguientes medidas básicas para proteger los datos personales en entidades microfinancieras:

- **Consentimiento:** Se refiere a la aceptación por parte del titular de los datos personales para el tratamiento de sus datos personales a cargo de la organización quien solicita recopilarlos. Ello puede incluir información sensible.
- **Transferencia de datos:** Consiste en la aceptación de la solicitud realizada al titular de los datos personales para compartir sus datos con entidades ajenas a la institución que prestan servicios de tratamiento.
- **Registro del banco de datos personales:** Consiste en la declaración de los bancos de datos personales y códigos de conducta de la organización a la Autoridad Nacional de Protección de Datos Personales (ANPDP).
- **Derechos fundamentales del titular de datos personales:** Son las disposiciones que permiten al titular de los datos personales, el acceso, rectificación, cancelación y oposición (ARCO por sus siglas en inglés) al tratamiento de sus datos personales.
- **Subcontratos:** Son normas que regulan los requisitos que deben cumplir las contrataciones de terceros antes de ofrecer sus servicios de tratamiento de datos personales.
- **Videovigilancia:** Son las disposiciones que establece la manera en que se deberán tratar los datos personales a través de sistemas de videovigilancia con fines de seguridad.
- **Políticas de seguridad de información:** Brindar documentos formales y controles necesarios para adaptar la organización a un entorno que contempla las bases de la seguridad de la información.

- **Gestión de activos:** Brinda los controles para resguardar los activos físicos (desktop, laptops, servidores, entre otros), los cuales gestionan datos personales.
- **Riesgos de seguridad:** Brinda procesos claves (recopilar, analizar, resolver y responder) para gestionar adecuadamente los riesgos relacionados a la seguridad de la información.
- **Seguridad de RR. HH:** Brinda pautas para concientizar y capacitar al personal (interno y externo) en la importancia de la seguridad de la información.
- **Incidentes de seguridad:** Brinda pautas para la gestión de incidentes relacionados a la seguridad de la información, la cual se promueve el uso de reportes para determinar las mejores acciones ante un evento.
- **Continuidad de la seguridad:** Brinda pautas para dar continuidad a la seguridad de la información luego de presentarse alguna interrupción en las operaciones.
- **Seguridad Interna:** Brinda consideraciones para proteger los centros de datos contra acciones de usuarios internos que pongan en riesgo la exposición a amenazas externa.
- **Seguridad Perimetral:** Brinda pautas para la detección y seguimiento de intrusos que intentan ingresar de forma no autorizada al perímetro de la empresa.
- **Gestión de Accesos Lógicos:** Brinda requisitos para el control de accesos a los sistemas de información de la organización.
- **Gestión de Accesos Físicos:** Brinda requisitos para el control de accesos físicos de la organización.
- **Cifrado:** Brinda pautas para el uso de las claves criptográficas en la organización.

5.1.3 Análisis de los estándares y marcos de trabajo de seguridad de la información

En la actualidad existen muchos estándares, marcos de trabajo y buenas prácticas de seguridad de información que ofrecen una variedad de controles aplicados a contextos específicos. Incluso algunos de estos documentos son una combinación o derivados de otros estándares y marcos de trabajo. En el siguiente análisis se comparará los mejores marcos de trabajos, estándares y buenas prácticas de seguridad que tienen controles más completos y con reconocimientos por instituciones que los han implementados. A continuación, se listará los elementos a comparar:

- COBIT 5 – Objetivos de Control para la Información y Tecnologías Relacionadas
- ISO 27001 – Sistema de Gestión de Seguridad de la Información (Requisitos)

- ISA 62433-2-1 – Seguridad para Automatización Industrial y Sistemas de Control (Establecimiento de un Programa de Seguridad de Sistemas de Control y Automatización Industrial)
- NIST 800-54 – Controles de Seguridad y Privacidad para Sistemas y Organizaciones Federales de Información
- CSICSC V7.1 v7.1 – Los controles de Seguridad Críticos de la CIS para una defensa cibernética efectiva.

Cada uno de los documentos mencionados anteriormente contiene una serie de controles y procesos orientados de satisfacer el aseguramiento de la información. En el punto siguiente, se procederá a listar los controles/procesos de cada estándar, marco de trabajo o buena práctica de seguridad de la información según las medidas de protección de datos personales. Posteriormente, se analizará la pertinencia de cada estándar/marco de trabajo respecto de las categorías elaboradas para la protección de datos personales.

Controles para usar según el estándar de seguridad de la información y/o seguridad informática respectivo					
Categorías	COBIT 5	ISO 27001	ISA 68443	NIST 800-53	CSI CSC 7.1
Política Seguridad de la Información	APO01.08, MEA03.02, MEA03.03, EDM01.02, APO13.02, MEA03.01 y MEA03.04	A.5.1.1, A.5.1.2, A.6.1.1, A.7.2.1, A.6.1.2, A.10.1.1, A.11.2.9, A.6.2.1, A.7.2.2, A.8.2.1, A.9.1.1, A.11.1, A.12.1.4, A.12.2.1, A.12.3.1, A.14.2.1, A.15.1.1, A.16.1.1, A.17.1.1, A.18.1.4 y A.18.2.1	4.3.2.6.1, 4.3.2.6.2, 4.3.2.6.4, 4.3.2.6.6, 4.3.2.6.7, 4.3.3.5.1, 4.3.3.6.6 y 4.3.3.7.1	AC-1	N/A
Gestión de Activos	BAI09.01, BAI09.02, BAI09.03, BAI09.04, BAI09.05, DSS05.02 y APO02.02	A.8.1.1, A.8.1.2, A.8.1.4, A.11.2.4, A.11.2.5 y A.11.2.8	4.2.3.4, 4.2.3.6 y 4.3.2.3.3	CM-8, RA-2 y PE-16	CSC 1, CSC 2
Gestión de Accesos Lógicos	DSS05.03, DSS05.04 y DSS06.03	A.6.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6, A.9.4.1 y A.9.4.4	4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.2, 4.3.3.7.3 y 4.3.3.7.4	PL-4, PS-4, AC-2, AC-3, AC-6, AC-7, CM-5 y IA-5.	CSC 5, CSC 12, CSC 14, CSC 15 y CSC 16

Gestión de Riesgos	APO12.01, APO12.02, APO12.03 y APO12.06	A.7.1.1, A.11.2.1, A.11.2.6, A.12.1.4, A.12.6.1, A.12.6.2, A.15.1.2, A.15.1.3, A.15.2.1 y A.15.2.2	4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.5, 4.2.3.6, 4.2.3.7, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.11, 4.2.3.12, 4.2.3.13 y 4.2.3.14	MP-5, PE-17, M-4, RA-3, RA-5, SI-2, SI-5, SA-4 y SA- 12	CSC 4, CSC 19 y CSC 20
Gestión de Recursos Humanos	APO07.01, APO07.02, APO07.03, APO 07.04, APO 07.05, APO07.06 y BAI05.07	A.6.1.1, A.7.2.2 y A.7.2.3	4.3.2.4.1, 4.3.2.4.2, 4.3.2.4.3, 4.3.2.4.4, 4.3.2.4.5 y 4.3.2.4.6.	AT-2, AT-3, AT-4 e IR-2	N/A
Cifrado	N/A	A.10.1.2	N/A	SC-13	CSC 15 y CSC 16
Gestión de Accesos Físicos	DSS01.04, DSS05.05 y DSS05.07	A.11.1.1, A.11.1.2, A.11.1.5 y A.11.1.6	4.3.3.7.2	PE-9, PE-13, PE- 14, PE-15, PE-10, PE-11, PE-4, PE- 16, PE-17, MA-2, MP-5 y MP-4	N/A
Gestión de Continuidad de Seguridad de la Información	DSS04.01, DSS04.02, DSS04.03, DSS04.04, DSS04.06, DSS04.07 y DSS04.08.	A.17.1.1, A.17.1.2 y A.17.1.3	4.3.2.5.1, 4.3.2.5.2, 4.3.2.5.3, 4.3.2.5.4, 4.3.2.5.5, 4.3.2.5.6 y 4.3.2.5.7	CP-2, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11 y CP-13	N/A

Gestión de Incidentes	BAI04.02, DSS02.01, DSS02.02, DSS02.03, DSS02.04, DSS02.05, DSS02.06 y DSS02.07	A.16.1.1, A.16.1.2, A.16.1.3 y A.16.1.5	4.3.4.5.1, 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4, 4.3.4.5.5, 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8, 4.3.4.5.9, 4.3.4.5.10, 4.3.4.5.11 y 4.4.3.4.	IR-8, AU-6, SI-2 y IR-4	CSC 19
------------------------------	--	--	---	----------------------------	--------

Tabla 17: Controles para usar según el estándar de seguridad de la información y/o seguridad informática

Elaboración: Propia

A continuación, se realizará el análisis de los estándares, marcos de trabajo y buenas prácticas de seguridad de información, con el fin de verificar cuál es la opción adecuada para cada categoría de protección de datos personales, respectivamente.

Comparación del estándar internacional de seguridad de la información y/o seguridad informática

Categorías	COBIT 5	ISO 27001	ISA 68443	NIST 800-53	CSI CSC 7.1
Política Seguridad de la Información	07 procesos con indicaciones de la creación de políticas, procedimientos y manuales para la seguridad de la información. Por otro lado, toda gira en torno a un Gobierno TI, por lo cual se desvía un poco el principio de proteger los datos personales.	22 controles con indicaciones para la creación de Políticas de Seguridad de la Información, realizar revisiones de las políticas, el marco legal, asignar responsabilidad. Se genera un entorno con predisposición para darle un enfoque a la protección de datos personales.	08 controles con indicaciones para una correcta implementación, desarrollo y seguimientos de Políticas de Ciberseguridad, Por ende, este estándar de seguridad está orientado a la Ciberseguridad, no a la seguridad de la información	01 control indicando la implementación de una Política para la Gestión de Accesos Lógicos	No hay información
Gestión de Activos	07 procesos que permite administrar de forma correcta los activos de la organización. Aunque solo toma dos componentes, como lo son el software y hardware, dejando de lado el concepto de activo de información, donde también pueden entrar documentos físicos, en los cuales	07 controles orientados a la protección de activo de información. Dentro de lo cual está estipulado el inventario, tener un propietario, y procesos que permitan proteger los datos personales que en esos activos conlleve.	03 controles que abarca el control de sistemas de información.	03 controles orientas a la gestión de activos lógicos. Donde se pide el inventario, priorización (Categorización) y remoción.	02 controles orientas a inventariar el hardware y software de la compañía

	puede haber datos personales				
Gestión de Accesos Lógicos	03 procesos en los que indica la segregación de funciones, las definiciones de roles, responsabilidades sobre los accesos a la información (Sistemas).	11 controles que indican los puntos que se deben considerar para realizar una correcta gestión de accesos lógicos. Como la segregación de tareas, registro de usuario, login, autenticación, uso de privilegios, entre otros.	17 controles muy específicos en temas de autenticación, estrategia de cuentas, contraseñas de acceso y retirar de usuarios cesados, pero están orientado a Sistema Industriales.	Brinda 08 controles, los cuales indican la autenticación, privilegios mínimos, gestión de cuentas, pero no abarcan los temas de contraseña, login y segregación de funciones.	05 controles que están orientados a la estructura lógico-interna de los sistemas de información. No a requisitos que deben cumplirse para un adecuado control de accesos lógicos.

Gestión de Riesgos	09 procesos que indican cómo se debe proceder ante los riesgos, desde el recopilado de datos, análisis de riesgo, tener una base de datos con los riesgos asociados y la gestión debida para responder ante ellos.	11 controles, pero ninguna habla específicamente sobre cómo se debe proceder ante los riesgos en forma secuencial. Cada control tiene un escenario diferente, con sus riesgos asociados.	14 controles dentro de los cuales brinda una secuencia de pasos concretos para la adecuada gestión de riesgos, como realizar una evaluación de riesgos, priorizar los sistemas, evaluación de vulnerabilidades, metodología de evaluación de riesgo, documentación, entre otros. Aun así, toca temas del sector industrial, pero siguen en la línea de proteger los activos de información.	09 controles donde indica realizar la evaluación de riesgos y vulnerabilidad. Además, se preocupa mucho en los proveedores y los riesgos que incluye hacer negocios con ellos.	03 controles en los que indica la evaluación constante de vulnerabilidades y pruebas con el equipo rojo para descartar futuros eventos negativos en la organización.
Gestión de Recursos Humanos	07 procesos que indican que los recursos humanos deben ser medibles, en términos de su capacidad, desempeño y cantidad (tiene que ser lo suficiente para lograr los objetivos de la organización). Además, identificar al personal clave de TI para evitar	03 controles que indican que 04 pasos puntuales: Responsabilidades, Capacitación, Concientización y Sanciones. Con el sentido de seguridad de la información en cada uno de los pasos, se puede dar un mayor enfoque a la protección de datos personales.	06 controles que indican que al personal se le debe capacitar, darle capacitaciones basado en un programa de entrenamiento. Además, supervisar y revisar este programa, y mantener un histórico de ello. Todo ello, basado en la ciberseguridad.	04 controles que indican que debe realizarse un entrenamiento de conciencia de seguridad a todo el personal. Además, este debe ser realizado de acuerdo con el rol que desempeñan en la organización. Asimismo, guardar un	No hay información.

	retrasos por posibles renuncias / despidos. Por último, habla de las capacitaciones que se les brinda a los usuarios para que cumplan con sus funciones de forma óptima.			registro de las capacitaciones que se hayan realizado. Por último, brindarle información sobre las funciones que deben realizar con respecto a incidentes.	
Cifrado	No brinda información.	01 control que indica que se debe desarrollar una política de uso de controles criptográficos para proteger la información.	No hay información.	03 controles que indican el establecimiento de claves criptográficas. Además, procesos criptográficos y el tipo de criptografía que se requiere para cada componente, en base al marco legal vigente.	01 control orientado específicamente al hash que se deberían implementar por tipo de tecnología. Asimismo, los campos que deberían considerarse para el cifrado.
Gestión de Accesos Físicos	03 procesos orientados al control de accesos físicos, como gestión del entorno, gestionar los accesos a la infraestructura TI. Aun así, no brinda información sobre el control a accesos físicos donde están	06 controles que abarcan la protección de los espacios ambientales de trabajo, velando por la protección de los activos de información (documentos, software, hardware). Asimismo, el control de ingreso y un agregado si la	01 control general sobre la gestión de los espacios físicos (candados, cerraduras, etc).	12 controles que indican mecanismos de protección en caso de emergencia sobre las instalaciones que alojan información de la organización. Además, indicaciones para contar con un sitio alternativo en caso de	No hay información.

	almacenados activos físicos como documentación con información confidencial.	organización transporta sus activos a otros lugares.		emergencia, y qué empleados deben contar con acceso a ello.	
Gestión de Continuidad de Seguridad de la Información	07 controles que solicitan contar con una política de continuidad de negocio, realizar ejercicios para probar y revisar el BCP. Además, gestionar acuerdos de respaldo para mantener la disponibilidad de la información.	04 controles que solicitan que se cuenten con planes para la continuidad de la seguridad de la información, así como proceso, procedimientos y controles extras para garantizar un nivel requerido básico de seguridad. Así como un adecuado respaldo de la información para continuar con las operaciones del negocio.	07 controles orientados a identificar qué activo debe ser considerado para agregarlo al plan de continuidad, una evaluación para ver el impacto que conllevaría no tener operativo un activo. Además, desarrollar el plan, definir los roles y responsabilidades. Por último, probar el plan y actualizarlo para subsanar los inconvenientes que se hayan encontrado.	09 controles que solicitan la creación de un plan de contingencia, realizar las pruebas necesarias, contar con un sitio alternativo para levantar los activos pertinentes (con un adecuado servicio de telecomunicaciones y el respaldo de los datos). Por último, solicita emplear mecanismos de seguridad alternativa para satisfacer las necesidades principales de seguridad.	No hay información.

Gestión de Incidentes	08 procesos que permiten identificar los activos importantes del negocio, clasificación de incidentes, peticiones de servicio. Además, implementar procedimientos para el tratamiento de incidentes. Por último, localizar los incidentes, resolverlos, cerrar las peticiones de servicio y generar informes de ser el caso (ISACA, 2012).	07 controles en los cuales se solicita brindar las responsabilidades y procedimientos para resolver los incidentes de seguridad. Se debe contar con una plataforma o canal para reportar los incidentes. Además, los colaboradores deben reportar cualquier anomalía que surge. Por último, evaluar, responder y aprender de los incidentes resueltos (ISO/IEC, 2013).	12 controles orientados a la implementación de procedimientos para responder ante incidentes. Además, se solicita la comunicación, el plan de respuesta y educar a los colaboradores en la denuncia de los incidentes. Asimismo, solicita que se debe documentar, comunicar los resultados de los incidentes resueltos. Por último, realizar simulacros para anticiparse a los eventos relaciones a incidentes de seguridad cibernética (ISA, 2018).	04 controles que solicitan un plan de respuesta ante incidentes dentro de la organización. Asimismo, realizar la revisión de auditoría para encontrar hallazgos que ayuden a esclarecer el incidente. Por último, solicita que la empresa que la empresa debe contemplar procesos para la detección, análisis, contención, erradicación y recuperación. Todo ello con respecto a incidentes de ciberseguridad (NIST, 2013).	01 control que indica las pautas que se deben tomar en cuenta para una correcta respuesta ante incidentes. Por ejemplo, planes, roles, funciones, capacitación, comunicaciones, supervisión de la administración. Todo ello, ligado a incidentes de seguridad informática. No contempla incidentes con activos de información físicos (documentos) (CIS, 2015).
------------------------------	--	--	--	---	---

Tabla 18: Comparación del estándar internacional de seguridad de la información y/o seguridad informática

Elaboración: Propia

5.1.4 Conclusiones del análisis

Luego del análisis realizado, se eligieron los estándares, marcos de trabajo y buenas prácticas de seguridad de la información más adecuados a las medidas de protección de datos personales. A continuación, los resultados del análisis:

➤ **Política de Seguridad de la Información**

Este proceso estará basado en el estándar internacional ISO 27001 “Sistema de Gestión de Seguridad de la Información - Requisitos” edición del 2013, porque brinda las políticas necesarias para adaptar la organización a un entorno que contempla las bases de la seguridad de la información. Además, contempla el marco legal y normativo impuesto por el gobierno. Por último, sugiere una constante revisión de los documentos para su actualización de ser necesarios.

➤ **Gestión de Activos**

Este proceso estará basado en el estándar internacional ISO 27001 “Sistema de Gestión de Seguridad de la Información - Requisitos” edición del 2013, pues brinda los requisitos necesarios para velar por la protección de los activos de información de la organización. Puesto que, es el único estándar / marco de trabajo que pone énfasis en los activos que no son hardware ni software. Solicita el inventario, revisión, asignación de propietario y trámite para el desuso.

➤ **Gestión de Accesos Lógicos**

Este proceso estará basado en el estándar internacional ISO 27001 “Sistema de Gestión de Seguridad de la Información - Requisitos” edición del 2013, porque brinda los requisitos necesarios para un adecuado control de accesos en la organización. Solicita la creación de procedimientos para adoptar medidas en cuanto a privilegios, segregación de funciones, interfaz de conexión al sistema y realizar revisiones periódicas, de esta manera revisar a los usuarios que tienen acceso a los sistemas de información de la organización.

➤ **Gestión de Accesos Físicos**

Este proceso estará basado en el estándar internacional ISO 27001 “Sistema de Gestión de Seguridad de la Información - Requisitos” edición del 2013, porque brinda los requisitos necesarios para un adecuado control de accesos físicos en la organización. Solicita la creación de procedimientos, adaptación de procesos, para un adecuado control de ingreso y gestión del espacio de trabajo seguro. En estos ambientes pueden estar almacenados de forma física o lógica información

confidencial de la organización, dentro de esta información pueden encontrarse datos personales / sensibles.

➤ **Gestión del Riesgos**

Este proceso estará basado en el marco de trabajo COBIT 5 “Objetivos de Control para la Información y Tecnologías Relacionadas”, porque brinda procesos específicos para una adecuada gestión de los riesgos relacionados a la seguridad de la información de la empresa. Puesto que, recopila datos relacionados, analiza el riesgo, mantiene un perfil de riesgo, gestiona el riesgo en los proveedores y la planificación de respuesta. Es el documento más completo, el cual mantiene un ciclo de riesgo adecuado.

➤ **Gestión de Seguridad en RRHH**

Este proceso estará basado en el estándar internacional ISO 27001 “Sistema de Gestión de Seguridad de la Información - Requisitos” edición del 2013, porque brinda los controles necesarios para concientizar y capacitar al personal (interno y externo) en la importancia de la seguridad de la información. Además, abarca el tema de sanciones para colaboradores que incurran continuamente en contra de la organización.

➤ **Cifrado**

Este proceso estará basado en el estándar internacional de ciberseguridad NIST 800-54 “Controles de Seguridad y Privacidad para Sistemas de Información y Organizaciones Federales”, porque brinda controles que permiten un adecuado uso de las claves criptográficas establecidas por la organización. Además, indican que estos procedimientos deben estar establecidos por mandato regulatorio y validación por un proveedor especialista en el cifrado.

➤ **Seguridad Interna**

Este proceso estará basado en el estándar internacional “CSC Center for Internet Security versión 7.1”, porque brinda controles específicos para resguardar la red interna de la organización, tales como detección antimalware, gestión de dispositivos interconectados, configuraciones para la prevención de pérdida de datos, entre otros.

➤ **Seguridad Perimetral**

Este proceso estará basado en el estándar internacional “CSC Center for Internet Security versión 7.1.”, porque brinda controles para asegurar la seguridad de la información dentro del perímetro lógico de la organización, mediante la gestión de

puertos virtuales, configuración del firewall, IPS dentro de la red perimetral, configuración del VPN, entre otros.

➤ **Gestión de Incidentes**

Este proceso estará basado en el estándar internacional ISO 27001 “Sistema de Gestión de Seguridad de la Información - Requisitos” edición del 2013, porque brinda los controles necesarios para gestionar los incidentes relacionados a la seguridad de la información de la empresa. Puesto que, brinda un enfoque de roles, revisión de eventos y vulnerabilidades, evaluación, respuesta y aprendizaje de los incidentes.

➤ **Gestión de Continuidad de Seguridad de la Información**

Este proceso estará basado en el estándar internacional ISO 27001 “Sistema de Gestión de Seguridad de la Información - Requisitos” edición del 2013, porque brinda los controles necesarios para darle continuidad a la seguridad de la información luego de presentarse alguna interrupción en las operaciones del negocio. Solicita que se cuente con planes, implementación, verificación, revisión y evaluación para la continuidad de la seguridad en la organización.

5.2 Diseño del modelo de referencia para la protección de datos personales en el sector microfinanciero peruano

En base al análisis realizado en la sección anterior, se diseñó el modelo de referencia para la protección de datos personales en el sector microfinanciero peruano. Este diseño se compone de 7 secciones: Entradas, ciclo de vida de datos personales, medidas legales, medidas organizativas, medidas técnicas, soporte y salidas.

5.2.1 Modelo de referencia para la protección de datos personales en el sector microfinanciero peruano

A continuación, se desarrollará el modelo de referencia por cada sección elaborada.

Figura 9: Modelo de referencia para la protección de datos personales en el sector microfinanciero peruano

Elaboración: Propia

5.2.2 Entradas

Figura 10: Sección de entradas del modelo de referencia propuesto

Las entradas representan toda aquella información básica y fundamental para tener conocimiento de la microfinanciera con respecto a los datos personales que trata y almacena. Estas entradas se pueden representar en documentos físicos, digitales, multimedia o hablado por alguien, sin embargo, debe ser de fuentes legítimas y con evidencias para realizar un óptimo diagnóstico del nivel de protección de datos personales. Las entradas son vitales para desarrollar el ciclo de vida del dato personal, ya que con ellas se puede, no solo saber los datos personales críticos y su titularidad, sino también la forma en que la microfinanciera los trata y gestiona, asimismo, los sistemas e infraestructura tecnológica que emplea para sus operaciones cotidianas. Para definir las entradas se empleó como guía los requisitos solicitados en la Directiva de Seguridad, Ley 29733 y su reglamento, y artículos científicos que sugieren las fuentes de información comunes para identificar el ciclo de vida del dato. Las entradas definidas para el presente modelo de referencia son las siguientes:

5.2.2.1 Roles

Representa las funciones y cargos de los colaboradores que tratan los datos personales en la microfinanciera y el área o departamento al cual pertenecen. Esta información puede estar dada en un documento formal en físico o digital, o en caso contrario, a través de la observación de sus funciones que lo evidencie y posteriormente redactarlo en un documento para que el responsable principal de la microfinanciera lo revise y confirme.

5.2.2.2 Políticas de seguridad de la información

Son el conjunto de procedimiento, pautas y normas que establece la microfinanciera sobre seguridad de la información. Estas indican que la forma adecuada de emplear la información de la empresa, incluyendo el manejo de los datos personales y sensibles que contengan de cualquier persona. Esta información será dada únicamente en un documento físico o digital aprobado por el responsable principal de la microfinanciera.

5.2.2.3 Procesos de negocio

Son los conjuntos de actividades secuencias que realizan los colaboradores dentro de la microfinanciera para brindar su servicio. Estos procesos pueden ser de apoyo, línea, tecnológicos o estratégicos. Principalmente, se encargan de ofrecer valor al negocio directa o indirectamente. Esta información será dada en documentos físico o digital, mediante entrevistas a los colaboradores y posterior a ello elaborando un documento que confirme las actividades que desarrollando en la microfinanciera y con la aprobación del responsable principal.

5.2.2.4 Aplicaciones tecnológicas

Se refiere a los sistemas de información que se emplea en la microfinanciera para automatizar y agilizar las tareas y tener un mejor control de las transacciones financieras que se realizan diariamente. Esta información será dada en documentos físico o digital, mediante entrevistas a los colaboradores y posterior a ello elaborando un documento que confirme las actividades que desarrollando en la microfinanciera y con la aprobación del responsable principal.

5.2.2.5 Infraestructura tecnológica

Es el conjunto de componentes tecnológicos que permite el soporte, comunicación y funcionamiento de las aplicaciones tecnológicas, así también, la capacidad para que los colaboradores laboren con normalidad. Esta información será dada en documentos físico o digital, mediante entrevistas a los colaboradores y posterior a ello elaborando un documento que confirme las actividades que desarrollando en la microfinanciera y con la aprobación del responsable principal.

5.2.2.6 Documentos y formularios de datos personales

Es la documentación física empleada para el registro o almacenamiento de los datos personales de los colaboradores, clientes o proveedores de la microfinanciera. Los documentos deberán ser legítimos y actualizados para la óptima evaluación del nivel de protección de datos personales. Esta información será dada únicamente en un documento físico o digital aprobado por el responsable principal de la microfinanciera.

5.2.3 Ciclo de vida del dato personal

Figura 11: Sección del ciclo de vida del dato personal del modelo propuesto

Es la secuencia de las etapas por las que transcurre el dato personal, desde su ingreso a la microfinanciera, hasta su transferencia o destrucción. Permite conocer a detalle las fuentes que generan el dato personal; las personas, los procesos donde se generan o tratan, las aplicaciones tecnológicas que los utilizan; y la infraestructura tecnológica que los soporta.

5.2.3.1.1 Captura

- **Propósito:** Definición de la razón por la cual se recopila cada dato personal, cuya finalidad debe ser alineada a los objetivos de la microfinanciera.
- **Consentimiento:** Autorización del titular de los datos personales para la recopilación de sus datos y el tratamiento que se dará.
- **Recopilación:** Obtención de los datos personales de un cliente, colaborador o proveedor de la microfinanciera, previamente sido informado y aceptado el tratamiento que se dará a futuro.

5.2.3.1.2 Gestión del dato personal

- **Registro:** Ingreso de los datos personales a los sistemas de la empresa o registros físicos.
- **Modificación:** Alteraciones en los datos personales con el propósito de corrección de errores, actualización de información o completar datos.
- **Identificar:** Descubrimiento de nuevos datos a partir de los datos existentes mediante una serie de lógica y relaciones.
- **Acceso:** Brindar permisos a las personas para desarrollar las acciones solicitadas.
- **Consulta:** Permiso de visualización de los datos personales solicitados.

5.2.3.1.3 Retención

- **Organización:** Definir el lugar donde se conservarán los datos personales.

- **Almacenamiento:** Conservación de los datos personales en medios digitales o físicos de la microfinanciera.
- **Recuperación:** Obtención de los datos personales que han sido archivados en un almacenamiento de escaso acceso con registros históricos.
- **Anonimización:** Cambios en los datos personales de tal forma que no se pueda identificar al titular. Esta acción es irreversible. Principalmente usado para guardar los datos personales que pasaron la fecha de finalización del tratamiento.
- **Disociación:** Cambios en los datos personales de tal forma que no se pueda identificar al titular. Esta acción es reversible.

5.2.3.1.4 Destrucción

- **Bloqueo:** Acción que impide el acceso al banco de datos personales. Principalmente uso cuando se modifican los datos o como paso previo a la supresión.
- **Archivamiento:** Almacenamiento de los datos personales en medios de lento acceso donde se guarda la información histórica por fines de auditoría u otros.
- **Supresión:** Eliminación de los datos personales de los medios digital o físicos de la microfinanciera o terceros.

5.2.3.1.5 Transmisión

- **Transferencia interna:** Compartir los datos personales con miembros de la misma institución, independiente de la localidad donde se ubique. En caso este en otro país, cumplimiento del marco legal del país de destino, caso contrario, cumplimiento del marco legal peruano.
- **Transferencia externa:** Compartir los datos personales con miembros externos a la empresa, cuya responsabilidad del tratamiento y seguridad de los datos recae en el titular del banco de datos, o en caso se haga titular el tercero, el destinatario responderá por su protección.

5.2.4 Medidas legales

Figura 12: Sección de medidas legales del modelo de referencia propuesto

En base al análisis elaborado sobre la normativa peruana (Ley 29733 – Ley de Protección de Datos Personales y su Reglamento) y la Directiva de Seguridad brindada por la Dirección Nacional de Protección de Datos Personales dieron como resultado 6 categorías y 21 lineamientos para cumplir adecuadamente con los principios rectores de la Ley. Dentro de los cuales se cubre la adecuada inscripción del banco de datos personales, Derechos Fundamentales del titular, Videovigilancia, Transferencia de datos, entre otros.

5.2.5 Medidas organizativas

Figura 13: Sección de las medidas organizativas del modelo propuesto

De acuerdo con el análisis elaborado para los procesos organizacionales de las microfinancieras estudiadas, los estándares internacionales de seguridad de la información (ISO 27001 y COBIT 5) usados dieron como resultado 6 categorías y 42 lineamientos para salvaguardar correctamente los activos de información. Los controles expuestos brindan pautas para cumplir con la documentación formal (Políticas de Seguridad), Gestión de Activos, Seguridad en Recursos Humanos, Gestión de los Incidentes de Seguridad de la Información y los planes de Continuidad de Negocio para una microfinanciera.

5.2.6 Medidas técnicas

Figura 14: Sección de las medidas técnicas del modelo de referencia propuesto

De acuerdo, al análisis elaborado sobre la estructura técnica que debería considerar una microfinanciera y los estándares internacionales de seguridad cibernética (NIST 800-54, ISO 27001 y CSC CSI 7.1) se consideró plantear 5 categorías base y 22 lineamientos para que una microfinanciero pueda cumplir adecuadamente con la protección de los datos personales. Dentro de los controles se menciona la gestión de un software antivirus, configuración del firewall, gestión de accesos lógicos, cifrado de la información relevante, entre otros.

5.2.7 Soporte

Figura 15: Sección de soporte del modelo de referencia propuesta

Son los estándares, marcos de referencias y buenas prácticas de seguridad de la información sobre los cuales se basan los controles de las medidas legales, organizativas y técnicas del modelo. Cada color corresponde a los documentos de cada medida. El total de controles que se eligieron de estos documentos fueron 85. Estos elementos son los siguientes: Ley 29733 – Ley de Protección de Datos Personales y su Reglamento, NIST 800-54, ISO 27001, COBIT 5 y CSC CSI 7.1.

5.2.8 Salidas

Figura 16: Sección de salidas del modelo de referencia propuesta

Son los elementos resultado de la aplicación de las medidas legales, organizativas y técnicas del modelo de referencia propuesto. Estos elementos son los siguientes:

5.2.8.1 Plan de protección de datos personales

Contiene el conjunto de controles propuestos para elevar el nivel de protección de datos personales. En el plan se genera mediante una matriz, en la cual se estima el tiempo de duración de implementación para los controles respectivos, los recursos y costos requeridos para la ejecución. Asimismo, este plan debe considerar la aprobación del Directorio o Gerencia General de la microfinanciera.

5.2.8.2 Políticas y procedimientos de protección de datos personales

Contienen un conjunto de documentos formales, basados en Políticas de Seguridad de la Información, las cuales permiten tener una estructura organizacional enfocada en el resguardo de la información de la microfinanciera. Dentro de ella podemos obtener plantillas para dictaminar los protocolos ante un ataque cibernético, política de escritorios limpios, políticas de uso adecuado de internet y correo, entre otros.

5.2.8.3 Indicadores del cumplimiento de controles

Son los resultados que la matriz del modelo de referencia ha obtenido luego de realizar la evaluación del nivel de cumplimiento de los datos personales en la microfinanciera. Los datos obtenidos permiten obtener indicadores sobre cada categoría y lineamiento en específico. Con esta información la organización puede proceder a elaborar un plan para proteger sus datos personales.

5.2.9 Herramientas del modelo de referencia

Para el modelo de referencia se propusieron 3 herramientas que permiten definir y medir el nivel de protección de datos personales de las entidades microfinancieras. A continuación, se explica cada uno de ellos:

5.2.9.1 Matriz de evaluación de las medidas legales

Para la evaluación de las medidas legales se empleó una matriz basada en la escala Likert con las siguientes escalas: Muy bajo (1), Bajo (2), Bueno (3), Adecuado (4) y Excelente (5). Esta matriz se divide en base a 5 categorías: Consentimiento, transferencia, inscripción del banco de datos, derechos A.R.C.O, Subcontratos y Videovigilancia. La matriz tiene en total 21 controles. Cada control tiene una serie de criterios para definir la escala que le corresponde. Para esta matriz, todos los controles tienen impacto alto debido al costo elevado de las sanciones por el incumplimiento de la Ley de protección de datos personales. Para el caso de la Cooperativa de Ahorro y Crédito “Vale un Perú”, la medida de transferencia no aplica, debido a que la cooperativa no realiza ningún envío de los datos personales de sus clientes, colaboradores o proveedores a otras empresas, tampoco comparte su información con otras sedes porque solo cuenta con una oficina principal. La matriz se muestra a continuación:

REGLAMENTO DE LEY 29733

MEDIDAS LEGALES	ARTÍCULO	CONTROLES	APLICA	IMPACTO			CUMPLIMIEN TO				PUNTAJE		
				BAJO	MODERADO	ALTO	MUY BAJO	BAJO	BUENO	EXCELENTE	ESPERADO	LOGRADO	(%)
CONSENTIMIENTO	11,12	La organización obtiene el consentimiento del apoderado para darle tratamiento de los datos personales.											
	11,14	La organización obtiene el consentimiento del apoderado para darle tratamiento a sus datos sensibles.											
	11,16	El titular de los datos personales puede revocar su consentimiento en cualquier momento de forma parcial, o total.											
	11,27,28	En caso se traten datos personales de menores de edad, debe tener el consentimiento de sus titulares o tutores.											
TRANSFERENCIA	11,19	La organización obtiene el consentimiento del titular para la transferencia de su información personal.											
	22,26	La persona jurídica o natural que recepcione la información personal realiza el tratamiento adecuadamente, tal cual la empresa emisora.											

INSCRIPCIÓN DE BANCO DE DATOS	78,81-84	El titular de banco de datos personales inscribe los bancos de datos personales cuando hayan sido creados, modificados o cancelados, en el registro nacional de protección de datos personales. Asimismo, las comunicaciones referidas al flujo transfronterizo.											
	78,89-91	El titular de banco de datos personales inscribe los códigos de conducta cuando hayan sido creados, modificados o cancelados en el registro nacional de protección de datos personales.											
DERECHOS A.R.C.O.	47-50	Los derechos arco solo pueden ser ejercidos por el dueño de la información personal											
	60	El dueño de la información personal tiene el derecho de verificar como se tratan sus datos.											
	61	El dueño de la información personal tiene el derecho de fiscalizar como la organización gestionar sus datos personales.											
	64	El dueño de la información personal tiene derechos a actualizar sus datos personales.											
	65	El dueño de la información personal tiene derechos a rectificar sus datos personales.											
	66	El dueño de la información personal tiene derechos a añadir datos faltantes sobre sus datos personales.											

	67-68	El dueño de la información personal tiene derechos a solicitar la eliminación o cancelación de sus datos personales cuando ya no sean necesarios para la organización o este lo disponga.											
	71	El dueño de la información personal tiene el derecho de oponerse al tipo de tratamiento que le estén dando a sus datos personales.											
SUBCONTRATOS	33-34	La organización contrata servicios de medios tecnológicos tercerizados garantizando el adecuado tratamiento de los datos.											
	35	La organización contrata servicios de medios tecnológicos tercerizados que tengan mecanismos adecuados para la prestación.											
	37-38	La organización contrata servicios adecuados para el tratamiento de la información personal.											
VIDEOVIGILANCIA	02-2020	El titular de datos personales o responsable de tratamiento cumple con lo dispuesto en la resolución N° 02-2020-JUS/DGTAIPD.											
TOTALES													

Tabla 19: Matriz de evaluación de las medidas legales

Elaboración: Propia

Criterios para la evaluación de los controles de las medidas legales

CONSENTIMIENTO

Art. 11-12 La organización obtiene el consentimiento del apoderado para darle tratamiento de los datos personales.

Muy bajo

El titular del banco de datos personales no solicita el consentimiento del titular de los datos personales cuando se traten sus datos personales.

Bajo

El titular del banco de datos personales solicita el consentimiento del titular de los datos personales de forma supeditada, repentina, poco clara o ambigua, cuando se traten sus datos personales.

Bueno

La organización solicita el consentimiento del titular de los datos personales de forma libre, previa, expresa, informada e inequívoca, cuando se traten sus datos personales.

Excelente

La organización solicita el consentimiento de la información personal mediante un documento escrito y/o digital de forma, claro, previo, expreso, inequívoco e informado.

Art. 11,14 La organización obtiene el consentimiento del apoderado para darle tratamiento de los datos sensibles.

Muy bajo

El titular del banco de datos personales no solicita el consentimiento del titular de los datos personales cuando se traten sus datos sensibles.

Bajo

El titular del banco de datos personales solicita el consentimiento del titular de los datos personales de forma supeditada, repentina, poco clara o ambigua, cuando se traten sus datos sensibles.

Bueno

El titular del banco de datos personales solicita el consentimiento del titular de los datos personales de forma libre, previa, expresa, informada e inequívoca, cuando se traten sus datos sensibles.

Excelente

La organización solicita el consentimiento de la información personal mediante un documento escrito y/o digital de forma, claro, previo, expreso, inequívoco e informado.

Art. 11,16 El titular de los datos personales puede revocar su consentimiento en cualquier momento de forma parcial, o total

Muy bajo

El titular de datos personales no puede revocar su consentimiento ni parcial ni totalmente.

Bajo

El titular de datos personales puede revocar su consentimiento solo parcialmente en cualquier momento.

Bueno

El dueño de la información personal puede retirar su consentimiento para que la organización deje de darle tratamiento de sus datos personales en cualquier momento, parcial o totalmente.

Excelente

El dueño de la información personal puede retirar su consentimiento para que la organización deje de darle tratamiento de sus datos personales en cualquier momento, parcial o totalmente. Además, la organización cuenta con medios digitales para lograr este cometido.

Art. 11,27,28 En caso se traten datos personales de menores de edad, debe tener el consentimiento de sus titulares o tutores.

Muy bajo

No se pide el consentimiento para el tratamiento de la información personal de menores de edad.

Bajo

Se solicita el consentimiento a menores de edad para el tratamiento de sus datos personales.

Bueno

Se solicita el consentimiento a los titulares o tutores de la menor edad para el tratamiento de sus datos personales.

Excelente

Se solicita el consentimiento a los titulares o tutores del menor de edad de forma libre, previa, expresa, informada e inequívoca, cuando se traten sus datos personales.

TRANSFERENCIA

Art. 11,19 La organización obtiene el consentimiento del titular para la transferencia de su información personal.

Muy bajo

El titular del banco de datos personales no solicita el consentimiento del titular de los datos personales cuando se transfiera sus datos personales.

Bajo

El titular del banco de datos personales solicita el consentimiento del titular de los datos personales de forma supeditada, repentina, poco clara o ambigua, cuando se transfiera sus datos personales.

Bueno

El titular del banco de datos personales solicita el consentimiento del titular de los datos personales de forma libre, previa, expresa, informada e inequívoca, cuando se transfieran sus datos personales.

Excelente

El titular del banco de datos personales solicita el consentimiento del titular de los datos personales mediante un documento escrito, de forma libre, previa, expresa, informada e inequívoca, cuando se transfieran sus datos personales, mediante un documento escrito, a través de una firma manuscrita, digital o cualquier otro mecanismo que garantice la voluntad inequívoca del titular.

Art. 22 La persona jurídica o natural que recepcione la información personal realiza el tratamiento adecuadamente, tal cual la empresa emisora.

Muy bajo

La organización no le comunicó al receptor de la información personal las condiciones en la que se debe gestionar el tratamiento de los datos ni las obligaciones que debe asumir.

Bajo

La organización le comunicó verbalmente al receptor de la información personal las condiciones en la que se debe gestionar el tratamiento de los datos ni las obligaciones que debe asumir.

Bueno

La organización firma un contrato con el receptor de la información personal las condiciones en la que se debe gestionar el tratamiento de los datos ni las obligaciones que debe asumir.

Excelente

La organización firma un contrato con el receptor de la información personal las condiciones en la que se debe gestionar el tratamiento de los datos ni las obligaciones que debe asumir. Además, se realizan revisiones anuales sobre los contratos.

INSCRIPCIÓN DEL BANCO DE DATOS PERSONALES

Art. 78,81-84 El titular de banco de datos personales inscribe los bancos de datos personales en el registro nacional de protección de datos personales.

Muy bajo

El titular del banco de datos personales no inscribe los bancos de datos personales en el Registro Nacional de Protección de Datos Personales.

Bajo

El titular del banco de datos personales no inscribe los bancos de datos personales en el Registro Nacional de Protección de Datos Personales.

Bueno

El titular de banco de datos personales inscribe los bancos de datos personales cuando hayan sido creados, modificados o cancelados, en el Ministerio de Justicia.

Excelente

El titular de banco de datos personales inscribe los bancos de datos personales cuando hayan sido creados, modificados o cancelados, en el en el Ministerio de Justicia.

Art. 24-26,77,83 El titular de banco de datos personales declara las comunicaciones correspondientes al flujo transfronterizo.

Muy bajo

El dueño de la información personal no ha declarado el flujo transfronterizo.

Bajo

El titular del banco de datos personales ha declarado el flujo transfronterizo solo en la inscripción del banco de datos personales y no ha adjuntado el formulario específico para este fin.

Bueno

El titular del banco de datos personales ha declarado el flujo transfronterizo solo en la inscripción del banco de datos personales y ha adjuntado el formulario específico para este fin.

Excelente

El titular del banco de datos personales ha declarado el flujo transfronterizo solo en la inscripción del banco de datos personales y ha adjuntado el formulario específico para este fin. Además, ha considerado correctamente la ubicación de los repositorios físicos dónde se almacena su información y el responsable del banco de datos.

DERECHOS A.R.C.O.

Art. 50 El responsable de los datos personales dispone de un documento de solicitud para que el titular pueda ejercer sus derechos.

Muy bajo

La microfinanciera no ha adjudicado ninguna ficha para que el titular del dato personal pueda ejercer sus derechos fundamentales.

Bajo

La microfinanciera tiene una ficha manual para que el titular del banco de datos pueda ejercer sus derechos fundamentales. Además, este documento no considera todo lo enmarcado por la Ley.

Bueno

La microfinanciera tiene una ficha para que el titular del banco de datos pueda ejercer sus derechos fundamentales. Este documento se puede solicitar bajo un terminal web o en la oficina principal de la empresa.

Excelente

La microfinanciera tiene una ficha para que el titular del banco de datos pueda ejercer sus derechos fundamentales. Este documento se puede solicitar bajo un terminal web o en la oficina principal de la empresa. Por otro lado, existen documentación formal en la cual se consideran los plazos de entrega para cada tipo de categoría de los derechos.

Art. 52, 56 El responsable de los datos personales definió e implemento procedimientos para la atención de solicitudes que no han sido completadas correctamente.

Muy bajo

La microfinanciera no ha considerado procedimientos formales para tratar una solicitud por derechos ARCO.

Bajo

La microfinanciera no ha considerado procedimientos formales para tratar una solicitud por derechos ARCO, pero si recibe los requerimientos del titular del dato personal para tratarlo de forma ad-hoc.

Bueno

La microfinanciera ha considerado procedimientos formales para tratar una solicitud por derechos ARCO.

Excelente

La microfinanciera ha considerado procedimientos formales para tratar una solicitud por derechos ARCO. Además, el personal está capacitado para atender las solicitudes en los tiempos establecidos por Ley.

Art. 55 La organización debe tener un documento que especifique los tiempos de respuesta ante la solicitud de un titular.

Muy bajo

El dueño de la información personal no emite ningún documento que confirme la recepción de la solicitud del titular de los datos personales.

Bajo

El dueño de la información personal emite un documento que confirme la recepción de la solicitud del titular, para realizar el ejercicio de sus derechos fundamentales. Además, el documento indica la fecha y hora en que fue entregado a la institución, el nombre completo del responsable quien recibió la solicitud y los tiempos límites de respuesta y ejercicio del derecho definido por el reglamento de la Ley 29733.

Bueno

El dueño de la información personal emite un documento que confirme la recepción de la solicitud del titular, para realizar el ejercicio de sus derechos fundamentales. Asimismo, el documento indica la fecha y hora en que fue entregado a la institución, el nombre completo del responsable quien recibió la solicitud y los tiempos límites de respuesta y ejercicio del derecho definido por el reglamento de la Ley 29733. También, se informa al titular de datos personales la respuesta acerca de la solicitud y el ejercicio dentro de los rangos de fechas indicados en el documento.

Excelente

El dueño de la información personal emite un documento que confirme la recepción de la solicitud del titular, para realizar el ejercicio de sus derechos fundamentales. Asimismo, el documento indica la fecha y hora en que fue entregado a la institución, el nombre completo del responsable quien recibió la solicitud y los tiempos límites de respuesta y ejercicio del derecho definido por el reglamento de la Ley 29733. También, se informa al titular de datos personales la respuesta acerca de la solicitud y el ejercicio dentro de los rangos de fechas indicados en el documento.

Art. 60 El titular de datos personales tiene derecho a solicitar toda la información relacionada al tratamiento de sus datos personales.

Muy bajo

El dueño de la información personal no permite a la organización recabar información sobre el tratamiento que se realiza con sus datos personales.

Bajo

El dueño de la información personal permite a la organización recabar solo cierta información sobre el tratamiento que se realiza con sus datos personales.

Bueno

El dueño de la información personal permite a la organización recabar toda la información sobre el tratamiento que se realiza con sus datos personales.

Excelente

El dueño de la información personal establece un procedimiento sencillo y breve que permita a la organización recabar toda la información con respecto al tratamiento que se realiza con su información personal.

Art. 61 El titular de datos personales tiene derecho a obtener toda la información relativa a sus propios datos personales, así como las condiciones y generalidades del tratamiento de estos.

Muy bajo

El responsable del banco de información personal no permite al cliente acceder a la información relativa a sus datos personales.

Bajo

El responsable del banco de información personal permite al cliente acceder a solo cierta información relativa a sus datos personales.

Bueno

El responsable del banco de información personales permite al cliente acceder a toda la información relativa a sus datos personales, así como las condiciones y generalidades del tratamiento de estos.

Excelente

El responsable del banco de información personales establece un procedimiento sencillo y breve que permite al titular de datos personales acceder a toda su información almacenada.

Art. 64 El dueño de la información personal tiene derechos a actualizar sus datos personales.

Muy bajo

El responsable del banco de información no permite la actualización de los datos personales del titular.

Bajo

El responsable del banco de información permite la actualización de los datos personales del titular.

Bueno

El responsable del banco de información permite al cliente actualizar sus datos personales, con previa entrega de la documentación que sustente adecuadamente la información que se va a actualizar, es decir, que se pueda corroborar que es verídica.

Excelente

El responsable del banco de información permite al cliente actualizar sus datos personales, con previa entrega de la documentación que sustente adecuadamente la información que se va a actualizar, es decir, que se pueda corroborar que es verídica. Asimismo, comunica el cumplimiento de lo solicitado.

Art. 65 El dueño de la información personal tiene derechos a rectificar sus datos personales.

Muy bajo

El responsable del banco de información no permite la rectificación de los datos personales del titular.

Bajo

El responsable del banco de información permite la rectificación de los datos personales del titular.

Bueno

El responsable del banco de información permite al cliente actualizar sus datos personales, con previa entrega de la documentación que sustente adecuadamente la información que se va a actualizar, es decir, que se pueda corroborar que es verídica.

Excelente

El responsable del banco de información permite al cliente actualizar sus datos personales, con previa entrega de la documentación que sustente adecuadamente la información que se va a actualizar, es decir, que se pueda corroborar que es verídica. Asimismo, comunica el cumplimiento de lo solicitado. En este caso, correspondiente a la actualización de datos.

Art. 66 El titular de datos personales tiene derecho a solicitar la inclusión de los datos personales faltantes que hacen que su información sea incompleta, omitida o eliminada en atención a su relevancia para dicho tratamiento.

Muy bajo

El responsable del banco de información no permite la inclusión de los datos personales faltantes del titular.

Bajo

El responsable del banco de información permite la inclusión de los datos personales faltantes del titular.

Bueno

El responsable del banco de información permite al titular de datos personales incluir sus datos personales faltantes, con previa entrega de la documentación que sustente la procedencia de la actualización solicitada.

Excelente

El responsable del banco de información establece un procedimiento sencillo y breve que permite al titular de datos personales incluir sus datos personales faltantes, con previa entrega de la documentación que sustente la procedencia de la actualización solicitada. Asimismo, comunica el cumplimiento de lo solicitado al titular de datos personales, e indicar a quienes fueron transferidos la inclusión de los datos personales.

Art. 67-68 El titular de los datos personales tiene derecho a solicitar la supresión o cancelación de sus datos personales que hayan sido transferidos o no, siempre y cuando cumpla con los requisitos de la ley.

Muy bajo

El responsable del banco de información no permite la supresión de la información personal del cliente para ningún caso que justifique el derecho.

Bajo

El responsable del banco de información permite la supresión de la información personal del cliente cuando hubiesen vencido el plazo del tratamiento.

Bueno

El responsable del banco de información permite la supresión de la información personal del cliente cuando estos ya no sean necesarios o su fin haya sido cumplido.

Excelente

El responsable del banco de información permite la supresión de la información personal del cliente cuando estos ya no sean necesarios, su fin haya sido cumplido o se solicite la revocación de este. Asimismo, comunica el cumplimiento de lo solicitado al titular de datos personales, e indicar a quienes fueron transferidos la supresión de la información personal.

Art. 71 El dueño de la información personal tiene el derecho de oponerse al tipo de tratamiento que le estén dando a sus datos personales.

Muy bajo

El responsable del banco de información no permite la oposición al tratamiento de la información personal del titular.

Bajo

El responsable del banco de información permite la oposición al tratamiento de la información personal del titular, pero sin un proceso establecido.

Bueno

El responsable del banco de información permite la oposición al tratamiento de la información personal del titular, pero bajo un proceso establecido.

Excelente

El responsable del banco de información permite la oposición al tratamiento de la información personal del titular, pero bajo un procedimiento establecido, el cual es revisado de forma anual.

SUBCONTRATOS

Art. 33 - 34 La organización contrata servicios de medios tecnológicos tercerizados garantizando el adecuado tratamiento de los datos.

Muy bajo

La organización contrata servicios de medios tecnológicos tercerizados sin informar a los titulares de los datos personales.

Bajo

La organización contrata servicios de medios tecnológicos tercerizados informando a los titulares de los datos personales, pero sin indicar en el contrato la no asunción de la titularidad de los bancos de datos personales ni la confidencialidad durante y después de la prestación.

Bueno

La organización contrata servicios de medios tecnológicos tercerizados informando al receptor la confidencialidad durante y después de la prestación, y la garantía de la devastación o impedimento de ingresar a los datos personales después de finalizada la prestación de servicios.

Excelente

La organización contrata servicios de medios tecnológicos tercerizados informando al receptor la confidencialidad durante y después de la prestación, y la garantía de la devastación o impedimento. Además, se mantiene una revisión anual de este procedimiento.

Art. 35,37-38 La organización contrata servicios de medios tecnológicos tercerizados que tengan mecanismos adecuados para la prestación.

Muy bajo

La organización contrata servicios de medios tecnológicos tercerizados que no tengan mecanismos tecnológicos adecuados.

Bajo

La organización contrata servicios de medios tecnológicos tercerizados que permitan seccionar las acciones que se realiza sobre los datos que almacenan.

Bueno

La organización contrata servicios de medios tecnológicos tercerizados con una empresa que tiene establecidos procedimientos, políticas y protocolos de seguridad para tratar los datos personales que tienen en custodia.

Excelente

La organización contrata servicios de medios tecnológicos tercerizados con una empresa que tiene establecidos procedimientos, políticas y protocolos de seguridad para tratar los datos personales que tienen en custodia. Por otro lado, se verifica que la empresa receptora cuente con mecanismos de devastación de información segura. Por último, se realiza una revisión anual del contrato.

VIDEOVIGILANCIA

02-2020 El titular de datos personales o responsable de tratamiento cumple con lo dispuesto en la resolución N° 02-2020-JUS/DGTAIPD.

Muy bajo

La organización no ha considerado lo dictaminado por la Ley para los afiches de videovigilancia.

Bajo

La organización está en proceso de implementación de lo dictaminado por la Ley para los afiches de videovigilancia.

Bueno

La organización ha considerado lo dictaminado por la Ley para los afiches de videovigilancia, pero no ha sido completado correctamente.

Excelente

La organización ha considerado lo dictaminado por la Ley para los afiches de videovigilancia. Además, ha sido completado correctamente.

5.2.9.2 Matriz de evaluación de las medidas organizativas

Para la evaluación de las medidas organizativas se empleó una matriz basada en la escala Likert con las siguientes escalas: Muy baja (1), Baja (2), Adecuado (3), Bueno (4) y Excelente (5). Esta matriz se divide en 6 categorías: Políticas de seguridad de la información, gestión de activos, riesgos de seguridad, seguridad en RR.HH., incidentes de seguridad y continuidad de la seguridad. La matriz contiene en total 42 controles. Cada control tiene una serie de criterios para definir la escala que le corresponde. Para esta matriz, el impacto de los controles varía dependiendo de su relación con la protección de los datos personales. En este segmento se ha determinado que la Cooperativa “Vale un Perú” será evaluada por todos los controles. La matriz se muestra a continuación:

MEDIDAS ORGANIZATIVAS	REFERENCIA	CONTROLES	APLICA	IMPACTO			CUMPLIMIENTO					PUNTAJE		
				BAJO	MODERADO	ALTO	MUY BAJO	BAJO	ADECUADO	BUENO	EXCELENTE	ESPERADO	LOGRADO	(%)
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	ISO 27001 A.5.1.1	Política General de Seguridad												
	ISO 27001 A.5.1.2	Revisión de la Política General de Seguridad												
	ISO 27001 A.6.1.1	Roles y Responsabilidades para el Resguardo de la Seguridad												
	ISO 27001 A.7.2.1	Responsabilidad de la Alta Dirección												
	ISO 27001	Política para la Revisión de los Derechos de Ingreso Lógicos												
	ISO 27001 A.10.1.1	Política de Validación de Lineamientos Criptográficos												
	ISO 27001 A.11.2.9	Política de Escritorios Ordenados												
	ISO 27001 A.6.2.1	Política de Control para los Dispositivos Móviles Internos												
	ISO 27001 A.7.2.2	Policita de entrenamiento al personal en términos de seguridad												
	ISO 27001 A.8	Política de gestión de activos												

	ISO 27001 A.8.2.1	Política de Segmentación de la Información													
	ISO 27001 A.9.1.1	Política de acceso de usuario a la red empresarial													
	ISO 27001 A.11.1	Política de seguridad física													
	ISO 27001 A.12.1.4	Política de desarrollo, prueba y producción													
	ISO 27001 A.12.2.1	Política de Protección Antimalware													
	ISO 27001 A.12.3.1	Política de respaldo de información													
	ISO 27001 A.14.2.1	Política de desarrollo seguro													
	ISO 27001 A.15.1.1	Política de seguridad con terceros													
	ISO 27001 A.16.1.1	Política de gestión de incidentes													
	ISO 27001 A.17.1.1	Política de continuidad de negocio													
	ISO 27001 A.18.1.4	Política de Privacidad de Información por Normativa													
	ISO 27001 A.18.2.1	Revisión Seguridad de la Información por una Entidad Especializada													

GESTIÓN ACTIVOS	DE	ISO 27001 A.8.1.1	Gestión de control e inventario de activos lógicos y físicos												
		ISO 27001 A.8.1.2	Gestión de Propietarios de los Activos												
		ISO 27001 A.8.1.4	Gestión de Retorno del Activo												
		ISO 27001 A.11.2.4	Mantenición de los Equipos Informáticos												
		ISO 27001 A.11.2.5	Gestión de la Separación de los Activos Informáticos												
		ISO 27001 A.11.2.8	Activos obsoletos												
RIESGOS SEGURIDAD	DE	COBIT 5 APO12.01	Recopilación de Datos Relevantes												
		COBIT 5 APO12.02	Analizar los Riesgos												
		COBIT 5 APO12.03	Conservar un Perfil Atento al Riesgo												
		COBIT 5 APO12.06	Determinar la Respuesta al Riesgo												
SEGURIDAD RRHH	EN	ISO 27001 A.6.1.1	Funciones y Responsabilidades de Seguridad de la Información												
		ISO 27001 A.7.2.2	Capacitación y Concientización en Seguridad de la Información												

	ISO 27001 A.7.2.3	Procesos disciplinarios													
INCIDENTES DE SEGURIDAD	ISO 27001 A.16.1.1	Detección de Responsabilidades y Flujo de Procedimientos													
	ISO 27001 A.16.1.2	Reporte de los Eventos Detectados													
	ISO 27001 A.16.1.3	Reporte de las Debilidades Detectadas													
	ISO 27001 A.16.1.5	Respuesta a los Incidentes Detectados													
CONTINUIDAD DE LA SEGURIDAD	ISO 27001 A.17.1.1	Continuidad de los Planes de Seguridad de la Información													
	ISO 27001 A.17.1.2	Implementación de la Continuidad de la Seguridad de la Información													
	ISO 27001 A.17.1.3	Verificación, Revisión y Evaluación del Plan de Continuidad													
TOTALES															

Tabla 20: Matriz de evaluación de las medidas organizativas

Elaboración: Propia

CRITERIOS PARA LA EVALUACIÓN DE LOS CONTROLES DE LAS MEDIDAS ORGANIZATIVAS

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Política General de Seguridad

Muy bajo

La gerencia no ha implementado ningún tipo de Política de Seguridad de la Información en la organización.

Bajo

La gerencia define y comunica a los colaboradores las Políticas de seguridad. La forma de difusión es verbal y no existe un documento que lo evidencie.

Adecuado

La gerencia define, aprueba, publica y comunica a los colaboradores las Políticas.

Bueno

La gerencia define, aprueba, publica y comunica a los colaboradores. Asimismo, todos logran entender el objetivo de las Políticas.

Excelente

La gerencia define, aprueba, publica y comunica a los colaboradores y partes externas involucradas. Asimismo, todos logran comprender el objetivo de las Políticas.

Revisión de la Política General de Seguridad

Muy bajo

Los documentos internos de seguridad no son revisadas desde su creación.

Bajo

Los documentos internos de seguridad son revisadas por un colaborador cada vez que la Gerencia lo solicite.

Adecuado

Los documentos internos de seguridad son revisadas anualmente. La revisión es realizada por un colaborador designado por la Gerencia.

Bueno

Los documentos internos de seguridad son verificados cada cierto tiempo (Bianual). La revisión es realizada por un colaborador designado por la Gerencia.

Excelente

Los documentos internos de seguridad son revisadas cada cierto tiempo (Trimestralmente). La revisión es por el encargado de seguridad de información y el informe aprobado por la Gerencia.

Roles y Responsabilidades para el Resguardo de la Seguridad

Muy bajo

Los colaboradores no tienen conocimientos de sus funciones y responsabilidad sobre los activos de información.

Bajo

El encargado de cada área brinda pautas a sus respectivos equipos acerca de la protección y del cuidado que se debe tener con los activos de información.

Adecuado

La microfinanciera ha definido los roles principales para mantener una adecuada seguridad de los activos de información. Ha sido gestionado por cada área, pero no existe un documento formal.

Bueno

La microfinanciera ha definido los roles principales para mantener una adecuada seguridad de los activos de información. Esto debe estar detallado en políticas y procedimientos, gestionado por cada área y autorizado por la Gerencia.

Excelente

La microfinanciera ha definido todos los roles para mantener una adecuada seguridad de los activos de información. Esto debe estar detallado en políticas y procedimientos, gestionado por cada área y autorizado por la Gerencia.

Responsabilidad de la Alta Dirección

Muy bajo

La gerencia no ha concientizado ni promovido la importancia de cumplir con las directrices correspondientes a seguridad de la información.

Bajo

Los colaboradores y terceros no tienen conocimiento acerca de las políticas y procedimientos acerca de seguridad de la información.

Adecuado

La gerencia publica las políticas y procedimientos en un repositorio, el cual esté al alcance de todos colaboradores y terceros.

Bueno

La gerencia inculca a sus colaboradores y terceros aplicar los conocimientos de seguridad en base a los documentos internos asociados a la seguridad de la información establecidos por la microfinanciera.

Excelente

La gerencia inculca a sus colaboradores y terceros aplicar los conocimientos de seguridad en base a los documentos internos asociados a la seguridad de la información establecidos por la microfinanciera. Además, se brinda una capacitación anual y boletines de información mensual.

Política de Validación de Lineamientos Criptográficos

Muy bajo

La microfinanciera no cuenta con pautas que sugieran el uso de controles criptográficos en sus documentos formales.

Bajo

Los colaboradores son instruidos en el uso de controles criptográficos, pero no lo usan para realizar sus funciones.

Adecuado

Los colaboradores coordinan entre ellos el uso de los controles criptográficas que van a necesitar para realizar sus funciones considerando la seguridad de los datos.

Bueno

La microfinanciera cuenta con pautas para el uso de herramientas de cifrado dentro de otros documentos de seguridad. Además, son utilizados en el día a día del colaborador.

Excelente

La microfinanciera ha desarrollado un documento interno para el uso de herramientas de cifrado, con el fin de proteger la información estática y la transaccional. La cual sirve de pauta para que los colaboradores tengan una guía sobre cómo cumplir sus funciones considerando los parámetros de seguridad publicados.

Política de Escritorios Ordenados

Muy bajo

Cualquier colaborador puede acceder a los activos de información.

Bajo

Los colaboradores son instruidos por sus superiores acerca del correcto uso de los activos de información.

Adecuado

Los colaboradores cuentan con un documento que dicta el correcto uso de los activos de información. Además, sobre el orden que se debe tener en sus sitios de trabajo.

Bueno

los colaboradores cuentan con una Política de escritorio y pantallas limpias, en el cual la microfinanciera especifica que los activos de información no deben estar al alcance de cualquier colaborador. El documento ha sido gestionado por el encargado de seguridad de información.

Excelente

Existe una Política de escritorio y pantallas limpias, en el cual la microfinanciera especifica que los activos de información no deben estar al alcance de cualquier colaborador. Este documento está aprobado por la gerencia y gestionado por el encargado de seguridad de información.

Política para la Revisión de los Derechos de Ingreso Lógicos

Muy bajo

La microfinanciera transfiere su información entre diferentes puntos, sedes y con otras organizaciones en texto plano, sin ningún tipo de control que proteja los datos personales.

Bajo

La microfinanciera transfiere su información entre diferentes puntos, sedes y con otras organizaciones en texto plano, pero utiliza una herramienta que almacena el adjunto y pide contraseña para mostrar el contenido.

Adecuado

La microfinanciera transfiere su información entre diferentes puntos, sedes y con otras organizaciones cifrando la información, cada equipo de trabajo tiene un método y/o utilizan herramientas diferentes.

Bueno

Existe un documento formal que indica las consideraciones necesarias para realizar la transferencia de información de punto a punto.

Excelente

Existen políticas, procedimientos y controles formales de transferencia a través del uso de todo tipo de equipo de comunicación que use la microfinanciera. Tiendo en consideración el marco legal y normativo vigente.

Política de Control para los Dispositivos Móviles Internos

Muy bajo

La microfinanciera ignora los requisitos legales con respecto de la protección de datos personales sobre sus sistemas de información.

Bajo

La microfinanciera conoce los requisitos legales con respecto de la protección de datos personales sobre sus sistemas de información. No hay documentación que lo evidencie.

Adecuado

La microfinanciera ha identificado de forma clara todos los requisitos legislativos regulatorios y contractuales que tengan injerencia en sus sistemas de información con respecto del tratamiento adecuado de los datos personales. Asimismo, el documento es revisando periódicamente (anual) por el encargado de seguridad.

Bueno

La microfinanciera ha identificado de forma clara todos los requisitos legislativos regulatorios y contractuales que tengan injerencia en sus sistemas de información con respecto del tratamiento adecuado de los datos personales. Asimismo, el documento es revisando periódicamente (bianual) por el encargado de seguridad.

Excelente

La microfinanciera ha identificado de forma clara todos los requisitos legislativos regulatorios y contractuales que tengan injerencia en sus sistemas de información con respecto del tratamiento adecuado de los datos personales. Asimismo, el documento es revisando periódicamente (trimestral) por el encargado de seguridad. Además, cuenta con el visto bueno de la alta dirección.

Policita de Entrenamiento al Personal en Términos de Seguridad

Muy bajo

No hay procedimientos para entrenar o capacitar al personal en temas de seguridad de la información.

Bajo

El personal tiene conocimientos escasos de seguridad de la información, pero no hay un documento que los soporte.

Adecuado

La microfinanciera genera un documento ad hoc para establecer el entrenamiento de su personal, en temas de seguridad de la información.

Bueno

La microfinanciera genera un documento formal, en el cual se establece la capacitación de seguridad de la información anual.

Excelente

La microfinanciera genera un documento formal, en el cual se establece la capacitación de seguridad de la información anual. Además, de entregar consejos mensuales para resguardar mejor la información y/o datos personales que maneje el personal.

Política de Segmentación de la Información

Muy bajo

La microfinanciera no cuenta con ningún tipo de procedimiento para segmentar el derecho de acceso de sus empleados.

Bajo

La microfinanciera cuenta con conocimientos simples para segmentar el derecho de acceso de sus empleados. Aún así, no existe un documento formal

Adecuado

La microfinanciera ha generado un documento formal, el cual establece cómo se deben brindar los accesos lógicos.

Bueno

La microfinanciera ha generado un documento formal, el cual establece cómo se deben brindar los accesos lógicos. Asimismo, se establece una revisión por el encargado de seguridad de la información.

Excelente

La microfinanciera ha generado un documento formal, el cual establece cómo se deben brindar los accesos lógicos. Asimismo, se establece una revisión por el encargado de seguridad de la información. Por último, se presentan los resultados ante la gerencia general.

Política de Acceso de Usuario a la Red Empresarial

Muy bajo

La microfinanciera no presenta un documento para realizar la segmentación de acceso a la red interna.

Bajo

La microfinanciera no presenta un documento para realizar la segmentación de acceso a la red interna, pero el personal de tecnología de información brinda pautas a los colaboradores.

Adecuado

La microfinanciera genera un documento interno formal para que el personal de soporte tecnológico pueda generar reglas lógicas y seccionar los permisos de los colaboradores, correspondiente a la red interna.

Bueno

La microfinanciera genera un documento interno formal para que el personal de soporte tecnológico pueda generar reglas lógicas y seccionar los permisos de los colaboradores, correspondiente a la red interna.

Excelente

La microfinanciera genera un documento interno formal para que el personal de soporte tecnológico pueda generar reglas lógicas y seccionar los permisos de los colaboradores, correspondiente a la red interna. Asimismo, se establece una revisión anual para verificar que el procedimiento se esté realizando correctamente.

Política de Respaldo de la Información

Muy bajo

No se revisan los sistemas de información en la microfinanciera.

Bajo

Personal de soporte TI realiza una revisión aleatoria y simple a los sistemas de información de la microfinanciera, utilizando su propio criterio y no apoyándose en las políticas y normas de seguridad impuestas.

Adecuado

Se revisa regularmente (anual) el software para cumplir con las normas interna de seguridad de la información de la microfinanciera. El responsable de Soporte TI en conjunto con el encargado de seguridad de información realizan la tarea, el primero recaba la información y el segundo la analiza y brinda feedback de ser necesario.

Bueno

Se revisa regularmente (bianual) el software para cumplir con las normas interna de seguridad de la información de la microfinanciera. El responsable de Soporte TI en conjunto con el encargado de seguridad de información realizan la tarea, el primero recaba la información y el segundo la analiza y brinda feedback de ser necesario.

Excelente

Se revisa regularmente (trimestral) el software para cumplir con las normas interna de seguridad de la información de la microfinanciera. El responsable de Soporte TI en conjunto

con el encargado de seguridad de información realizan la tarea, el primero recaba la información y el segundo la analiza y brinda feedback de ser necesario.

Política de Protección Antimalware

Muy bajo

La microfinanciera no cuenta con una solución tecnológica para la protección antimalware y/o virus informático.

Bajo

La microfinanciera realiza una revisión manual de cada dispositivo informático para revisar si el activo cuenta con un virus informático.

Adecuado

La microfinanciera ha instalado una solución tecnológica antimalware en todos los dispositivos.

Bueno

La microfinanciera ha instalado una solución tecnológica integral antimalware, en la cual se ha implementado un agente (instalado y actualizado) en todos los activos informáticos.

Excelente

La microfinanciera ha instalado una solución tecnológica integral antimalware, en la cual se ha implementado un agente (instalado y actualizado) en todos los activos informáticos. Además, tiene un plan de reportes periódica para la gestión antimalware.

Política de Privacidad de Información por Normativa

Muy bajo

La microfinanciera no cuenta con un documento que acredite el adecuado tratamiento de los datos personales (privacidad y protección de la información).

Bajo

La microfinanciera describe en alguno de sus documentos, el compromiso que tiene en salvaguardar la información del cliente, empleado y/o tercero, pero no menciona el marco legal y normativo en el cual se apoya.

Adecuado

La microfinanciera cuenta con un documento que garantice la privacidad y la protección de la información, considerando lo requerido por la legislación y regulaciones pertinentes. La cual es gestionada por un colaborador que no es el responsable de seguridad.

Bueno

La microfinanciera cuenta con un documento que garantice la privacidad y la protección de la información, considerando lo requerido por la legislación y regulaciones pertinentes. La cual gestionada por el encargado de seguridad de información.

Excelente

La microfinanciera cuenta con un documento que garantice la privacidad y la protección de la información, considerando lo requerido por la legislación y regulaciones pertinentes. La cual gestionada por el encargado de seguridad de información y autorizada por la gerencia y legal.

Revisión Seguridad de la Información por una Entidad Especializada

Muy bajo

No existe revisión de las medidas impuestas a la microfinanciera en términos de seguridad de la información.

Bajo

La revisión de las medidas de seguridad implementadas es realizada por un colaborador de la organización, designado por la gerencia. El cual no es el encargado de seguridad de información.

Adecuado

Las medidas de seguridad de la información son revisadas por el encargado de seguridad de información / auditoría interna una vez al año, dependiendo el alcance de la revisión.

Bueno

La microfinanciera gestiona la revisión de sus medidas de seguridad de forma periódica, dentro su alcance llega a controles, políticas y procedimientos de seguridad de la información.

Excelente

La microfinanciera realiza la revisión de la gestión de seguridad de la información en una empresa que brinde toda la credibilidad de un buen trabajo. Asimismo, los resultados son expuestos ante la gerencia general.

GESTIÓN DE ACTIVOS

Gestión de control e inventario de activos lógicos y físicos

Muy bajo

Los activos de información no están inventariados.

Bajo

Solo los activos de información considerados más importantes han sido identificados e inventariados.

Adecuado

Los activos de información han sido clasificados de acuerdo con categorías, pero se desconoce su ubicación dentro de la microfinanciera. El inventario fue gestionado por un colaborador que no es el encargado de seguridad de información.

Bueno

Se identificaron los activos lógicos y físicos asociados a la gestión de la información. Además, realiza un inventario de dichos activos de información. El cual es gestionado por el encargado de seguridad de información.

Excelente

Se identificaron los activos lógicos y físicos asociados a la gestión de la información. Además, realiza un inventario de dichos activos de información. El cual es gestionado por el encargado de seguridad de información.

Gestión de Propietarios de los Activos

Muy bajo

Los activos de información no cuentan con un responsable.

Bajo

Algunos activos de información tienen asignado un propietario. Se hace la auto designación al gerente del área que usa más el activo de información y/o es quien lo brinda.

Adecuado

Los activos que están verificados en el inventario de la microfinanciera deben tener un “propietario”. Se hace la auto designación al gerente del área que usa más el activo de información y/o es quien lo brinda.

Bueno

Los activos que están verificados en el inventario de la microfinanciera deben tener un “propietario”. El encargado de seguridad de información es el encargado de esta designación.

Excelente

Los activos que están verificados en el inventario de la microfinanciera deben tener un “propietario”. El encargado de seguridad de información es el encargado de esta designación y ha sido aprobado por la gerencia.

Gestión del Retorno del Activo

Muy bajo

Al colaborador y usuario interno/externo no se le informa que debe devolver los activos de información.

Bajo

Al colaborador y usuario interno/externo sabe que debe devolver los activos de información una vez culminada sus labores. La información la obtiene de forma verbal.

Adecuado

Al colaborador y usuario interno/externo sabe que debe devolver los activos de información una vez culminada sus labores. La información está escrita en alguno de los documentos de la organización.

Bueno

Los colaboradores y usuario externos retornar los activos una vez haya finalizado su contrato o la prestación de sus servicios en la microfinanciera. El documento debe ser firmado por el responsable de soporte TI y el usuario. Asimismo, quien debe gestionar el documento es el encargado de seguridad de la información.

Excelente

Los colaboradores y usuario externos retornar los activos una vez haya finalizado su contrato o la prestación de sus servicios en la microfinanciera. El documento debe ser firmado por el responsable de soporte TI y el usuario. Asimismo, quien debe gestionar el documento es el encargado de seguridad de la información. Por último, la verificación es realizada por el responsable de soporte TI.

Mantenimiento de los Equipos Informáticos

Muy bajo

No se les brinda mantenimiento a los equipos.

Bajo

Se mantiene de manera adecuada la conservación de los dispositivos para verificar su buen rendimiento. Puesto que, la microfinanciera no debe verse afectada por la indisponibilidad de un activo por falta de revisiones periódicas (anual). Por último, los activos de información

tangibles como documentos son resguardados para evitar su alteración/destrucción no autorizado.

Adecuado

Se mantiene de manera adecuada la conservación de los dispositivos para verificar su buen rendimiento. Puesto que, la microfinanciera no debe verse afectada por la indisponibilidad de un activo por falta de revisiones periódicas (bianual). Por último, los activos de información tangibles como documentos son resguardados para evitar su alteración/destrucción no autorizado.

Bueno

Se mantiene de manera adecuada la conservación de los dispositivos para verificar su buen rendimiento. Puesto que, la microfinanciera no debe verse afectada por la indisponibilidad de un activo por falta de revisiones periódicas (trimestral). Por último, los activos de información tangibles como documentos son resguardados para evitar su alteración/destrucción no autorizado.

Excelente

Se mantiene de manera adecuada la conservación de los dispositivos para verificar su buen rendimiento. Puesto que, la microfinanciera no debe verse afectada por la indisponibilidad de un activo por falta de revisiones periódicas (mensual). Por último, los activos de información tangibles como documentos son resguardados para evitar su alteración/destrucción no autorizado.

Gestión de la Separación de los Activos Informáticos

Muy bajo

Cualquier colaborador puede retirar a los activos de información.

Bajo

El equipo, la información o el software son retirados sin autorización escrita, pero se le informa verbalmente al jefe del área para su conocimiento.

Adecuado

El equipo, la información o el software no son retirados de su lugar sin una previa autorización del área encargada.

Bueno

El equipo, la información o el software no son retirados de su lugar sin una previa autorización del encargado de seguridad de información.

Excelente

El equipo, la información o el software no son retirados de su lugar sin una previa autorización del encargado de seguridad de información y el visto buena de la Gerencia.

RIESGOS DE SEGURIDAD

Recopilación de Datos Relevantes

Muy bajo

No se recopilan datos para notificar riesgos TI.

Bajo

Se identifica y recopilan algunos datos para realizar una identificación y notificación de riesgos relacionados a TI. La gestión es realizada por el dueño del proceso.

Adecuado

Se identifica y recopilan datos relevantes para realizar una identificación, análisis y notificación de riesgos relacionados a TI. La gestión es realizada por el dueño del proceso.

Bueno

Se identifica y recopilan datos relevantes para realizar una identificación, análisis y notificación de riesgos relacionados a TI. La gestión es realizada por el dueño del proceso con conjunto con el encargado de seguridad de información.

Excelente

Se identifica y recopilan datos relevantes para realizar una identificación, análisis y notificación de riesgos relacionados a TI. La gestión es realizada por el dueño del proceso con conjunto con el encargado de seguridad de información y presentado ante la Gerencia.

Analizar los Riesgos

Muy bajo

No se analizan los riesgos en la microfinanciera.

Bajo

Desarrollan información incompleta, la cual no permite tomar decisiones adecuadas relacionadas con el riesgo. El documento formal es elaborado por un colaborador designado por el dueño del proceso.

Adecuado

Desarrollan información útil, la cual permite tomar decisiones adecuadas relacionadas con el riesgo. El documento formal es elaborado por el dueño del proceso.

Bueno

Desarrollan información útil, la cual permite tomar decisiones adecuadas relacionadas con el riesgo. El documento formal es presentado ante la Gerencia y elaborado por el dueño del proceso.

Excelente

Desarrollan información útil, la cual permite tomar decisiones adecuadas relacionadas con el riesgo. El documento formal es presentado ante la Gerencia y elaborado por el dueño del proceso en conjunto con el encargado de seguridad de información.

Conservar un Perfil Atento al Riesgo

Muy bajo

La microfinanciera no mantiene un perfil directo al riesgo.

Bajo

Mantiene un inventario de los algunos riesgos conocidos y sus atributos, falta el impacto potencial y no cuenta con todas las respuestas asociadas. Además, los recursos, capacidades y actividades para tomar brindar un adecuado control al riesgo necesarias no son claramente especificadas. No hay un documento formal.

Adecuado

Mantiene un inventario de los riesgos conocidos y sus atributos, como el impacto potencial y las respuestas asociadas. Además, los recursos, capacidades y actividades necesarias para tomar brindar un adecuado control al riesgo. El documento formal es elaborado por el dueño del proceso.

Bueno

Mantiene un inventario de los riesgos conocidos y sus atributos, como el impacto potencial y las respuestas asociadas. Además, los recursos, capacidades y actividades necesarias para tomar brindar un adecuado control al riesgo. El documento formal es presentado ante la Gerencia y elaborado por el dueño del proceso.

Excelente

Mantiene un inventario de los riesgos conocidos y sus atributos, como el impacto potencial y las respuestas asociadas. Además, los recursos, capacidades y actividades necesarias para tomar brindar un adecuado control al riesgo. El documento formal es presentado ante la Gerencia y elaborado por el dueño del proceso en conjunto con el encargado de seguridad de información.

Determinar la Respuesta al Riesgo

Muy bajo

No responden al riesgo cuando este ha sido detectado.

Bajo

Responde de forma tardía a los eventos relacionados con TI. Un empleado designado por su jefe inmediato es quien realiza la respuesta.

Adecuado

Responde de forma oportuna. De tal manera, que se delimita la magnitud de pérdida por eventos relacionados con TI. Un empleado designado por su jefe inmediato es quien realiza la respuesta.

Bueno

Responde de forma oportuna y con medidas efectivas. De tal manera, que se delimita la magnitud de pérdida por eventos relacionados con TI. El responsable de riesgos operativos lidera la respuesta.

Excelente

Responde de forma oportuna y con medidas efectivas. De tal manera, que se delimita la magnitud de pérdida por eventos relacionados con TI. El encargado de seguridad de información en conjunto con el responsable de riesgos operativos lidera la respuesta.

SEGURIDAD EN RECURSOS HUMANOS

Funciones y Responsabilidades de Seguridad de la Información

Muy bajo

No se han definido y asignado las responsabilidades de la seguridad de la información

Bajo

Se han definido y asignado algunas las responsabilidades de la seguridad de la información al personal que corresponda. Documento formal gestionado por el encargado de seguridad de información.

Adecuado

Se han definido y asignado todas las responsabilidades de la seguridad de la información al personal que corresponda. Asimismo, se dispone de su constante capacitación (anual) para que puedan cumplir sus funciones sin incurrir en algún incumplimiento de estas, con relación a seguridad de la información. Documento formal gestionado por el encargado de seguridad de información.

Bueno

Se han definido y asignado todas las responsabilidades de la seguridad de la información al personal que corresponda. Asimismo, se dispone de su constante capacitación (bianual) para que puedan cumplir sus funciones sin incurrir en algún incumplimiento de estas, con relación a seguridad de la información. Documento formal gestionado por el encargado de seguridad de información.

Excelente

Se han definido y asignado todas las responsabilidades de la seguridad de la información al personal que corresponda. Asimismo, se dispone de su constante capacitación (trimestral) para que puedan cumplir sus funciones sin incurrir en algún incumplimiento de estas, con relación a seguridad de la información. Documento formal gestionado por el encargado de seguridad de información.

Capacitación y Concientización en Seguridad de la Información

Muy bajo

Ninguno de los trabajadores de la organización recibe educación de concientización y capacitación sobre la importancia de la seguridad de la información.

Bajo

Algunos de los trabajadores de la organización reciben educación de concientización y capacitación sobre la importancia de la seguridad de la información.

Adecuado

Todos los trabajadores de la organización reciben educación de concientización y capacitación sobre la importancia de la seguridad de la información.

Bueno

Todos los trabajadores de la organización y los contratistas reciben educación de concientización y capacitación sobre la importancia de la seguridad de la información.

Excelente

Todos los trabajadores de la organización y los contratistas reciben una adecuada educación de concientización y capacitación de la importancia de la seguridad de la información. Asimismo, actualizaciones regulares sobre las políticas y procedimientos organizacionales que vayan de la mano con sus funciones.

Procesos Disciplinarios

Muy bajo

No existe un proceso disciplinario formal, por parte de la organización.

Bajo

Existe un proceso disciplinario formal, por parte de la organización, el cual no es comunicado a tiempo al trabajador que comete alguna infracción contra la compañía, en términos de seguridad de la información. Documento realizado por algún empleado guiándose de las normas instituciones y legales.

Adecuado

Existe un proceso disciplinario formal, por parte de la organización, el cual es expresado de forma escrita y oral, con el fin de tomar las medidas respectivas, en base a la infracción que se haya cometido. Documento realizado por algún empleado guiándose de las normas instituciones y legales.

Bueno

Existe un proceso disciplinario formal, por parte de la organización, el cual es expresado de forma escrita y oral, con el fin de tomar las medidas respectivas, en base a la infracción que se haya cometido. Documento gestionado por el responsable legal.

Excelente

Existe un proceso disciplinario formal, por parte de la organización, el cual es expresado de forma escrita y oral, con el fin de tomar las medidas respectivas, en base a la infracción que se haya cometido. Documento gestionado por el responsable legal y aprobado por el encargado de seguridad de información.

INCIDENTES DE SEGURIDAD

Detección de Responsabilidades y Flujo de Procedimientos

Muy bajo

La microfinanciera no establece responsabilidades y procedimientos, por parte de la gerencia.

Bajo

La microfinanciera establece algunas responsabilidades y procedimientos, por parte de la gerencia, para garantizar una respuesta a los incidentes de seguridad de la información que surjan. Un empleado designado por la gerencia o seguridad de la información gestiona la actividad.

Adecuado

La microfinanciera establece responsabilidades y procedimientos, por parte de la gerencia, los cuales garantizan una respuesta eficaz y adecuada a los incidentes que surjan. El encargado de seguridad de información gestiona la actividad.

Bueno

La microfinanciera establece responsabilidades y procedimientos, por parte de la gerencia, los cuales garantizan una respuesta eficaz y adecuada a los incidentes que surjan. El encargado de seguridad de información gestiona la actividad.

Excelente

La microfinanciera establece responsabilidades y procedimientos, por parte de la gerencia, los cuales garantizan una respuesta eficaz y adecuada a los incidentes que surjan. El encargado de seguridad de información en conjunto con el responsable de soporte TI es quien gestiona esta actividad.

Reporte de los Eventos Detectados

Muy bajo

No se reportan los eventos de seguridad a través de canales (plataformas digitales o documentos).

Bajo

Se reportan los eventos de seguridad (de forma verbal). Quien recepción es el responsable de soporte TI o el encargado de seguridad de información.

Adecuado

Se reportan los eventos de seguridad a través de medios tecnológicos. Quien recepciona es el responsable de soporte TI o el encargado de seguridad de la información.

Bueno

Se reportan los eventos de seguridad a través de medios tecnológicos. Quien recepciona es el responsable de soporte TI.

Excelente

Se reportan los eventos de seguridad a través de medios tecnológicos. Quien recepciona es el responsable de soporte TI y el responsable de Seguridad. De tal forma, dar pronta respuesta al incidente.

Reporte de las Debilidades Detectadas

Muy bajo

Los trabajadores no reportan los incidentes de seguridad.

Bajo

Los colaboradores de la microfinanciera reportan los incidentes de seguridad con muy poca frecuencia.

Adecuado

La microfinanciera genera capacitaciones y consejos para que los colaboradores reportes los incidentes de seguridad que puedan visualizar. Además, estos mismos son interiorizados por el personal de forma correcta.

Bueno

La microfinanciera genera capacitaciones y consejos para que los colaboradores reportes los incidentes de seguridad que puedan visualizar. La mayoría de los incidentes son reportados a tiempo.

Excelente

La microfinanciera genera capacitaciones y consejos para que los colaboradores reportes los incidentes de seguridad que puedan visualizar. Además, estos mismos son interiorizados por el personal de forma correcta. Todos los incidentes son reportados.

Respuesta a los Incidentes Detectados

Muy bajo

No existen procedimientos establecidos por la microfinanciera para responder a los incidentes relacionados a seguridad de la información.

Bajo

Existen procedimientos establecidos por la microfinanciera para responder a algunos incidentes relacionados a seguridad de la información. Los cuales han sido gestionados por un colaborador sin un rol definido.

Adecuado

Existen procedimientos establecidos por la microfinanciera para responder a los incidentes relacionados a seguridad de la información. Los cuales han sido gestionados por un colaborador sin un rol definido.

Bueno

Existen procedimientos establecidos por la microfinanciera para responder a los incidentes relacionados a seguridad de la información. Los cuales han sido gestionados por el responsable de seguridad.

Excelente

Existen procedimientos establecidos por la microfinanciera para responder a los incidentes relacionados a seguridad de la información. Los cuales han sido gestionados por el responsable de seguridad y aprobados por la Gerencia

CONTINUIDAD DE LA SEGURIDAD

Continuidad de los Planes de Seguridad de la Información

Muy bajo

La microfinanciera no determina que se requiere en términos de seguridad para armar un plan de continuidad.

Bajo

La microfinanciera determina algunos requisitos que se requiere en términos de seguridad para armar un plan de continuidad en situaciones adversas. Existe un equipo designado que deberá reestablecer la seguridad de la información en la empresa, según lo mencionado por el responsable de seguridad o la gerencia (comunicación verbal).

Adecuado

La microfinanciera determina que se requiere en términos de seguridad para armar un plan de continuidad en situaciones adversas. Existe un equipo designado que deberá reestablecer la seguridad de la información en la empresa, según los protocolos descritos.

Bueno

La microfinanciera determina que se requiere en términos de seguridad para armar un plan de continuidad en situaciones adversas. Es decir, ante una posible falla de todas las operaciones de la organización por factores externos. Además, el equipo designado tiene la capacidad de activar los protocolos necesarios para reestablecer la seguridad de la información en la organización. Este criterio es realizado por un colaborador designado por la gerencia.

Excelente

La microfinanciera determina que se requiere en términos de seguridad para armar un plan de continuidad en situaciones adversas. Es decir, ante una posible falla de todas las operaciones de la organización por factores externos. Además, el equipo designado tiene la capacidad de activar los protocolos necesarios para reestablecer la seguridad de la información en la organización. Este criterio es realizado por el encargado de seguridad de información.

Implementación de la Continuidad de la Seguridad de la Información

Muy bajo

La microfinanciera no realiza ninguna acción para garantizar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.

Bajo

La microfinanciera implementa en algunos procesos y procedimientos el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.

Adecuado

La microfinanciera establece e implementa procedimientos para asegurar la continuidad de la seguridad de la información durante una situación adversa.

Bueno

La microfinanciera establece e implementa procedimientos para asegurar la continuidad de la seguridad de la información durante una situación adversa. La cual es revisada de forma anual.

Excelente

La microfinanciera establece e implementa procedimientos para asegurar la continuidad de la seguridad de la información durante una situación adversa. La cual es revisada de forma semestral.

Verificación, Revisión y Evaluación del Plan de Continuidad

Muy bajo

La microfinanciera no verifica los controles de continuidad de seguridad de la información.

Bajo

La microfinanciera verifica algunos controles de continuidad de seguridad de la información establecida e implementada de forma regular. Todo ello, con la finalidad de asegurar su validez y efectividad durante situaciones adversas. Gestionado por un empleado designado por la gerencia, el cual no tiene los conocimientos suficientes.

Adecuado

La microfinanciera verifica los controles de continuidad de seguridad de la información establecida e implementada de forma regular. Todo ello, con la finalidad de asegurar su validez y efectividad durante situaciones adversas. Gestionado por un empleado designado por la gerencia, el cual no tiene los conocimientos suficientes.

Bueno

La microfinanciera verifica los controles de continuidad de seguridad de la información establecida e implementada de forma regular. Todo ello, con la finalidad de asegurar su validez y efectividad durante situaciones adversas. Gestionado por el responsable de soporte TI y administrativo.

Excelente

La microfinanciera verifica los controles de continuidad de seguridad de la información establecida e implementada de forma regular. Todo ello, con la finalidad de asegurar su validez y efectividad durante situaciones adversas. Gestionado por el encargado de seguridad de información.

5.2.9.3 Matriz de evaluación de las medidas técnicas

Para la evaluación de las medidas técnicas se empleó una matriz basada en la escala Likert con las siguientes escalas: Muy baja (1), Baja (2), Adecuado (3), Bueno (4) y Excelente (5). Esta matriz contiene 5 medidas: Accesos lógicos, accesos físicos, cifrado, seguridad perimetral y seguridad interna. La matriz tiene en total 22 controles. Cada control tiene una serie de criterios para definir la escala que le corresponde. La matriz se muestra a continuación:

MEDIDAS DE TÉCNICAS	REFERENCIA	CONTROLES	APLICA	IMPACTO			CUMPLIMIENTO				
				BAJO	MODERAD	ALTO	MUY BAJO	BAJO	ADECUAD	BUENO	EXCELENT
ACCESOS LÓGICOS	ISO 27001 A.6.1.2	Segmentación de Funciones									
	ISO 27001 A.9.2.1	Gestión de Registro de los Usuarios Lógicos									
	ISO 27001 A.9.2.2	Aprovisionamiento de Accesos Lógicos al Usuario									
	ISO 27001 A.9.2.3	Gestión de Verificación de Accesos de Usuarios Privilegiados									
	ISO 27001 A.9.2.5	Revisión de los Derechos de Acceso de los Usuarios									
	ISO 27001 A.9.2.6	Validación y Ajuste de los Accesos Brindados									
	ISO 27001 A.9.4.1	Restricción a la Información según el Acceso									
	ISO 27001 A.9.4.4	Utilización de Software para Control de Privilegios									

ACCESOS FÍSICOS	ISO 27001 A.11.1.1	Elaborar un Perímetro para la Seguridad Física											
	ISO 27001 A.11.1.2	Aseguramiento de los Controles Físicos											
	ISO 27001 A.11.1.5	Asegurar las Áreas de Trabajo											
	ISO 27001 A.11.1.6	Verificar la Distribución Segura en Zonas de Carga											
CIFRADO	NIST 800-54 SC-13	Asignación de Protección Criptográfica											
SEGURIDAD PERIMETRAL	CSC CSI 7.1 CSC 9.3	Verificar los Accesos a Puertos Lógicos											
	CSC CSI 7.1 CSC 9.6	Implementación y Revisión de la Solución Tecnológica Firewall											
	CSC CSI 7.1 CSC 8.1	Manejo y Control de las Herramientas de Ciberseguridad											
	CSC CSI 7.1 CSC 8.6	Implementar un IPS dentro de la red organizacional											
SEGURIDAD INTERNA	CSC CSI 7.1 CSC 15.5	Implementación de Redes Inalámbricas Seguras											

	CSC CSI 7.1 CSC 15.3	Aseguramiento de las Redes Inalámbricas									
	CSC CSI 7.1 CSC 13.5	Restricción de Acceso a los Dispositivos de Almacenamiento Externo									
	CSC CSI 7.1 CSC 13.9	Uso de herramientas de Ciberseguridad – DLP									
	CSC CSI 7.1 CSC 8.2	Uso de herramienta de Ciberseguridad - Antimalware									

Tabla 21: Matriz de evaluación de las medidas técnicas

Elaboración: Propia

CRITERIOS PARA LA EVALUACIÓN DE LOS CONTROLES DE LAS MEDIDAS TÉCNICAS

ACCESOS LÓGICOS

Segmentación de Funciones

Muy bajo

No hay segregación de funciones en la microfinanciera.

Bajo

Pocos colaboradores cumplen con el criterio de segregación de funciones.

Adecuado

Las tareas o áreas donde el colaborador pueda presentar algún conflicto de interés son segregadas de acuerdo con sus funciones. Existen algunos empleados que no se rigen bajo este criterio.

Bueno

Las tareas o áreas donde el colaborador pueda presentar algún conflicto de interés son segregadas de acuerdo con sus funciones. El representante del área es quién divide las tareas para cada colaborador respetando la correcta segregación de funciones.

Excelente

Las tareas o áreas donde el colaborador pueda presentar algún conflicto de interés son segregadas de acuerdo con sus funciones. El representante del área es quién divide las tareas para cada colaborador respetando la correcta segregación de funciones y el encargado de seguridad de la información verifica la segregación.

Gestión de Registro de los Usuarios Lógicos

Muy bajo

Los sistemas de información no tienen un proceso de registro y des registro.

Bajo

Se implementó un proceso de registro y des-registro de los usuarios, de tal forma habilitar/deshabilitar los derechos de acceso a los sistemas de información de la microfinanciera. Se han detectado errores donde el usuario es deshabilitado y sigue teniendo acceso. Nadie verifica el cumplimiento.

Adecuado

Se implementó un proceso de registro y des-registro de los usuarios, de tal forma habilitar/deshabilitar los derechos de acceso a los sistemas de información de la

microfinanciera. Un colaborador verifica el cumplimiento sin tener los conocimientos necesarios.

Bueno

Se implementó un proceso de registro y des-registro de los usuarios, de tal forma habilitar/deshabilitar los derechos de acceso a los sistemas de información de la microfinanciera. El responsable de Soporte TI gestiona el cumplimiento.

Excelente

Se implementó un proceso de registro y des-registro de los usuarios, de tal forma habilitar/deshabilitar los derechos de acceso a los sistemas de información de la microfinanciera. El responsable de seguridad verifica el cumplimiento de este criterio y el responsable de Soporte TI gestiona el cumplimiento.

Aprovisionamiento de Accesos Lógicos al Usuario

Muy bajo

No existe un documento de gestión de accesos.

Bajo

Se brindan accesos mínimos a un usuario, luego tiene que estar solicitando más accesos. No hay un documento formal.

Adecuado

Se tiene un documento que indica los accesos que debe tener un usuario, pero no es muy específico.

Bueno

Se implementó un documento formal para la provisión de los accesos de un usuario. Se le conoce como el proceso de Gestión de Accesos. Gestionado por el encargado de seguridad de información.

Excelente

Se implementó un documento formal para la provisión de los accesos de un usuario. Se le conoce como el proceso de Gestión de Accesos. Gestionado por el encargado de seguridad de información y aprobado por la gerencia.

Gestión de Verificación de Accesos de Usuarios Privilegiados

Muy bajo

El usuario final tiene accesos privilegiados desde la creación de su cuenta.

Bajo

El usuario tiene accesos privilegiados por default y posteriormente, se le retiran por el responsable de accesos.

Adecuado

Se restringe y controla la asignación de permisos privilegiados. El empleado que brinda los accesos no analiza la petición.

Bueno

Se restringe y controla la asignación de permisos privilegiados. El empleado que brinda los accesos privilegiados analiza y brinda los accesos sin consultar al responsable de seguridad.

Excelente

Se restringe y controla la asignación de permisos privilegiados. El encargado de seguridad de información analiza y aprueba los permisos solicitados.

Revisión de los Derechos de Acceso de los Usuarios

Muy bajo

No se verifican los accesos a los usuarios.

Bajo

La revisión la hace el encargado de seguridad de información cuando hay algún incidente y lo ve necesario.

Adecuado

Los dueños de los activos verifican los derechos de acceso de los usuarios de forma periódica (anual) dando prioridad a los sistemas Core. La revisión la hace el encargado de seguridad de información.

Bueno

Los dueños de los activos verifican los derechos de acceso de los usuarios de forma periódica (bianual) dando prioridad a los sistemas Core. La revisión la hace el encargado de seguridad de información.

Excelente

Los dueños de los activos verifican los derechos de acceso de los usuarios de forma periódica (trimestral) dando prioridad a los sistemas Core. La revisión la hace el encargado de seguridad de información.

Validación y Ajuste de los Accesos Brindados

Muy bajo

No se retiran los accesos brindados a un colaborador luego del cese.

Bajo

Algunos accesos se retiran del colaborador luego del cese.

Adecuado

Personal de Soporte TI realiza la gestión de retiro de acceso de acuerdo con lo dispuesto por su documento interno.

Bueno

Personal de Soporte TI realiza la gestión de retiro de acceso de acuerdo con lo dispuesto por su documento interno. El encargado de Seguridad de la Información revisa que se estén retirando los accesos de forma correcta anualmente.

Excelente

Personal de Soporte TI realiza la gestión de retiro de acceso de acuerdo con lo dispuesto por su documento interno. El encargado de Seguridad de la Información revisa que se estén retirando los accesos de forma correcta semestralmente.

Restricción a la Información según el Acceso

Muy bajo

No se restringe el acceso a la información.

Bajo

Algunos sistemas de información cuentan con restricciones claras para cada usuario.

Adecuado

Se restringe el acceso a la información y a las funciones de aplicación del sistema de acuerdo con el criterio del encargado de seguridad de la información. Para esta acción, se tomó en cuenta la necesidad de cada usuario para cumplir adecuadamente con sus funciones. La restricción es aprobada por el propietario del sistema de información y revisada por el responsable de seguridad.

Bueno

Se restringe el acceso a la información y a las funciones de aplicación del sistema de acuerdo con el criterio del encargado de seguridad de la información. La restricción es aprobada por el propietario del sistema de información y revisada por el responsable de seguridad.

Excelente

Se restringe el acceso a la información y a las funciones de aplicación del sistema de acuerdo con la política de control de acceso. Para esta acción, se tomó en cuenta la necesidad de cada usuario para cumplir adecuadamente con sus funciones. La restricción

es aprobada por el propietario del sistema de información y revisada por el responsable de seguridad.

Utilización de Software para Control de Privilegios

Muy bajo

No se restringe el acceso al programa de código fuente.

Bajo

Se restringe el acceso al programa de código fuente. Quien da el acceso es un empleado con conocimientos, pero no solicita autorización.

Adecuado

Se restringe el acceso al programa de código fuente, solo pocos usuarios calificados tienen acceso. Quien da el acceso es un empleado con conocimientos, pero no solicita autorización.

Bueno

Se restringe el acceso al programa de código fuente, solo pocos usuarios calificados tienen acceso. Asimismo, quien da el visto bueno es el responsable de soporte TI.

Excelente

Se restringe el acceso al programa de código fuente, solo pocos usuarios calificados tienen acceso. Asimismo, quien da el visto bueno es el encargado de seguridad de información.

ACCESOS FÍSICOS

Elaborar un Perímetro para la Seguridad Física

Muy bajo

No existen medidas para la restricción de accesos físicos a cualquier instalación dentro de la microfinanciera.

Bajo

Existen señalizaciones que sugieren el acceso restringido en algunas zonas de la microfinanciera, nadie vigila el cumplimiento.

Adecuado

Los perímetros de seguridad de la microfinanciera están definidos y son de público conocimiento entre los colaboradores y externos. Esto incluye las instalaciones donde se procesa información. Los colaboradores han comprendido esta medida, pero nadie verifica el cumplimiento.

Bueno

Los perímetros de seguridad de la microfinanciera están definidos y son de público conocimiento entre los colaboradores y externos. Esto incluye las instalaciones donde se procesa información. El responsable de administración verifica el cumplimiento de este criterio.

Excelente

Los perímetros de seguridad de la microfinanciera están definidos y son de público conocimiento entre los colaboradores y externos. Esto incluye las instalaciones donde se procesa información. El responsable de administración verifica el cumplimiento de este criterio, además el encargado de seguridad de información apoya en la gestión de cumplimiento.

Aseguramiento de los Controles Físicos

Muy bajo

No existen controles a los accesos físicos que delimiten el ingreso a los empleados, externos.

Bajo

Algunas señalizaciones sugieren controles de accesos físicos, pero los empleados muestran desconocimientos de ellas.

Adecuado

Las áreas seguras son protegidas mediante controles adecuados de ingreso, de tal forma que solo puede ingresar personal autorizado. Nadie verifica el cumplimiento de la misma.

Bueno

Las áreas seguras son protegidas mediante controles adecuados de ingreso, de tal forma que solo puede ingresar personal autorizado. El responsable de administración es quien da el visto bueno y verifica el cumplimiento a los controles.

Excelente

Las áreas seguras son protegidas mediante controles adecuados de ingreso, de tal forma que solo puede ingresar personal autorizado. El encargado de seguridad de información es quien da el visto bueno y verifica el cumplimiento a los controles.

Asegurar las Áreas de Trabajo

Muy bajo

No existe(n) procedimiento(s) para el trabajo en áreas seguras.

Bajo

Existen pautas que se le indican a los trabajadores para trabajar en áreas seguras. Comunicación verbal brindada por el personal administrativo.

Adecuado

Existe(n) procedimiento(s) para el trabajo en áreas seguras. Este documento es gestionado y aprobado por el encargado de seguridad de información.

Bueno

Existe(n) procedimiento(s) para el trabajo en áreas seguras. Este documento debe ser aprobado por la Gerencia y gestionado por el encargado de seguridad de información.

Excelente

Existe(n) procedimiento(s) para el trabajo en áreas seguras. Este documento debe ser aprobado por la Gerencia y gestionado por el encargado de seguridad de información en conjunto por el área de administrativa.

Verificar la Distribución Segura en Zonas de Carga

Muy bajo

No se controlan las zonas de descarga.

Bajo

Las zonas de descarga son supervisadas algunas veces por un colaborador de turno.

Adecuado

Las zonas de descarga son supervisadas por un personal de seguridad física encargado.

Bueno

Las zonas de descarga son supervisadas por una persona de seguridad encargado. Además, se realizan revisiones inopinadas para verificar la gestión.

Excelente

Las zonas de descarga son supervisadas por una persona de seguridad encargado. Además, se realizan revisiones inopinadas para verificar la gestión. Esta acción se realiza de forma trimestral.

CIFRADO

Asignación de Protección Criptográfica

Muy bajo

El sistema de información no contiene procesos criptográficos.

Bajo

El sistema de información contiene algunos procesos criptográficos definidos por la organización. Tarea gestionada un empleado designado por el responsable de soporte TI.

Adecuado

El sistema de información contiene procesos criptográficos definidos por la organización y el tipo de criptografía requerida para cada componente. De acuerdo con el marco legal y normativo vigente. Tarea gestionada un empleado designado por el responsable de soporte TI.

Bueno

El sistema de información contiene procesos criptográficos definidos por la organización y el tipo de criptografía requerida para cada componente. De acuerdo con el marco legal y normativo vigente. Tarea gestionada por el responsable de soporte TI.

Excelente

El sistema de información contiene procesos criptográficos definidos por la organización y el tipo de criptografía requerida para cada componente. De acuerdo con el marco legal y normativo vigente. Tarea gestionada por el responsable de soporte TI en conjunto con el encargado de seguridad de información.

SEGURIDAD PERIMETRAL

Verificar los Accesos a Puertos Lógicos

Muy bajo

Los puertos lógicos no son revisados, además no se tiene un inventario de ello.

Bajo

Algunos puertos lógicos están inventariados por la organización.

Adecuado

Algunos puertos lógicos están inventariados por la organización. Además, se tiene un inventario de estos.

Bueno

Se definen puertos exclusivos para cada servicio que se necesite (de entrada y salida). Los puertos son definidos por el encargado de Soporte TI. Además, se tiene un inventario actualizado de los puertos lógicos usados.

Excelente

Se definen puertos exclusivos para cada servicio que se necesite (de entrada y salida). Los puertos son definidos por el encargado de Soporte TI y validados por el encargado de

seguridad de información. Además, se tiene un inventario actualizado de los puertos lógicos usados.

Implementación y Revisión de la Solución Tecnológica Firewall

Muy bajo

La compañía no utiliza firewalls para proteger su información.

Bajo

La compañía utiliza firewall en host, pero en pocas computadoras.

Adecuado

La organización implementa la tecnología de firewall dentro de su red perimetral o en su defecto en host, de acuerdo con la VLAN.

Bueno

Coloque los firewalls de la aplicación frente a cualquier servidor crítico para verificar y validar el tráfico que va al servidor. Cualquier servicio o tráfico no autorizado se debe bloquear y generar una alerta.

Excelente

Coloque los firewalls de la aplicación frente a cualquier servidor crítico para verificar y validar el tráfico que va al servidor. Cualquier servicio o tráfico no autorizado se debe bloquear y generar una alerta.

Manejo y Control de las Herramientas de Ciberseguridad

Muy bajo

La microfinanciera no monitorea los equipos tecnológicos.

Bajo

Utiliza herramientas automatizadas para monitorear continuamente las estaciones de trabajo con antivirus y firewalls. Todos los eventos de detección de programa maligno se deben enviar a las herramientas de administración antimalware de la empresa y a los servidores de registro de eventos.

Adecuado

Utiliza herramientas automatizadas para monitorear continuamente las estaciones de trabajo, servidores con antivirus, antispymware, firewalls personales y funcionalidad IPS basada en host. Todos los eventos de detección de programa maligno se deben enviar a las herramientas de administración antimalware de la empresa y a los servidores de registro de eventos.

Bueno

Utiliza herramientas automatizadas para monitorear continuamente las estaciones de trabajo, servidores con antivirus, antispymware, firewalls personales y funcionalidad IPS basada en host. Todos los eventos de detección de programa maligno se deben enviar a las herramientas de administración antimalware de la empresa y a los servidores de registro de eventos.

Excelente

Utiliza herramientas automatizadas para monitorear continuamente las estaciones de trabajo, servidores y dispositivos móviles con antivirus, antispymware, firewalls personales y funcionalidad IPS basada en host. Todos los eventos de detección de programa maligno se deben enviar a las herramientas de administración antimalware de la empresa y a los servidores de registro de eventos.

Implementar un IPS dentro de la red organizacional

Muy bajo

La microfinanciera no tiene implementada tecnología IPS.

Bajo

Los dispositivos IPS basados en red son implementados para el bloqueo de firmas incorrectas conocidas o el comportamiento de posibles ataques.

Adecuado

Los dispositivos IPS basados en red son implementados para complementar IDS mediante el bloqueo de firmas incorrectas conocidas o el comportamiento de posibles ataques.

Bueno

Los dispositivos IPS basados en red son implementados para complementar IDS mediante el bloqueo de firmas incorrectas conocidas o el comportamiento de posibles ataques. Un IPS configurado correctamente en la red puede proporcionar automatización para bloquear el tráfico inadecuado.

Excelente

Los dispositivos IPS basados en red son implementados para complementar IDS mediante el bloqueo de firmas incorrectas conocidas o el comportamiento de posibles ataques. Un IPS configurado correctamente en la red puede proporcionar automatización para bloquear el tráfico inadecuado. Al evaluar productos IPS basados en la red, incluya aquellos que utilicen técnicas distintas de la detección basada en firmas (como los enfoques basados en la máquina virtual o en el recinto de seguridad) para su consideración.

SEGURIDAD INTERNA

Implementación de Redes Inalámbricas Seguras

Muy bajo

Las conexiones inalámbricas de la microfinanciera pasan en texto plano.

Bajo

Las conexiones inalámbricas de la microfinanciera utilizan la protección de acceso protegido a Wi-Fi 2 (WPA2).

Adecuado

Asegúrese de que todo el tráfico inalámbrico aproveche al menos el cifrado del (WEP) utilizado con al menos la protección de acceso protegido a Wi-Fi 2 (WPA2).

Bueno

Asegúrese de que todo el tráfico inalámbrico aproveche al menos el cifrado del (TKIP) utilizado con al menos la protección de acceso protegido a Wi-Fi 2 (WPA2).

Excelente

Asegúrese de que todo el tráfico inalámbrico aproveche al menos el cifrado del Estándar de cifrado avanzado (AES) utilizado con al menos la protección de acceso protegido a Wi-Fi 2 (WPA2).

Aseguramiento de las Redes Inalámbricas

Muy bajo

No hay detección de intrusos para redes inalámbricas.

Bajo

Usa los sistemas de detección de intrusos inalámbricos (WIDS) para identificar dispositivos inalámbricos no autorizados y detectar intentos de ataque y compromisos exitosos.

Adecuado

Usa los sistemas de detección de intrusos inalámbricos (WIDS) para identificar dispositivos inalámbricos no autorizados y detectar intentos de ataque y compromisos exitosos.

Bueno

Usa los sistemas de detección de intrusos inalámbricos (WIDS) para identificar dispositivos inalámbricos no autorizados y detectar intentos de ataque y compromisos

exitosos. Además de WIDS, todo el tráfico inalámbrico debe ser monitoreado por WIDS a medida que el tráfico pasa a la red cableada.

Excelente

Usa los sistemas de detección de intrusos inalámbricos (WIDS) para identificar dispositivos inalámbricos no autorizados y detectar intentos de ataque y compromisos exitosos. Además de WIDS, todo el tráfico inalámbrico debe ser monitoreado por WIDS a medida que el tráfico pasa a la red cableada.

Restricción de Acceso a los Dispositivos de Almacenamiento Externo

Muy bajo

Cualquier colaborador de la microfinanciera puede almacenar información en sus dispositivos removibles.

Bajo

Se configuran algunas computadoras para que no escriban datos en tokens USB o discos duros USB. Si se requieren tales dispositivos, se debe usar un software empresarial que pueda configurar los sistemas para permitir el acceso a dispositivos USB específicos (basados en el número de serie u otra propiedad exclusiva).

Adecuado

Se configuran algunas computadoras para que no escriban datos en tokens USB o discos duros USB. Si se requieren tales dispositivos, se debe usar un software empresarial que pueda configurar los sistemas para permitir el acceso a dispositivos USB específicos (basados en el número de serie u otra propiedad exclusiva). Se debe mantener un inventario de todos los dispositivos autorizados.

Bueno

Se configuran algunas computadoras para que no escriban datos en tokens USB o discos duros USB. Si se requieren tales dispositivos, se debe usar un software empresarial que pueda configurar los sistemas para permitir el acceso a dispositivos USB específicos (basados en el número de serie u otra propiedad exclusiva), y que pueda encriptar automáticamente todos los datos colocados en dichos dispositivos. Se debe mantener un inventario de todos los dispositivos autorizados.

Excelente

Se configuran las computadoras para que no escriban datos en tokens USB o discos duros USB. Si se requieren tales dispositivos, se debe usar un software empresarial que pueda configurar los sistemas para permitir el acceso a dispositivos USB específicos (basados

en el número de serie u otra propiedad exclusiva), y que pueda encriptar automáticamente todos los datos colocados en dichos dispositivos. Se debe mantener un inventario de todos los dispositivos autorizados.

Uso de herramientas de Ciberseguridad – DLP

Muy bajo

No se aplican DLP en la microfinanciera.

Bajo

Utiliza la prevención de pérdida de datos basada en host (DLP) para algunos de sus procesos.

Adecuado

Utiliza la prevención de pérdida de datos basada en host (DLP) para imponer las ACL. En la mayoría de las organizaciones, el acceso a los datos está controlado por las ACL que se implementan en el servidor. Una vez que los datos se han copiado en un sistema de escritorio, las ACL ya no se aplican y los usuarios pueden enviar los datos a quien quieran.

Bueno

Utiliza la prevención de pérdida de datos basada en host (DLP) para imponer las ACL incluso cuando los datos se copian de un servidor. En la mayoría de las organizaciones, el acceso a los datos está controlado por las ACL que se implementan en el servidor. Una vez que los datos se han copiado en un sistema de escritorio, las ACL ya no se aplican y los usuarios pueden enviar los datos a quien quieran.

Excelente

Utiliza la prevención de pérdida de datos basada en host (DLP) para imponer las ACL incluso cuando los datos se copian de un servidor. En la mayoría de las organizaciones, el acceso a los datos está controlado por las ACL que se implementan en el servidor. Una vez que los datos se han copiado en un sistema de escritorio, las ACL ya no se aplican y los usuarios pueden enviar los datos a quien quieran.

Uso de herramienta de Ciberseguridad - Antimalware

Muy bajo

Los dispositivos no cuentan con software antimalware.

Bajo

Utiliza revisiones manuales para verificar antimalware en cada uno de los dispositivos de la organización (servidores y computadoras), el responsable de Soporte TI controla esto.

Adecuado

Utiliza un software antimalware en cada uno de los dispositivos de la organización (servidores y computadoras), el responsable de Soporte TI controla esto.

Bueno

Utiliza un software antimalware que ofrezca una infraestructura centralizada que compile información sobre la reputación de los archivos o haga que los administradores envíen actualizaciones manualmente a todas las máquinas. Después de aplicar una actualización, los sistemas automatizados deben verificar que cada sistema haya recibido su actualización de firma.

Excelente

Utiliza un software antimalware que ofrezca una infraestructura centralizada que compile información sobre la reputación de los archivos o haga que los administradores envíen actualizaciones automáticamente a todas las máquinas. Después de aplicar una actualización, los sistemas automatizados deben verificar que cada sistema haya recibido su actualización de firma.

6 CAPÍTULO 5: RESULTADOS DEL PROYECTO

En este capítulo, se presenta la microfinanciera donde se validó el modelo de referencia, el proceso de implementación que se siguió, los resultados obtenidos y el plan de continuidad. Además, se explica el plan de costos de la implementación en la microfinanciera.

6.1 Validación de las medidas legales, organizativas y técnicas del modelo propuesto en una entidad microfinanciera

6.1.1 Presentación de la microfinanciera

La validación se realizó en la Cooperativa de Ahorro y Crédito “Vale un Perú” (VALEUN). Es una empresa del sector microfinanciero ubicada en la Avenida Arequipa N° 1936 – Lince, Lima. Tiene una trayectoria de 55 años al servicio exclusivo de las personas pertenecientes del sector militar. La cantidad de socios activos afiliados a la COOPAC “VALEUN”, hasta Setiembre del 2020, fue de 2891. La Gerente General de la cooperativa es María del Carmen Laguna Arce. La cooperativa ofrece los siguientes productos financieros:

- Productos de créditos:
 - Crédito Comerciales: Son los financiamientos que se ofrecen a las personas naturales o jurídicas, cuyo propósito es la inversión en la producción y comercialización de bienes o servicios en sus diferentes fases.
 - Crédito a las Microempresas (MES): Son los financiamientos que se ofrecen a las personas naturales o jurídicas, cuyo objetivo es la inversión en las actividades productivas, de comercialización o prestación de servicios.
 - Créditos de Consumo: Son los préstamos de dinero a las personas naturales, cuyo propósito son los pagos de servicios, bienes o gastos no relacionados a actividades empresariales.
 - Créditos Hipotecarios para Vivienda: Son los préstamos de dinero a las personas naturales, cuyo propósito es la compra, construcción, refacción, ampliación, mejoramiento, remodelación y/o subdivisión de una vivienda propia avalada por un hipoteca inscrita en el sistema convencional de créditos hipotecarios u otro similares.
- Productos de ahorros:

- Deposito a la Vista: Se entiende por Depósitos a la Vista el dinero colocado en la Cooperativa por el depositante, quien a su vez adquiere el derecho de disponer total o parcialmente en cualquier momento del saldo en la forma convenida.
- Ahorro A Plazo: Se entiende por ahorro a plazo al dinero colocado por los socios de la Cooperativa, con la característica de que deben mantenerse durante un periodo de tiempo previamente acordado entre la Cooperativa y el depositante. Este tipo de depósito se respalda con un documento idóneo “Certificado de depósito de ahorro a plazo C.D.A.P.”
- Ahorro Contractual: Se entiende por ahorro contractual aquel en el cual el asociado se compromete a depositar una cuota fija mensual, por un periodo determinado al final del cual le será devuelto con los respectivos rendimientos.
 - Bono navideño: Es aquel ahorro contractual que se constituye antes del 31 de marzo y el cual se restituye el capital y los intereses generados en la primera semana del mes de diciembre.
 - Bono Vacacional: Es aquel ahorro contractual, en el cual se restituye el capital los intereses generados a partir del décimo mes de constituido el depósito.
- Ahorro Permanente: Se entiende por Depósito de ahorro permanente el dinero colocado en la Cooperativa por el depositante a través de deducción de nómina o pago directo, equivalente al 1% del salario mínimo legal mensual vigente. Dicho ahorro es obligatorio para todos los asociados.

Figura 17: Sede de la Cooperativa de Ahorro y Crédito "Vale un Perú"

Fuente: Google Maps

6.1.2 Proceso de validación

6.1.2.1 Definición

A continuación, se presenta el proceso de validación y se explica cada una de la secuencia:

Figura 18: Proceso de validación del modelo

Fuente: Propia

1) Recopilación de la información

Consiste en la obtención de toda la información correspondiente al tratamiento y almacenamiento de los datos personales que maneja la microfinanciera. La información recopilada se muestra en la sección de entrada del modelo de referencia propuesto. Esta información es la siguiente: Roles, políticas de seguridad de la información, procesos de negocio, aplicaciones de la organización, infraestructura tecnológica y documentos asociados a la información personal de sus socios, empleados o proveedores, entre otros.

2) Diagnóstico

Es la fase del proceso de validación donde a partir de la información recopilada se elabora el flujo de vida del dato personal. Se arma un mapa donde se muestra los procesos por donde transcurre el dato personal, la infraestructura tecnológica donde se almacenan y se obtienen, los sistemas y áreas que tratan los datos y las fases del dato personal. Posterior a ello, se realiza la evaluación de la microfinanciera con respecto al nivel de protección de los datos personales. Para esto, se emplea 3 matrices: Matriz de evaluación de las medidas legales, matriz de evaluación de las medidas organizativas y matriz de evaluación de las medidas técnicas. Cada matriz comprende una lista de controles a evaluar. Los controles están basados en el marco legal, estándar de seguridad, marco de trabajo y buena práctica de seguridad de la información, contemplados en el modelo de referencia. Las matrices están sujetas al cumplimiento de los controles y el impacto de cada uno de ellos en la microfinanciera. Las escalas utilizadas para medir el cumplimiento y el impacto corresponden a la escala Likert. Estas son las siguientes: Muy baja, baja, adecuado, bueno y excelente. Como resultado de esta evaluación, se producen estadísticas que permiten conocer las medidas más urgentes de atender.

3) Plan de mejora

Según el resultado emitido de la evaluación de las medidas legales, organizativas y técnicas, se propone un listado de controles para incrementar el nivel de protección de datos personales al mínimo sugerido. Los controles atienden principalmente a los indicadores más bajos de la evaluación. Este listado debe ser revisado y aprobado por el encargado de la microfinanciera. Después de la aprobación, se elabora un plan de mejor que contendrá la lista de controles propuestos anteriormente con los tiempos para implementar cada control y los responsables a cargo. Es necesario considerar los criterios de impacto, facilidad de cumplimiento, recursos, costos, entre otros.

4) Implementación

En esta fase se lleva a cabo la implementación de los controles propuestos en el plan de mejora. Posterior a la implementación de los controles, nuevamente se realiza la evaluación de la cooperativa para conocer el nivel de protección de datos personales y se compara con el nivel inicial para determinar la mejora lograda.

6.1.2.2 Herramientas de validación

En la fase de Diagnostico del proceso de validación y de Implementación, se emplearon las matrices de evaluación de las medidas legales, organizativas y técnicas. Estas fueron

plasmadas en hojas de cálculo en Excel, de manera que permitan colocar el impacto y cumplimiento de cada control de las medidas, y automatizar los resultados del nivel de protección de datos personales de la Cooperativa de Ahorros y Créditos “Vale un Perú”. Cada uno de los controles fueron evaluados en base a sus criterios de evaluación y calculados según la escala Likert (revisar el punto 5.2.8 del documento).

MATRIZ DE CUMPLIMIENTO DE LAS MEDIDAS LEGALES														
REGlamento de Ley 29733														
MEDIDAS LEGALES	ARTÍCULO D	CONTROLES	APLICA	IMPACTO				CUMPLIMIENTO			PUNTAJE		%	
				BAJO	MODERADO	ALTO	MUY BAJO	BAJO	BIENO	EXCELENTE	ESPERADO	LOGRADO		
CONSENTIMIENTO	11.2	Solicitar el consentimiento del titular de los datos personales para realizar el tratamiento de sus datos personales.	SI	X				X				12	9	75%
	11.4	Solicitar el consentimiento del titular de los datos personales para realizar el tratamiento de sus datos personales.	SI	X				X				12	9	75%
	11.6	Solicitar el consentimiento para el tratamiento de datos personales al titular de datos personales de fono, libro, correo, dirección o teléfono.	SI	X				X				12	9	75%
	11.27.28	En caso de tratar datos personales de menores de edad, debe tener el consentimiento de sus titulares o tutores.	NO	X										
TRANSFERENCIA	11.9	Solicitar el consentimiento del titular de datos personales para transferir sus datos a nivel nacional o internacional.	NO	X										
	22	El receptor de la transferencia de los datos personales asume el rol de titular del banco de datos personales o responsable del tratamiento y realiza el tratamiento conforme a la finalidad por la cual fueron recopilados y los mismos obligaciones del emisor.	NO	X										
	78.61-64	El titular de banco de datos personales inscribe los bancos de datos personales en el registro nacional de protección de datos personales.	SI	X				X				12	9	75%
INSCRIPCIÓN DE BANCO DE DATOS	24.25.26.77.8	El titular de banco de datos personales declara los convencimientos correspondientes al flujo transfronterizo.	SI	X				X				12	9	75%
	50	El responsable de los datos personales dispone de un documento de política que el titular puede ejercer sus derechos.	SI	X				X				12	100%	
	52-55	El responsable de los datos personales define e implementa procedimientos para la situación de solicitudes que no han sido completados correctamente.	SI	X				X				12	100%	
	55	El titular del banco de datos personales o responsable del tratamiento debe tener un documento que especifique los tiempos de respuesta ante la solicitud de un titular de datos personales.	SI	X				X				12	100%	
	60	El titular de datos personales tiene derecho a solicitar toda la información relacionada al tratamiento de sus datos personales.	SI	X				X				12	100%	
	61	El titular de datos personales tiene derecho a obtener toda la información relativa a sus propios datos personales, así como las condiciones y generalidades del tratamiento de los mismos.	SI	X				X				12	100%	
	64	El titular de datos personales tiene derecho a solicitar la actualización de los datos personales que fueron modificados a la fecha del ejercicio del derecho.	SI	X				X				12	100%	
DERECHOS A.R.C.O.	65	El titular de datos personales tiene derecho a solicitar la rectificación de los datos personales que resulten ser erróneos, inexactos o falsos.	SI	X				X				12	100%	
	66	El titular de datos personales tiene derecho a solicitar la eliminación de los datos personales faltantes que haya que su información no completa, emitida o obtenida en situación y su eliminación para dicho tratamiento.	SI	X				X				12	100%	
	67-68	El titular de los datos personales tiene derecho a solicitar la supresión o cancelación de sus datos personales que hayan sido transferidos o no, siempre y cuando cumpla con los requisitos de la ley.	SI	X				X				12	100%	
	71	El titular de datos personales tiene derecho a oponer al tratamiento de sus datos personales cuando no es habida brevedad se consintió para la recopilación.	SI	X				X				12	100%	
	33-34	El titular del banco de datos personales o responsable del tratamiento contrata servicios de medios tecnológicos tecnológicos garantizando el adecuado tratamiento de los datos.	SI	X				X				12	100%	
SUBCONTRATOS	35,37,38	El titular del banco de datos personales o responsable del tratamiento contrata servicios de medios tecnológicos tecnológicos que tengan mecanismos adecuados para la protección.	SI	X				X				12	100%	
	08-2020	El titular de datos personales o responsable de tratamiento cumple con lo dispuesto en la resolución N° 08-2020-JUS/DT/FPD.	SI	X				X				12	100%	
TOTALES												88	100	92.6%

		PUNTAJE	
MEDIDAS	LOGRADO	ESPERADO	100%
CONSENTIMIENTO	97	96	100%
TRANSFERENCIA			
INSCRIPCIÓN DE BANCO DE DATOS	18	24	100%
DERECHOS A.R.C.O.	120	120	100%
SUBCONTRATOS	24	24	100%
VIDEOSURVEILLANCIA	12	12	100%
TOTALES	113	211	92.6%

MEDIDAS	PUNTAJE		
	LOGRADO	ESPERADO	SI
CONSENTIMIENTO	21	56	15%
TRANSFERENCIA	18	24	15%
INSCRIPCIÓN DE BANCO DE DATOS	100	100	100%
DERECHOS A.R.C.O.	24	24	100%
SUBCONTRATOS	24	24	100%
VIDEOSURVEILLANCIA	12	12	100%
TOTALES	189	204	92.6%

Figura 19: Hoja de cálculo de la matriz de evaluación de las medidas legales

Elaboración: Propia

MATRIZ DE CUMPLIMIENTO DE LAS MEDIDAS ORGANIZATIVAS														
MEDIDAS DE ORGANIZATIVAS	REFERENCIA	CONTROLES	IMPACTO			CUMPLIMIENTO			PUNTAJE					
			APLICA BAJO	MODERADO	ALTO	MUY BAJO	BAJO	ADECUADO	BIENO	EXCELENTE ESPERADO		LOGRADO	(%)	
GESTIÓN DE ACTIVOS	ISO 27001 A.11.1	Políticas de seguridad física	SI		X				X		8	6	75%	
	ISO 27001 A.12.1.4	Políticas de desarrollo, prueba y producción	NO		X									
	ISO 27001 A.12.2.1	Políticas de Protección Antivirus	SI		X				X		8	4	50%	
	ISO 27001 A.12.3.1	Políticas de respaldo de información	SI		X				X		8	4	50%	
	ISO 27001 A.14.2.1	Políticas de desarrollo seguro	NO		X									
	ISO 27001 A.15.1.1	Políticas de seguridad con terceros	SI		X				X		8	6	75%	
	ISO 27001 A.16.1.1	Políticas de gestión de incidentes	SI		X				X		8	4	50%	
	ISO 27001 A.17.1.1	Políticas de continuidad de negocio	SI		X				X		8	4	50%	
	ISO 27001 A.18.1.4	Políticas de Privacidad de Información por Normativa	SI		X				X		8	6	75%	
	ISO 27001 A.18.2.1	Revisión Seguridad de la Información por una Entidad Especializada	SI		X				X		8	4	50%	
	ISO 27001 A.8.1.1	Gestión de control e inventario de activos lógicos y físicos	SI			X			X		12	6	50%	
	ISO 27001 A.8.1.2	Gestión de Propietarios de los Activos	SI		X				X		8	4	50%	
	ISO 27001 A.8.1.4	Gestión de Retorno del Activo	SI			X			X		12	6	50%	
	ISO 27001 A.11.2.4	Manejo de los Equipos Informáticos	SI			X			X		12	6	50%	
RIESGOS DE SEGURIDAD	ISO 27001 A.11.2.5	Gestión de la Separación de los Activos Informáticos	SI		X				X		8	4	50%	
	ISO 27001 A.11.2.8	Actores externos	SI		X				X		8	4	50%	
	COBIT 5 APO12.01	Revisión de Datos Relevantes	SI			X			X		12	6	50%	
	COBIT 5 APO12.02	Análisis de Riesgos	SI			X			X		12	6	50%	
SEGURIDAD EN RRHH	COBIT 5 APO12.03	Conocer un Perfil Asunto al Riesgo	SI			X			X		12	9	75%	
	COBIT 5 APO12.04	Definir la Respuesta al Riesgo	SI			X			X		12	9	75%	
	ISO 27001 A.6.1.1	Funciones y Responsabilidades de Seguridad de la Información	SI		X				X		8	4	50%	
	ISO 27001 A.7.2.2	Capacitación y Concientización en Seguridad de la Información	SI			X			X		12	6	50%	
INCIDENTES DE SEGURIDAD	ISO 27001 A.7.2.3	Procedimientos disciplinarios	SI		X				X		8	4	50%	
	ISO 27001 A.16.1.1	Detección de Responsabilidades y Rol de Procedimientos	SI			X			X		12	6	50%	
	ISO 27001 A.16.1.2	Reporte de los Eventos Detectados	SI			X			X		12	6	50%	
	ISO 27001 A.16.1.3	Reporte de los Daños Detectados	SI			X			X		12	9	75%	
CONTINUIDAD DE LA SEGURIDAD	ISO 27001 A.16.1.5	Reporte a los Incidentes Detectados	SI			X			X		12	6	50%	
	ISO 27001 A.17.1.1	Continuidad de los Planes de Seguridad de la Información	SI		X				X		8	6	75%	
	ISO 27001 A.17.1.2	Implementación de la Continuidad de la Seguridad de la Información	SI		X				X		8	6	75%	
	ISO 27001 A.17.1.3	Verificación, Revisión y Ejecución del Plan de Continuidad	SI		X					X	8	8	100%	
TOTALES											88	230	61.2%	

PUNTAJE	
MEASURAS DE SEGURIDAD	LOGRADO
POLÍTICA DE SDI	100
GESTIÓN DE ACTIVOS	160
RIESGOS DE SEGURIDAD	90
SEGURIDAD EN RRHH	140
INCIDENTES DE SEGURIDAD	27
CONTINUIDAD DE SEGURIDAD	20
TOTALES	210

MEDIDAS DE SEGURIDAD	PUNTAJE		
	LOGRADO	ESPERADO	(%)
POLÍTICA DE RRHH	100	100	100%
SECCIÓN DE ACTIVOS	30	60	50%
RIESGOS DE SEGURIDAD	30	48	62.5%
SEGURIDAD EN RRHH	14	28	50%
INCIDENTES DE SEGURIDAD	27	48	56.2%
CONTINUIDAD DE SEGURIDAD	20	24	83.3%
TOTALES	230	316	61.2%

Figura 20: Hoja de cálculo de la matriz de evaluación de las medidas organizativas

Elaboración: Propia

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
1	MATRIZ DE CUMPLIMIENTO DE LAS MEDIDAS DE TÉCNICAS																							
2	MEDIDAS DE TÉCNICAS	REFERENCIA	CONTROLES	APLICA	IMPACTO			CUMPLIMIENTO			PUNTAJE													
BAJO					MODERADO	ALTO	MUY BAJO	BAJO	BUENO	EXCELENTE	LOGRADO	ESPERADO	(%)											
6	ACCESOS LÓGICOS	ISO 27001 A.6.1.2	Segmentación de Funciones	SI			X			X		9	12	75%										
7		ISO 27001 A.3.2.1	Gestión de Registro de los Usuarios Lógicos	SI	X					X		6	8	75%										
8		ISO 27001 A.3.2.2	Asignamiento de Acceso Lógico al Usuario	SI		X				X		9	12	75%										
9		ISO 27001 A.3.2.3	Gestión de Verificación de Acceso de Usuarios Privilegiados	SI		X			X			6	12	50%										
10		ISO 27001 A.3.2.5	Restricción de los Derechos de Acceso de los Usuarios	SI		X				X		9	12	75%										
11		ISO 27001 A.3.2.6	Validación y Ajuste de los Accesos Brindados	SI	X					X		6	8	75%										
12	ACCESOS FÍSICOS	ISO 27001 A.3.4.1	Restricción de la Información según el Acceso	SI		X				X		9	12	75%										
13		ISO 27001 A.3.4.4	Utilización de Software para Control de Privilegios	SI		X				X		6	8	75%										
14		ISO 27001 A.11.11	Elaborar un Perfilado para la Seguridad Física	SI		X				X		9	12	75%										
15		ISO 27001 A.11.12	Asignamiento de los Controles Físicos	SI		X				X		9	12	75%										
16		ISO 27001 A.11.15	Asignar las Áreas de Trabajo	SI		X			X			6	12	50%										
17		ISO 27001 A.11.16	Verificar la Distribución Segura en Zonas de Carga	SI		X				X		9	12	75%										
18	CIFRADO	NIST 800-54 SC-103	Asignación de Protección Criptográfica	SI		X			X			6	12	50%										
19		ISO 27001 A.11.15	Verificar los Accesos a Puertos Lógicos	SI		X			X			6	12	50%										
20	SEGURIDAD PERIMETRAL	ISO 27001 A.11.15	Implementación y Restricción de la Solución Tecnológica Firewall	SI		X			X			6	12	50%										
21		ISO 27001 A.11.15	Mantenimiento y Control de las Herramientas de Ciberseguridad	SI		X			X			6	12	50%										
22		ISO 27001 A.11.15	Implementar un IPS dentro de la red organizacional	SI		X			X			6	12	50%										
23		ISO 27001 A.11.15	Implementación de Redes Inalámbricas Seguras	SI		X			X			6	12	50%										
24	SEGURIDAD INTERNA	ISO 27001 A.11.15	Asignamiento de los Datos Inalámbricos	SI		X			X			9	12	75%										
25		ISO 27001 A.11.15	Restricción de Acceso a los Dispositivos de Almacenamiento Externo	SI		X			X			9	12	75%										
26		ISO 27001 A.11.15	Uso de herramientas de Ciberseguridad - DLP	SI		X	X					0	12	0%										
27		ISO 27001 A.11.15	Uso de herramientas de Ciberseguridad - Antivirus	SI		X				X		9	12	75%										
28	TOTALES											156	252	61.9%										
30												PUNTAJE												
31												LOGRADO	ESPERADO	(%)										
32												ACCESOS LÓGICOS	60	96	61%									
33												ACCESOS FÍSICOS	33	48	68%									
34												CIFRADO	6	12	50%									
35												SEGURIDAD PERIMETRAL	24	48	50%									
36												SEGURIDAD INTERNA	33	60	55%									

PUNTAJE		PUNTAJE	PUNTAJE
LOGRADO	ESPERADO		
ACCESOS LÓGICOS	40	48	71%
ACCESOS FÍSICOS	33	48	69%
CIFRADO	6	12	50%
SEGURIDAD PERIMETRAL	24	48	50%
SEGURIDAD INTERNA	24	48	50%
TOTALES	156	252	61.5%

Figura 21: Hoja de cálculo de la matriz de evaluación de las medidas técnicas

Elaboración: Propia

Figura 22: Hoja de cálculo con los indicadores del nivel de cumplimiento por cada medida del modelo de referencia y el nivel total de protección de datos personales

Elaboración: Propia

6.1.2.3 Ejecución

En los siguientes párrafos se explica detalladamente la ejecución del proceso de validación del modelo de referencia propuesto.

6.1.2.3.1 Recopilación de información

En esta primera parte del proceso de validación, se obtiene toda la información de la microfinanciera referida a los datos personales que se tratan y almacenan. Se solicitó al encargado de la microfinanciera un documento donde se indique los roles o jerarquía

organizacional de la empresa, los documentos donde estén detallados las políticas de seguridad de información que se han implementado, documentos donde se tengan diagramados los procesos de negocio y la respectiva caracterización de cada uno de ellos, catalogo donde se indique las aplicaciones móviles, web o de escritorio que se utilicen en la microfinanciera para las operaciones, el catálogo de la infraestructura tecnológica que emplea para el soporte de las aplicaciones del negocio, redes y telecomunicaciones, y el uso personal o compartido de las computadoras de los colaboradores, y por último, los documentos o formularios donde se registra la información personal de los clientes, colaboradores o proveedores de la microfinanciera.

En la Cooperativa de Ahorro y Crédito “Vale un Perú”, se recopiló la siguiente información:

- **Roles**

La COOPAC “VALEUN” tiene un manual de organización y funciones de los colaboradores. Este define un organigrama de las áreas de la empresa. Con esta información se puede conocer los roles involucrados en el tratamiento de los datos personales.

- **Comité Administrativo:** Desempeña su labor con la diligencia, cuidado y reserva debidos, velando siempre por los mejores intereses de la empresa y de sus accionistas. Tiene un control superior con respecto a la toma de decisiones en la cooperativa. Supervisa semanalmente la situación económica y revisa en conjunto con el Gerente General las oportunidades de inscripción de socios potenciales.
- **Gerente General:** Es el funcionario ejecutivo de más alto nivel en la Cooperativa COOP, es responsable de la gestión administrativa, técnica, financiera y legal de la misma. Asimismo, la representa legal y formalmente ante terceros, con las atribuciones, facultades y limitaciones impuestas por la Legislación Cooperativa y el Estatuto vigente. Reporta semanalmente al Consejo de Administración.
- **Administración:** Es responsable de la documentación e información bajo su custodia y del apoyo en las labores propias de su cargo a los demás puestos de trabajo en la Cooperativa.
- **Contabilidad:** Se encarga del registro y control de las operaciones contables en los libros de acuerdo con los dispositivos legales vigentes y preparar de

manera oportuna y veraz la información financiera, técnica y estadística de su competencia que es solicitada por los organismos supervisores correspondientes, por el Consejo de Administración y la Gerencia.

- **Vigilancia:** Presta el servicio de protección integral, seguridad y vigilancia en todas las instalaciones y ambientes de la Cooperativa, por las horas que se le requiera.
- **Limpieza:** Se encarga de mantener las instalaciones con el higiene y cuidado óptimos para las operaciones del personal de la Cooperativa.
- **Operaciones:** Se encarga del control y de las acciones necesarias sobre las operaciones administrativas, de uso y manejo del desembolso y recuperación de los fondos de la Cooperativa.
- **Caja:** Se encarga del adecuado manejo de los movimientos de ingresos y egresos de las operaciones en efectivo en moneda nacional o extranjera de la Cooperativa.
- **Créditos y cobranzas:** Se encarga de las colocaciones de créditos, recuperaciones y el adecuado proceso de información captación y registro de nuevos socios, así como el control y administración de la tramitación, análisis, calificación y formalización de los créditos y cobranzas en la Cooperativa.
- **Soporte TI:** Mantiene el funcionamiento de los sistemas de información de la cooperativa, evitando sus interrupciones y brindando apoyo a las consultas y problemas que surjan en las operaciones.

Figura 23: Organigrama de la Cooperativa de Ahorro y Crédito "Vale un Perú"

Fuente: Propia

- **Políticas de seguridad de la información**

La COOP "VALEUN" no tiene implementadas políticas de seguridad de información. Tampoco existe ninguna documentación al respecto. Asimismo, el conocimiento del personal con respecto al tema es bajo.

- **Procesos de negocio**

La COOP "VALEUN" cuenta con un manual de procesos y procedimientos administrativos y operativos. En este documento se muestra diagramas de flujo de actividades de cada proceso y procedimiento (ver ANEXO D). Los procesos definidos en el documento son los 9 siguientes:

- Admisión de nuevo colaborador
- Admisión de nuevo socio.
- Pago de planillas
- Apertura de cuenta de ahorros.
- Apertura de cuenta de depósito plazo.
- Apertura de cuenta de aportaciones.
- Cierre de módulo de préstamos
- Desembolso de crédito
- Retiro del socio

Sin embargo, se realizaron entrevistas con cada dueño de proceso para recabar información más detallada y comparar si el proceso que se describe en el documento tiene relación con el proceso que explica el encargado del proceso. A partir de esto, se identificó que el proceso de “Retiro de socio” no cumplía con lo definido, debido a que en la práctica no se realizaban algunas actividades importantes. Entre las actividades que no se cumplían estaban el registro del retiro del socio en el sistema y el cierre de su cuenta en el sistema VITEC.

Por otra parte, mediante las entrevistas también se descubrieron procesos que no estaban documentados (ver ANEXO D). Estos procesos son:

- Estado de cuenta del préstamo
- Refinanciamiento del préstamo
- Emisión de reportes
- Cancelación de cuenta de depósito a plazo.
- Atención de incidentes tecnológicos.
- Cancelación de préstamos

- **Aplicaciones**

La Cooperativa de Ahorro y Créditos “Vale un Perú” cuenta con sistema para la gestión de créditos y préstamos de los socios. En este sistema se registra la información del socio, los movimientos que realiza, los préstamos solicitados y su estado de cuenta. Este sistema tiene como nombre “VITEC”, tiene de antigüedad 9 años, es una aplicación de escritorio desarrollado en el lenguaje de programación Visual Basic 6.0 y emplea una base de datos Oracle 10g. Es el sistema principal de la empresa debido a que sirve para manejar las operaciones diarias. El sistema es usado por el Gerente General, Jefe de Operaciones, Jefe de Créditos y Préstamos, Analista de Créditos y Préstamos, y Cajero.

Vitec B Associates SAC - [Expediente de créditos]

Opciones window

Expediente de Crédito

Año: 2013 Tipo de Crédito: P FICHA ASOCIADA N° Exp: 1000

Datos del Asociado

Asociado: 980 CIP: 326895000 Nombre: AYASTA AGAPITO JAIME

Ingreso: 00-11-2000 Delegado:

Estado: ACTIVO Condición: NORMAL

Fec. Apertura: 13-03-2013 Plazo: 5 Meses

Fec. Aprobación: Gracia: 15 Días

Importe: 200.00 Fec. Desemb.: Cuotas: m

Pagare: Finalidad: JUROS

Condición: NORMAL

Observaciones:

Requisitos Avalos

Condiciones Valoración

Programa de Pago

Refinanciación / Cancelación

Efectivo: 400.00

#	Cuo.	Vencimiento	Capital	Interes	Cuota	Desgra	Encaje	Interes	Descto	Pagado	Saldo
1	01-03-2013	m m	100.00	10.00	110.00	0.00	0.00	0.00	0.00	110.00	0.00
2	01-04-2013	m m	100.00	10.00	110.00	0.00	0.00	0.00	0.00	110.00	0.00
3	01-05-2013	m m	100.00	10.00	110.00	0.00	0.00	0.00	0.00	110.00	0.00
4	30-06-2013	m m	100.00	10.00	110.00	0.00	0.00	0.00	0.00	110.00	0.00
Total:			400.00	40.00	440.00	0.00	0.00	0.00	0.00	440.00	0.00

Rechazo: 1 EXP. NO VALUADO

Estado: PENDIENTE DE APROBACION

Referencia:

Actualizado por: I. DEUCAR el 13-03-2013

Figura 24: Interfaz gráfica 1 de la ventana "Expediente de créditos" del sistema VITEC

Vitec B Associates SAC - [Expediente de créditos]

Opciones window

Expediente de Crédito

Año: 2013 Tipo de Crédito: P FICHA ASOCIADA N° Exp: 1000

Datos del Asociado

Asociado: 257 CIP: 60381700 Nombre: ANCASSI BABILON DE PORTILLA GLORIA

Ingreso: 20-06-2005 Delegado:

Estado: ACTIVO Condición: NORMAL

Fec. Apertura: 13-03-2013 Plazo: 4 Meses

Fec. Aprobación: Gracia: 15 Días

Importe: 2000.00 Fec. Desemb.: Cuotas: m

Pagare: Finalidad: JUROS

Condición: NORMAL

Observaciones:

Requisitos Avalos

Condiciones Valoración

Programa de Pago

Refinanciación / Cancelación

Efectivo: 2000.00

#	Cuo.	Vencimiento	Capital	Interes	Cuota	Desgra	Encaje	Interes	Descto	Pagado	Saldo
1	13-03-2013	m m	2000.00	200.00	2200.00	0.00	0.00	0.00	0.00	2200.00	0.00
2	13-04-2013	m m	2000.00	200.00	2200.00	0.00	0.00	0.00	0.00	2200.00	0.00
3	13-05-2013	m m	2000.00	200.00	2200.00	0.00	0.00	0.00	0.00	2200.00	0.00
4	13-06-2013	m m	2000.00	200.00	2200.00	0.00	0.00	0.00	0.00	2200.00	0.00
Total:			8000.00	800.00	8800.00	0.00	0.00	0.00	0.00	8800.00	0.00

Rechazo: 2 EXP. NO VALUADO

Estado: PENDIENTE DE APROBACION

Referencia:

Actualizado por: P. DEUCAR el 13-03-2013

Figura 25: Interfaz gráfica 2 de la ventana "Expediente de créditos" del sistema VITEC

- Infraestructura tecnológica
 - Servidor de aplicaciones y base de datos:

La cooperativa tiene un servidor físico que es empleado como aplicaciones y base de datos. Ese servidor almacena el sistema de gestión de créditos y préstamos “VITEC” y a la vez contiene el motor de base de datos Oracle 11g. Las especificaciones principales de este servidor son las siguientes:

- Procesador: Intel Core i7-960 de 8 núcleos a 3.3 GHz
- Memoria RAM: 8 Gb DDR3
- Disco Duro: 1 TB SATA 2.5 a 5,400 RPM

o Servidor de archivos:

Por otra parte, la cooperativa tiene un servidor de archivos donde los colaboradores hacen público entre ellos los archivos de hoja de cálculo con los que trabajan y para mantener un histórico de los registros de préstamos y cobranzas. Sin embargo, en este servidor no se maneja restricciones de acceso a la información. Las especificaciones principales de este servidor son las siguientes:

- Procesador: Intel Core i5-4670 de 4 núcleos a 3.8 GHz
- Memoria RAM: 4 Gb DDR3
- Disco Duro: 1 TB SATA 2.5 a 5,400 RPM

Figura 26: Servidor de archivos y servidor aplicaciones y base de datos de la Cooperativa de Ahorro y Crédito "Vale un Perú"

○ Computadoras de escritorio:

La cooperativa dispone de 11 computadoras de escritorio para el uso de los colaboradores. Estas computadoras almacenan los datos personales con trabajan los colaboradores. En el caso de la computadora de la Gerente General, contenía información de los empleados con sus sueldos y los contactos de los proveedores de la cooperativa. Las especificaciones de las computadoras son las siguientes:

- Procesador: Intel Core i5-3570 de 4 núcleos a 3.4 GHz
- Memoria RAM: 4 Gb DDR3
- Disco Duro: 500Gb SATA 2.5 a 5,400 RPM

Figura 27: Computadora de escritorio de la Cooperativa de Ahorro y Crédito "Vale un Perú"

● **Documentos**

La Cooperativa de Ahorro y Créditos “Vale un Perú” maneja la siguiente lista de documentos:

- Formularios de inscripción de socios: Contiene la información personal del cliente interesado en convertirse socio de la cooperativa. Se indica

principalmente, sus nombres, apellidos, DNI, sexo, fecha de nacimiento, número de teléfono y celular, sueldo promedio en los últimos 5 meses, domicilio, estado civil, datos personales del cónyuge y datos personales del aval. Esta ficha se entrega al cliente en el proceso de Admisión de nuevo socio. Se almacena en el expediente del socio.

- Expediente de socios: Es un historial de todos los movimientos realizados por el socio en su cuenta de la cooperativa. En él está registrado la cantidad de dinero que se prestó o ahorro a su cuenta desde su ingreso. Estos documentos son almacenados en un armario y ordenados de forma alfabética.

Figura 28: Armario de expedientes de la Cooperativa de Ahorro y Crédito "Vale un Perú"

- Lista de datos personales de los empleados: Contiene la información personal de los colaboradores de la cooperativa. Los datos almacenados son los siguientes: Nombres, apellidos, fecha de nacimiento, sueldo, DNI, sexo, número de teléfono y domicilio. Se almacenan en una CPU que funge de Servidor de Archivos. Dentro de este compartido, están almacenados los bancos de datos de los datos personales que maneja "Vale un Perú".

6.1.2.3.2 Diagnóstico

En esta etapa del proceso de validación, con la información recopilada en la etapa anterior, se elabora el mapa del ciclo de vida del dato personal para conocer el flujo del dato personal

a lo largo de la cooperativa. Este flujo permite descubrir las fuentes que generan los datos personales, los sistemas informáticos que los tratan y almacenan en la infraestructura tecnológica, los roles que emplean los datos personales y fases por las que transcurre. Posterior a ello, se realiza una evaluación del nivel de protección de datos personales de la cooperativa a fin saber, en la condición en las que se encuentra, los aspectos más críticos y urgentes que se deben atender, y, a la vez, el nivel de cumplimiento de la Ley 29733 – Ley de protección de datos personales.

- **Ciclo de vida del dato personal**

De la información obtenida en la etapa anterior, se construyó el ciclo de vida del dato personal en la COOPAC “VALEUN”.

Figura 29: Mapa del ciclo de vida del dato personal de la Cooperativa de Ahorro y Crédito "Vale un Perú". Parte 1

Fuente: Propia

Figura 30: Mapa del ciclo de vida del dato personal de la Cooperativa de Ahorro y Crédito "Vale un Perú". Parte 2

Fuente: Propia

Captura	Gestión de dato personal	Retención	Destrucción	Transición
Admisión de nuevo socio	Apertura de cuenta de ahorros	Almacenar movimientos en expedientes	Retiro de socio	Emisión de reportes
Admisión de nuevo colaborador	Apertura de cuenta de dep. a plazo	Registro de cambio de datos del empleado en documento Excel	Cancelación de cuenta depósito a plazo	
	Apertura cuenta aportaciones	Guardar créditos solicitados en sistema VITEC	Cancelación de préstamo	
	Desembolso de crédito			
	Refinanciamiento de crédito			
	Pago de Planillas			

Tabla 22: Detalle del ciclo de vida del dato personal de la Cooperativa de Ahorro y Crédito "Vale un Perú"

Fuente: Propia

- **Evaluación de las medidas legales**

Para esta matriz, todos los controles tienen impacto alto debido al costo elevado de las sanciones por el incumplimiento de la Ley de protección de datos personales. Para el caso de la Cooperativa de Ahorro y Crédito “Vale un Perú”, la medida de transferencia no aplica, debido a que la cooperativa no realiza ningún envío de los datos personales de sus clientes, colaboradores o proveedores a entidades o personas externas a la empresa. La matriz se muestra a continuación:

REGLAMENTO DE LEY 29733													
MEDIDAS LEGALES	ARTÍCULO	CONTROLES	APLICA	IMPACTO			CUMPLIMIENTO			PUNTAJE			
				BAJO	MODERADO	ALTO	MUY BAJO	BAJO	BUENO	EXCELENTE	ESPERADO	LOGRADO	(%)
CONSENTIMIENTO	11,12	Solicitar el consentimiento del titular de los datos personales para realizar el tratamiento de sus datos personales.	SI			X	X				12	0	0%
	11,14	Solicitar el consentimiento del titular de los datos personales para realizar el tratamiento de sus datos sensibles.	SI			X	X				12	0	0%
	11,16	Solicitar el consentimiento para el tratamiento de datos personales al titular de datos personales de forma libre, previo, expreso e informado.	SI			X		X			12	3	25%
	11,27, 28	En caso se traten datos personales de menores de edad, debe tener el consentimiento de sus titulares o tutores.	NO			X							
TRANSFERENCIA	11,19	Solicitar el consentimiento del titular de datos personales para transferir sus datos a nivel nacional e internacional.	NO			X							
	22	El receptor de la transferencia de los datos personales asume el rol de titular del banco de datos personales o responsable del tratamiento y realiza el tratamiento conforme a la finalidad por la cual fueron recopilados y las misma obligaciones del emisor.	NO			X							
INSCRIPCIÓN DE BANCO DE DATOS	78,81-84	El titular de banco de datos personales inscribe los bancos de datos personales en el registro nacional de protección de datos personales.	SI			X			X		12	9	75%
	24,25, 26,77, 83	El titular de banco de datos personales declara las comunicaciones correspondientes al flujo transfronterizo.	SI			X	X				12	0	0%

DERECHOS A.R.C.O.	50	El responsable de los datos personales dispone de un documento de solicitud para que el titular pueda ejercer sus derechos.	SI			X		X			12	3	25%
	52-56	El responsable de los datos personales definió e implemento procedimientos para la atención de solicitudes que no han sido completadas correctamente.	SI			X		X			12	3	25%
	55	La organización debe tener un documento que especifique los tiempos de respuesta ante la solicitud de un titular de datos personales.	SI			X		X			12	3	25%
	60	El titular de datos personales tiene derecho a solicitar toda la información relacionada al tratamiento de sus datos personales.	SI			X		X			12	3	25%
	61	El titular de datos personales tiene derecho a obtener toda la información relativa a sus propios datos personales, así como las condiciones y generalidades del tratamiento de los mismos.	SI			X		X			12	3	25%
	64	El titular de datos personales tiene derecho a solicitar la actualización de los datos personales que fueron modificados a la fecha del ejercicio del derecho.	SI			X		X			12	3	25%
	65	El titular de datos personales tiene derecho a solicitar la rectificación de los datos personales que resulten ser erróneos, inexactos o falsos.	SI			X		X			12	3	25%
	66	El titular de datos personales tiene derecho a solicitar la inclusión de los datos personales faltantes que hacen que su información sea incompleta, omitida o eliminada en atención a su relevancia para dicho tratamiento.	SI			X		X			12	3	25%
	67-68	El titular de los datos personales tiene derecho a solicitar la supresión o cancelación de sus datos personales que hayan sido transferidos o no, siempre y cuando cumpla con los requisitos de la ley.	SI			X		X			12	3	25%
	71	El titular de datos personales tiene derecho a oponer al tratamiento de sus datos personales cuando no se hubiese brindado su consentimiento para la recopilación.	SI			X		X			12	3	25%

SUBCONTRATOS	33-34	La organización contrata servicios de medios tecnológicos tercerizados garantizando el adecuado tratamiento de los datos.	SI			X	X				12	0	0%
	35,37,38	La organización contrata servicios de medios tecnológicos tercerizados que tengan mecanismos adecuados para la prestación.	SI			X	X				12	0	0%
VIDEOGILANCIA	02-2020	El titular de datos personales o responsable de tratamiento cumple con lo dispuesto en la resolución N° 02-2020-JUS/DGTAIPD.	SI			X	X				12	0	0%
TOTALES										X	204	42	20.6%

Tabla 23: Matriz de evaluación de las medidas legales del estado actual de la Cooperativa de Ahorro y Crédito “Vale un Perú”

Fuente: Propia

El resultado final de la evaluación de las medidas legales fue el siguiente:

- Consentimiento, la microfinanciera se encuentra en una etapa muy inmadura del proceso para obtener el consentimiento de los datos personales que trata.
- Transferencia, no aplica para este caso, ya que la microfinanciera solo tiene un local.
- Inscripción de banco de datos, la microfinanciera ha inscrito 2 bancos de datos de 6 quería debería tener correctamente inscritos. Además, no ha declarado el flujo transfronterizo.
- Derechos ARCO, la microfinanciera cuenta con controles básicos/manuales para poder darle solución a una consulta para ejercer los derechos fundamentales.
- Subcontratos, la microfinanciera no ha elaborado un plan para tratar este punto, todos los contratos no cuentan con cláusulas de protección de datos personales.
- Videovigilancia, la microfinanciera no ha actualizado los afiches según la actualización de la Ley.

Por ello, el resultado es de un 21% de cumplimiento en las medidas legales:

MEDIDAS	PUNTAJE		
	LOGRA	ESPER	(%)
CONSENTIMIENTO	3	36	8%
TRANSFERENCIA	N/A	N/A	N/A
INSCRIPCIÓN DE BANCO DE DATOS	9	24	38%
DERECHOS A.R.C.O.	30	120	25%
SUBCONTRATOS	0	24	0
VIDEOGILANCIA	0	12	0
TOTALES	42	204	21%

Tabla 24: Resultados de la evaluación de las medidas legales

Fuente: Propia

• Evaluación de las medidas organizativas

Para esta matriz, los controles han sido divididos entre impactos altos y medios, ya que el factor organizacional es importante para cualquier empresa, pero la información y procesos de Seguridad de la Información se pueden tratar de formas distintas, según la

entidad. Para el caso de la Cooperativa de Ahorro y Crédito “Vale un Perú”, todas las medidas organizativas aplican. La matriz se muestra a continuación:

MEDIDAS DE ORGANIZATIVAS	REFERENCIA	CONTROLES	APLICA	IMPACTO			CUMPLIMIENTO					PUNTAJE		
				BAJO	MODERADO	ALTO	MUY BAJO	BAJO	ADECUADO	BUENO	EXCELENTE	ESPERADO	LOGRADO	(%)
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	ISO 27001 A.5.1.1	Política General de Seguridad	SI		X		X					8	0	0%
	ISO 27001 A.5.1.2	Revisión de la Política General de Seguridad	SI		X		X					8	0	0%
	ISO 27001 A.6.1.1	Roles y Responsabilidades para el Resguardo de la Seguridad	SI			X		X				12	3	25%
	ISO 27001 A.7.2.1	Responsabilidad de la Alta Dirección	SI			X		X				12	3	25%
	ISO 27001	Política para la Revisión de los Derechos de Ingreso Lógicos	SI		X			X				8	2	25%
	ISO 27001 A.10.1.1	Política de Validación de Lineamientos Criptográficos	SI		X		X					8	0	0%
	ISO 27001 A.11.2.9	Política de Escritorios Ordenados	SI		X		X					8	0	0%
	ISO 27001 A.6.2.1	Política de Control para los Dispositivos Móviles Internos	SI		X		X					8	0	0%
	ISO 27001 A.7.2.2	Política de entrenamiento al personal en términos de seguridad	SI		X		X					8	0	0%
	ISO 27001 A.8	Política de gestión de activos	SI		X		X					8	0	0%

	ISO 27001 A.8.2.1	Política de Segmentación de la Información	SI		X		X					8	0	0%
	ISO 27001 A.9.1.1	Política de acceso de usuario a la red empresarial	SI		X		X					8	0	0%
	ISO 27001 A.11.1	Política de seguridad física	SI		X		X					8	0	0%
	ISO 27001 A.12.1.4	Política de desarrollo, prueba y producción	NO		X		X							
	ISO 27001 A.12.2.1	Política de Protección Antimalware	SI		X			X				8	2	25%
	ISO 27001 A.12.3.1	Política de respaldo de información	SI		X			X				8	2	25%
	ISO 27001 A.14.2.1	Política de desarrollo seguro	NO		X									
	ISO 27001 A.15.1.1	Política de seguridad con terceros	SI		X		X					8	0	0%
	ISO 27001 A.16.1.1	Política de gestión de incidentes	SI		X		X					8	0	0%
	ISO 27001 A.17.1.1	Política de continuidad de negocio	SI		X		X					8	0	0%
	ISO 27001 A.18.1.4	Política de Privacidad de Información por Normativa	SI		X			X				8	2	25%
	ISO 27001 A.18.2.1	Revisión Seguridad de la Información por una Entidad Especializada	SI		X		X					8	0	0%

GESTIÓN DE ACTIVOS	ISO 27001 A.8.1.1	Gestión de control e inventario de activos lógicos y físicos	SI			X	X					12	0	0%
	ISO 27001 A.8.1.2	Gestión de Propietarios de los Activos	SI		X			X				8	2	25%
	ISO 27001 A.8.1.4	Gestión de Retorno del Activo	SI			X	X					12	0	0%
	ISO 27001 A.11.2.4	Mantenimiento de los Equipos Informáticos	SI			X		X				12	3	25%
	ISO 27001 A.11.2.5	Gestión de la Separación de los Activos Informáticos	SI		X		X					8	0	0%
	ISO 27001 A.11.2.8	Activos obsoletos	SI		X		X					8	0	0%
RIESGOS DE SEGURIDAD	COBIT 5 APO12.01	Recopilación de Datos Relevantes	SI			X		X				12	3	25%
	COBIT 5 APO12.02	Analizar los Riesgos	SI			X		X				12	3	25%
	COBIT 5 APO12.03	Conservar un Perfil Atento al Riesgo	SI			X	X					12	0	0%
	COBIT 5 APO12.06	Determinar la Respuesta al Riesgo	SI			X		X				12	3	25%
SEGURIDAD EN RRHH	ISO 27001 A.6.1.1	Funciones y Responsabilidades de Seguridad de la Información	SI		X		X					8	0	0%
	ISO 27001 A.7.2.2	Capacitación y Concientización en Seguridad de la Información	SI			X	X					12	0	0%

	ISO 27001 A.7.2.3	Procesos disciplinarios	SI		X		X					8	0	0%
INCIDENTES DE SEGURIDAD	ISO 27001 A.16.1.1	Detección de Responsabilidades y Flujo de Procedimientos	SI			X		X				12	3	25%
	ISO 27001 A.16.1.2	Reporte de los Eventos Detectados	SI			X	X					12	0	0%
	ISO 27001 A.16.1.3	Reporte de las Debilidades Detectadas	SI			X	X					12	0	0%
	ISO 27001 A.16.1.5	Respuesta a los Incidentes Detectados	SI			X		X				12	3	25%
CONTINUIDAD DE LA SEGURIDAD	ISO 27001 A.17.1.1	Continuidad de los Planes de Seguridad de la Información	SI		X		X					8	0	0%
	ISO 27001 A.17.1.2	Implementación de la Continuidad de la Seguridad de la Información	SI		X		X					8	0	0%
	ISO 27001 A.17.1.3	Verificación, Revisión y Evaluación del Plan de Continuidad	SI		X		X					8	0	0%
TOTALES												376	34	9.0%

Tabla 25: Matriz de evaluación de las medidas organizativas del estado actual de la Cooperativa de Ahorro y Crédito “Vale un Perú”

Fuente: Propia

El resultado final de la evaluación de las medidas organizativas fue el siguiente:

- Políticas de Seguridad de la Información, la microfinanciera no cuenta con una gestión integral documentaria de Seguridad de la Información, pero tiene algunos procesos ad-hoc que utiliza para realizar algunas funciones como designar permisos para los usuarios, documentos de privacidad de la información, entre otros.
- Gestión de Activos, la microfinanciera tiene pocos controles efectivos ante el uso de activos de información, solo cuenta con procedimiento manuales para darle mantenimiento a los equipos e indicar quién es el propietario.
- Riesgos de Seguridad, la microfinanciera solo actúa ante un riesgo cuando este ya se ha materializado, no cuenta con una estructura real para mitigar los riesgos inherentes y/o residuales.
- Seguridad en Recursos Humanos, la microfinanciera no realiza ningún tipo de actividad para concientizar a sus colaboradores.
- Incidentes de Seguridad, la microfinanciera solo tiene definido quién debe actuar cuando se produce un rol, esta persona es el encargado del área donde se produzca el incidente. Por otro lado, no cuentan con una base para incidentes como tal.
- Continuidad de Negocio, la microfinanciera no cuenta con ningún lineamiento para realizar la ejecución de planes de acción para la continuidad de la empresa ante algún evento perjudicial.

Por ello, el porcentaje obtenido es del 9% de cumplimiento.

MEDIDAS DE SEGURIDAD	PUNTAJE		
	LOGRA	ESPER	(%)
POLÍTICA DE SDI	14	168	8%
GESTIÓN DE ACTIVOS	5	60	8%
RIESGOS DE SEGURIDAD	9	48	19%
SEGURIDAD EN RRHH	0	28	0
INCIDENTES DE SEGURIDAD	6	48	13%
CONTINUIDAD DE SEGURIDAD	0	24	0
TOTALES	34	376	9.0%

- **Evaluación de las medidas técnicas**

Para esta matriz, los controles han sido divididos entre impactos altos y medios, ya que el factor técnico tiene relevancia para la Seguridad de la Información, como para la Ciberseguridad. En estas categorías se van a medir el nivel de cumplimiento de cada lineamiento (físico y lógico), respecto de lo indicado en el cuadro. Para el caso de la Cooperativa de Ahorro y Crédito “Vale un Perú”, todas las medidas técnicas aplican. La matriz se muestra a continuación:

MEDIDAS DE TÉCNICAS	REFERENCIA	CONTROLES	APLICA	IMPACTO			CUMPLIMIENTO				PUNTAJE			
				BAJO	MODERADO	ALTO	MUY BAJO	BAJO	ADECUADO	BUENO	EXCELENTE	LOGRADO	ESPERADO	(%)
ACCESOS LÓGICOS	ISO 27001 A.6.1.2	Segmentación de Funciones	SI			X		X				3	12	25%
	ISO 27001 A.9.2.1	Gestión de Registro de los Usuarios Lógicos	SI		X		X					0	8	0%
	ISO 27001 A.9.2.2	Aprovisionamiento de Accesos Lógicos al Usuario	SI			X		X				3	12	25%
	ISO 27001 A.9.2.3	Gestión de Verificación de Accesos de Usuarios Privilegiados	SI			X	X					0	12	0%
	ISO 27001 A.9.2.5	Revisión de los Derechos de Acceso de los Usuarios	SI			X		X				3	12	25%
	ISO 27001 A.9.2.6	Validación y Ajuste de los Accesos Brindados	SI		X			X				2	8	25%
	ISO 27001 A.9.4.1	Restricción a la Información según el Acceso	SI			X		X				3	12	25%
	ISO 27001 A.9.4.4	Utilización de Software para Control de Privilegios	SI		X		X					0	8	0%
ACCESOS FÍSICOS	ISO 27001 A.11.1.1	Elaborar un Perímetro para la Seguridad Física	SI			X		X				3	12	25%
	ISO 27001 A.11.1.2	Aseguramiento de los Controles Físicos	SI			X		X				3	12	25%
	ISO 27001 A.11.1.5	Asegurar las Áreas de Trabajo	SI			X		X				3	12	25%
	ISO 27001 A.11.1.6	Verificar la Distribución Segura en Zonas de Carga	SI			X			X			6	12	50%
CIFRADO	NIST 800-54 SC-13	Asignación de Protección Criptográfica	SI			X	X					0	12	0%
SEGURIDAD PERIMETRAL	CSC CSI 7.1 CSC 9.3	Verificar los Accesos a Puertos Lógicos	SI			X			X			6	12	50%
	CSC CSI 7.1 CSC 9.6	Implementación y Revisión de la Solución Tecnológica Firewall	SI			X			X			6	12	50%

	CSC CSI 7.1 CSC 8.1	Manejo y Control de las Herramientas de Ciberseguridad	SI			X	X					0	12	0%
	CSC CSI 7.1 CSC 8.6	Implementar un IPS dentro de la red organizacional	SI			X	X					0	12	0%
SEGURIDAD INTERNA	CSC CSI 7.1 CSC 15.5	Implementación de Redes Inalámbricas Seguras	SI			X			X			6	12	50%
	CSC CSI 7.1 CSC 15.3	Aseguramiento de las Redes Inalámbricas	SI			X	X					0	12	0%
	CSC CSI 7.1 CSC 13.5	Restricción de Acceso a los Dispositivos de Almacenamiento Externo	SI			X	X					0	12	0%
	CSC CSI 7.1 CSC 13.9	Uso de herramientas de Ciberseguridad – DLP	SI			X	X					0	12	0%
	CSC CSI 7.1 CSC 8.2	Uso de herramienta de Ciberseguridad - Antimalware	SI			X		X				3	12	25%
TOTALES												50	252	19.8%

Tabla 26: Matriz de evaluación de las medidas técnicas del estado actual de la Cooperativa de Ahorro y Crédito “Vale un Perú”

Fuente: Propia

El resultado final de la evaluación de las medidas técnicas fue el siguiente:

- Accesos Lógicos, la microfinanciera cuenta con algunos puntos para la revisión y otorgamiento de accesos a los servicios informáticos, tales como la verificación de accesos brindados, funciones de usuarios privilegiados, entre otros.
- Accesos Físicos, la microfinanciera tiene definido segmentos de área segura para laborar, también la tiene en la zona de carga, dónde incluso tiene un control de bitácora y cercado de perímetro.
- Cifrado, la microfinanciera no ha implementado una tecnología de cifrado para sus datos personales clave.
- Seguridad Perimetral, la microfinanciera tiene considerados algunos aspectos para la seguridad externa de la red, como la configuración del firewall local y el bloqueo de dispositivos USB en algunos activos.
- Seguridad Interna, la microfinanciera considera aspectos de implementación de redes inalámbricas en otro segmento de red para sus colaboradores e invitados, la revisión de malware en los dispositivos se realiza de forma manual.

Por ello, el porcentaje obtenido es del 19,8% de cumplimiento.

MEDIDAS DE SEGURIDAD	PUNTAJE		
	LOGRA	ESPER	(%)
ACCESOS LÓGICOS	14	84	17%
ACCESOS FÍSICOS	15	48	31%
CIFRADO	0	12	0%
SEGURIDAD PERIMETRAL	12	48	25%
SEGURIDAD INTERNA	9	60	15%
TOTALES	50	252	19.8%

Tabla 27: Resultados de la evaluación de las medidas técnicas

Fuente: Propia

6.1.2.3.3 Plan de mejora

En esta fase de la validación, se propone un conjunto de controles que incrementen el nivel de protección de los datos personales. Este listado de controles toma como prioridad a las

medidas con cumplimiento muy bajo que resultan de gran urgencia implementarse en la cooperativa. A continuación, se listará los controles legales, organizativos y técnicos:

- Controles legales
 - Regularización de la inscripción de los bancos de datos personales ante la Autoridad Nacional de Protección de Datos Personales (ANPDP).
 - Incluir las cláusulas de consentimiento en la Ficha de Inscripción de nuevo socio y Contrato de colaboradores.
 - Incluir en el contrato de proveedores y/o colaboradores el Acuerdo de Confidencialidad.
 - Incluir en la Ficha de Inscripción de nuevo socio los Derechos Fundamentales del titular de los datos personales.
- Controles organizativos:
 - Creación de 17 políticas de seguridad de información.
 - Creación de 2 instructivos de seguridad de la información.
 - Creación de un curso de concientización de seguridad de la información.
 - Implementación del sistema de gestión de servicios TI (iTop).
 - Creación de la matriz de incidentes tecnológicos.
 - Creación de la matriz de riesgos tecnológicos y activos físicos.
 - Creación de la matriz de activos.
- Controles técnicos:
 - Implementación de antivirus en 8 computadoras de escritorio (Avast Pro-Antivirus 2019).
 - Verificación y activación del Firewall Windows Local.
 - Definir reglas de entradas y salidas por segmento de red.
 - Adquisición de llaves y cerraduras (armario de expedientes)
 - Aislamiento del centro de datos.
 - Canaletas para cableado.
 - Documento de identificación laboral
 - Bitácora de ingresos y salidas.
 - Revisión de accesos lógicos del sistema VITEC.
 - Reordenamiento de carpetas compartidas por área y función.
 - Bloqueo de puerto USB

6.1.2.3.4 Implementación

En esta fase, se llevan a cabo todos los controles que se han definido en la fase anterior. Debido a las restricciones de presupuesto y recursos de la Cooperativa de Ahorro y Créditos “Vale un Perú”, se tuvieron que priorizar las medidas más urgentes que deberán atenderse para evitar las costosas sanciones que impone la Autoridad Nacional de Protección de Datos Personales (ANPDP). Por ello, las medidas implementadas fueron las siguientes:

- Regularización de la inscripción de los bancos de datos personales ante la Autoridad Nacional de Protección de Datos Personales (ANPDP).
- Incluir las cláusulas de consentimiento en la Ficha de Inscripción de nuevo socio y Contrato de colaboradores.
- Incluir en el contrato de proveedores y/o colaboradores el Acuerdo de Confidencialidad.
- Incluir en la Ficha de Inscripción de nuevo socio los Derechos Fundamentales del titular de los datos personales.
- Creación de 17 políticas de seguridad de información.
- Creación de 2 instructivos de seguridad de la información.
- Creación de un curso de concientización de seguridad de la información.
- Implementación del sistema de gestión de servicios TI (iTop).
- Implementación de antivirus en 5 computadoras de escritorio (Avast Pro-Antivirus 2019).
- Verificación y activación del Firewall Windows Local.
- Definir reglas de entradas y salidas por segmento de red.
- Adquisición de llaves y cerraduras (armario de expedientes)

A continuación, se detalla cómo se ha implementado los controles:

- **Políticas de seguridad de la información**

Se desarrollaron las siguientes políticas (ver Anexos E):

- Política de inventario de activos.
- Política de acceso a la red y seguridad lógica.
- Política de administración de las operaciones y comunicaciones.
- Política de adquisición, desarrollo, instalación y mantenimiento de los sistemas de información.

- Política de clasificación de la información.
- Política de control de acceso y seguridad física.
- Política de cumplimiento.
- Política de escritorios y pantallas limpias.
- Política de gestión de acceso de usuarios.
- Política de gestión de incidentes de seguridad de información.
- Política de protección ante virus informáticos y código malicioso.
- Política de seguridad de la información en contrato con terceros.
- Política de seguridad de la información con recursos humanos.
- Política de uso y seguridad de internet.
- Política de uso y seguridad de correo electrónico.
- Política general de seguridad y protección de datos personales
- **Instructivos de seguridad de la información**

Se desarrollaron los siguientes instructivos (ver Anexo E):

- Instructivo de gestión de altas, modificaciones y bajas de accesos.
- Instructivo de revisión de software no autorizado.
- **Inscripción de los bancos de datos de los clientes, colaboradores y prospectos de la cooperativa “Vale un Perú”**

← → ↻ 🔒 https://prodpe.minjus.gob.pe/prodpe_web/BancoDato_verResultado 🔍 ☆ 🇵🇪 🇸🇪

Ministerio de Justicia y Derechos Humanos | **Autoridad Nacional de Protección de Datos Personales**

Resultado de Búsqueda de Bancos de Datos Personales inscritos

Tipo: Código Reg.: Titular ó Empresa: Nombre del banco de datos:

Código Captcha:

Tipo	Cod.Reg	Titular del Banco de Datos	Denominación	Categoría de Datos	Finalidad	Res.Directoral
PRI	03068	COOPERATIVA DE AHORRO Y CREDITO VALE UN PERU	COLABORADORES.	Datos de carácter identificativo: Nombres y apellidos, N° DNI, N° RUC, N° de pasaporte, dirección del domicilio, teléfono, dirección de correo electrónico, imagen, firma. Datos de características personales: Estado civil, fecha de nacimiento, nacionalidad, sexo, profesión, edad, datos de familiares, nivel educativo. Datos económicos-financieros y de seguros: Créditos, préstamos, avales, datos bancarios, información tributaria, seguros, tarjetas de crédito, bienes patrimoniales, planes de pensiones/jubilación, hipotecas, deudas. Datos personales: Pertenencia a clubes o asociados. Datos sensibles: Información relativa a la salud física o mental, ingresos económicos, afiliación sindical, huella digital.	Gestión de recursos humanos, elaboración de planilla.
PRI	03069	COOPERATIVA DE AHORRO Y CREDITO VALE UN PERU	SOCIOS.	Datos de carácter identificativo: Nombres y apellidos, N° DNI, N° RUC, N° de pasaporte, dirección del domicilio, teléfono, dirección de correo electrónico, imagen, firma, carné de extranjería. Datos de características personales: Estado civil, fecha de nacimiento, nacionalidad, sexo, profesión, edad, datos familiares, nivel educativo, dirección del centro laboral. Datos económicos-financieros y de seguros: Créditos, préstamos, avales, datos bancarios, historial de créditos, información tributaria, tarjetas de crédito, bienes patrimoniales, hipotecas, deudas. Datos de carácter social: pertenencia a clubes o asociaciones. Datos sensibles: Información relativa a la salud física o mental, ingresos económicos, huella digital.	Gestión de socios, marketing, gestión de relaciones con productos y servicios, solicitud, evaluación, otorgamiento y seguimiento de créditos.
PRI	03070	COOPERATIVA DE AHORRO Y CREDITO VALE UN PERU	PROSPECTOS.	Datos de carácter identificativo: Nombres y apellidos, N° DNI, N° RUC, N° de pasaporte, dirección del domicilio, teléfono, dirección de correo electrónico, imagen, firma, carné de extranjería. Datos de características personales: Estado civil, fecha de nacimiento, nacionalidad, sexo, profesión, edad, datos familiares. Datos económicos-financieros y de seguros: Datos bancarios, información tributaria. Datos sensibles: Huella digital.	Gestión de clientes, marketing, gestión de relaciones con productos y servicios.

Tipos: NAT-Persona Natural, PUB-Entidad Pública, PRI-Persona Jurídica

Nota: Se recomienda usar de preferencia el navegador Google Chrome. Si está utilizando el navegador Internet Explorer versión 8.0, 9.0 o 10.0 y tiene problemas para acceder al contenido de esta página debe activar la vista de compatibilidad de su navegador desde el menú 'Herramientas'

Figura 31: Registro de los bancos de datos de la Cooperativa de Ahorro y Crédito "Vale un Perú"

- **Curso de capacitación sobre seguridad de la información**

Se realizó un curso sobre seguridad de la información donde se explicó a los colaboradores de la cooperativa “Vale un Perú” los conceptos, importancia, los beneficios y la forma de cómo lograr y realizar los trabajos de forma segura, basados en los principios de integridad, confidencialidad y disponibilidad. Posterior a la capacitación se elaboró un examen para evaluar el aprendizaje y comprensión del tema. Los resultados fueron los siguientes:

CARGO	NOMBRE	PUNTAJE
Gerente General	María Laguna	16
Analista de Operaciones	Melissa Urtecho	16
Asistente de Operaciones	John Aponte	18
Contador	Miguel Cornejo	20
Asistente de Soporte TI	Rodolfo Urbina	20
Operador TI	Alfredo Martinez	18
Cajera	Ana María Hilasaca	12
Vigilante	Baltazar Gómez	14
Limpieza	María Rosales	14
Analista de Crédito	Karen Vidal	16
Auxiliar de Crédito	Rosales Balta	18
Recepcionista	Ariana Ríos	14

Tabla 28: Evaluación del curso de capacitación sobre seguridad de la información

Fuente: Propia

Figura 32: Resultado aprobados de la evaluación del curso de capacitación sobre seguridad de la información en la Cooperativa de Ahorro y Crédito "Vale un Perú"

Fuente: Propia

Luego de recopilar toda la información respectiva de la primera evaluación. Además, de haber realizado las subsanaciones respectivas, en base a las categorías y lineamientos de bajo rendimiento. Se volvió a realizar la evaluación para constatar el crecimiento porcentual del nivel de cumplimiento de las medidas legales, organizativas y técnicas. El resultado obtenido fueron los siguientes:

- **Evaluación de las medidas legales**

La evaluación se hizo luego de haber realizado la subsanación de los controles de bajo rendimiento, se inscribieron bancos de datos personales ante la Autoridad Nacional de Datos Personales, asimismo se creó una ficha para la obtención del conocimiento de datos personales, entre otras actividades. La matriz se muestra a continuación:

REGLAMENTO DE LEY 29733													
MEDIDAS LEGALES	ARTÍCULO	CONTROLES	APLICA	IMPACTO			CUMPLIMIENTO			PUNTAJE			
				BAJO	MODERADO	ALTO	MUY BAJO	BAJO	BUENO	EXCELENTE	ESPERADO	LOGRADO	(%)
CONSENTIMIENTO	11,12	La organización obtiene el consentimiento del apoderado para darle tratamiento a sus datos personales.	SI			X			X		12	9	75%
	11,14	La organización obtiene el consentimiento del apoderado para darle tratamiento a sus datos sensibles.	SI			X			X		12	9	75%
	11,16	El titular del banco de datos personales arma una solicitud de consentimiento libre, previo, expreso e informado.	SI			X			X		12	9	75%
	11,27,28	En caso se traten datos personales de menores de edad, debe tener el consentimiento de sus titulares o tutores.	NO			X							
TRANSFERENCIA	11,19	La organización obtiene el consentimiento del titular para la transferencia de su información personal.	NO			X							
	22	El receptor de la transferencia de los datos personales asume el rol de titular del banco de datos personales o responsable del tratamiento y realiza el tratamiento conforme a la finalidad por la cual fueron recopilados y las misma obligaciones del emisor.	NO			X							
INSCRIPCIÓN DE BANCO DE DATOS	78,81-84	El titular de banco de datos personales inscribe los bancos de datos personales en el registro nacional de protección de datos personales.	SI			X			X		12	9	75%
	24,25,26,77,83	El titular de banco de datos personales declara las comunicaciones referidas al flujo transfronterizo.	SI			X			X		12	9	75%
DERECHOS A.R.C.O.	50	El responsable de los datos personales cuenta con una solicitud (ficha) para que el titular pueda ejercer sus derechos.	SI			X				X	12	12	100%
	52,56	El responsable de los datos personales cuenta con procedimientos para atender solicitudes que no han sido completadas correctamente (05 días hábiles).	SI			X				X	12	12	100%

	55	La organización debe tener un documento donde especifique los tiempos de respuesta ante la solicitud de un titular de datos personales.	SI			X				X	12	12	100%
	60	El dueño de la información personal tiene el derecho de verificar como se tratan sus datos.	SI			X				X	12	12	100%
	61	El titular de datos personales tiene derecho a obtener toda la información relativa a sus datos personales, así como las condiciones y generalidades del tratamiento de los mismos.	SI			X				X	12	12	100%
	64	El dueño de la información personal tiene derechos a actualizar sus datos personales.	SI			X				X	12	12	100%
	65	El titular de datos personales tiene derecho a rectificar los datos que resulten ser inexactos, erróneos o falsos.	SI			X				X	12	12	100%
	66	El dueño de la información personal tiene derechos a añadir datos faltantes sobre sus datos personales.	SI			X				X	12	12	100%
	67-68	El dueño de la información personal tiene derechos a solicitar la eliminación o cancelación de sus datos personales cuando ya no sean necesarios para la organización o este lo disponga.	SI			X				X	12	12	100%
	71	El dueño de la información personal tiene el derecho de oponerse al tipo de tratamiento que le estén dando a sus datos personales.	SI			X				X	12	12	100%
SUBCONTRATOS	33-34	La organización contrata servicios de medios tecnológicos tercerizados garantizando el adecuado tratamiento de los datos.	SI			X				X	12	12	100%
	35,37,38	La organización contrata servicios de medios tecnológicos tercerizados que tengan mecanismos adecuados para la prestación.	SI			X				X	12	12	100%
VIDEOGILANCIA	02-2020	El titular de datos personales o responsable de tratamiento cumple con lo dispuesto en la resolución N° 02-2020-JUS/DGTAIPD.	SI			X				X	12	12	100%
TOTALES										X	204	189	92.6%

Tabla 29: Nueva evaluación de las medidas legales posterior a la implementación

- **Evaluación de las medidas organizativas**

La evaluación se realizó luego de haber elaborado un conjunto de procedimiento y políticas de Seguridad de la Información (y subcategorías), además de la creación de artefactos para la sección de reportería y almacenamiento de inventarios. Por otro lado, se generaron planes de continuidad, respuesta ante incidentes, matriz de gestión de accesos, entre otros. Con el fin, de elevar el nivel de protección de la microfinanciera, respecto de los datos personales que maneja. La matriz se muestra a continuación:

MEDIDAS DE ORGANIZATIVAS	REFERENCIA	CONTROLES	APLICA	IMPACTO			CUMPLIMIENTO				PUNTAJE			
				BAJO	MODERADO	ALTO	MUY BAJO	BAJO	ADECUADO	BUENO	EXCELENTE	ESPERADO	LOGRADO	(%)
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	ISO 27001 A.5.1.1	Política General de Seguridad	SI		X				X			8	4	50%
	ISO 27001 A.5.1.2	Revisión de la Política General de Seguridad	SI		X				X			8	4	50%
	ISO 27001 A.6.1.1	Roles y Responsabilidades para el Resguardo de la Seguridad	SI			X					X	12	12	100%
	ISO 27001 A.7.2.1	Responsabilidad de la Alta Dirección	SI			X				X		12	9	75%
	ISO 27001 7.4.3	Política para la Revisión de los Derechos de Ingreso Lógicos	SI		X					X		8	6	75%
	ISO 27001 A.10.1.1	Política de Validación de Lineamientos Criptográficos	SI		X				X			8	4	50%
	ISO 27001 A.11.2.9	Política de Escritorios Ordenados	SI		X					X		8	6	75%
	ISO 27001 A.6.2.1	Política de Control para los Dispositivos Móviles Internos	SI		X				X			8	4	50%
	ISO 27001 A.7.2.2	Policita de entrenamiento al personal en términos de seguridad	SI		X					X		8	6	75%
	ISO 27001 A.8	Política de gestión de activos	SI		X					X		8	6	75%
	ISO 27001 A.8.2.1	Política de Segmentación de la Información	SI		X					X		8	6	75%
	ISO 27001 A.9.1.1	Política de acceso de usuario a la red empresarial	SI		X				X			8	4	50%
	ISO 27001 A.11.1	Política de seguridad física	SI		X					X		8	6	75%
	ISO 27001 A.12.1.4	Política de desarrollo, prueba y producción	NO		X									
	ISO 27001 A.12.2.1	Política de Protección Antimalware	SI		X				X			8	4	50%
	ISO 27001 A.12.3.1	Política de respaldo de información	SI		X				X			8	4	50%

	ISO 27001 A.14.2.1	Política de desarrollo seguro	NO		X									
	ISO 27001 A.15.1.1	Política de seguridad con terceros	SI		X					X		8	6	75%
	ISO 27001 A.16.1.1	Política de gestión de incidentes	SI		X				X			8	4	50%
	ISO 27001 A.17.1.1	Política de continuidad de negocio	SI		X				X			8	4	50%
	ISO 27001 A.18.1.4	Política de Privacidad de Información por Normativa	SI		X					X		8	6	75%
	ISO 27001 A.18.2.1	Revisión Seguridad de la Información por una Entidad Especializada	SI		X				X			8	4	50%
GESTIÓN DE ACTIVOS	ISO 27001 A.8.1.1	Gestión de control e inventario de activos lógicos y físicos	SI			X			X			12	6	50%
	ISO 27001 A.8.1.2	Gestión de Propietarios de los Activos	SI		X				X			8	4	50%
	ISO 27001 A.8.1.4	Gestión de Retorno del Activo	SI			X			X			12	6	50%
	ISO 27001 A.11.2.4	Mantenimiento de los Equipos Informáticos	SI			X			X			12	6	50%
	ISO 27001 A.11.2.5	Gestión de la Separación de los Activos Informáticos	SI		X				X			8	4	50%
	ISO 27001 A.11.2.8	Activos obsoletos	SI		X				X			8	4	50%
RIESGOS DE SEGURIDAD	COBIT 5 APO12.01	Recopilación de Datos Relevantes	SI			X			X			12	6	50%
	COBIT 5 APO12.02	Analizar los Riesgos	SI			X			X			12	6	50%
	COBIT 5 APO12.03	Conservar un Perfil Atento al Riesgo	SI			X				X		12	9	75%
	COBIT 5 APO12.06	Determinar la Respuesta al Riesgo	SI			X				X		12	9	75%
SEGURIDAD EN RRHH	ISO 27001 A.6.1.1	Funciones y Responsabilidades de Seguridad de la Información	SI		X				X			8	4	50%
	ISO 27001 A.7.2.2	Capacitación y Concientización en Seguridad de la Información	SI			X			X			12	6	50%
	ISO 27001 A.7.2.3	Procesos disciplinarios	SI		X				X			8	4	50%
	ISO 27001 A.16.1.1	Detección de Responsabilidades y Flujo de Procedimientos	SI			X			X			12	6	50%

INCIDENTES DE SEGURIDAD	ISO 27001 A.16.1.2	Reporte de los Eventos Detectados	SI			X			X			12	6	50%
	ISO 27001 A.16.1.3	Reporte de las Debilidades Detectadas	SI			X			X			12	9	75%
	ISO 27001 A.16.1.5	Respuesta a los Incidentes Detectados	SI			X			X			12	6	50%
CONTINUIDAD DE LA SEGURIDAD	ISO 27001 A.17.1.1	Continuidad de los Planes de Seguridad de la Información	SI		X				X			8	6	75%
	ISO 27001 A.17.1.2	Implementación de la Continuidad de la Seguridad de la Información	SI		X				X			8	6	75%
	ISO 27001 A.17.1.3	Verificación, Revisión y Evaluación del Plan de Continuidad	SI		X					X		8	8	100%
TOTALES												376	230	61.2%

Tabla 30: Nueva evaluación de las medidas organizativas posterior a la implementación

Elaboración: Propia

- **Evaluación de las medidas técnicas**

La evaluación de las medidas técnicas se realizó luego de varias reuniones con el consultor de Tecnología de la Información de la microfinanciera, se realizaron acciones de configuración de firewall de Windows sobre los dispositivos de la empresa, también se instaló una solución antimalware en las computadoras y servidores, en conjunto un plan para las revisiones periódicas. Por otro lado, se configuró la red inalámbrica para que utilice un tipo de HASH más potente, para esta acción se tuvo que hablar con el proveedor de internet para solicitar un nuevo router, entre otras actividades. La matriz resultante se muestra a continuación:

MEDIDAS DE TÉCNICAS	REFERENCIA	CONTROLES	APLICA	IMPACTO			CUMPLIMIENTO				PUNTAJE			
				BAJO	MODERADO	ALTO	MUY BAJO	BAJO	ADECUADO	BUENO	EXCELENTE	LOGRADO	ESPERADO	(%)
ACCESOS LÓGICOS	ISO 27001 A.6.1.2	Segmentación de Funciones	SI			X				X		9	12	75%
	ISO 27001 A.9.2.1	Gestión de Registro de los Usuarios Lógicos	SI		X					X		6	8	75%
	ISO 27001 A.9.2.2	Aprovisionamiento de Accesos Lógicos al Usuario	SI			X				X		9	12	75%
	ISO 27001 A.9.2.3	Gestión de Verificación de Accesos de Usuarios Privilegiados	SI			X			X			6	12	50%
	ISO 27001 A.9.2.5	Revisión de los Derechos de Acceso de los Usuarios	SI			X				X		9	12	75%
	ISO 27001 A.9.2.6	Validación y Ajuste de los Accesos Brindados	SI		X					X		6	8	75%
	ISO 27001 A.9.4.1	Restricción a la Información según el Acceso	SI			X				X		9	12	75%
	ISO 27001 A.9.4.4	Utilización de Software para Control de Privilegios	SI		X					X		6	8	75%
ACCESOS FÍSICOS	ISO 27001 A.11.1.1	Elaborar un Perímetro para la Seguridad Física	SI			X				X		9	12	75%
	ISO 27001 A.11.1.2	Aseguramiento de los Controles Físicos	SI			X				X		9	12	75%
	ISO 27001 A.11.1.5	Asegurar las Áreas de Trabajo	SI			X			X			6	12	50%
	ISO 27001 A.11.1.6	Verificar la Distribución Segura en Zonas de Carga	SI			X				X		9	12	75%
CIFRADO	NIST 800-54 SC-13	Asignación de Protección Criptográfica	SI			X			X			6	12	50%

SEGURIDAD PERIMETRAL	CSC CSI 7.1 CSC 9.3	Verificar los Accesos a Puertos Lógicos	SI			X			X			6	12	50%
	CSC CSI 7.1 CSC 9.6	Implementación y Revisión de la Solución Tecnológica Firewall	SI			X			X			6	12	50%
	CSC CSI 7.1 CSC 8.1	Manejo y Control de las Herramientas de Ciberseguridad	SI			X			X			6	12	50%
	CSC CSI 7.1 CSC 8.6	Implementar un IPS dentro de la red organizacional	SI			X			X			6	12	50%
SEGURIDAD INTERNA	CSC CSI 7.1 CSC 15.5	Implementación de Redes Inalámbricas Seguras	SI			X			X			6	12	50%
	CSC CSI 7.1 CSC 15.3	Aseguramiento de las Redes Inalámbricas	SI			X				X		9	12	75%
	CSC CSI 7.1 CSC 13.5	Restricción de Acceso a los Dispositivos de Almacenamiento Externo	SI			X				X		9	12	75%
	CSC CSI 7.1 CSC 13.9	Uso de herramientas de Ciberseguridad – DLP	SI			X	X					0	12	0%
	CSC CSI 7.1 CSC 8.2	Uso de herramienta de Ciberseguridad - Antimalware	SI			X				X		9	12	75%
TOTALES												156	252	61.9%

Tabla 31: Nueva evaluación de las medidas técnicas posterior a la implementación

Elaboración: Propia

Los resultados obtenidos de las 3 evaluaciones realizadas demuestran el nivel de crecimiento que la microfinanciera ha obtenido luego de utilizar nuestro modelo de referencia para implementar la protección de datos personales. De esta manera, cumple con el marco normativo y eleva su nivel reputacional con sus clientes al salvaguardar sus datos de forma óptima. Se mejoraron aspectos legales, de cara ante la Autoridad Nacional de Protección de Datos Personales. Se mejoraron aspectos organizativos, capacitación al personal, implementación de documentación interna, artefactos para procesos, entre otros. Por último, se mejoró la parte técnica, en la cual se configuraron varias directivas lógicas e implementación de herramientas para evitar la fuga, modificación e indisponibilidad de la información (incluye datos personales).

6.1.3 Resultados de la validación

6.1.3.1 Resultados de la primera evaluación

Inicialmente se realizó una evaluación de las medidas legales, organizativas y técnicas con la información recopilada en la fase 1 del proceso de implementación. Podemos observar la carencia de controles, lineamientos y artefactos de control para gestionar adecuadamente los datos personales que convergen por la red interna de la microfinanciera. Los resultados fueron los siguientes:

CUMPLIMIENTO ORGANIZATIVAS	9%
----------------------------	----

Figura 33: Nivel de cumplimiento inicial por cada medida organizativa

Fuente: Propia

CUMPLIMIENTO LEGAL	21%
---------------------------	------------

Figura 34: Nivel de cumplimiento inicial por cada medida legal

Fuente: Propia

CUMPLIMIENTO TÉCNICAS	20%
------------------------------	------------

Figura 35: Nivel de cumplimiento inicial por cada medida técnica

Fuente: Propia

NIVEL DE PROTECCIÓN DE DATOS PERSONALES INICIAL **17%**

Figura 36: Nivel inicial total del porcentaje de protección de datos personales en el sector microfinanciero peruano

Elaboración: Propia

Un 17% de cumplimiento, respecto del modelo de referencia que hemos planteado demuestra la carencia de controles y lineamientos para proteger los datos personales que la microfinanciera almacena y gestiona. En las medidas organizativas presenta un déficit mayor, porque no considera ningún documento formal para la Seguridad de la Información, solo procedimiento ad-hoc y sin base documental.

6.1.3.2 Resultados de la segunda evaluación

Posterior a la implementación de los controles definidos en el plan de mejora, se realizó una nueva evaluación del nivel de protección de datos personales. Cabe resaltar que los controles propuestos en el plan de mejora fueron revisados por especialistas en seguridad de la información y especialista en protección de datos personales. Esta revisión de los expertos se realizó para confirmar que las propuestas que se están realizando son adecuadas a la necesidad de la Cooperativa “Vale un Perú”.

La evaluación que se realizó empleando las propuestas del plan de mejora mostró los siguientes resultados:

Figura 37: Nivel de cumplimiento final de las medidas organizativas

Fuente: Propia

CUMPLIMIENTO LEGAL**92%**

Figura 38: Nivel de cumplimiento final de las medidas legales

Fuente: Propia

CUMPLIMIENTO TÉCNICAS**69%**

Figura 39: Nivel de cumplimiento final de las medidas técnicas

Fuente: Propia

NIVEL DE PROTECCIÓN DE DATOS PERSONALES CON EL PLAN DE MEJORA IMPLEMENTADO	74%
---	------------

Figura 40: Nivel de total final de la protección de datos personales

Fuente: Propia

Figura 41: Comparación del nivel de protección de datos personales antes y actual

Fuente: Propia

Al comparar los niveles de cumplimiento, podemos verificar el incremento porcentual luego de haber realizado la implementación del modelo de referencia para la protección de datos personales. En las medidas legales, se crearon documentos para la solicitud del consentimiento de datos, también se actualizó este consentimiento sobre sus trabajadores y socios. Se realizó la inscripción de 6 bancos de datos personales ante la Autoridad Nacional de Protección de Datos Personales, se generaron adendas en los contratos de los terceros y colaboradores para anexar un capítulo de protección de datos personales. Por último, se generaron los documentos necesarios para que los titulares de los datos puedan ejercer de forma correcta sus derechos fundamentales (Derechos A.R.CO.).

En las medidas organizativas, se crearon 17 políticas relacionadas a la seguridad de la información, 2 procedimientos para el alta, modificación y baja de usuarios. Asimismo, se brindó un curso de capacitación de seguridad de la información con su respectiva evaluación, se brindaron 6 artefactos para que los colaboradores responsables de cada proceso puedan evaluar sus riesgos e incidentes. Además, artefactos para contener el control de inventario y planes de continuidad de negocio.

Por último, dentro de las medidas técnicas se generaron artefactos y revisiones para la matriz de accesos lógicos del sistema Core, se diseñó una estructura logística para proteger los activos de información física (candados, tapetes, cajones, entre otros). Se realizó el desarrollo de cifrado de información para las claves de los usuarios en el sistema principal de la microfinanciera. Asimismo, se configuró el firewall local de Windows en las computadoras del personal, y la instalación de una solución antimalware en los equipos, con el fin de detectar y prevenir el contagio por virus informático o código malicioso.

6.2 Plan de continuidad para la actualización de las medidas legales, organizativas y técnicas del modelo de referencia

El plan de continuidad consiste en las acciones a tomar para mantener actualizadas las medidas legales, organizativas y técnicas del modelo de referencia propuesto frente a los cambios que se presenten en el marco legal, marco de trabajo o buenas prácticas de seguridad de información, o las tendencias del uso de nuevas tecnologías en el sector microfinanciero. Para ello, se definió el siguiente conjunto de actividades:

6.2.1 Actualización del marco legal, estándar, marco de trabajo o buenas prácticas de seguridad de información

Periódicamente, el marco legal, estándar, marco de trabajo o buena práctica de seguridad de la información son actualizados por las instituciones que los crearon. Ello tiene como fin, ofrecer controles que vayan acorde a la realidad actual de las organizaciones y cubriendo las nuevas brechas que se dan a conocer como producto de evolución tecnológica. Por ello, se propone como plan de continuidad, adecuar las nuevas versiones de los documentos legales, marcos de trabajo o buenas prácticas de seguridad de la información en el modelo de referencia propuesto. A continuación, los detalles:

- Mensualmente se averiguará la fecha de actualización de la Ley 29733 o su reglamento, ISO 27001, NIST 800-53, CIS CSC V7.1 y COBIT 5.

En caso se conozca la fecha de actualización del marco legal o normativo, se procederá a lo siguiente:

- **Conocer las novedades y cambios de la actualización que incorporará la nueva versión del marco legal, estándar, marco de trabajo o buena práctica de seguridad de la información**

Inicialmente, se hace una breve investigación de las novedades que incorporará la nueva actualización del marco legal o normativo, a fin de anticiparse a los posibles cambios que tendrá el modelo de referencia propuesto. Asimismo, se pueda tener un contexto que explique las razones por las cuales se están agregando nuevos controles, modificando algunos, o incluso, eliminarlos.

- **Adquirir la actualización del marco legal, estándar, marco de trabajo o buena práctica de seguridad de la información para el estudio**

Una vez publicada la actualización del marco legal o documentos normativos de seguridad de la información, se deberá adquirirlos para hacer la revisión correspondiente. Esto nos permite tener la información completa, el contexto de los cambios, los nuevos elementos y los datos que fueron eliminados o reemplazados. Es necesario adquirir la norma original y legítima de la institución a cargo.

- **Estudiar el documento a fin de entender y analizar las nuevas disposiciones que establece el nuevo marco legal o las normas.**

Se requiere leer y estudiar la actualización del marco legal, estándar, marco de trabajo o buenas prácticas de seguridad de la información a fin conocer las nuevas disposiciones y entender el contexto bajo el cual fueron incorporadas. Además, es

necesario anotar los elementos que han sido eliminados o reemplazados y elaborar diagramas que concentren los elementos más importantes de las nuevas disposiciones. Esto nos permitirá, en los pasos siguientes, determinar la aplicación en el modelo de referencia.

- **Determinar las diferencias de la nueva actualización con la versión anterior.**

Al conocer la nueva actualización de marco legal, estándar, marco de trabajo, o buena práctica de seguridad de información, podemos realizar un contraste de los elementos nuevos, cambiados o eliminados de la versión anterior. Se requerirá analizar si las nuevas disposiciones van acorde a la realidad de las microfinancieras peruanas y elegir cuál de ellas serán incluidas al modelo de referencia.

- **Identificar las medidas que cambiarían del modelo actual.**

Con los pasos anteriores se recopiló todos los cambios que trajo la nueva actualización del marco legal, estándar, marco de trabajo, o buena práctica de seguridad de información, ahora, se deberá definir qué medidas del modelo de referencia propuesto aplicarían. Para ello, se asociará bajo los conceptos y principios de cada medida, el impacto en el ciclo de vida del dato personal y su aplicación al sector microfinanciero.

Por otro lado, en el caso que los controles de las nuevas disposiciones no se adecuen o formen parte de las medidas legales, organizativas o técnicas del modelo de referencia actual, se requiere crear una nueva medida. Esta medida deberá cubrir la necesidad por la cual se habilitaron los nuevos controles en la actualización del marco legal, estándar o buena práctica de seguridad de información.

- **Integrar los controles de la nueva actualización al modelo actual.**

Una vez identificadas las medidas del modelo de referencia que se actualizarán con las nuevas disposiciones del marco legal o normativo, se agregarán o eliminarán los nuevos controles en la matriz de evaluación de las medidas afectadas (legal, organizativa o técnica). Por cada uno, se describirá sus criterios de evaluación según la escala Likert (1 a 5) a fin de calcular el nivel de cumplimiento de la protección de datos personales en la microfinanciera.

- **Validar el modelo actualizado con expertos en el marco legal o la norma que se haya actualizado.**

Cuando el modelo y la matriz hayan sido modificados, se deberá solicitar a un experto del marco legal o normativo actualizado, la revisión de los criterios en la

matriz de evaluación de protección de datos personales. La razón de ello es confirmar que la forma como se definió los criterios a evaluar del nuevo control, están acorde a un nivel de cumplimiento de seguridad de información. Esto quiere decir, respetando las necesidades básicas para que la microfinanciera proteja los datos personales que trata.

6.2.2 Adquisición de nuevas tecnologías:

Constantemente se dan a conocer nuevas tecnologías que brindan soluciones a las empresas. Estas tecnologías son incorporadas en el entorno empresarial con el fin de mejorar las operaciones de las empresas e incrementar sus ventas. Esto se aplica también en el sector microfinanciero. Muchas de estas tecnologías soportan procesos de negocio que tratan datos personales y por los cuales, dan paso a riesgos de seguridad, las cuales, el modelo de referencia propuesto deberá mitigarlos. Para ello, se propone el siguiente plan de continuidad en el caso el sector microfinanciero adopte las nuevas tendencias tecnológicas. A continuación, los detalles:

- Trimestralmente se averiguará las tendencias en la adopción de las nuevas tecnologías en el sector microfinanciero peruano. Para ello, se revisará informes, reportes de tendencias tecnológicas, encuestas a empleados de microfinancieras, entre otros documentos.

En caso se detecte la nueva tecnología:

- **Estudiar la nueva tecnología.**

Se deberá conocer la necesidad que cubre la nueva tecnología y el entorno bajo el cual se aplica (como dispositivos electrónicos, servidores on-premise, servidores cloud, servicios en la nube, etc.). Asimismo, investigar las vulnerabilidades que tiene y las amenazas que podrían explotarla. Ello permite descubrir los posibles riesgos a los que la microfinanciera pueda exponerse al incorporarlos en sus operaciones.

- **Analizar el impacto de la nueva tecnología en los datos personales que trata la microfinanciera.**

Luego del estudio de la nueva tecnología, se deberá analizar los procesos de las microfinancieras que se verían afectados con la implementación, además de los datos personales que se tratarán con ella. Es necesario verificar las características que tienen estos datos personales, como el formato del dato (medio digital, físico, video, audio, etc.), si es sensible y la finalidad de su recopilación. También,

averiguar la forma en como la nueva tecnología trata los datos personales, como el lugar donde los almacena, la forma en los procesa, los medios por los cuales los trata, entre otros factores que corresponden al ciclo de vida del dato personal.

- **Verificar si las medidas propias del modelo soportan la nueva tecnología.**

En base a las vulnerabilidades de la nueva tecnología, los procesos impactados y los datos personales que se procesen, se deberá conocer si los controles de las medidas del modelo propuesto cubren las brechas de seguridad de la implementación de la nueva tecnología.

Si el impacto de la nueva tecnología es alto para los datos personales y los controles del modelo no son suficientes para soportarla, se realizará lo siguiente:

- **Búsqueda de estándares, marcos de trabajo o buenas prácticas de seguridad de la información para la nueva tecnología.**

El modelo de referencia al no contar con controles que soporten la nueva tecnología se procederá a la investigación y búsqueda de marcos legales, estándar, y/o buenas prácticas de seguridad que propongan acciones para proteger los datos personales acorde a la realidad del sector microfinanciero. Estos documentos deberán ser elaborados por instituciones legítimas y ser comprobados su efectividad en la tecnología a tratar. Posterior a ello, se deberá seleccionar todos los estándares, marcos de trabajo y/o buenas prácticas de seguridad de la información que sean candidatos para ser incluidos en el modelo de referencia.

- **Revisar los estándares, marcos de trabajo o buenas prácticas de seguridad de la información que hayan sido seleccionados.**

Se deberá hacer un estudio del estándar, marco de trabajo o buena práctica de seguridad de la información seleccionados, a fin de conocer las medidas y sus controles que proponen para la nueva tecnología. Para ello, se deberá categorizar cuales de sus controles se adecuan a las medidas ya existentes del modelo de referencia, y cuáles de ellos proponen otras medidas. Asimismo, conocer el contexto por el cual se propone medidas distintas.

- **Análisis de los estándares, marcos de trabajo o buenas prácticas de seguridad de la información seleccionado.**

Una vez conocidos los estándares, marcos de trabajo o buenas prácticas de seguridad de la información, se realizará un benchmarking en base a las medidas del modelo de referencia y la forma como cubre las brechas de seguridad de la información de

la nueva tecnología. La finalidad de ello es reconocer y elegir cuál de ellos ofrece los mejores controles y puedan integrarse mejor al modelo de referencia.

- **Integrar los estándares, marcos de trabajo o buenas prácticas de seguridad de la información al modelo de referencia.**

Los controles de los documentos de seguridad de la información seleccionados deberán incluirse dentro de cada medida del modelo propuesto, basando en sus conceptos y principios. En caso los controles de los estándares, marcos de trabajo o buenas prácticas de seguridad de la información no encajen dentro de las medidas del modelo de referencia, se requerirá crear una nueva medida. Esta medida deberá cubrir la necesidad por la cual se habilitaron los nuevos controles en la nueva tecnología. De tal forma, en un futuro, otros documentos de seguridad de la información puedan ser incluidos en las nuevas medidas.

Posterior a ello, se añadirán las medidas y controles a las matrices de evaluación del modelo de referencia (legal, organizativa o técnica). Por cada uno, se describirá sus criterios de evaluación según la escala Likert (1 a 5) a fin de calcular el nivel de cumplimiento de la protección de datos personales en la microfinanciera.

- **Validar el modelo actualizado con expertos en la norma seleccionada y en la nueva tecnología.**

Cuando el modelo y las matrices hayan sido modificados, se deberá solicitar a un experto del marco legal o normativo, la revisión de los criterios en la matriz de evaluación de protección de datos personales. La razón de ello es para confirmar que la forma como se definió los criterios a evaluar del nuevo control está acorde a un nivel de cumplimiento de seguridad de información.

6.3 Costos y presupuestos

6.3.1 Apoyo interno

En el proyecto participan consultores quienes desempeñar las tareas de las fases de Recopilación, Diagnostico y Plan de mejora. El costo de los consultores se mide en función a las horas trabajadas. No se incluye la fase de Implementación, debido a que los costos de esta fase varían dependiendo del nivel de cumplimiento de la microfinanciera. A continuación, se presenta el costo del proyecto por fase y las horas empleadas por cada recurso:

COSTO POR FASE (NO INCLUYE LA MPLEMENTACIÓN)

Fase	Recurso	Horas	Costo/hora	Costo	Costo por Fase
Recopilación	Consultor 1	100	S/31.25	S/3,125.00	S/6,406.25
	Consultor 2	105	S/31.25	S/3,281.25	
Diagnostico	Consultor 1	20	S/31.25	S/625.00	S/1,406.25
	Consultor 2	25	S/31.25	S/781.25	
Plan de mejora	Consultor 1	60	S/31.25	S/1,875.00	S/4,062.50
	Consultor 2	70	S/31.25	S/2,187.50	
				Total	S/11,875.00

Tabla 32: Costo por fase (no incluye la implementación)

Elaboración: Propia

COSTO POR PERSONAL (NO INCLUYE LA IMPLEMENTACIÓN)

Recurso	Horas	Costo/hora	Costo
Consultor 1	180	S/31.25	S/5,625.00
Consultor 2	200	S/31.25	S/6,250.00
Total			S/11,875.00

Tabla 33: Costo por personal (no incluye la implementación)

Elaboración: Propia

Para estimar los costos del personal incluyendo la fase de implementación, se realizó en función a los controles más comunes para las medidas legales, organizativas y técnicas. Los resultados fueron los siguientes:

COSTOS POR FASE (INCLUYE LA IMPLEMENTACIÓN)

Fase	Recurso	Horas	Costo/hora	Costo	Costo por Fase
Recopilación	Consultor 1	100	S/31.25	S/3,125.00	S/6,406.25
	Consultor 2	105	S/31.25	S/3,281.25	
Diagnostico	Consultor 1	20	S/31.25	S/625.00	S/1,406.25
	Consultor 2	25	S/31.25	S/781.25	
Plan de mejora	Consultor 1	60	S/31.25	S/1,875.00	S/4,062.50
	Consultor 2	70	S/31.25	S/2,187.50	
Implementación	Consultor 1	147	S/31.25	S/4,593.75	S/16,062.50
	Consultor 2	367	S/31.25	S/11,468.75	

Total	S/27,937.50
--------------	--------------------

Tabla 34: Costo por fase (incluye la implementación)

Elaboración: Propia

COSTO POR PERSONAL (INCLUYE LA IMPLEMENTACIÓN)

Recurso	Horas	Costo/hora	Costo
Consultor 1	327	S/31.25	S/10,251.45
Consultor 2	567	S/31.25	S/18,285.75
Total			S/27,937.50

Tabla 35: Costo por personal (incluye la implementación)

Elaboración: Propia

COSTO DE MATERIALES

		Costo unitario (S/.)	Cantidad	Costo total (S/.)
Costos de Trámites				
1	Inscripción de bancos de datos en RNPDP	S/ 52.30	5	S/ 261.50
Subtotal				S/ 261.50
Costos de Software y Hardware				
1	Antivirus AVAST Pro 2020	S/ 85.00	8	S/ 680.00
2	PC Desktop Core i7 3770 RAM 8gb HDD 1TB	S/ 3,000.00	1	S/ 3,000.00
Subtotal				S/ 3,680.00
Costos Fijos Adicionales				
1	Cerrojo Doble Acero	S/ 53.00	5	S/ 265.00
2	Candados Estándar Bronce	S/ 10.00	15	S/ 150.00
3	Canaleta 20x10cm 2m	S/ 6.00	2	S/ 12.00
Subtotal				S/ 427.00
Total				S/ 4,368.50

Tabla 36: Costos de Materiales

Elaboración: Propia

6.3.2 Enfoque de gestión de costes

6.3.2.1 Indicadores de costes

Al aplicar un Modelo de Referencia que permita la protección de los datos personales, se estima que el retorno de inversión no se evidenciará por las ganancias que pueda generar el implementar el Modelo. En este caso, el Modelo de Referencia de Protección de Datos Personales genera un retorno de la inversión al prevenir pérdidas en las microfinancieras por

posibles ataques informáticos, sanciones administrativas por incumplimiento del marco legal, errores de los colaboradores/proveedores relacionados a seguridad de la información, fuga de información, corte operativo de las actividades del negocio y por falta de lineamiento orientados en seguridad de la información. A esta situación, se le conoce como el retorno de la inversión en seguridad.

Se analizan 03 posibles escenarios en los cuales el modelo permite a la microfinanciera evidenciar el impacto (en términos económicos) que hubiera afrontado al no tener implementada la solución propuesta, es decir, el Modelo de Referencia para la Protección de Datos Personales. Se considera que el valor de la UIT es S/.4,300 (2020).

Para el calculo del retorno de inversión, se emplea el ROSI (Retorno sobre la Inversión en Seguridad de la Información). Este porcentaje permite justificar la inversión en seguridad de la información en términos monetarios. No surge como beneficios contables, sino como la reducción de la perdida. La fórmula es la siguiente:

$$\text{ROSI (\%)} = (\text{Inversión} - \text{Costos}) / \text{Costos}$$

6.3.2.2 Retorno de inversión por aspectos legales

En el aspecto legal, la microfinanciera se ve resguardada por el modelo de referencia, puesto que consideramos todos los puntos de inflexión recurrentes y auditados por el Ministerio de Justicia y Derechos Humanos – MINJUS, exactamente del órgano Autoridad Nacional de Protección de Datos Personales (ANPDP).

Por ello, en este caso se realizará el ejercicio de ejemplificar el valor por concepto de sanciones administrativas que la microfinanciera “Vale un Perú” hubiera recibido al no implementar el Modelo de Referencia y ser fiscalizada por el MINJUS.

#	Inciso	Infracción	UIT	Sanción (S/.)
1	b	Leve	2.5	10,750.00
2	c	Leve	2.5	10,750.00
3	e	Leve	2.5	10,750.00
4	a	Grave	10	43,000.00
5	b	Grave	10	43,000.00
TOTAL			118,250.00	

Tabla 37: Posibles infracciones impuestas por incumplimiento de las medidas legales

Elaboración: Propia

Atributos	Valor
Inversión del Proyecto	32,306.00
Sanciones Impuestas	118,250.00
ROSI (%)	266%

Tabla 38: ROSI para aspectos legales

Elaboración: Propia

El ROSI % fue 266%, lo cual refiere un alto indicador de beneficio para la entidad financiera. Dando como resultado que el Modelo es altamente recomendable.

6.3.2.3 Retorno de inversión por aspectos organizativos

En el aspecto organizacional, la microfinanciera “Vale un Perú” protege los datos personales mediante los 39 controles de seguridad de la información que contiene la submedidas general – Medidas Organizativas. En el caso, el ente regulador (ANPDP) realice una inspección cuando la microfinanciera no tiene implementado del Modelo de Referencia para la Protección de Datos Personales.

#	Inciso	Infracción	UIT	Sanción (S/.)
1	a	Leve	2.5	10,750.00
2	d	Leve	2.5	10,750.00
3	f	Leve	2.5	10,750.00
4	c	Grave	8	34,400.00
5	g	Grave	8	34,400.00
TOTAL			101,050.00	

Tabla 39: Posibles infracciones impuestas por incumplimiento de las medidas organizativas

Elaboración: Propia

Atributos	Valor
Inversión del Proyecto	32,306.00
Sanciones Impuestas	101,050.00
ROSI (%)	213%

Tabla 40: ROSI para aspectos organizativos

Elaboración: Propia

El ROSI % en este escenario fue del 213%, lo cual refiere un alto indicador de beneficio para la entidad financiera. Dando como resultado la efectividad del Modelo ante un escenario de riesgo altamente probable.

6.3.2.4 Retorno de inversión por aspectos técnicos

En el aspecto técnico, la entidad financiera “Vale un Perú” protege a los datos personales, a los cuales da tratamiento bajo 02 marcos de trabajo orientados a la Ciberseguridad. Las medidas técnicas elaboradas para proteger los datos personales tienen como base el cumplimiento de 25 controles orientados a seguridad de la información. En el caso, el MINJUS bajo su órgano fiscalizador “Autoridad Nacional de Protección de Datos Personales” haya decidido realizar una inspección a la microfinanciera antes de implementar el modelo, el resultado hubiera sido el siguiente:

#	Inciso	Infracción	UIT	Sanción (S/.)
1	a	Leve	2.5	10,750.00
2	d	Leve	2.5	10,750.00
3	f	Leve	2.5	10,750.00
4	b	Grave	10	43,000.00
TOTAL			75,250.00	

Tabla 41: Posibles infracciones impuestas por incumplimiento de las medidas técnicas

Elaboración: Propia

Atributos	Valor
Inversión del Proyecto	32,306.00
Sanciones Impuestas	75,250.00
ROSI	133%

Tabla 42: ROSI para aspectos técnicos

Elaboración: Propio

El ROSI % en este escenario fue del 133%, lo cual refiere un alto indicador de beneficio para la entidad financiera. Dando como resultado la efectividad del Modelo ante un escenario de riesgo altamente probable.

En conclusión, si generamos un escenario general de fiscalización por parte del MINJUS a la Cooperativa de Ahorro y Crédito “Vale un Perú”, sin considerar la implementación de las 03 medidas generales (Legal, Organizativa y Técnica) tendría como resultado las siguientes sanciones administrativas.

#	Inciso	Infracción	UIT	Sanción (S/.)
1	a	Leve	2	8,600.00
2	b	Leve	2	8,600.00
3	c	Leve	3	12,900.00
4	d	Leve	3	12,900.00
5	e	Leve	1	4,300.00
6	f	Leve	2	8,600.00
7	a	Grave	8	34,400.00
8	b	Grave	7	30,100.00
9	c	Grave	6	25,800.00
10	g	Grave	6.5	27,950.00
TOTAL				174,150.00

Tabla 43: Posibles infracciones impuestas por incumplimiento de las medidas legales, organizativas y técnicas

Elaboración: Propia

Atributos	Valor
Inversión del Proyecto	S/ 32,306.00
Sanciones Impuestas	S/ 174,150.00
ROSI	439%

Tabla 44: ROSI del proyecto

Elaboración: Propia

El retorno de inversión general es del 439%, lo cual indica que la implementación del Modelo de Referencia genera un alto impacto en la microfinanciera.

Por otro lado, se adjunta el gráfico general de sanciones por cada medida evaluada, respecto de la inversión que necesitó el Modelo de Referencia para ser implementado en la microfinanciera.

Figura 42: Comparación del monto de inversión vs el gasto del proyecto

Elaboración: Propia

7 CAPÍTULO 6: GESTIÓN DEL PROYECTO

En este capítulo se explicará los resultados en términos de gestión de proyectos. Se dará a conocer los tiempos reales con los planificados y se evidenciará la gestión realizada para el logro del producto final del proyecto.

7.1 Gestión de recursos humanos

7.1.1 Descripción de roles

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

- **Comité de proyectos**
 - Dar un veredicto de los proyectos presentados, con respecto a la pertinencia, viabilidad e integridad con la carrera.
 - Verificar el cumplimiento de la documentación de cada proyecto.
 - Decidir la continuidad de los proyectos.
- **Director de la PMO**
 - Controla y gestiona los proyectos.
 - Coordinar actividades con los Senior Portfolio Manager de las empresas virtuales.
- **Senior Portfolio Manager**
 - Supervisar, coordinar y controlar los portafolios de proyectos y las diferentes actividades que tiene asignadas.
 - Administrar, eficientemente, los recursos asignados a su cargo.
 - Resolver, adecuadamente, cualquier incidente que esté dentro de su ámbito sin afectar los intereses ni la imagen de la Escuela.
 - Realizar cualquier actividad que pudiese ser solicitada por el Director de la PMO y por el Comité de proyectos de la Escuela.
- **Portfolio Manager**
 - Supervisar, coordinar y controlar los proyectos, y las diferentes actividades que tiene asignadas dentro de su portafolio.
 - Administrar, eficientemente, los recursos asignados a su cargo.
 - Velar por el adecuado cumplimiento de los proyectos sin afectar la calidad esperada de los mismos.
 - Resolver, adecuadamente, cualquier incidente que esté dentro de su ámbito sin afectar los intereses ni la imagen de la Escuela.
 - Realizar cualquier actividad que pudiera ser solicitada por el Director de la PMO y por el Comité de proyectos de la Escuela.
- **Asesor Cliente**
 - Cumplir el rol de Product Manager en los proyectos profesionales que tiene asignados.

- Realizar cualquier actividad que sea solicitada por su Portfolio Manager, el Senior Portfolio Manager, el Director de la PMO y por el Comité de Proyectos de la Escuela.
- **Project Manager**
 - Gestionar, según el Project Management Body Of Knowledge, su proyecto profesional, siguiendo los lineamientos de la Dirección de Proyectos durante todos sus procesos: Inicio, Planificación, Ejecución, Seguimiento y Control, y Cierre.
 - Aplicar, adecuadamente, las metodologías ágiles en el proceso de ejecución de su proyecto (cualquiera sea su naturaleza).
 - Administrar, eficientemente, todos los recursos asignados a su cargo.
 - Realizar cualquier actividad que pudiese ser solicitada por su Portfolio Manager, por el Senior Portfolio Manager, por el Director de la PMO y por el Comité de Proyectos de la Escuela.
- **Recurso Humano**
 - Realizar las funciones asignadas por los Project Manager, tales como, investigación de artículos científicos, pruebas de caja negra, desarrollo de software basado en requerimientos y verificación de procesos de negocio.
 - Certificar a los proyectos de acuerdo a la evaluación brindada.

Para más información, ver el documento Descripción de Roles y Responsabilidades.

7.1.2 Adquisición de personal

El procedimiento para el requerimiento y adquisición de personal es como sigue:

- Llenar el formato de la solicitud de asignación de recurso según a la empresa virtual (IT Service, IT Research, Software Factory y IT Consulting).
- Enviar el formato mediante correo de cada empresa virtual.
- Completar las actas de reunión
- Realizar la evaluación del desempeño del recurso solicitado

Luego de ello, el recurso será enviado en el transcurso de la semana. Además, cada recurso brinda servicios por el periodo de 7 días académicos

7.1.3 Requerimientos de personal para el proyecto

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/.)
<i>Investigación de artículos científicos</i>	Externo	Inicio	3	7 horas	1
<i>Evaluación de procesos de negocio</i>	Externo	Ejecución	2	7 horas	1

7.1.4 Horarios definidos para el proyecto

El proyecto se desarrolla en el siguiente horario: Los días Lunes y Viernes de 4:00pm a 7:00pm en los diversos campus de la Universidad Peruana de Ciencias aplicadas (UPC). Los avances trabajados fuera del horario definido se reportarán para el seguimiento correspondiente y respetando el cronograma del proyecto.

7.1.5 Criterios de liberación del personal contratado

Se realizará liberación de personal solamente en casos de:

- Acusaciones graves entre los integrantes del proyecto y el personal de apoyo.
- Incumplimiento reiterado de las actividades del proyecto por parte del personal de apoyo.
- Retiro extraordinario del ciclo del personal de apoyo.
- Petición de los Project Manager para expulsión como apoyo del proyecto.

7.1.6 Planes de formación para recursos TDP

Para la formación del recurso de TPD, se realiza lo siguiente:

- Inducción al proyecto a desarrollar
- Capacitación de los temas relacionados al proyecto
- Explicación de las tareas a realizar

7.1.7 Personal de expertos requeridos para el proyecto

Para la evaluación del modelo desarrollado, se necesita de los siguientes perfiles de expertos:

- **Especialista en protección de datos personales**

Evaluará si los procesos y procedimientos propuestos del modelo son los más eficientes para la protección de datos personales y verifica si cumple con el marco legal y normativo vigente.

- **Especialista en seguridad de información**

Evaluará los procesos y procedimientos propuestos del modelo en función a los estándares de seguridad de información.

7.2 Roles y responsabilidades

7.2.1 Roles

Código de Rol	<i>CP</i>
Nombre del Rol	<i>Comité de Proyectos</i>

Código de Rol	<i>DPMO</i>
Nombre del Rol	<i>Director de la PMO</i>

Código de Rol	<i>Senior Portfolio Manager</i>
Nombre del Rol	<i>SPM</i>

Código de Rol	<i>Portfolio Manager</i>
Nombre del Rol	<i>PFM</i>

Código de Rol	<i>Asesor Cliente</i>
Nombre del Rol	<i>AC</i>

Código de Rol	<i>Project Manager</i>
Nombre del Rol	<i>PM</i>

Código de Rol	<i>Recurso Humano</i>
Nombre del Rol	<i>RH</i>

7.2.2 Características del rol requerido e identificación del recurso humano de la organización

Rol	Conocimiento	Habilidades	Actitudes
<i>Comité de Proyectos</i>	<i>PMBOK</i>	<ul style="list-style-type: none">• <i>Habilidades comunicativas.</i>• <i>Habilidades para la gestión</i>	<ul style="list-style-type: none">• <i>Actitud responsabilidad</i>• <i>Actitud de compromiso con el proyecto</i>

		<ul style="list-style-type: none"> y seguimiento de actividades. 	<ul style="list-style-type: none"> Actitud de mejora constante
Director de la PMO	PMBOK	<ul style="list-style-type: none"> Inteligencia emocional Habilidades comunicativas. Habilidades para la gestión y seguimiento de actividades. Habilidades de liderazgo. 	<ul style="list-style-type: none"> Actitud responsabilidad Actitud de compromiso con el proyecto Actitud de mejora constante Trabajo en equipo
Senior Portfolio Manager	PMBOK	<ul style="list-style-type: none"> Inteligencia emocional Habilidades comunicativas. Habilidades para la gestión y seguimiento de actividades. Habilidades de liderazgo. 	<ul style="list-style-type: none"> Actitud responsabilidad Actitud de compromiso con el proyecto Actitud de mejora constante Autodidacta Trabajo en equipo
Portfolio Manager	PMBOK	<ul style="list-style-type: none"> Inteligencia emocional Habilidades comunicativas. Habilidades para la gestión y seguimiento de actividades. Habilidades de liderazgo. Habilidades en asesoría en proyectos. 	<ul style="list-style-type: none"> Actitud responsabilidad Actitud de compromiso con el proyecto Actitud de mejora constante
Asesor Cliente	PMBOK	<ul style="list-style-type: none"> Inteligencia emocional Habilidades comunicativas. Habilidades para la gestión y seguimiento de actividades. Habilidades de liderazgo 	<ul style="list-style-type: none"> Actitud responsabilidad Actitud de compromiso con el proyecto

		<ul style="list-style-type: none"> • <i>Habilidades en asesoría en proyectos.</i> 	
<i>Project Manager</i>	<i>PMBOK</i>	<ul style="list-style-type: none"> • <i>Inteligencia emocional</i> • <i>Habilidades comunicativas.</i> • <i>Habilidades para la gestión y seguimiento de actividades.</i> • <i>Habilidades de liderazgo.</i> 	<ul style="list-style-type: none"> • <i>Actitud responsabilidad</i> • <i>Actitud de compromiso con el proyecto</i> • <i>Actitud de mejora constante</i> • <i>Autodidacta</i> • <i>Trabajo en equipo</i>
<i>Recurso Humano (Requerido)</i>	<i>Modelamiento de Procesos</i>	<ul style="list-style-type: none"> • <i>Habilidades de consultoría</i> • <i>Habilidades para la gestión y seguimiento de actividades.</i> • <i>Habilidades comunicativas</i> 	<ul style="list-style-type: none"> • <i>Actitud responsabilidad</i> • <i>Actitud de compromiso con el proyecto</i>
<i>Recurso Humano (Requerido)</i>	<i>Seguridad de la información</i>	<ul style="list-style-type: none"> • <i>Habilidades para la investigación de fuentes académicas sobre el tema del proyecto.</i> • <i>Habilidades comunicativas.</i> • <i>Habilidades para la gestión y seguimiento de actividades.</i> 	<ul style="list-style-type: none"> • <i>Actitud responsabilidad</i> • <i>Actitud de compromiso con el proyecto</i> • <i>Actitud de mejora constante</i> • <i>Autodidacta</i>

Tabla 45: Matriz de características de roles

7.2.3 Recursos humanos requeridos en el tiempo

Número Estimado	Fecha requerida proyectada	Fecha de retiro proyectada	Tiempo requerido por recurso
10	13/08/2018	12/10/2018	20 horas
6	18/03/2019	14/06/2019	15 horas

7.3 Gestión de las comunicaciones

Información requerida	Contenido	Encargado	Stakeholders	Medio de comunicación	Perioridicidad	Código EDT
Definición del proyecto	<ul style="list-style-type: none"> - Problema - Objetivo General y Específicos - Alcance - Restricciones - Impacto - Stakeholder - Riesgos 	Project Manager	<ul style="list-style-type: none"> - Comité de Proyectos - Portfolio Manager - Asesor Cliente 	<ul style="list-style-type: none"> - Plantilla PMBOK – Project Charter - Correo electrónico 	1 vez durante el proyecto	1.1.1
Entregables del proyecto	<ul style="list-style-type: none"> - Listado de documentos con las fechas a presentar, requisitos de calidad y criterios de aceptación 	Project Manager	<ul style="list-style-type: none"> - Portfolio Manager - Asesor Cliente 	<ul style="list-style-type: none"> - Plantilla PMBOK – Diccionario EDT - Correo electrónico 	Mensual	1.2.1
Estado del proyecto	<ul style="list-style-type: none"> - Nivel del cumplimiento del alcance, calidad, comunicación y tiempo de los paquetes de trabajo y entregables 	Project Manager	<ul style="list-style-type: none"> - Portfolio Manager 	<ul style="list-style-type: none"> - Plantilla de Informe semanal de la UPC - Correo electrónico 	Semana	1.4.2
Temas conversados en las reuniones	<ul style="list-style-type: none"> - Agenda de la reunión - Detalle de lo conversado - Acuerdos realizados - Tareas pendientes 	Project Manager	<ul style="list-style-type: none"> - Asesor Cliente 	<ul style="list-style-type: none"> - Plantilla de Acta de reunión de la UPC - Correo electrónico 	Semanal	1.4.1

Equipo del proyecto	<ul style="list-style-type: none"> - Lista de las personas que forman parte del equipo - Roles de cada integrante 	Project Manager	<ul style="list-style-type: none"> - Portfolio Manager 	<ul style="list-style-type: none"> - Plantilla PMBOK – Gestión de recursos humanos - Correo electrónico 	Mensual	1.2.3
Antecedentes y situación actual del sector microfinanciero	<ul style="list-style-type: none"> - Análisis del sector microfinanciero - Detalle sobre las regulaciones, marcos legales y normativas para la protección de datos personales 	Project Manager	<ul style="list-style-type: none"> - Comité de Proyectos - Portfolio Manager - Asesor Cliente 	<ul style="list-style-type: none"> - Documento del Marco Teórico - Presentación interactiva 	Trimestral	1.3.1
Diseño del modelo referencia	<ul style="list-style-type: none"> - Definición del modelo propuesto - Fases y procesos del modelo - Entregables del modelo 	Project Manager	<ul style="list-style-type: none"> - Comité de Proyectos - Portfolio Manager - Asesor Cliente - Empresa microfinanciera 	<ul style="list-style-type: none"> - Documento del diseño del modelo - Presentación interactiva 	Semestral	1.3.2
Resultados de la validación del modelo	<ul style="list-style-type: none"> - Registro de resultados - Precisión del modelo 	Project Manager	<ul style="list-style-type: none"> - Comité de Proyectos - Portfolio Manager - Asesor Cliente - Empresa microfinanciera 	<ul style="list-style-type: none"> - Documento de validación del modelo 	2 veces durante el proyecto	1.3.4
Problemas por mejorar	<ul style="list-style-type: none"> - Registro de observaciones identificadas durante la fase de ejecución del proyecto 	Project Manager	<ul style="list-style-type: none"> - Comité de Proyectos - Portfolio Manager - Asesor Cliente 	<ul style="list-style-type: none"> - Documento de lecciones aprendidas 	Mensual	1.5.1

	- Soluciones ante problemas detectados					
--	--	--	--	--	--	--

Tabla 46: Matriz de la gestión de las comunicaciones

7.4 Matriz de asignación de responsabilidades

Código EDT	Entregable	Comité de Proyectos	Director de la PMO	Portfolio Manager	Asesor Cliente	Project Manager	Recurso Humano
1.1	Inicio	A	C	F, V	F, V	R	-
1.1.1	Project Charter	A	C	F, V	F, V	R	-
1.2	Planificación	C	C	F, V	V	R	-
1.2.1	Diccionario EDT	C	C	A, F, V	V	R	-
1.2.2	Matriz de trazabilidad de requisitos	C	C	A, F, V	V	R	-
1.2.3	Gestión de recursos humanos	C	C	A, F, V	V	R	-
1.2.4	Descripción de roles y responsabilidades	C	C	A, F, V	V	R	-
1.2.5	Matriz RAM	C	C	A, F, V	V	R	-
1.2.6	Matriz de riesgos	C	C	A, F, V	V	R	-
1.2.7	Matriz de comunicaciones	C	C	A, F, V	V	R	-
1.3	Ejecución					R	-
1.3.1	Memoria	A	C	F, V	V	R	P

1.3.2	Documento de análisis del modelo	A	C	F, V	V	R	-
1.3.3	Diseño de modelo de referencia	A	C	F, V	V	R	-
1.3.4	Documento de validación del modelo	A	C	F, V	V	R	-
1.3.5	Documento del plan de continuidad	A	C	F, V	V	R	-
1.4	Control y monitoreo					R	-
1.4.1	Acta de reunión	C	C	C	F, V	R	-
1.4.2	Informe semanal	C	C	F, V	C	R	-
1.5	Cierre					R	-
1.5.1	Lecciones aprendidas	A	C	V	F, V	R	-

Tabla 47: Matriz de asignación de responsabilidades

8 CONCLUSIONES

- El compromiso de la Gerencia General de la microfinanciera es fundamental para el desarrollo e implementación del modelo de referencia, ya que permite disponer de los recursos necesarios (Colaboradores, tiempo, presupuesto, entre otros).
- La microfinanciera hubiera podido ser sancionada por el órgano supervisor (Autoridad Nacional de Protección de Datos Personales) al no contar con las medidas respectivas de protección y tratamiento. Según el cuadro de sanciones especificado en la Ley 29733, se estimó que el incumplimiento de la microfinanciera antes de implementar el modelo de referencia era de 40.5 UITs equivalente a S/ 170,100.00.
- Algunas tecnologías orientadas a la seguridad informática no pudieron ser implementadas, ya que se excedían del presupuesto de la microfinanciera. Las herramientas descartadas fueron (Firewall Fortinet, y Checkpoint Antivirus). De igual manera, se realizaron acciones manuales para mitigar los riesgos que había detectado nuestro modelo de referencia.
- Los documentos internos de seguridad deben adecuarse a la realidad de cada empresa. En el caso de “Vale un Perú” se logró establecer y aprobar por la Gerencia General, 17 políticas que cubren todos los aspectos de la microfinanciera.
- Los colaboradores de “Vale un Perú” fortalecieron los conocimientos de protección de datos personales y seguridad de la información, luego de recibir la capacitación correspondiente.
- La microfinanciera logró robustecer sus procesos normativos, organizacionales y aspectos técnicos, luego de implementado el modelo de referencia. En todas las categorías se ajustaron los controles, logrando un estándar para el sector microfinanciero.

9 RECOMENDACIONES

- Elaborar un contrato con el personal de Soporte Tecnológico, con el fin de regularizar sus actividades y resguardar el nivel de confidencialidad de la empresa.
- Solicitar el consentimiento de datos personales a los socios antiguos.
- Adquirir una herramienta centralizada para darle seguimiento a los eventos de virus informático y código malicioso en los dispositivos de los usuarios.
- Migrar la infraestructura tecnológica a la plataforma de Microsoft 365 (entorno cloud), adquiriendo la licencia Microsoft Business Premium. Con esta licencia,

podrán asegurar su información contra ataques maliciosos, gestionar los accesos, optimizar rendimiento, configurar políticas de inicio de sesión, entre otros.

- El responsable de los datos personales de “Vale un Perú” debería ser el Analista de Operaciones. Actualmente, es la Gerente General, pero indicaron que próximamente evaluarán traspasar esta responsabilidad.
- Los archivadores están en un pasillo, se ha asegurado su acceso con candados (la llave se distribuyó entre los encargados), pero se recomienda que estén en otro ambiente, el cuál pueda ser controlado ante cualquier evento.
- Los CPU que fungen como servidores, deberían estar en un ambiente más seguro (alejado de la zona de trabajo, temperatura adecuada, cerrado, entre otros). Actualmente, están en un cuarto al lado de la sala de reuniones. Asimismo, se aseguró su ingreso con la instalación de una cerradura y control de acceso utilizando una bitácora.
- Realizar un respaldo de información del servidor de archivos, de la base de datos y configuración de su sistema Core. Esta actividad debe realizarse una vez cada año como mínimo, el responsable de verificar el cumplimiento debe ser el Analista de Operaciones y quien ejecute la acción será Soporte Tecnológico.

10 GLOSARIO

Ley 29733 - Ley de Protección de Datos Personales: La legislación peruana cuyo objetivo es garantizar el derecho fundamental de la protección de las privacidades de las personas, para lo cual se requiere un tratamiento proporcional y seguro de los datos personales, acorde a finalidad por la que fue consentida por su titular, y evitando que sea de tráfico o uso ilícito (Congreso de la República del Perú, 2011).

Banco de datos personales: Es el conjunto organizado de datos personales, automatizado o no, independiente del soporte, forma o modalidad de su creación, organización, formación, almacenamiento y acceso (Congreso de la República del Perú, 2011).

Banco de datos personales de administración privada: Es el banco de datos personales cuyo origen no esté vinculado al ejercicio del dominio público, y el titular sea una persona natural o jurídica de derecho privado (Congreso de la República del Perú, 2011).

Datos personales: Es toda información permita determinar, directa o indirectamente, la identidad de una persona natural a través de medios razonablemente utilizados (Congreso de la República del Perú, 2011).

Datos sensibles: Es el dato personal compuesto por datos biométricos; ingresos económicos, opiniones, o convicciones políticas, religiosas, filosóficas o morales; datos referidos al origen racial y étnico; salud o vida sexual; o afiliación sindical (Congreso de la República del Perú, 2011).

Seguridad de la Información: Son un conjunto de medidas que permite resguardar la confidencialidad, integridad y disponibilidad de la información mitigando los riesgos a los que se expone (INDECOPI, 2014).

Incidente de seguridad de la información: Es el evento asociado a un posible error en los controles, o una circunstancia desconocida con alta probabilidad de comprometer la operatividad del negocio y amenazar la seguridad de la información (ISO/IEC, 2013).

ISO/IEC 27001 – Sistema de Gestión de Seguridad de la Información: Es una norma internacional que detalla los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información en un entorno organizativo (ISO/IEC, 2013).

PMBOK – Guía de los fundamentos para la dirección de proyectos: Es manual que establece las bases para la dirección de proyectos y describe el conocimiento y prácticas aplicables a la mayoría de los proyectos desde que se inicia hasta su finalización. Esta guía brinda normas, métodos, procesos y prácticas establecidas. Además, de un vocabulario propio para la dirección de proyectos (PMI, 2014).

11 REFERENCIAS

- Accenture. (03 de 2016). *Accenture*. Obtenido de The State of Cybersecurity and Digital Trust 2016: https://www.accenture.com/t00010101T000000__w__it-it/_acnmedia/PDF-23/Accenture-State-Cybersecurity-and-Digital-Trust-2016-Report-June.pdf
- Arana , R., Núñez, J., Ore, J., & Velazco, D. (2017). *Planeamiento Estratégico del Sistema de Cajas Rurales de Ahorro y Crédito en el Perú*. Surco: CENTRUM .
- Capillo, J. (2015). *Evolución de las EDPYMES*. Obtenido de Evolución de las EDPYMES - TESIS: http://www.biblioteca.udep.edu.pe/bibvirudep/tesis/pdf/1_111_204_70_1031.pdf
- Cepymenews España. (16 de Junio de 2017). *Un 69% de las empresas ha experimentado el robo de datos por parte de empleados*. Obtenido de Portal de Noticias de Pymes, autónomos y emprendedores: <https://cepynews.es/69-las-empresas-ha-experimentado-robo-datos-parte-empleados/>
- CIS. (15 de Octubre de 2015). CIS Critical Security Controls. *The CIS Critical Security Controls for Effective Cyber Defense(6)*. Recuperado el 14 de Mayo de 2019
- Congreso de la República del Perú. (3 de Julio de 2011). *Ley de protección de datos personales*. Obtenido de Ministerio de Justicia del Perú: <https://www.minjus.gob.pe/wp-content/uploads/2013/04/LEY-29733.pdf>
- Deloitte. (07 de 2016). *La Evolución de la Gestión de Ciber-Riesgos y Seguridad de la Información*. Obtenido de Encuesta 2016 sobre Tendencias de Ciber-Riesgos y Seguridad de la Información en Latinoamérica: [https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/Deloitte%202016%20Cyber%20Risk%20%20Information%20Security%20Study%20-%20Latinoam%20-%20Resultados%20Generales%20vf%20\(Per%20BA\).pdf](https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/Deloitte%202016%20Cyber%20Risk%20%20Information%20Security%20Study%20-%20Latinoam%20-%20Resultados%20Generales%20vf%20(Per%20BA).pdf)
- Economipedia. (s.f.). *Economipedia*. Obtenido de Entidad Financiera: <http://economipedia.com/definiciones/entidad-financiera.html>

- Ernst & Young. (12 de 2015). *Crear confianza en el Mundo Digital*. Obtenido de Encuesta Global sobre Seguridad de la información de EY de 2015: - [https://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2015/\\$FILE/ey-encuesta-global-seguridad-informacion-2015.pdf](https://www.ey.com/Publication/vwLUAssets/ey-encuesta-global-seguridad-informacion-2015/$FILE/ey-encuesta-global-seguridad-informacion-2015.pdf)
- Ernst & Young. (Diciembre de 2017). *Recuperación la Ciberseguridad: Prepárese para enfrentar los ataques cibernéticos*. Obtenido de Encuesta Global de Seguridad de la Información: [https://www.ey.com/Publication/vwLUAssets/EY-recuperando-la-ciberseguridad/\\$File/EY-recuperando-la-ciberseguridad.pdf](https://www.ey.com/Publication/vwLUAssets/EY-recuperando-la-ciberseguridad/$File/EY-recuperando-la-ciberseguridad.pdf)
- Gestión. (15 de 11 de 2015). *Diario Gestión*. Obtenido de Ley de Protección de Datos Personales: <https://gestion.pe/tendencias/management-empleo/ley-proteccion-datos-personales-32297>
- Gestión. (04 de Mayo de 2015). *Empresas recibirían multas de hasta S/. 385,000 por mal uso de sus bases de datos*. Obtenido de Diario Gestión: <https://gestion.pe/economia/empresas-recibirian-multas-s-385-000-mal-bases-datos-88485>
- Gestion. (15 de Febrero de 2016). *Mafias ahora roban datos de personas para obtener préstamos y celulares*. Obtenido de Diario Gestion Perú: <https://gestion.pe/tu-dinero/mafias-roban-datos-personas-obtener-prestamos-celulares-145116>
- Gestión. (05 de 06 de 2017). *El ABC de la protección de datos personales (data privacy)*. Obtenido de <https://gestion.pe/blog/reglasdejuego/2017/06/el-abc-de-la-proteccion-de-datos-personales-data-privacy.html?ref=gesrhttps://gestion.pe/blog/reglasdejuego/2017/06/el-abc-de-la-proteccion-de-datos-personales-data-privacy.html?ref=gesr>
- Gestión. (19 de Agosto de 2017). *El sector financiero en Perú presenta vulnerabilidades en seguridad cibernética*. Obtenido de Diario Gestión: <https://gestion.pe/tecnologia/sector-financiero-peru-presenta-vulnerabilidades-seguridad-cibernetica-141940>
- Gestión. (22 de 11 de 2017). *Empresas peruanas destinarán hasta 7% de su presupuesto de TI a ciberseguridad en próximos años*. Obtenido de Diario Gestión:

<https://gestion.pe/tecnologia/empresas-peruanas-destinaran-7-presupuesto-ciberseguridad-proximos-anos-153235>

- INDECOPI. (20 de Noviembre de 2014). NTP-ISO/IEC 27001. *Norma Técnica Peruana - NTP-ISO/IEC 27001*. Lima, Lima, Perú. Recuperado el 12 de Junio de 2019
- ISA. (Setiembre de 2018). ISA/IEC 62443. *Industrial communication networks - Network and system security*. Recuperado el 2 de Junio de 2019
- ISACA. (2012). COBIT 5 Framework. *Un marco de Negocio para el Gobierno y la Gestión de las TI de la empresa*. ISACA. Recuperado el 3 de Mayo de 2019
- ISO/IEC. (1 de Octubre de 2013). ISO/IEC 27001. *Tecnología de la Información – Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información - Requisitos, 2*. Recuperado el 4 de Junio de 2019
- Kaspersky Lab. (Diciembre de 2017). *Kaspersky Lab Daily*. Obtenido de The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within: https://www.kaspersky.com/blog/the-human-factor-in-it-security/?_ga=2.191172588.756368325.1526090245-1556602387.1526090245
- Microfinanzas. (2016). *Microfinanzas*. Obtenido de ¿Qué son las cajas municipales?: <https://microfinanzasglobal.com/caja-municipal/>
- Ministerio de Justicia. (03 de 04 de 2018). *Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales*. Recuperado el 23 de 02 de 2015, de Registro de Sanciones Impuestas por la APDP: https://www.minjus.gob.pe/wp-content/uploads/2017/11/Cuadro-de-publicaci%C3%B3n-de-Sanciones-NOV_2017.pdf
- Municipalidad de Lima. (s.f.). *Municipalidad de Lima*. Obtenido de Caja Metropolitana: <http://www.munlima.gob.pe/caja-municipal>
- NIST. (Abril de 2013). NIST Special Publication 800-53. *Security and Privacy Controls for Federal Information Systems and Organizations(4)*. Recuperado el 20 de Julio de 2019

- PeCERT. (08 de 01 de 2016). *Coordinación de Emergencias en Redes Teleinformáticas*. Obtenido de Norma Técnica Peruana ISO/IEC 27001:2014: http://www.pecert.gob.pe/_publicaciones/2014/ISO-IEC-27001-2014.pdf
- PMI. (21 de 04 de 2014). *Project Management Institute*. Obtenido de PMBOK 6ta Edición: https://www.edu.xunta.gal/centros/cfrpontevedra/aulavirtual2/pluginfile.php/13688/mod_folder/content/0/libros_pmbok_guide5th_spanish.pdf?forcedownload=1
- PwC - Perú. (5 de 12 de 2016). *20th Global CEO Survey*. Recuperado el 26 de 09 de 2016, de PwC - Perú: <https://www.pwc.pe/es/publicaciones/assets/20-ceo-survey-peru.pdf>
- RPP. (29 de Octubre de 2017). *Denuncian venta de bases de datos de peruanos en Wilson*. Obtenido de RPP Noticias: <http://rpp.pe/lima/seguridad/video-denuncian-venta-de-bases-de-datos-de-peruanos-en-wilson-noticia-1085561>
- RRP. (24 de Octubre de 2017). *El INEI habría incumplido ley de Datos Personales al firmar convenios por censo*. Obtenido de RPP Noticias: <http://rpp.pe/politica/estado/video-el-inei-habria-incumplido-ley-de-datos-personales-al-firmar-convenios-por-censo-noticia-1084609>
- SBS. (02 de 04 de 2009). *Superintendencia de Banca y Seguros del Perú*. Obtenido de Circular G-140: <http://www.sesdis.org.pe/intranet/wp-content/uploads/2016/08/Circular-140-2009.pdf>
- Vojislav B., M., & J. Leon, Z. (2000). *Evaluating the Quality of Reference Models*. Obtenido de Evaluating the Quality of Reference Models: http://sci-hub.tw/10.1007/3-540-45393-8_35

12 ANEXOS

12.1 Diagramas de los procesos de negocios de la Cooperativa de Ahorros y Créditos “Vale un Perú”

1) Retiro de socio

2) Refinanciación de préstamo

3) Estado de cuenta de préstamo

Powered by
bizagi
Modeler

4) Emisión de reportes

Powered by
bizagi
Modeler

5) Desembolso de crédito

Powered by
bizagi
Modeler

6) Cierre de módulo de contabilidad

Powered by
bizagi
Modeler

7) Cierre del módulo de préstamos

Powered by
bizagi
Modeler

8) Cancelación de préstamo

Powered by
bizagi
Modeler

9) Cancelación de cuenta de depósito a plazo

10) Atención de incidentes tecnológicos

11) Apertura de cuenta depósito a plazo

12) Apertura de cuenta de aportaciones

13) Apertura de cuenta de ahorros

14) Admisión de nuevo socio

15) Admisión de nuevo colaborador

12.2 Políticas e instructivos de seguridad de la información para la Cooperativa de Ahorros y Créditos “Vale un Perú”

POLÍTICA DE INVENTARIO DE ACTIVOS

1. OBJETIVO

La Política de Inventario de Activos de Información de “Vale un Perú” tiene por objetivo mantener un registro y control formal del íntegro de los activos de Información de la compañía, con la finalidad de poder establecer controles, y/o mecanismos de protección acordes a cada tipo de activo. Cabe resaltar que esta política fue desarrollada de acuerdo con lo contemplado en la ISO/IEC 27011:2014, y en la Circular N° G- 140 -2009 “Gestión de la seguridad de la información”.

2. ALCANCE

Esta política es de estricto cumplimiento de todas aquellas personas que mantienen un vínculo laboral con la empresa, de manera temporal o permanente, bajo todas las modalidades de contrato.

3. DESCRIPCIÓN

- a. El Encargado de seguridad de información en coordinación con el propietario deben identificar los activos de información asociadas a los procesos.
- b. La actualización de este proceso se debe realizar de forma anual y/o cuando se estime que un activo de información ha aumentado su nivel de sensibilidad. La responsabilidad de la decisión corresponde al propietario de los activos de información¹ en coordinación con el Encargado de seguridad de información.
- c. “Vale un Perú”, deberá realizar anualmente un inventario de activos de información, el cual deberá tener de manera detallada los Sistemas de Información, los equipos de cómputo, otros equipos informáticos, y los documentos físicos y/o medios magnéticos, con clasificación Altamente Confidencial, que se encuentren involucrados en las operaciones de la empresa.

¹ Colaborador de “Vale un Perú” responsable de verificar y validar los controles de seguridad asociados a los activos de información de la compañía. Esta responsabilidad recae principalmente sobre los encargados de cada área.

- d. Todo activo de información físico, de “Vale un Perú”, debe contar con un identificador único, y fácilmente ubicable para su revisión, el cual deberá ser actualizado, y/o revisado anualmente, por el responsable de la ejecución del inventario de activos.
 - e. Es responsabilidad de los propietarios del(los) activo(s) de información en coordinación con el Encargado de seguridad de información, el asegurar la correcta ejecución del inventario de activos de información de “Vale un Perú”. Dicha actividad deberá revisar también, la clasificación de los mencionados activos.
 - f. Toda adquisición de equipos de cómputo, sistemas de información, base de datos u otro activo de información, debe ser registrada por el propietario del activo, y/o custodio de los activos de información² en el inventario de activos de información correspondiente.
 - g. Dentro del Inventario de Activos de TI debe existir una sección para el inventario de software a fin de mantener siempre actualizadas las versiones de software instaladas en todos los equipos de cómputo de “Vale un Perú”. Asimismo, al desinstalar software, se debe actualizar la correspondiente sección en el Inventario de activos de TI y el número de licencias asociadas. Esto es responsabilidad del área de Soporte TI.
 - h. Se debe establecer un cronograma y/o plan formal de toma de inventario anual de activos de información. Este debe ser avalado por el Encargado de seguridad de información de “Vale un Perú”, y aprobado por la Gerencia General.
- **Consideraciones para la gestión del inventario de activos de información**
 - a. El Encargado de seguridad de información debe identificar los activos de información y registrarlos en el Formato “Inventario de Activos de Información” ubicado en su repositorio personal.
 - b. La categorización de activos es la siguiente:

² Rol correspondiente a áreas y/o cargos que tienen bajo su responsabilidad la custodia de los activos de información sin interesar su ubicación física, lógica, medio de resguardo, tecnología o propósito de uso.

- ✓ Activos de información: Los activos de información pueden ser categorizados en los siguientes tipos: Información electrónica, documento en papel, información hablada.
 - ✓ Activos de Software: Los activos de Software pueden ser categorizados en los siguientes tipos: Software desarrollado por terceros, software desarrollado internamente, software de administración de Base de Datos, otro software.
 - ✓ Activos físicos: Equipo de procesamiento, equipo de comunicaciones, medio de almacenamiento, mobiliario y equipamiento, otros equipos.
 - ✓ Servicios: Servicios de tratamientos y comunicaciones, servicios generales (calefacción, alumbrado, energía, aire acondicionado).
- c. La clasificación de la información de “Vale un Perú” es la siguiente:
- ✓ Altamente Confidencial: Esta información debe ser conocida únicamente por el propietario de información y su uso o difusión hacia un grupo de personas debe ser limitado.
 - ✓ Confidencial: Su distribución debe estar restringida a un pequeño grupo de personas, pues revelarla sin permiso puede tener un impacto negativo de grandes alcances para la Cooperativa, sus accionistas, socios de negocios, empleados y/u otros clientes.
 - ✓ Interna: La información interna es la clasificación más común que se maneja en la Compañía. Su distribución está generalmente restringida a un grupo más grande de personas. Revelarla sin autorización puede repercutir negativamente, originando un impacto moderado en las operaciones del negocio.
 - ✓ Publica: La información pública no es confidencial y está enfocada al uso general tanto dentro como fuera de la Compañía.
- d. El registro del inventario de los activos de información deberá indicar como mínimo los siguientes datos:
- ✓ Código único del Activo.
 - ✓ Línea de negocio
 - ✓ Proceso
 - ✓ Nombre de Activo
 - ✓ Usuario asignado al Activo.
 - ✓ Descripción

- ✓ Propietario de la Información responsable del Inventario
 - ✓ Custodio
 - ✓ Tipo
 - ✓ Ubicación del Activo.
 - ✓ Datos personales
 - ✓ Datos tarjeta
 - ✓ Impacto: P1 Confidencial, P2 Integridad, P3 Disponibilidad
- e. En caso de cambios y/o modificaciones en alguna de las características, y/o condiciones de los activos de Información, éstas deben ser actualizadas en el inventario de Activos de Información por el propietario y/o custodio asociado.

4. INCUMPLIMIENTO

- a. El incumplimiento de esta política puede generar el desconocimiento o falta de enfoque en los principales activos de información de la compañía no permitiendo un adecuado proceso de análisis y evaluación de riesgos asociados a estos activos. Esto puede afectar la confidencialidad, integridad y disponibilidad de la información de “Vale un Perú”.
- b. El incumplimiento de la presente política representa una falta, la cual puede seguir las medidas correspondientes en el Artículo 29 del Reglamento Interno de Trabajo de “Vale un Perú”.

POLÍTICA DE CONTROL DE ACCESO A LA RED Y SEGURIDAD LÓGICA

1. OBJETIVO

La política de Control de Acceso y Seguridad Lógica a la Información de “Vale un Perú” tiene como objetivo controlar el acceso a los principales sistemas de información y activos críticos de la compañía. Esta política fue desarrollada de acuerdo con lo contemplado en la ISO/IEC 27001:2014 y en la Circular N° G- 140 -2009 “Gestión de la Seguridad de la Información”.

2. ALCANCE

Esta política es de estricto cumplimiento de todas aquellas personas que mantienen un vínculo laboral con la empresa, de manera temporal o permanente, bajo todas las modalidades de contrato.

3. DESCRIPCIÓN

3.1. Control de acceso a la red

- a. Los accesos a los servicios de red son asignados por el área de Soporte TI en la creación de los usuarios.
- b. Todos los usuarios de “Vale un Perú” deben acceder a los Servicios de Red (impresión, carpetas compartidas, servidores, internet, entre otros) de la empresa a través de una cuenta en el dominio. Esto es requerido mediante la Solicitud de Autorización de Accesos a Sistemas y Asignación de Equipos.
- c. El acceso a las herramientas tecnológicas se realizará solamente a través de equipos de la empresa y/o configurados por personal de “Vale un Perú”, a excepción de las aplicaciones web (si hubieran). Asimismo, el acceso a dichas herramientas considera la sensibilidad de los datos a los que se accede por lo que se realizará una autenticación mediante contraseña fuerte o de ser el caso mediante una doble autenticación. Es responsabilidad del Encargado de seguridad de información definir los lineamientos bajo los cuales se basará el área de Soporte TI para la ejecución de controles de acceso.
- d. La habilitación de los accesos a los servicios de Internet a través de dispositivos móviles (Smartphone, laptops, tablets, entre otros) se destinarán sólo al personal debidamente autorizado y de acuerdo con el perfil aprobado. Es responsabilidad del Encargado de seguridad de información y el Responsable de Soporte TI validar estos perfiles.

- e. Los usuarios pueden utilizar sus computadoras o los servicios de red para visualizar, descargar, guardar, recibir o enviar archivos de video, música, imágenes o similares, siempre y cuando no esté relacionado con:
 - ✓ Contenido ofensivo de cualquier clase, incluyendo material pornográfico.
 - ✓ Promover la discriminación sobre la base de raza, género, nacionalidad, edad, estado civil, orientación sexual, religión o discapacidad.
 - ✓ Comportamiento violento o intimidante, apuestas, juegos o beneficio económico personal.
- f. Se restringe el acceso a la red a través de equipos de terceros (proveedor). En caso de requerirlo por asuntos de negocio, se deberá solicitar la autorización al Encargado de seguridad de información indicando el sustento correspondiente.
- g. Los usuarios no deben participar en juegos de entretenimiento en línea o de manera local. Asimismo, no deben acceder a servicios de radio ni de TV por demanda y no deben tratar de violar la seguridad de las computadoras, servidores y equipos de comunicaciones de la empresa.
- h. El Encargado de seguridad de información es responsable del control de los accesos a los servicios de red, y la realización de pruebas de intrusión y evaluación de vulnerabilidades de forma periódica. Es responsabilidad del Responsable de Soporte TI el monitoreo de la red interna y externa de “Vale un Perú”, de acuerdo con lo estipulado en la Política de Administración de las Operaciones y Comunicaciones.
- i. Es responsabilidad del Encargado de seguridad de información en coordinación con Gerencia General realizar el monitoreo periódico de los accesos para sincerar su autorización y correcta asignación a los usuarios.
- j. En el caso de un cese de un colaborador que maneje información Altamente Confidencial, el jefe inmediato deberá notificar al responsable de Soporte TI, GDH, Administración y Seguridad de la Información esta decisión a fin de retirarle los accesos lógicos correspondientes de inmediato. En caso excepcional que se desee mantener activo algún acceso (personal cesado) el jefe inmediato debe informar esto a Soporte TI y Seguridad de la Información indicando el sustento correspondiente del requerimiento y fecha de caducidad del pedido (esta fecha no deberá exceder los 30 días).

3.1. Gestión de acceso de usuarios

- a. Cualquier tipo de acceso a recursos de la red proporcionados por “Vale un Perú” obliga la configuración de una contraseña de acceso al equipo bajo los lineamientos indicados en la Política de Gestión de Acceso de Usuarios.
- b. Todo sistema de información de “Vale un Perú” requiere de una cuenta de acceso y contraseña en el momento en que se inicia una sesión, así como después de cierto periodo de inactividad. Los parámetros específicos dependerán de lo definido entre las áreas de Soporte TI y Seguridad de la Información. La complejidad de la contraseña inicial de acceso al equipo debe considerar lo estipulado en la Política de Gestión de Acceso de Usuarios.
- c. La gestión y administración operativa de los accesos de usuarios a los sistemas de información de “Vale un Perú”, son responsabilidad del área de Soporte TI o del personal que la misma designe como responsable para tales efectos.
- d. Los privilegios especiales, se deben restringir a aquellas personas responsables de la administración de los sistemas, pudiendo existir excepciones cuando el propietario del activo y El Encargado de seguridad de información las autorice formalmente. Todo privilegio especial debe ser debidamente registrado y monitoreado mediante la creación de un requerimiento formal vía correo electrónico dirigido a Responsable de Soporte TI, con copia al Encargado de seguridad de información y Gerente General.
- e. Los cambios en la configuración del sistema operativo y en actividades relacionadas a los privilegios del sistema, deben ser realizados por los administradores del sistema, no por los usuarios finales de “Vale un Perú”.
- f. Las solicitudes para nuevos accesos de usuario y modificaciones en los privilegios deben estar autorizados por el responsable o gerente de área, por el(los) propietario(s) de los activos involucrados y el área de seguridad de la información antes de ser ejecutadas por el área de Soporte TI. Los registros de estas solicitudes deben conservarse por un periodo mínimo de un año.
- g. Los visitantes y/o terceros de “Vale un Perú” no deben recibir accesos de usuario ni privilegios para usar los equipos o redes de “Vale un Perú”, a menos que obtengan la autorización formal del gerente de área y en caso se requiera accesos a sistemas por el(los) propietario(s) de los activos involucrados y el área de seguridad de la información.

- h. Los privilegios otorgados a los colaboradores de “Vale un Perú” deben tener validez por períodos no mayores a un año. Los privilegios otorgados a los visitantes y/o terceros de “Vale un Perú” deben tener validez por períodos de 90 días o menos y, según sea necesario, se debe pedir una nueva autorización de sus privilegios al propietario de la información cada 90 días.
- i. El propietario del activo en coordinación con el Encargado de seguridad de información es responsable de coordinar una revisión anual de los privilegios otorgados a los usuarios de su área, registrando a través de correo electrónico, las revocaciones o modificaciones de privilegios que resulten de la revisión.
- j. Asimismo, al momento del cese de la relación laboral, el Responsable de Recursos Humanos, debe de emitir una notificación a los involucrados en el proceso de ceses (Soporte TI, Seguridad de la información y Administración).
- k. En el caso de un cese de un colaborador que maneje información confidencial, el jefe inmediato deberá notificar a las áreas de los Responsables de Soporte TI, GDH, Administración y SDI esta decisión a fin de retirarle los accesos lógicos correspondientes de inmediato.
- l. El jefe de área deberá informar acerca de los cambios por ascensos o movimientos a las áreas involucradas. El área de Soporte e Infraestructura TI realiza de acuerdo con los procedimientos definidos los cambios y/o actualizaciones que sean necesarios para el colaborador. GDH, debe informar sobre los nuevos ingresos a las áreas involucradas y validar los ascensos o movimientos de los colaboradores de la empresa.
- m. En caso excepcional que se desee mantener algunos accesos (limitados) el jefe inmediato debe solicitar el permiso correspondiente al Encargado de seguridad de información y al Responsable de Soporte TI, indicando el tiempo que se requerirán estos accesos (debe ser el tiempo mínimo indispensable) y el sustento correspondiente.

3.2. Responsabilidades de usuario y gestión de contraseña de usuario

- a. Es responsabilidad de los propietarios de los activos (gerencias), establecer los accesos a los diferentes tipos de información de la Cooperativa para el personal a su cargo. Asimismo, es su responsabilidad revisar y/o evaluar periódicamente los

- privilegios de los colaboradores a su cargo y solicitar se restrinja o revoque cualquier privilegio en caso sea necesario.
- b. La sesión de usuario quedará bloqueada automáticamente luego de un periodo de inactividad que será definido por el Responsable de Soporte TI y Seguridad de la Información. Al crearse una cuenta de usuario se le asignará una contraseña temporal que deberá ser cambiada en el primer inicio de sesión. Las cuentas de usuarios quedarán bloqueadas automáticamente después de 3 intentos fallidos (por un lapso 30 minutos) y sólo podrá ser desbloqueada por el personal el Responsable de Soporte TI durante ese lapso de tiempo.
 - c. El Encargado de seguridad de información, es responsable de informar a los usuarios que es obligatorio el cambio de su contraseña inicial y que debe ser compleja.
 - d. La asignación de la contraseña para acceso a la red y la contraseña para acceso a sistemas debe ser realizada de forma individual, por lo que queda prohibido el uso de contraseñas compartidas. El Encargado de seguridad de información y el Responsable de Soporte TI evaluarán los casos excepcionales relacionados a la presente política.
 - e. Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá reportarlo vía e-mail indicando si es de acceso a la red o a los sistemas de información, a fin de que se le proporcione una nueva contraseña temporal. Cabe resaltar que esta contraseña temporal deberá ser cambiada inmediatamente por el usuario.
 - f. Está prohibido que los identificadores de usuarios y contraseñas se encuentren de forma visible en cualquier medio impreso o escrito en el área de trabajo del usuario, de manera de que se permita a personas no autorizadas su conocimiento.
 - g. Se debe de considerar el monitoreo de eventos relacionados a la seguridad en el uso de sesiones en la red de “Vale un Perú”. Algunos de estos eventos son:
 - ✓ Inicios de sesión fallidos.
 - ✓ Principales motivos de fallas en el proceso de inicio de sesión.
 - ✓ Cambios en la definición de políticas de red
 - ✓ Creación, modificación y eliminación de usuarios de red.
 - ✓ Actividad de cuentas con privilegios de administrador.
 - h. El Responsable de Soporte TI es responsable del cambio de contraseñas por defecto (fabricante) en los productos o equipos adquiridos por “Vale un Perú”. Para el caso de Software recién adquirido, el Responsable de Soporte TI deberá modificar las

cuentas especiales que vienen por defecto luego de su instalación, esto con el objetivo de evitar accesos no autorizados.

3.3. Control de acceso remoto

- a. Los controles referidos al acceso remoto a la red de “Vale un Perú”, se encuentran especificados en la Política de Acceso Remoto y Computación Móvil.

4. INCUMPLIMIENTO

- a. El incumplimiento de esta política puede generar la materialización de riesgos de acceso lógico a los activos de información de la compañía (sistemas, correo electrónico, servicios de red) pudiendo afectar la confidencialidad, integridad y disponibilidad de la información de “Vale un Perú”.
- b. El incumplimiento de la presente política, que ocasione cualquier riesgo o pérdida para la compañía, pueden conllevar a una acción disciplinaria o legal, según lo definido en el documento “Reglamento Interno de Trabajo”.

POLÍTICA DE ADMINISTRACIÓN DE LAS OPERACIONES Y COMUNICACIONES

1. OBJETIVO

La política de administración de las operaciones y comunicaciones de “Vale un Perú” tiene por objetivo garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones. Esta política fue desarrollada de acuerdo con lo contemplado en la Circular N° G- 140 - 2009 “Gestión de la seguridad de la información” y la ISO/IEC 27001:2014.

2. ALCANCE

Esta política aplica a toda la información producida, procesada, transmitida y almacenada en “Vale un Perú”. Asimismo, aplica a todos los sistemas y bases de datos asociadas con el almacenamiento, procesamiento y transmisión de la información por y a favor de “Vale un Perú”. Esta política es de estricto cumplimiento, de todas aquellas personas que mantienen un vínculo laboral con la empresa, de manera temporal o permanente, bajo todas las modalidades de contrato.

3. DESCRIPCIÓN

1. Procedimientos y responsabilidades de operación
 - a. Cada área deberá asegurar la documentación formal de sus procedimientos operativos, estableciendo las responsabilidades y los recursos utilizados para su ejecución.
 - b. Los datos y sistemas informáticos en producción podrán ser modificados estrictamente por personal autorizado y de acuerdo con los procedimientos establecidos. Esto requerirá una aprobación de los propietarios de los activos de información involucrados.
 - c. El Responsable de Soporte TI debe definir procedimientos sobre el buen uso de los recursos informáticos. Los procesos de “Vale un Perú” deberán considerar la segregación de tareas. Las actividades y tareas que involucren información sensible o Altamente Confidencial (ej. datos sensibles de clientes y/o datos de titulares de tarjetas) deben requerir por lo menos de dos personas para su acceso, una para el tratamiento y la otra para su supervisión o aprobación.
 - d. Las configuraciones y puestas en marcha de servicios de Tecnología de la Información son normadas por el Responsable de Soporte TI de “Vale un Perú”, y analizadas previamente por el Encargado de seguridad de información.

- e. El personal de la Jefatura de Soporte TI y Jefatura de Desarrollo puede alterar la prioridad o paralizar la ejecución de un proceso o tarea en los equipos de la compañía que consuma recursos excesivos de los activos de información o que degrada significativamente el tiempo de respuesta de los sistemas de información; culminar las sesiones del usuario o cortar las conexiones si se identifica un incumplimiento de las políticas de seguridad establecidas en coordinación con el área de Seguridad de la Información o un consumo de recursos excesivos de TI.
- f. El Responsable de Soporte TI deberá:
 - ✓ Elaborar y difundir al personal pertinente, un plan de recuperación ante desastres (DRP) que permita recuperar los sistemas críticos de la compañía ante un evento severo que genere la indisponibilidad de estos sistemas y/o servicios TI. Como buena práctica, el personal que brinda soporte a los sistemas y/o aplicaciones críticas de “Vale un Perú” deberá contar con una persona de reemplazo que asuma estas funciones en caso de indisponibilidad del personal primario.
 - ✓ Realizar revisiones concernientes a los sistemas operativos, motores bases de datos, software de administración de equipos y demás activos de software en producción, los cuales deberán mantenerse en su versión más actualizada y estable.
 - ✓ El Encargado de seguridad de información deberá definir los niveles de riesgo existentes en la contratación del personal externo para el mantenimiento de los sistemas de información críticos en “Vale un Perú”. Los contratos establecidos para este fin deberán contener cláusulas que aseguren la confidencialidad de la información (principalmente relacionada a datos sensibles de clientes y/o datos de titulares de tarjetas) y propiedad intelectual del producto de software.

2. Planificación y aceptación de sistemas

- a. El Responsable de Soporte TI efectuará todo el proceso propio de la planificación, desarrollo o adquisición de los sistemas, ejecutar los procesos de pruebas, adaptación y puesta en producción de los sistemas de información de “Vale un Perú”.

- b. Únicamente se utilizarán sistemas de información certificados y provenientes de proveedores formalmente constituidos. La aceptación de los sistemas de información es responsabilidad del responsable del proceso (propietario del sistema) y la puesta en producción del Responsable de Soporte TI previo análisis y pruebas de certificación en coordinación con el Encargado de seguridad de información. El Encargado de seguridad de información, deberá realizar pruebas o diagnósticos de seguridad de los sistemas de información de la compañía.
- c. Toda prueba de las aplicaciones o de los sistemas de información, se deberá realizar teniendo en cuenta las medidas de protección de los archivos que se encuentren en dicho momento en producción.

3. Mantenimiento de infraestructura

- a. El mantenimiento de la infraestructura de Tecnología de la Información es de exclusiva responsabilidad del Responsable de Soporte TI de “Vale un Perú”.
- b. El cambio de archivos de sistema no está permitido, sin una justificación aceptable y verificable por el Responsable de Soporte TI y el Encargado de seguridad de información.
- c. Es responsabilidad del Responsable de Soporte TI el llevar un registro formal del mantenimiento efectuado sobre la infraestructura de Tecnología de la Información y de los cambios realizados desde su instalación.

4. Gestión interna de respaldo y recuperación

- a. “Vale un Perú” deberá establecer procedimientos rutinarios para el respaldo de la información de acuerdo con la criticidad de esta, realizando copias de seguridad y pruebas de recuperación.
- b. La Jefatura de Soporte TI tiene establecido procedimientos para el respaldo de la información de los equipos críticos (servidores) de acuerdo con la criticidad de la misma realizando copias de seguridad, llevando un registro de los mismos. Asimismo, mantiene un registro de los fallos reportados en el proceso de respaldo y recuperación de la información, así como un registro de las medidas correctivas efectuadas.
- c. Las copias lógicas de respaldo son custodiadas en un lugar seguro, el cual cuenta con las condiciones ambientales adecuadas.

- d. El Encargado de seguridad de información debe revisar de manera semestral o cuando lo considere conveniente, el cumplimiento del procedimiento “Respaldo de Datos”.

5. Evaluación de tráfico de red

- a. El Responsable de Soporte TI en coordinación con el Encargado de seguridad de información, realiza mensualmente la revisión de tráfico de la banda ancha mediante reportes provistos por los proveedores de Internet.
- b. El Responsable de Soporte TI, en coordinación con el Encargado de seguridad de información, genera trimestralmente el reporte antimalware con la herramienta Antivirus de la compañía, con la finalidad de monitorear la seguridad de la red corporativa de “Vale un Perú”.
- c. Las Áreas de Soporte TI y Seguridad de la Información, son las únicas autorizadas, para monitorear la red, al menos una vez al año, con cualquiera de los métodos existentes con la finalidad de resolver problemas de servicio, como parte de las operaciones rutinarias de la red, para diagnóstico, mantenimiento o para resolver problemas de seguridad. La información recopilada será clasificada como altamente confidencial.
- d. El tráfico de red es monitoreado, mensualmente, por el personal de Soporte TI y Seguridad de la Información con la finalidad de optimizar la utilización del ancho de banda, eliminar y bloquear virus informáticos y observar el funcionamiento general de la red. Este monitoreo permite visualizar los recursos de red utilizados por las distintas aplicaciones, ya sea en forma general o para un dispositivo de red específico.
- e. El cifrado para la información sensible que transita en la red de “Vale un Perú” y los servicios que se encuentran publicados en Internet, se realiza mediante el certificado SSL (archivo de datos que vincula digitalmente una clave de encriptación con los datos de la empresa) para proteger los datos recogidos y enviados.
- f. El uso de sniffers (software que permite analizar el tráfico de la red) o dispositivos que operan en modo promiscuo está prohibido, salvo requerimiento de Soporte TI o Seguridad de la Información.
- g. Está prohibido obtener o intentar obtener información a través de cualquiera de sus formas, de los dispositivos conectados a la red de “Vale un Perú”, a menos que se trate del responsable de Soporte TI.

- h. El área de Soporte TI y Seguridad de la Información tienen la autoridad para cancelar el servicio a cualquier subred o dispositivo de red que viole estas políticas o que afecte el desempeño de la red de “Vale un Perú” hasta que se aclare el incidente con el Comité de Seguridad de la Información.

6. Política de Firewall

- El equipo de firewall de “Vale un Perú”, es un elemento importante de la seguridad de la red del recinto. El equipo de firewall restringe el acceso de la compañía, en formas específicas y permite analizar el tráfico en formas concretas. Combinado con otros controles de seguridad complementarios, el Firewall puede proteger los activos y la información de “Vale un Perú”, contra algunas amenazas que se relacionan con las conexiones a Internet. Este equipo mejora las habilidades de “Vale un Perú” para detectar y responder a situaciones de seguridad que puedan ocurrir.
- Se realizará una evaluación de vulnerabilidades al servidor anualmente (Seguridad de la Información). El personal de Soporte TI cooperará con el personal designado para completar cualquier acción necesaria especificada por el área de Seguridad de la Información.
- Se evaluará todo cambio de alto impacto sobre las reglas de Firewall entre el personal de Soporte TI y el área de Seguridad de la Información.
- Se evaluará cualquier situación o incidente de seguridad que envuelva al sistema entre el personal de Soporte TI y el área de Seguridad de la Información.
- Se realizarán auditorías al sistema de administración para verificar que esté funcionando correctamente y que no representa riesgo para la red (Seguridad de Información).
- Es responsabilidad de Soporte TI de responder con celeridad cualquier situación que pueda poner en riesgo al sistema y la red de “Vale un Perú”.
- Se mantendrá actualizado el inventario de actualizaciones y parches de seguridad de los firewalls (Soporte TI).

4. INCUMPLIMIENTO

- a. El incumplimiento de esta política puede generar la materialización de riesgos de accesos y/o modificaciones no autorizadas, pérdida, fuga y uso no adecuado de la información considerada como altamente confidencial, así como problemas de disponibilidad de información en “Vale un Perú”.

- b. El incumplimiento de la presente política, dependiendo del tipo y la gravedad de la infracción podrá seguir las medidas correspondientes en el Artículo 29 del Reglamento Interno de Trabajo de “Vale un Perú”.

POLÍTICA DE ADQUISICIÓN, DESARROLLO, INSTALACIÓN Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN Y APLICATIVOS

1. OBJETIVO

La política de adquisición, desarrollo, instalación y mantenimiento de los sistemas de información y aplicativos de “Vale un Perú” tiene por objetivo establecer los lineamientos para una adecuada gestión de la seguridad de la información durante todo el ciclo de vida de desarrollo de software. Cabe resaltar que esta política fue desarrollada de acuerdo con lo contemplado en la 27001:2014 y en la Circular N° G- 140 - 2009 “Gestión de la seguridad de la información”.

2. ALCANCE

Esta política es de cumplimiento de todos los colaboradores de “Vale un Perú” y de todas aquellas personas que mantienen un vínculo laboral con la empresa de manera temporal o permanente y bajo todas las modalidades de contrato.

3. DESCRIPCIÓN

Todo desarrollo y mantenimiento de sistemas de la Cooperativa, deberá seguir la metodología definida por la Jefatura de Desarrollo, la cual contempla las siguientes etapas según sea el caso:

- ✓ Análisis
- ✓ Diseño
- ✓ Programación
- ✓ Certificación
- ✓ Documentación
- ✓ Capacitación
- ✓ Implementación

En el desarrollo de sistemas se empleará los lenguajes de programación establecidos o estándares definidos por Soporte TI, a fin de reducir el tiempo requerido para su desarrollo y facilitar el mantenimiento de estos.

3.1. Gestión de Proyectos de Desarrollo de Sistemas de Información y/o Aplicativos

- a. Todos los proyectos de desarrollo, realizados de manera interna o por un tercero, deben utilizar la metodología de Gestión de Proyectos de TI y las herramientas de desarrollo formalmente aceptadas por el Responsable de Soporte TI de “Vale un Perú”.

- b. Adicionalmente toda solicitud de desarrollo, realizada de manera interna o por un tercero, debe contar con los requerimientos de Seguridad de la Información. Con este fin, el Encargado de seguridad de información de “Vale un Perú” firma la especificación funcional (aprobación), la cual incluye los requerimientos funcionales, técnicos y administrativos de seguridad. Asimismo, es responsable de validar el cumplimiento de dichos requerimientos en la fase de certificación. Los cambios a los sistemas de información y/o aplicativos de “Vale un Perú” que sean considerados como proyectos deben ser solicitados de manera formal. Los proyectos, deben tener la aprobación de las siguientes personas dependiendo la naturaleza de la necesidad:
- ✓ Propietario³ del Sistema y/o aplicativo.
 - ✓ Responsable de Soporte TI
 - ✓ Gerente General
 - ✓ Responsable de Seguridad de Información
- c. Para todos los desarrollos de Sistemas de Información, los Analistas y Programadores deben considerar la Seguridad de la Información, durante toda la fase de desarrollo (desde el principio del proceso de análisis y diseño de los sistemas, hasta su pase a producción).
- d. Todo desarrollo de sistemas o mantenimiento será documentado de acuerdo con la metodología de gestión de proyectos de TI estipulada en el Manual de Tecnología de la Información, para facilidad de personas no familiarizadas con dichos sistemas.

3.2. Requisitos de Seguridad en los sistemas y/o aplicativos

- a. Los requisitos de seguridad deben ser identificados durante el desarrollo, adquisición y/o mantenimiento de los sistemas y/o aplicativos de la Cooperativa, los cuales deben incluir como mínimo las siguientes medidas de control:
- ✓ Requisitos de gestión de accesos (usuarios / contraseñas / entre otros).
 - ✓ Requisitos de perfiles y privilegios.
 - ✓ Requisitos de mantenimiento de usuarios y perfiles.
 - ✓ Requisitos de pistas de auditoría.

³ El rol de propietario de sistema de información es asignado a cada gerente involucrado.

- ✓ Requisitos de consistencia e integridad (valores fuera de rango, caracteres inválidos, datos incompletos, entre otros).
- b. Todo desarrollo de proyectos debe cumplir con la matriz de requerimientos de seguridad de la información para proyectos. Dependiendo de la validación, definición o especificación dentro del documento funcional.

3.3. Procesamiento correcto en las aplicaciones

- a. Como parte de las pruebas en las fases de desarrollo y certificación se debe considerar las siguientes validaciones:
 - ✓ Validación de datos de entrada: valores fuera de rango, caracteres inválidos, datos incompletos, datos que exceden los límites permitidos.
 - ✓ Control de proceso interno: comprobaciones del correcto funcionamiento del proceso (validación de datos generados por el sistema, tiempos de respuesta, funciones para cambio de datos, alertas de procesamiento.
 - ✓ Validación de datos de salida: datos exactos, completos y precisos.

3.4. Controles Criptográficos

- a. Los Colaboradores no deben implementar controles criptográficos sin que éstos hayan sido previamente evaluados por el Soporte e Infraestructura TI y el Encargado de seguridad de información y aprobados por el Comité de Seguridad de la Información.
- b. La información clasificada como Altamente Confidencial debe ser protegida por controles criptográficos que aseguren la confidencialidad de esta, tanto durante su transmisión como su almacenamiento.
- c. Los sistemas de información de “Vale un Perú” que procesen tanto información categorizada como altamente confidencial deberán ser identificados por el propietario de información y notificados al responsable de seguridad de información de tal manera que se evalúe qué controles criptográficos necesitan ser implementados para mejorar la seguridad de la información que procesan. (Los controles criptográficos a nivel de sistemas de información se pueden dividir en tres: A nivel de Infraestructura de soporte del aplicativo, a nivel del procesamiento en base de datos y/o a nivel de aplicación).

- d. Los Propietarios de los activos deberán velar por la implementación de controles criptográficos para la información altamente confidencial que esté dentro de su ámbito de responsabilidad.
- e. Antes de implementar un control criptográfico, se deben desarrollar los procedimientos y controles necesarios para evitar la pérdida de la información encriptada ante una posible pérdida la clave de encriptación.
- f. El uso de controles criptográficos dependerá del requerimiento de protección que sea requerido por el Propietario de Información o entes externos reguladores, el cual debe ser evaluado por el Encargado de seguridad de información y el Responsable de Soporte TI para validar el requerimiento o proponer medidas mitigantes de control en caso no sea justificable el mismo, considerado el nivel de complejidad asociado a la implementación de este tipo de control.

3.5. Desarrollo por Personal Externo

- a. El encargado de seguridad de información debe verificar que los acuerdos suscritos con Terceros contemplen cláusulas de confidencialidad con el personal involucrado en el desarrollo que permite asegurar la confidencialidad de la información de la Cooperativa. Asimismo, se debe considerar lo siguiente:
 - ✓ Acuerdos de niveles de servicio (SLAs).
 - ✓ Procedimientos de auditoría.
 - ✓ Cumplimiento con Los documentos internos de seguridad.
 - ✓ Requerimientos de pruebas y validación.
 - ✓ Acuerdos de confidencialidad
 - ✓ Acuerdos de conocimiento y cumplimiento de normas, leyes y estándares relacionados con la seguridad de la información. P.E. Ley de protección de datos personales, Payment Card Industry Data Standard (PCI-DSS).
- b. El Responsable de Soporte TI debe participar en el proceso de desarrollo de software, asegurándose que el producto satisface los requisitos de seguridad mínimos según metodología.
- c. El Personal Externo deberá tener en consideración que, según lo indicado en el acuerdo de confidencialidad, está estrictamente prohibido divulgar o revelar información de carácter altamente confidencial de “Vale un Perú”.

- d. Los sistemas y/o software provistos por entidades externas deberán ser revisados antes de efectuar su pase a producción y deberán contar con la autorización de los Propietarios de los sistemas y el Encargado de seguridad de información previo al pase a producción.

3.6. Adquisición de sistemas de información y/o aplicativos

- a. El Responsable de Soporte TI y los Propietarios del(los) sistema(s) de información de “Vale un Perú”, son los responsables de la definición de los requerimientos técnicos y funcionales respectivamente para todo requerimiento de adquisición de sistemas de información y/o aplicativos con la validación del Encargado de seguridad de información.
- b. La Jefatura de Desarrollo será responsable de:
 - ✓ Propiciar la adquisición de licencias individuales y licencias concurrentes.
 - ✓ Promover la adquisición y asesoramiento en sistemas de información y/o aplicativos de vanguardia.
 - ✓ Garantizar que la adquisición de sistemas de información y/o aplicativos provengan de proveedores formales que cuenten con la representación Oficial de la marca de software.
 - ✓ Promover el uso de sistemas de información y/o aplicativos que mantengan la independencia de “Vale un Perú” y/o cualquiera de sus colaboradores con respecto a sus proveedores.
- c. Todo sistema de información y/o aplicativo, que se desee adquirir, deberá cumplir y respetar Los documentos internos de seguridad aprobadas por el Encargado de seguridad de información de “Vale un Perú”.

3.7. Seguridad de los archivos de sistema

- a. Las áreas Usuarias (Propietarios de activos) deberán justificar y sustentar la solicitud de desarrollo o modificación de un sistema y/o aplicación.
- b. Esta estrictamente prohibido que el Personal de Soporte TI y/o terceros subcontratados, tenga acceso a los datos del ambiente de producción, sin embargo, se les debe asignar el acceso al ambiente de desarrollo, el cual contiene la información de producción enmascarada (altamente confidencial). En casos estrictamente

necesarios y excepcionales, el Encargado de seguridad de información evaluará el requerimiento de acceso.

- c. Este estrictamente prohibido que el Personal de certificación cuente con acceso a los datos del ambiente de producción, sin embargo, se les debe asignar el acceso al ambiente de certificación, el cual contiene la información de producción enmascarada (altamente confidencial).
- d. Es responsabilidad del Administrador de base de datos (DBA) que el proceso enmascaramiento se ejecute inmediatamente después de la restauración de la base de datos. Luego de finalizado este proceso, se deberá habilitar el acceso a la base de datos para los ambientes de desarrollo y certificación.
- e. El Responsable de Base de Datos debe informar al Encargado de seguridad de información cada vez que se realice alguna restauración o mantenimiento en las bases de datos de la Cooperativa y en caso se requiera acceso de consulta a las bases de datos de “Vale un Perú”.
- f. En “Vale un Perú”, se respetan los derechos de autor, por lo tanto, todos los sistemas de información y/o aplicativos que se utilicen deben ser de origen legal y contar con la licencia vigente respectiva.

3.8. Instalación de sistemas de información y/o aplicativos

- a. La instalación de sistemas de información y/o aplicativos es única y exclusiva responsabilidad del Responsable Soporte TI de “Vale un Perú” con el apoyo de su área.
- b. Está prohibido la instalación de sistemas de información y/o aplicativos que, desde el punto de vista del Encargado de seguridad de información, el Responsable de Soporte TI, pudiera poner en riesgo los recursos y/o activos de “Vale un Perú”. Toda instalación de sistemas de información y/o aplicativos, deberá contar con la aprobación formal y/o visto bueno de los propietarios de los sistemas y el Encargado de seguridad de información.
- c. Con el propósito de proteger la integridad de los servidores, equipos de telecomunicaciones y dispositivos móviles que soportan los sistemas de información de “Vale un Perú”, es imprescindible que todos y cada uno de los equipos de “Vale un Perú”, dispongan de aplicativos de seguridad (antivirus, firewalls, privilegios de

acceso, y otros que apliquen) según lo estipulado en la “Política de Protección ante Virus Informáticos y Código Malicioso”.

3.9. Actualización de los sistemas de información y/o aplicativos

- a. Corresponde al Responsable de Soporte de “Vale un Perú”, autorizar cualquier adquisición y actualización de los sistemas de información.
- b. La actualización de los sistemas de información y/o aplicativos es responsabilidad del Responsable de Soporte TI (coordinación con certificación, Redes y Servidores, y aprobación del usuario solicitante o propietario del sistema). Queda prohibida la actualización realizada por cualquier otro empleado no designado según lo estipulado.

3.10. Pruebas a los Cambios

- a. Se deberá efectuar el plan de pruebas, las cuales deberán ser como mínimo de los siguientes tipos:
 - ✓ Pruebas funcionales unitarias.
 - ✓ Pruebas de Integración.
 - ✓ Pruebas de carga y stress.
- b. El Encargado de seguridad de información realizará las pruebas asociadas al cumplimiento de requerimientos de seguridad considerados en la fase de definición funcional.
- c. Toda prueba debe ser realizada en un ambiente de certificación controlado e independiente del ambiente de producción. Los datos empleados para la ejecución del plan de pruebas deben mantener las características de los datos originales almacenados en el ambiente de producción. Para mayor detalle referente a las fases de las pruebas se debe revisar el Manual del TI.

3.11. Pase a Producción

- a. El Responsable de Soporte TI es responsable de los cambios realizados al pase al ambiente de Producción, para ello se deberá contar con un inventario y/o registro de todos los archivos, ya sean nuevos o modificados, que deberán ponerse en operación dentro del ambiente de Producción.
- b. Para tal efecto deberá indicar expresamente:

- ✓ La ruta lógica en el servidor de desarrollo de donde se obtendrán los archivos a migrar al ambiente de Producción.
 - ✓ Número de la versión aprobada por el propietario del sistema, como resultado de las pruebas realizadas en el ambiente de calidad.
 - ✓ Resultado de la ejecución del plan de pruebas.
 - ✓ Instructivo operativo/técnico de instalación.
 - ✓ En caso sea necesario, el resultado del análisis de impacto, se entregará el resultado de la revisión del Encargado de seguridad de información.
- c. Todo pase a producción de un requerimiento, deberá contar con la aprobación formal previa del propietario del sistema, Responsable de Soporte TI y el Encargado de seguridad de información.
 - d. Se deberá mantener un registro formal y actualizado de todos los cambios solicitados y efectuados a los sistemas de información y/o aplicativos de “Vale un Perú”.
 - e. El Encargado de seguridad de información deberá efectuar revisiones periódicas de los sistemas en el ambiente de producción a fin de asegurar que sólo se hayan efectuado los cambios autorizados.

3.12. Control de acceso al código fuente de los sistemas y/o aplicativos

- a. Es responsabilidad del Responsable de Soporte TI mantener en ambientes separados, las fuentes de los sistemas y los archivos ejecutables de producción.
- b. El acceso a las fuentes de los sistemas de información de “Vale un Perú”, está limitado exclusivamente al personal del área de Soporte TI. Queda terminantemente prohibido que personal ajeno a esta definición tenga acceso libre a este ambiente.
- c. Todo acceso a los programas fuentes será controlado por la Responsable de Soporte TI para evitar accesos y/o cambios no autorizados en los sistemas de la Cooperativa. Así como tener el registro de los cambios efectuados.

3.13. Derechos de propiedad

- a. Todo sistema de información y/o aplicativo adquirido por “Vale un Perú”, sea por compra, donación o cesión es propiedad de la Cooperativa y mantendrá los derechos que la ley de propiedad intelectual le confiera.

- b. Soporte TI deberá tener un registro actualizado de todos los sistemas de información y/o aplicativos propiedad de “Vale un Perú”. Además, se validado por el Encargado de seguridad de información.

4. INCUMPLIMIENTO

- a. El incumplimiento de esta política puede generar la materialización de riesgos de accesos y/o modificaciones no autorizadas, pérdida, fuga y uso no adecuado de la información considerada como altamente confidencial en “Vale un Perú”.
- b. El incumplimiento de la presente política, dependiendo del tipo y la gravedad de la infracción podrá seguir las medidas correspondientes en el Artículo 29 del Reglamento Interno de Trabajo de “Vale un Perú”.

POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

1. OBJETIVO

La política de clasificación de la información tiene por objetivo establecer los lineamientos requeridos para la clasificación de la información de “Vale un Perú” teniendo en cuenta para ello, la criticidad y sensibilidad de esta, para las operaciones de “Vale un Perú”. Cabe resaltar que esta política ha sido desarrollada de acuerdo con lo establecido en la ISO/IEC ISO/IEC 2700 y en la Circular de la SBS N° G- 140 -2009 “Gestión de la seguridad de la información”.

2. ALCANCE

Esta política es de cumplimiento de todos los colaboradores de “Vale un Perú” de Lima y Provincias y de todas aquellas personas que mantienen un vínculo laboral con la empresa de manera temporal o permanente y bajo todas las modalidades de contrato.

3. DESCRIPCIÓN

3.1. Responsabilidades para con la información

- a. Todo activo de información que utilice un proceso y/o área de “Vale un Perú” debe tener un propietario asignado.
- b. Los propietarios del(los) activo(s) de información son los responsables de asignar la clasificación apropiada, según la sensibilidad de la información, tal y como se define en la presente política. Deben tomar decisiones sobre quiénes van a tener acceso a la información, y el uso que se le dará. También deben coordinar con el área de Seguridad de la Información de “Vale un Perú”, las medidas necesarias para asegurar que se utilice el control apropiado en el almacenamiento, manejo, distribución y usos normales de esta información.
- c. El área de Seguridad de la Información tiene la potestad de recomendar y asesorar a los propietarios del(los) activo(s) de información respecto a la clasificación, acceso y uso adecuado de ésta.

3.2. Etiquetado

- a. La clasificación de la información se encuentra especificada en la Política de Inventario de Activos.
- b. Toda copia impresa, manuscrita u otra manifestación de información Altamente confidencial, debe portar evidencia clara de la etiqueta “Altamente confidencial” en la parte superior derecha de cada página. En caso estuviera encuadernado, deberá

tener una etiqueta apropiada de “Altamente confidencial” en la carátula, en la página del título y en la contra caratula.

- c. Todo USB, Disco Externo, CD-ROM, DVD o cualquier otro medio magnético de almacenamiento, que contenga información “Altamente Confidencial”, debe ser etiquetado externamente con su clasificación apropiada.
- d. La información clasificada como “Altamente Confidencial”, se debe etiquetar de manera apropiada desde el momento en que se crea hasta su eliminación o cambio de clasificación.
- e. Los colaboradores de “Vale un Perú”, no deberán quitar o cambiar las etiquetas de clasificación de datos a la información, a menos que se obtenga el permiso previo del propietario² de la información y del Encargado de seguridad de información de “Vale un Perú”.
- f. Toda agrupación, y/o recolección de información debe etiquetarse con la clasificación más crítica de la información agrupada. Para tal efecto, si se crea un reporte y/o base de datos, y la misma contiene información sólo para “Pública”, “Interna”, “Confidencial” y “Altamente Confidencial”, todo el reporte y/o base de datos debe clasificarse y etiquetarse como “Altamente confidencial”.
- g. Toda información sin etiqueta cae dentro de la clasificación predeterminada como “Información Interna”.

3.3. Otras etiquetas

- a. Se permiten otras etiquetas en la clasificación de datos específicos para las áreas y/o gerencia de “Vale un Perú”, pero éstas deben ser consistentes, con el sistema de clasificación de la información definida en esta política. Estas etiquetas adicionales, pueden incluir el uso de palabras como "Privado" o "Financiero.”

3.4. Distribución de la información

- a. Los propietarios del(los) activo(s) de información “Altamente Confidencial” deben asegurarse de que las copias impresas, lógicas y/o medios magnéticos se encuentren adecuadamente etiquetados, con su clasificación de “Altamente Confidencial” antes de proceder a su distribución.
- b. Los colaboradores de “Vale un Perú” tienen prohibida la distribución de la información “Altamente Confidencial”, en cualquiera de los medios impresos,

lógicos y/o magnéticos, en los que esta pueda encontrarse, sin el conocimiento y autorización del propietario de la información.

3.5. Desclasificación de la información

- a. Si se conoce la fecha de vencimiento de la información “Altamente Confidencial”, ésta debe señalarse de manera clara, en todos los medios en que esta información se manifieste.
- b. Los colaboradores que poseen información “Altamente Confidencial”, nominada para desclasificación en una fecha ya vencida, deben comunicar de manera formal, al propietario de la información para su desclasificación definitiva.
- c. El propietario de la información puede desclasificar en cualquier momento la clasificación actual de la información antes de la fecha de desclasificación. En este sentido el propietario de la información debe cambiar la etiqueta de clasificación que aparece en el documento original y notificar al Encargado de seguridad de información de “Vale un Perú” y a todos los destinatarios y/o usuarios actuales de la información desclasificada.
- d. Por lo menos una vez al año, los propietarios del(los) activo(s) de información deben revisar la confidencialidad asignada a la información de “Vale un Perú” que le ha sido confiada, con el fin de determinar si la información puede o no ser desclasificada.

3.6. Eliminación de la información

- a. Toda información “Altamente Confidencial” de “Vale un Perú”, debe eliminarse de manera segura, cuando ésta ya no sea necesaria para efectos del negocio. Para tal efecto, los propietarios del(los) activo(s) de información, deben revisar el valor y utilidad de la información periódicamente.
- b. Toda información “Altamente Confidencial”, que no vaya a usarse nuevamente debe ser colocada en cajas lacradas hasta el momento que sea trasladada para su disposición por personal de “Vale un Perú” o por una empresa externa contratada para tal fin.
- c. La eliminación de información Altamente Confidencial impresa en papel debe realizarse a través del uso de máquinas trituradoras u otro mecanismo de similar efectividad.

- d. Los colaboradores de “Vale un Perú” no deben eliminar información, ni archivos potencialmente importantes para la empresa, sin autorización previa del propietario de la información.
- e. Los discos duros interno y otros medios magnéticos, no pueden ser donados, desechados, como tampoco reutilizados, antes de ser sometidos a un proceso de eliminación de información según lo indicado en el Procedimiento de Eliminación de Medios de Información del Manual de Procedimientos del SGSI.

3.7. Extravío y/o divulgación de la información

- a. En caso de que la información “Altamente Confidencial” se perdiera y/o se divulgara a partes no autorizadas, se debe notificar tanto al propietario de la información como al Encargado de seguridad de información de “Vale un Perú”.

4. INCUMPLIMIENTO

- a. El cumplimiento de esta política involucra a todo el personal y terceros que tengan acceso a la información y recursos informáticos de la compañía. Esto puede afectar la confidencialidad, integridad y disponibilidad de la información de “Vale un Perú”
- b. El incumplimiento de la presente política representa una falta, la cual puede seguir las medidas correspondientes en el Artículo 29 del Reglamento Interno de Trabajo de “Vale un Perú”.

POLÍTICA DE CONTROL DE ACCESO FÍSICO Y SEGURIDAD FÍSICA

1. OBJETIVO

La Política de Control de Acceso Físico y Seguridad Física de “Vale un Perú” tiene por objetivo evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización, evitar pérdidas, daños, robo o puesta en peligro de los activos de información y la interrupción de las actividades de la organización. Esta política fue desarrollada de acuerdo a lo contemplado en la ISO/IEC 27001:2014y en la Circular N° G- 140 -2009 “Gestión de la seguridad de la información”.

2. ALCANCE

La presente política considera a áreas sensibles que abarcan a los medios de procesamiento de información, clasificada como altamente confidenciall en “Vale un Perú”. Asimismo, es de estricto cumplimiento de todos los colaboradores y terceros que mantienen un vínculo laboral con la empresa, de manera temporal o permanente, bajo todas las modalidades de contrato.

3. DESCRIPCIÓN

3.1. Áreas Sensibles

- a. Las áreas sensibles de “Vale un Perú” son aquellas oficinas y/o áreas en las cuales se procesa, almacena y/o accede a información catalogada como altamente confidencial. En este sentido, las áreas sensibles son:

CENTRO DE DATOS (LINCE)

- ✓ Cuarto de monitoreo (Al lado de Cobranzas)
- ✓ Zonas de acceso al local (Cochera)

- b. Los propietarios del(los) activo(s) de información con el apoyo del área de Seguridad de la Información deben identificar las áreas sensibles dentro de la empresa para protegerlas de manera eficiente y oportuna.
- c. El Encargado de seguridad de información de “Vale un Perú” deberá validar y aprobar la relación de áreas sensibles de la empresa. El Encargado de seguridad de información debe monitorear la implementación de controles de acceso apropiados para las áreas sensibles.

Categoría	Nivel de Criticidad	Áreas	Medidas de control
Nivel 1	Muy alta	<ul style="list-style-type: none"> Centros de Datos 	<ul style="list-style-type: none"> Mecanismos de control de acceso físico (lectores de acceso, vidrio blindado). (FALTA) Mecanismos de control ambientales (detectores de humo, extintores). (FALTA) Bitácoras de ingreso y salida de personas. (FALTA) Monitoreo externo e interno (cámaras de seguridad). (FALTA)
Nivel 3	Medio	Zonas de acceso al edificio	<ul style="list-style-type: none"> Barreras perimétricas (naturales o físicas). Bitácoras de ingreso y salida de personas. Monitoreo externo e interno (cámaras de seguridad). (FALTA)

3.1.1. Perímetro de seguridad física

- Los perímetros de seguridad se utilizan para proteger las áreas que contienen información y medios de procesamiento de información, estos son controlados y restringidos únicamente a personas autorizadas.
- El perímetro de las áreas sensibles está delimitado por elementos de protección, tales como: Puertas, Cerraduras (mecánicas), Bitácoras de ingreso y salida de personas (en caso sea necesario), Vidrio blindado, Personal de seguridad.

3.1.2. Controles físicos de entrada

- a. El acceso a las áreas donde se procesa o almacena información sensible de “Vale un Perú” debe protegerse mediante controles de ingreso apropiados para asegurar que solo se le permita el acceso al personal autorizado. El Responsable de Soporte TI es responsable del control de acceso a la Sala de Servidores y Centro de Datos. El área de administración es responsable de las zonas de acceso al edificio a las oficinas de Pardo y Aliaga, Orquídeas y Andrés Reyes.
- b. El acceso a las áreas sensibles debe estar delimitado por elementos de protección, tales como:
 - ✓ Bitácora de accesos: Se registra fecha y hora de entrada, salida de los visitantes, estos debieran ser supervisados a no ser que su acceso haya sido previamente aprobado; solo se les deberá permitir el acceso para propósitos específicos y autorizados.
 - ✓ Identificación visible: Se requiere que todos los colaboradores, contratistas y terceros utilicen alguna forma de identificación visible.
 - ✓ Monitoreo interno: Los accesos a las áreas seguras o los medios de procesamiento de información confidencial deber ser restringida a los terceros, solo cuando sea estrictamente necesario este acceso será autorizado por la Gerente General, en coordinación con el Encargado de seguridad de información. Este acceso debe ser monitoreado.
- c. Todo colaborador de “Vale un Perú”, deberá contar con Fotocheck de identificación (intransferible y deberá colocarlo en un lugar visible durante toda su jornada laboral).
- d. En caso de extravío y/o robo del fotocheck personal, se deberá notificar al área de administración a fin de tomar las acciones pertinentes.
- e. El área de Administración deberá velar por el correcto registro y declaración de equipos de cómputo, equipos informáticos y/o electrónicos de los colaboradores al momento del ingreso y salida de las instalaciones de “Vale un Perú”.
- f. En el caso de un cese de un colaborador que maneje información altamente confidencial, el jefe inmediato deberá notificar a las áreas de Soporte TI, Recursos Humanos, Administración y Seguridad de la Información esta decisión a fin de retirarle los accesos físicos correspondientes en el momento.

3.1.3. Protección contra amenazas externas e internas

- a. Con el propósito de evitar daños o pérdidas que afecten la seguridad de los activos de información de “Vale un Perú”, se tiene implementado controles para evitar el daño por fuego, inundaciones, explosión y otras formas de desastres naturales o causados por el hombre:
 - ✓ Se debe evitar el almacenamiento de los suministros a granel como papelería en las áreas seguras.
 - ✓ Los medios de respaldo de información deben ubicarse a una distancia segura para evitar el daño colateral.
 - ✓ Controles de Amenaza contra incendios (extintores).
- b. Se deben establecer las condiciones ambientales básicas de temperatura, higiene, aislamiento eléctrico y sonoro, y otras medidas similares de acuerdo con los requerimientos específicos de los equipos de cómputo. Se deben instalar sistemas automáticos de detección y respuesta automática ante condiciones ambientales que afecten el correcto funcionamiento de los equipos. Cuando no se pueda disponer de un sistema de extinción automática de incendios, deben contarse con extintores manuales revisados y vigentes.
- c. El centro de procesamiento de datos (centro de datos) debe contar con mecanismos de control de acceso físico tales como:
 - ✓ Controles de Amenaza contra incendios (extintores)
 - ✓ Controles de Aire Acondicionado (sistema de aire acondicionado)
 - ✓ Controles de Sistema Eléctrico (banco de baterías)
 - ✓ Controles de Seguridad Física (cerradura)
- d. No se deben ingerir alimentos o bebidas, así como colocar o manipular líquidos cerca de los equipos o dispositivos de procesamiento de información en el centro de datos.

3.1.4 Trabajo en áreas sensibles

- a. El acceso de terceras personas a áreas sensibles debe ser autorizado, supervisado y solo cuando sea requerido.
- b. No se permite el trabajo no supervisado, de igual manera, no se permite las grabaciones ni fotografías (equipo fotográfico, video, audio y cámaras) en las áreas sensibles.
- c. El Encargado de seguridad de información debe revisar de manera anual o cuando lo considere conveniente, el cumplimiento del procedimiento relacionado al acceso físico a áreas sensibles de “Vale un Perú”.

3.1.4. Áreas de acceso público

- a. Toda persona ajena a “Vale un Perú” deberá anunciarse formalmente ante el área de recepción del edificio e indicar el propósito de su visita.
- b. Los visitantes y/o personal externo deberán entregar un documento de identidad válido y deberán contar con una autorización formal, previa al ingreso a las instalaciones de “Vale un Perú”.
- c. Todo colaborador, visitante y/o personal externo deberán declarar al personal de Seguridad, al momento de ingreso a las instalaciones, oficinas y/o ambientes de “Vale un Perú”, cualquier equipo de cómputo u otro equipo informático con el que vayan a ingresar.
- d. El desplazamiento de visitante y/o personal externo dentro de las instalaciones debe ser restringido sólo a las áreas que están involucradas en su visita, el responsable del área visitada deberá monitorear permanentemente su actividad. En caso un colaborador identifique una persona desconocida sin pase de visitante deberá comunicar inmediatamente al personal de Seguridad.
- e. Los visitantes y/o personal externo deberán mantener el pase de visitante de manera visible durante el ingreso y desplazamiento a las oficinas y/o ambientes autorizados de “Vale un Perú”, bajo ningún motivo, prestar y/o intercambiar el pase de visitante proporcionado por “Vale un Perú”.
- f. Los visitantes y/o personal externo deberán devolver el pase de visitante proporcionado, al término de sus actividades en las oficinas y/o ambientes de “Vale un Perú”.
- g. En caso de extravío y/o robo del pase de visitante, se deberá notificar al personal de seguridad de “Vale un Perú”.
- h. En caso de que algún proveedor posea un objeto extraño a su salida, este deberá ser revisado y registrado por personal de seguridad.

3.1.5. Monitoreo interno

- a. Todas las áreas sensibles que contengan información altamente confidencial deberán contar con cerradura y vigilancia constante por parte del propietario y/o Responsable de Soporte TI.

3.2. Equipos de seguridad

3.2.1. Ubicación y protección del equipo

- a. Todo ingreso de visitantes y/o personal externo a áreas sensibles de “Vale un Perú”, deberá ser autorizado por el Responsable área visitada. Adicionalmente, se deberá llevar una bitácora de ingreso a dichas áreas sensibles en la cual deberá indicarse de manera expresa: nombre del visitante y/o personal externo, motivo de ingreso, fecha y hora de ingreso y nombre del propietario de la información que autorizó el mencionado ingreso para las áreas sensibles.
- b. Todos los computadores portátiles de “Vale un Perú” deberán asegurarse a los escritorios de los usuarios con dispositivos y/o mecanismos de seguridad proporcionados por el área de Administración.
- c. Los equipos de cómputo u otro equipo informático, así como los equipos que pertenecen a los colaboradores y que hayan sido traídos a las oficinas de “Vale un Perú” por visitantes y/o personal externo, no deben salir de las mismas a menos que estén acompañados de una autorización firmada por el gerente del área y/o por el personal responsable designado por el mismo para tales efectos.
- d. Para las conexiones a la red de datos de “Vale un Perú”, se deberá tener en consideración lo indicado en la “Política de Control de Acceso y Seguridad Lógica”.

3.2.2. Servicios públicos de soporte

- a. Todos los servidores, computadores personales, equipos de comunicación y otros equipos de las oficinas de “Vale un Perú”, deben usar controles que regulen el voltaje. Para tales efectos, se emplearán pozos a tierra, líneas exclusivas y/o equipos de estabilización eléctrica.
- b. Los servidores de producción deben, además, poseer sistemas de energía ininterrumpida, autorizados por el Comité de Seguridad de la Información de “Vale un Perú”.

3.2.3. Seguridad del cableado

- a. El acceso a los ambientes de equipos de comunicaciones y cableado deberá estar permitido sólo al personal autorizado por el Responsable de Seguridad.

- b. El cableado deberá estar ubicado y protegido físicamente con gabinetes cerrados. Las llaves de los mencionados gabinetes deberán estar bajo custodia del Responsable de Soporte TI o por el personal designado por el mismo, para tales efectos.

3.2.4. Mantenimiento de equipo en áreas sensibles

- a. El acceso a la sala de servidores, a los ambientes de equipos de comunicaciones y cableado, deberá estar permitido sólo al personal autorizado por el Responsable de Soporte TI de “Vale un Perú”.
- b. Todo ingreso y egreso a la sala de servidores, deberá ser registrado de manera formal en una bitácora de ingreso.
- c. Los servidores, equipos de comunicaciones y el cableado deberán estar ubicados y protegidos físicamente con gabinetes cerrados.

3.2.5. Seguridad de la eliminación o reutilización del equipo

- a. Previo a la eliminación (destrucción física) de equipos que almacenen información altamente confidencial de “Vale un Perú”, se debe destruir, borrar o sobrescribir la información utilizando técnicas que no hagan posible la recuperación de la información original.

3.2.6. Autorización para trasladar equipos de cómputo

- a. Los equipos de cómputo u otro equipo informático, así como los equipos que pertenecen a los colaboradores y que hayan sido traídos a las oficinas de “Vale un Perú” por visitantes y/o personal externo, no deben salir de las mismas a menos que estén acompañados de una autorización firmada por el responsable del área y/o por el personal responsable designado por el mismo para tales efectos.

4. INCUMPLIMIENTO

- a. El incumplimiento de esta política puede generar la materialización de riesgos tales como robo o pérdida de activos, fuga de información, acceso no autorizado, entre otros; pudiendo afectar la confidencialidad, integridad y disponibilidad de la información de “Vale un Perú”.

- b. El incumplimiento de la presente política representa una falta, la cual puede seguir las medidas correspondientes en el Artículo 29 del Reglamento Interno de Trabajo de “Vale un Perú”.

POLÍTICA DE CUMPLIMIENTO

1. OBJETIVO

La Política de Cumplimiento de “Vale un Perú” (en adelante, la Política) tiene por objetivo asegurar el cumplimiento de las disposiciones contenidas en normas, políticas, contratos o requerimientos legales, así como los controles relacionados con la Seguridad de la Información, definidos para “Vale un Perú” (en adelante la Cooperativa). Esta política ha sido desarrollada de acuerdo con lo establecido en la Circular N° G- 140 -2009 “Gestión de la seguridad de la información” y en la ISO/IEC 27001:2014.

2. ALCANCE

La Política es de estricto cumplimiento para todas aquellas personas que mantienen un vínculo laboral con la empresa, de manera temporal o indefinida, bajo todas las modalidades de contrato.

3. DESCRIPCIÓN

3.1. Cumplimiento de las disposiciones legales

- a. El Responsable de Soporte TI, debe custodiar los documentos originales que acrediten la propiedad de la totalidad de licencias, manuales de software y recursos informáticos adquiridos por la Cooperativa. Asimismo, deberán implementar controles de licenciamiento para los softwares utilizados en la empresa a fin de garantizar el uso de productos bajo licencia y respetar el número máximo de usuarios permitidos. Finalmente, deberán registrar las actividades en los sistemas informáticos, a fin de contar con pruebas ante violaciones de Los documentos internos de seguridad cometidas internamente o por terceros.
- b. Todo contrato de proyectos de Tecnología de Información, adquisición y transferencia a terceros de software y/o recursos informáticos, deberá contar con la revisión y conformidad de la Gerencia General y el Encargado de seguridad de información. Este último debe preservar la confidencialidad, integridad y disponibilidad de la información involucrada.
- c. El área de cumplimiento normativo verifica con frecuencia el nivel de cumplimiento de las normas externas e internas de la Cooperativa en referencia a las obligaciones regulatorias vigentes. Para esto los gestores de cumplimiento normativo con el soporte de la Gerencia Legal definen y notifican el grado de cumplimiento de las normas que tienen a su cargo.

- d. La Cooperativa, frente a cualquier indicio o sospecha razonable de incumplimiento del Reglamento Interno de Trabajo, acuerdo de confidencialidad, normativa o política interna, se reserva el derecho a examinar la información almacenada en sus sistemas de información, adoptándose las medidas disciplinarias pertinentes para el personal que las incumpla.
- e. Todos los colaboradores, terceros y/o externos contratados por la Cooperativa, deberán cumplir Los documentos internos de seguridad definidas por la Cooperativa, evitando el uso de los recursos y servicios informáticos para fines no autorizados.
- f. Es responsabilidad de la Gerencia General el asegurar el cumplimiento de las políticas y los procedimientos de Seguridad de la Información que formen parte de sus funciones, garantizando la difusión de estas con el personal a su cargo.
- g. El Encargado de seguridad de información realizará revisiones anuales (de acuerdo con la programación establecida) de Los documentos internos de seguridad implementadas, evaluando su cumplimiento.

3.2. Lineamientos de Retención de Registros

- a. Entiéndase como registro, la evidencia generada por los procesos de la Cooperativa, así como por los equipos informáticos: equipos de comunicación, equipos de seguridad, aplicativos, servidores, entre otros (registros de auditoría). Por lo tanto, los registros pueden tener una presentación física como electrónica.
- b. Esta política tiene por objetivo describir los lineamientos que nos permitan administrar apropiadamente los registros de la Cooperativa, siendo de debido cumplimiento para todos los colaboradores.
- c. Cada propietario en coordinación con el Encargado de seguridad de información debe evaluar y definir cuáles son los registros que deben ser respaldados por ser de vital importancia para la operación de la empresa y el seguimiento de incidencias y auditorías.
- d. Cada propietario debe definir el tiempo de retención para los registros de sus procesos, teniendo en cuenta las restricciones de los entes reguladores o supervisores de la empresa. Entiéndase como tiempo de retención, el plazo que la empresa almacenará los registros en formato físico o electrónico en sus instalaciones o en instalaciones de terceros.

- e. Para el caso de los registros generados por los equipos informáticos: equipos de comunicación, equipos de seguridad, aplicativos, servidores, entre otros (registros o logs de auditoría) serán configurados, respaldados y custodiados por el responsable de Soporte TI.
- f. Los registros de auditoría deben ser conservados en producción por un periodo no menor a 10 años. Al igual que dichos registros transaccionales, estos deben ser guardados en medios de almacenamiento físico que permitan su posible restauración en cualquier momento.
- g. Cada propietario es responsable de validar la eliminación de registros una vez culminado el periodo de retención. Para estos se deberá programar actividades de eliminación en coordinación de las áreas de Soporte TI y Seguridad de la Información.

4. INCUMPLIMIENTO

- a. El incumplimiento de la Política puede generar la materialización de riesgos de acceso lógico a los activos de software de la Cooperativa (sistemas, carpetas compartidas, correo electrónico, servicios, entre otros) pudiendo afectar la confidencialidad, integridad y disponibilidad de la información confidencial de la empresa.
- b. El incumplimiento de la presente Política representa una falta, la misma que se encuentra regulada bajo el Artículo 29 del Reglamento Interno de Trabajo de la empresa.

POLÍTICA DE ESCRITORIOS, PANTALLAS LIMPIAS Y EQUIPOS DESATENDIDOS

1. OBJETIVO

La Política de Escritorios y Pantallas limpias de “Vale un Perú” tiene como objetivo describir los lineamientos que nos permitan proteger la información capturada, almacenada y emitida a través de impresoras, fax, fotocopiadore, escáner, equipos multifuncionales y cámaras digitales. Esta política fue desarrollada de acuerdo con lo contemplado en la ISO/IEC 27001:2014, y en la Circular N° G- 140 - 2009 “Gestión de la seguridad de la información”.

2. ALCANCE

Esta política es de estricto cumplimiento de todas aquellas personas que mantienen un vínculo laboral con la empresa, de manera temporal o permanente, bajo todas las modalidades de contrato.

3. DESCRIPCIÓN

- a. Los usuarios deben guardar los documentos y medios de almacenamiento de información (laptop sin cable de seguridad, CDs, DVDs, memorias USB, discos externos y otros) cuando no se estén utilizando. Asimismo, la información altamente confidencial debe ser guardada bajo llave (gavetas, archivadores con llave y caja fuerte) cuando no está siendo utilizada o cuando la oficina se encuentra vacía.
- b. Cuando los usuarios se retiren o suspendan sus labores, deben dejar los equipos bloqueados (Alt+Ctrl+Supr y Enter, en Windows) o cerrar su sesión de trabajo.
- c. Los usuarios deben evitar la grabación de archivos importantes en el escritorio de la computadora para evitar su divulgación, alteración o pérdida en caso de que un tercero obtenga acceso no autorizado al equipo. La información de carácter altamente confidencial debe ser almacenada y tratada en un ambiente seguro de almacenamiento (servidor de archivos o fileserver).
- d. Las estaciones de trabajo asignadas deberán ser apagadas por el usuario al término de sus labores o culminado el día de trabajo, con el fin de que otras personas no puedan acceder a su información.
- e. Las fotocopadoras, escáner, cámaras digitales y otras tecnologías de reproducción utilizados por el personal de “Vale un Perú” deben ser aquellas proporcionadas y autorizadas por la empresa. Por otra parte, los documentos que contienen información de carácter altamente confidencial debieran retirarse inmediatamente de

la impresora. Es responsabilidad de todos los colaboradores de “Vale un Perú” el cumplimiento de este lineamiento.

- f. Los usuarios deben destruir las impresiones que dejen de utilizar y que contengan información altamente confidencial¹, usando las trituradoras de papel disponibles en las oficinas o algún otro mecanismo de eliminación segura que no permita recuperar la información.
- g. Es responsabilidad del área de Seguridad de la Información, la verificación del cumplimiento de la presente política y de tomar las acciones correctivas para mitigar el riesgo de pérdida, manipulación, fuga de la información o suplantación.

4. INCUMPLIMIENTO

- a. El incumplimiento de esta política puede generar la materialización de riesgos de accesos y/o modificaciones no autorizadas, pérdida, fuga y uso no adecuado de la información considerada como altamente confidencial en “Vale un Perú”.
- b. El incumplimiento de la presente política, dependiendo del tipo y la gravedad de la infracción podrá seguir las medidas correspondientes en el Artículo 29 del Reglamento Interno de Trabajo de “Vale un Perú”.

POLÍTICA DE GESTIÓN DE ACCESO DE USUARIOS

1. OBJETIVO

La política de gestión de accesos de usuarios de “VALE UN PERÚ” tiene por objetivo describir los lineamientos que nos permitan gestionar adecuadamente los accesos de usuarios y sus contraseñas de los colaboradores evitando el acceso no autorizado a la red y sistemas de información. Cabe resaltar que esta política fue desarrollada de acuerdo con lo contemplado en la ISO/IEC 27001 y en la Circular N° G- 140 - 2009 “Gestión de la seguridad de la información”.

2. ALCANCE

Esta política es de cumplimiento de todos los colaboradores de “VALE UN PERÚ”.

3. DESCRIPCIÓN

3.1. Gestión de Usuarios

- a. Todo colaborador que ingresa a laborar a “VALE UN PERÚ” recibirá un usuario para su acceso a la red y a los sistemas, esto con el propósito de vincularlo a los usuarios y a los perfiles asociados a los sistemas, para responsabilizarlo de sus acciones. Dichos accesos tendrán un nivel de permiso o privilegio asignado, correspondientes a sus funciones desempeñadas en la empresa. El área de seguridad de la Información revisará con los niveles de acceso a los diversos sistemas de la compañía.
- b. La Gerencia General debe informar oportunamente los cambios de puesto de los colaboradores (Ascensos y Movimientos Internos) a través de un correo al Encargado de seguridad de información y al nuevo jefe del colaborador, para que inicien el proceso de altas o bajas de accesos de acuerdo con el Instructivo de gestión de altas, modificaciones y bajas de usuarios.
- c. Los privilegios especiales del personal de Soporte TI, tal como la capacidad de examinar los archivos de otros usuarios y/o modificar el estado de seguridad de los sistemas deberán ser restringidos únicamente a los responsables directos del manejo del sistema y/o temas de seguridad definidos por cada área responsable.
- d. Las cuentas de servicios de red que no han sido utilizadas en más de un año o que nunca han sido utilizadas serán desactivadas previa revisión de Seguridad de la Información, salvo excepciones que serán previamente aprobadas por el Responsable de Seguridad de Información de la Cooperativa.

- e. Las cuentas de usuario creadas para el desarrollo y pruebas de los diversos sistemas deben ser utilizadas únicamente para los fines descritos, siendo responsabilidad del Responsable de Soporte TI el cumplimiento de este lineamiento. El Encargado de seguridad de información en coordinación con el Responsable de Soporte TI evaluarán la eliminación de las cuentas de desarrollo y pruebas que no sean necesarias luego de culminado el proceso de desarrollo.
- f. Las cuentas de altos privilegios tales como: administración del sistema operativo o de la base de datos, serán utilizadas exclusivamente para estos fines y no para labores diarias.
- g. Por ningún motivo, se efectuarán reasignaciones a otros usuarios de las cuentas y privilegios existentes. Las cuentas de acceso y privilegios de los usuarios que dejen de laborar en la Cooperativa serán desactivados con Soporte TI. En caso de que se requiera que las cuentas de red y acceso a los sistemas de un colaborador cesado se mantengan activas por un tiempo determinado, se deberá solicitar la autorización correspondiente al Encargado de seguridad de información, indicando el tiempo que permanecerá activa (debe ser el mínimo indispensable), la persona responsable de las cuentas y el sustento correspondiente.
- h. El Responsable de Recursos Humanos comunicará el cese del colaborador para la desactivación de los accesos. Lo comunicará a las áreas de Seguridad de la Información, Soporte TI, Administración y al área de pertenencia del colaborador.
- i. Toda cuenta de usuario debe tener asociada obligatoriamente una contraseña. Dicha contraseña debe ser exigida en el proceso de autenticación y no puede estar en blanco. Toda cuenta de usuario debe establecerse acorde a la nomenclatura estándar definida en “VALE UN PERÚ”.
- j. Se prohíbe el uso de cuentas genéricas, que permitan el acceso de varios usuarios haciendo uso de una misma identificación. En aquellos casos en que sea absolutamente necesario y justificado el uso de éstas, su creación deberá contar con una aprobación explícita del Responsable de Seguridad de Información. No se debe permitir la utilización de cuentas de usuarios duplicadas, que correspondan a personas diferentes, en los sistemas de “VALE UN PERÚ”.
- k. Todo colaborador que se percate de una mala asignación de privilegios a alguna cuenta de usuario deberá notificarlo inmediatamente como incidente a las áreas de Seguridad de la Información y Soporte TI para que tomen acción al respecto.

- l. Las cuentas de administrador de las computadoras de “VALE UN PERÚ” deben contar con contraseñas basadas en los lineamientos de seguridad de la empresa y ser cambiadas periódicamente.
- m. El Encargado de seguridad de información debe revisar de manera anual o cuando lo considere pertinente, el cumplimiento del procedimiento de “Altas, Bajas y Modificaciones de Cuentas” del área de Soporte TI. La creación de cuentas de usuarios se realizará según lo estipulado en el Instructivo de Altas, Bajas y Modificaciones de cuentas. Para el caso de los ceses, el Encargado de seguridad de información debe revisar de manera quincenal o cuando lo considere conveniente, que se hayan restringido los accesos o deshabilitado al personal cesado. Para el caso de cuentas que manejen información sensible¹ de la empresa, el jefe directo debe notificar la desactivación de las cuentas inmediatamente ocurra el cese del colaborador.

3.2. Gestión de Contraseñas

- a. Las contraseñas son personales e intransferibles. No se deben transmitir las contraseñas verbalmente a través de líneas telefónicas, ni a través del correo electrónico. Compartir la contraseña está considerada una “Falta Grave”, la cual será sancionada de acuerdo con lo estipulado en el Reglamento Interno de Trabajo
- b. Los usuarios no deben anotar las contraseñas de acceso en lugares visibles y/o públicos o de fácil localización, tales como: debajo del teclado o teléfono, detrás de una foto, etc. Cualquier contraseña encontrada en estos medios, debe notificada al área de Seguridad de Información como un incidente.
- c. El usuario debe efectuar el cambio de sus contraseñas cada vez que considere que éstas han sido vulneradas o divulgadas a terceros, ello, independientemente del cambio automático solicitado por el sistema y de la notificación al área de seguridad de la información. Al crearse una cuenta de usuario se le asignará una contraseña temporal que deberá ser cambiada en el primer inicio de sesión. Las cuentas de usuarios quedarán bloqueadas automáticamente después de 3 intentos fallidos y sólo podrá ser desbloqueada por el personal del área de Soporte TI.
- d. Cada persona es totalmente responsable de las acciones efectuadas con sus cuentas de usuario asignadas. Por tal motivo, ninguna persona debe alejarse de su puesto de trabajo dejando su PC sin bloquear, toda vez que las acciones que se realicen durante

- su ausencia son de su total responsabilidad, sin importar si puede demostrar que no estaba frente a su PC.
- e. Las contraseñas deben estar conformadas por caracteres alfanuméricos y con un largo mínimo de 8 caracteres. Es recomendable que el usuario, al registrarlas, considere que esta debe ser fácil de recordar, difícil de adivinar y que cumpla con las siguientes características:
 - ✓ En el proceso de cambio de contraseñas, esta no se debe ser igual a las últimas 5 contraseñas utilizadas.
 - ✓ La contraseña no debe estar en Blanco.
 - ✓ La vigencia de la contraseña es de 30 días.
 - f. Las contraseñas, no deben ser visibles por pantalla al momento de ser ingresadas. No deben ser identificadas en el momento de la transmisión y deben viajar por la red encriptados, con algoritmos no reversibles.
 - g. Las cuentas de usuario de servicio de red cuyas contraseñas no tienen fecha de expiración son:
 - ✓ Cuentas especiales (Directivos, Gerencia General) y algunos casos excepcionales, debidamente justificados.
 - ✓ Usuarios requeridos para la ejecución de Software tales como cuentas de sistemas/aplicaciones, servicios y bases de datos.
 - h. Para los administradores de sistemas:
 - ✓ Las contraseñas deben permanecer encriptados con algoritmos y residir en archivos ocultos y protegidos en los sistemas.
 - i. En la medida de lo posible, se debe:
 - ✓ Evitar que las contraseñas, sean escritas o pasadas como parámetro, en archivos, programas, shell, procesos batch o log de procesos en forma visible.
 - ✓ Incorporar en las aplicaciones a ser desarrolladas por personal interno o por empresas externas, un mecanismo que permita desconectar al usuario y la ejecución de su trabajo realizado en la aplicación, después de un tiempo prudente de inactividad de este usuario de acuerdo con lo requerido por el área de seguridad de la información.
 - ✓ Toda contraseña, provista por el fabricante a cualquier sistema, debe ser cambiada de acuerdo con los estándares de “VALE UN PERÚ”. De igual forma

cualquier contraseña provista por un proveedor, de hardware o software, debe ser cambiada.

- j. El Encargado de seguridad de información debe revisar que los requerimientos descritos para la conformación de las contraseñas sean configurados y ejecutados por el Responsable de Soporte TI.

4. INCUMPLIMIENTO

- ✓ El incumplimiento de esta política puede generar la materialización de riesgos de acceso lógico a los activos de información de la compañía (sistemas, correo electrónico, servicios) pudiendo afectar la confidencialidad, integridad y disponibilidad de la información de la empresa.
- ✓ El incumplimiento de la presente política representa una falta, la cual puede seguir las medidas correspondientes en el Artículo 29 del Reglamento Interno de Trabajo de “Vale un Perú”.

POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE INFORMACIÓN

1. OBJETIVO

La Política de Gestión de Incidentes de Seguridad de la Información de “Vale un Perú” tiene por objetivo establecer los lineamientos para una adecuada gestión de los incidentes que comprometan la integridad, confidencialidad y disponibilidad de la información en “Vale un Perú”, permitiendo definir las acciones a tomar a fin de minimizar el daño producido por los potenciales incidentes de seguridad. Esta política fue desarrollada de acuerdo con lo contemplado en la ISO/IEC 27001:2014 y en la Circular N° G- 140 -2009 “Gestión de la seguridad de la información”.

2. ALCANCE

Esta política es de estricto cumplimiento de todas aquellas personas que mantienen un vínculo laboral con la empresa, de manera temporal o permanente, bajo todas las modalidades de contrato.

3. DESCRIPCIÓN

3.1. Lineamientos y Responsabilidades

- a. El Encargado de seguridad de información definirá el personal que conformará el equipo de respuesta a incidentes, quienes serán los responsables de recolectar evidencias, investigar, diagnosticar, informar y solucionar un incidente de seguridad. Asimismo, reportará al Encargado de seguridad de información.
- b. Todo incidente originado intencionalmente o recurrente será elevado e informado a Encargado de seguridad de información, a fin de que se definan las medidas pertinentes.
- c. Las medidas a tomar no se limitarán sólo a la pérdida de privilegios de los recursos de procesamiento de información, sino será evaluado por el Encargado de seguridad de información y la Gerencia General ya que se considerará las medidas indicadas en el Reglamento Interno de Trabajo.
- d. En caso de que el incidente o vulnerabilidad de seguridad la información no pueda ser resuelto internamente, se buscará apoyo a través de contactos de cooperación o asesores.
- e. El Encargado de seguridad de información revisará periódicamente los registros de incidentes y/o vulnerabilidades de seguridad, para analizar las actividades ejecutadas y estudiar las posibles mejoras o cambios que puedan efectuarse ante futuros incidentes, previniendo la recurrencia de estos y evitando que estos se transformen

en problemas que generen una pérdida financiera o un impacto alto en la compañía. Este análisis deberá aportar información para la implementación de las siguientes medidas:

- ✓ Correctivas: para apoyar a la solución del incidente.
 - ✓ Preventivas: para evitar la ocurrencia de este o emprender oportunidades de mejora que puedan disminuir la situación de riesgo actual.
- f. Los roles y responsabilidades involucradas en la Gestión de Incidentes de Seguridad de la Información figuran en el Procedimiento de Gestión de Incidentes y Vulnerabilidades de Seguridad de la Información del Manual de Procedimientos del SGSI.

3.2. Tipos de Incidentes o Vulnerabilidades

- a. Los principales incidentes o vulnerabilidades de seguridad de la información son:
- ✓ Fuga o pérdida de información (Memos, Autorización de Cargo de Prima, Orden de pago, Solicitud de endoso, Solicitud de Siniestro, File de propuesta de cliente, Solicitud de certificado, entre otros).
 - ✓ Pérdida o robos de dispositivos (PC, Laptop, PoS, Teléfonos, entre otros).
 - ✓ Mal funcionamiento o indisponibilidad de sistemas (sistemas con información con información corrupta).
 - ✓ Error en controles de acceso (Accesos lógicos no autorizados a sistemas críticos).
 - ✓ Violaciones de accesos (Acceso no autorizado a los activos, a las instalaciones, modificación o eliminación no autorizada, Virus, Spam, Phishing, entre otros).

3.3. Etapas en la Gestión de Incidentes de Seguridad de la Información

- a. Las etapas que se consideran en la Gestión de Incidentes de Seguridad de la Información son: (1) Detección, (2) Comunicación y registro del evento, (3) Análisis e investigación, (4) Contactar con Áreas Involucradas, (5) Recolección de evidencias y (6) Respuesta a incidentes y/o vulnerabilidades y Retroalimentación al usuario.

3.4. Reporte de Incidentes

- a. Todos los empleados de la compañía deben conocer y reportar los diferentes tipos de eventos y debilidades de forma oportuna que puedan tener un fuerte impacto en la

seguridad de la información de “Vale un Perú”. Estos eventos deberán ser reportados inmediatamente al Encargado de seguridad de información vía mail.

- b. El área de Seguridad de la Información llevará un control del registro de los incidentes y vulnerabilidades reportados por los colaboradores. Los canales y el esquema de comunicación apropiados para el reporte de incidentes son de conocimiento de todo el personal de “Vale un Perú” y figura en el Procedimiento de Gestión de Incidentes y Vulnerabilidades de Seguridad de la Información del Manual de Procedimientos del SGSI.

4. INCUMPLIMIENTO

- a. El incumplimiento de esta política puede generar la materialización de riesgos de accesos y/o modificaciones no autorizadas, pérdida, fuga y uso no adecuado de la información considerada como altamente confidencial, accesos vulnerados, pérdida o robo de activos de información, entre otros.
- b. El incumplimiento de la presente política, dependiendo del tipo y la gravedad de la infracción podrá seguir las medidas correspondientes en el Artículo 29 del Reglamento Interno de Trabajo de “Vale un Perú”.

POLÍTICA DE PROTECCIÓN ANTE VIRUS INFORMÁTICOS Y CÓDIGO MALICIOSO

1. OBJETIVO

La Política de Protección ante Virus Informáticos y Código Malicioso de “Vale un Perú” tiene por objetivo definir los requerimientos mínimos, que garanticen una adecuada protección ante posibles infecciones de virus informáticos y/o códigos maliciosos, que pudieran afectar negativamente la integridad, disponibilidad y confidencialidad de la información de la empresa. Cabe resaltar que esta política fue desarrollada de acuerdo con lo indicado en la ISO/IEC 27001:2014 y en la Circular N° G- 140 -2009 “Gestión de la seguridad de la información”.

2. ALCANCE

Esta política es de cumplimiento de todos los colaboradores de “Vale un Perú” y de todas aquellas personas que mantienen un vínculo laboral con la empresa de manera temporal o permanente y bajo todas las modalidades de contrato.

3. DESCRIPCIÓN

- a. La organización deberá establecer mecanismos para prevenir y detectar la introducción de software malicioso (antivirus). Los usuarios son conocedores desde su incorporación en la compañía de un “Reglamento de Uso de PC”, donde se les indica cómo hacer uso eficiente de los recursos informáticos.
- b. El software antivirus deberá ser actualizado y habilitado en todas las computadoras y servidores de “Vale un Perú”. No está permitido el uso de otro tipo de software antivirus que no esté aprobado por el Encargado de seguridad de información.
- c. Cualquier usuario que identifique la existencia de algún virus deberá comunicar inmediatamente al Encargado de seguridad de información y al Responsable de Soporte TI. Lo mismo aplica a cualquier medida de protección que se considere desactualizada, que no esté funcionando correctamente o cuando se detecte algún comportamiento sospechoso en los sistemas
- d. Todo colaborador que sospeche o identifique algún equipo infectado con virus, deberá desconectarlo de la red de la organización y notificado a las áreas de Seguridad de la Información y Soporte TI.
- e. Todo servidor, computador personal, equipo portátil y cualquier otro equipo informático, propiedad de “Vale un Perú” debe tener instalado el software antivirus corporativo aprobado por el Encargado de seguridad de información.

- f. Queda prohibida la conexión a la red de datos de “Vale un Perú”, de cualquier equipo informático que no cuente con el software antivirus corporativo instalado y actualizado previamente.
- g. Los equipos informáticos, propiedad de los colaboradores, proveedores y/o terceros, que requieran conectarse a la red de datos de “Vale un Perú”, deberán ser evaluados y autorizados por el Responsable de Soporte TI y el Encargado de seguridad de información, con la finalidad de verificar que cuenten con un antivirus, que cumpla los requerimientos y estándares de seguridad informática de la empresa. Solo se brindará acceso en caso sea estrictamente necesario para las labores del personal.
- h. Todo medio magnético, debe ser analizado previamente a su lectura/escritura, por el software antivirus corporativo de “Vale un Perú”.
- i. Todo software y archivos descargados de fuentes externas a “Vale un Perú”, a través de Internet o cualquier otra red pública, deben ser analizados por el software antivirus corporativo, antes de que el software sea ejecutado, o que los archivos sean utilizados por otros programas.
- j. Antes de descomprimir archivos, o software descargado de fuentes externas a “Vale un Perú”, el usuario deberá analizarlo mediante el software antivirus corporativo.
- k. Los colaboradores, deberán verificar periódicamente, que el software antivirus instalado en su estación de trabajo, se encuentre actualizado, caso contrario, informar inmediatamente al Responsable de Soporte TI.
- l. Antes de restaurar los archivos de los sistemas informáticos de “VALE UN PERÚ”, desde un medio de respaldo, dichos archivos deberán ser analizados por el software antivirus.

- **Requerimientos del software antivirus corporativo**

- a. El antivirus corporativo de “Vale un Perú”, deberá contemplar como mínimo las siguientes características:
 - ✓ Detección y protección en tiempo real
 - ✓ Las definiciones y librerías de virus deberán actualizarse como mínimo una vez al día.
 - ✓ Contar con facilidades que incluyan, como mínimo, medidas que protejan contra amenazas de red y software espía.

- ✓ Permitir la programación de tareas de revisión y búsqueda automática de virus informáticos y código malicioso.
- b. Es responsabilidad del Responsable de Soporte TI de “Vale un Perú”, el asegurar que se mantenga actualizado, el antivirus corporativo en todo servidor, computador personal, equipo portátil y cualquier otro equipo informático propiedad de “Vale un Perú”.

- **Restricciones y limitaciones**

- a. Los Colaboradores de “Vale un Perú”:
 - ✓ No deberán copiar o descargar archivos provenientes de fuentes, y/o sitios web desconocidos o de bajo nivel de confiabilidad.
 - ✓ No deberán utilizar software que haya sido suministrado por fuentes externas a la empresa, o que provenga de personas u organizaciones distintas de los proveedores conocidos y confiables. Solamente se utilizará software verificado o autorizado por el Encargado de seguridad de información, o el Responsable de Soporte TI.
 - ✓ No deberán intentar eliminar los virus informáticos de sus sistemas, a menos que lo hagan mientras estén en comunicación o recibiendo asistencia del personal designado por el Responsable de Soporte TI.
 - ✓ No deberán escribir, generar, compilar, copiar, recolectar, propagar, ejecutar o tratar de introducir códigos, archivos y/o programas diseñados para autorreplicarse, dañar, o de alguna manera, entorpecer el desempeño de cualquier equipo informático de “Vale un Perú”.
 - ✓ No deberán efectuarse actualizaciones automáticas de software, en los computadores de “Vale un Perú”, a través del uso de la tecnología “push”, a menos que el software utilizado, haya sido aprobado por el Encargado de seguridad de información, o por el Responsable de Soporte TI de “Vale un Perú”.
- b. El usuario no debe tener la posibilidad de deshabilitar la ejecución de los sistemas antivirus y no deben ejecutar sistemas y/o aplicaciones que sospechen posee un contenido malicioso o cuya fuente de origen no es confiable. Asimismo, los usuarios quedan prohibidos de participar en la distribución de malware.

4. INCUMPLIMIENTO

- a. El incumplimiento de esta política puede generar la materialización de riesgos de infección y daño de los equipos informáticos, así como la propagación de virus a través de la red interna de “Vale un Perú”.
- b. El incumplimiento de la presente política representa una falta, la cual puede seguir las medidas correspondientes en el Artículo 29 del Reglamento Interno de Trabajo de “Vale un Perú”.

POLÍTICA DE SEGURIDAD DE INFORMACIÓN EN CONTRATOS CON TERCEROS

1. OBJETIVO

La política de seguridad de información en contratos con terceros tiene por objetivo definir y establecer los roles y responsabilidades de terceros, así como establecer controles que permitan reducir los riesgos de seguridad de la información asociados a los servicios brindados por terceros a “Vale un Perú”. Cabe resaltar que esta política fue desarrollada de acuerdo con lo contemplado en la ISO/IEC 27001 y en la Circular N° G- 140 - 2009 “Gestión de la seguridad de la información”.

2. ALCANCE

Esta política tiene alcance de aplicación a todos los contratos o acuerdos existentes entre “Vale un Perú” y terceros (proveedores de servicios, outsourcing, asesores, contratistas, entre otros).

3. REQUISITOS DE SEGURIDAD ANTES DE LA CONTRATACIÓN

- a. Cuando la empresa requiera la contratación de terceros, el encargado de seguridad de información en coordinación con la Gerencia General y Soporte TI deben realizar la evaluación de riesgo de seguridad de información a fin de definir principalmente: el tipo de acceso requerido, sustento del acceso solicitado, clasificación de la información / evaluación de impacto, medidas de mitigación y control. Lo definido en la evaluación de riesgos deberá documentarse en el contrato.
- b. El acceso de terceros a la información, sistemas de información, instalaciones de procesamiento, instalaciones administrativas u otras áreas de servicios críticos se aplicará sólo luego de la implementación de controles apropiados y la firma respectiva del contrato y/o acuerdo que defina las condiciones para la conexión o el acceso. Asimismo, es responsabilidad del Responsable de Soporte TI solicitar permiso a las áreas pertinentes (Seguridad de la Información y Administración) estos accesos. No está permitido el acceso a los datos personales (información sensible) y datos de titulares de tarjetas, las alternativas a este acceso tendrán que ser evaluado por el encargado de seguridad de información y Soporte TI.
- c. Los terceros que presten servicios a “Vale un Perú”, deben firmar el respectivo contrato y acuerdo de confidencialidad. El contrato debe definir el tipo de información tratada (intercambiada, transferida, almacenada) y el objetivo de hacerlo. Si la información que se intercambia transfiere, almacena o trata entre las

partes es confidencial o sensible, el acuerdo de confidencialidad puede formar parte del mismo contrato (cláusula) o como un acuerdo separado.

- d. Los terceros que como parte del servicio traten datos personales de clientes, proveedores, empleados, entre otros; deberán firmar un acuerdo (ej. cláusula) respecto al conocimiento de las medidas requeridas por la Ley N° 29733 - Ley de Protección de Datos Personales y su adecuación o alineamiento.
- e. La información involucrada en el servicio del tercero debe ser clasificada y controlada de acuerdo con la política de clasificación de información de “Vale un Perú”. Para el intercambio o transferencia de información entre “Vale un Perú” y el tercero, esta deberá estar adecuadamente clasificada y etiquetada.
- f. La conexión entre sistemas de “Vale un Perú” y los sistemas de terceros deberá ser aprobada por el Responsable de Seguridad a fin de comprometer la seguridad de la información.

4. REQUISITOS DE SEGURIDAD DURANTE EL SERVICIO

- a. Soporte TI deberá validar que las condiciones de entrega de servicio del tercero se den según lo definido antes de la contratación.
- b. El área de Seguridad de la Información es responsable de realizar una visita anual a los proveedores que realicen el tratamiento de información sensible (datos sensibles de clientes, datos de titulares de tarjetas, entre otros) de “Vale un Perú” con el objetivo de validar el cumplimiento de los requisitos de seguridad exigidos a nivel contractual (referentes a la Ley de Protección de Datos Personales, ISO 27001 “Sistema de Gestión de Seguridad de la Información”, Superintendencia de Banca y Seguros - SBS, entre otros). Al respecto se emitirá un informe con los resultados de la evaluación.

5. REQUISITOS DE SEGURIDAD AL TÉRMINO DEL VÍNCULO CONTRACTUAL

- a. Todo Gestor de Servicio debe informar al área de Soporte e Infraestructura TI, Administración y al Encargado de seguridad de información, sobre la culminación del vínculo contractual con el tercero y/o sus empleados con la finalidad de asegurar

el retorno de los activos de la empresa, la restricción de los accesos a las instalaciones y a los sistemas de información de “Vale un Perú”.

- b. El área de Seguridad de la Información debe registrar en una bitácora los terceros que brindan algún tipo de servicio a “Vale un Perú” y que como parte del servicio se considere el tratamiento (intercambio, transferencia, almacenamiento) de información Confidencial (ej. datos personales y/o datos de tarjetas).

6. INCUMPLIMIENTO

- a. El incumplimiento de esta política puede generar la materialización de riesgos asociado a los servicios de terceros con “Vale un Perú”, lo cual compromete los activos de información de la compañía (sistemas, correo electrónico, servicios) pudiendo afectar la confidencialidad, integridad y disponibilidad de la información de la empresa.
- b. El incumplimiento de la presente política representa una falta, la cual puede seguir las medidas correspondientes en el Artículo 29 del Reglamento Interno de Trabajo de “VALE UN PERÚ”.

POLÍTICA DE SEGURIDAD DE INFORMACIÓN CON RECURSOS HUMANOS

1. OBJETIVO

La Política de Seguridad de Información con Recursos Humanos de “Vale un Perú” tiene por objetivo definir los requisitos de Seguridad de la Información antes, durante y al finalizar el empleo. Asimismo, coordinar la concientización y entrenamiento de los colaboradores de “Vale un Perú” y brindar los lineamientos para la definición de los procesos disciplinarios. Cabe resaltar que esta política fue desarrollada de acuerdo a lo contemplado en la ISO/IEC 27001:2014 y en la Circular N° G- 140 - 2009 “Gestión de la seguridad de la información”.

2. ALCANCE

Esta política es de cumplimiento de todos los colaboradores de “Vale un Perú” y de todas aquellas personas que mantienen un vínculo laboral con la empresa de manera temporal o permanente y bajo cualquier modalidad de contrato.

3. DESCRIPCIÓN

3.1. Requisitos de Seguridad antes del Empleo

- a. Las responsabilidades de los empleados con acceso a la información confidencial o altamente confidencial de la empresa están definidas en la Política de Clasificación de la Información.
- b. El Responsable de Recursos Humanos es responsable de obtener y resguardar los compromisos de confidencialidad y/o consentimientos para el tratamiento de datos personales de colaboradores que se incorporarán a la Cooperativa.
- c. Como parte de los documentos de ingreso, los colaboradores de “Vale un Perú” reciben y/o firman lo siguiente:
 - ✓ Código de Ética: Define los lineamientos básicos a considerar como parte de una conducta y comportamiento ético del colaborador, a fin de cumplir con las políticas y procedimientos de “Vale un Perú”.
 - ✓ Convenio de Confidencialidad: Define las cláusulas de confidencialidad entre el colaborador y la empresa.
 - ✓ Ley de Protección de Datos Personales: Define el consentimiento por parte del colaborador para obtener sus datos personales y sensibles, como parte del proceso de vinculación a la Cooperativa.
- d. Todos los candidatos para contratar como empleados deben ser adecuadamente seleccionados considerando lo siguiente:
 - ✓ Validación de datos personales.

- ✓ Validación de datos profesionales.
- ✓ Validación de referencias laborales.
- ✓ Validación de récord crediticio.

3.2. Requisitos de Seguridad durante el Empleo

- a. Los Responsable de Recursos Humanos y Seguridad de la Información son responsables de asegurar que los colaboradores entiendan sus responsabilidades y la relación con el proceso de seguridad de la información a fin de reducir los riesgos de hurto, fraude o mal uso de las instalaciones y sus activos de información. Para lo cual los nuevos colaboradores reciben como parte del programa de inducción, temas relacionados a seguridad de la información.
- b. El personal de “Vale un Perú”, no debe interceptar o divulgar el contenido de las comunicaciones o contribuir a que otros lo hagan. El contenido de las comunicaciones, ocasionalmente, puede ser revisado o auditado, en caso sea necesario para actividades de mantenimiento, seguridad, auditoría o en la resolución de algún problema.
- c. La falta de cumplimiento o la violación de alguna política de la seguridad de información, podrá derivar en la aplicación de sanciones disciplinarias, que en su mayor grado pueden alcanzar la desvinculación y/o aplicación de las acciones legales que correspondan, según se indica en el Reglamento Interno de Trabajo y Código de Ética de la Cooperativa.
- d. Cualquier colaborador que tenga conocimiento de una violación de alguna política de seguridad de la información, debe informarla al Encargado de seguridad de información y Recursos Humanos.
- e. El Responsable Recursos Humanos en coordinación con la Gerencia General, es responsable de la definición de términos y condiciones para los contratos de empleo. El área de Seguridad de la Información es responsable de comunicar y concientizar a los colaboradores lo referente a Los documentos internos de seguridad vigentes a la fecha.
- f. El Encargado de seguridad de información en coordinación con el Responsable de Recursos Humanos efectuarán programas de inducción a los nuevos colaboradores y sesiones de capacitación a los colaboradores. Dicha actividad está a cargo del

Encargado de seguridad de información y son dictadas en forma anual, para asegurar el cumplimiento de las políticas y procedimientos de seguridad de la información.

3.3. Requisitos de Seguridad al finalizar el Empleo

- a. El Responsable de Recursos Humanos debe informar a los Responsables de Soporte de TI, Administración y Seguridad de la Información, sobre la culminación del vínculo laboral con los empleados con la finalidad de asegurar el retorno de los activos de la empresa, la restricción de los accesos a las instalaciones y a los sistemas de información de “Vale un Perú”.
- b. En el caso de un cese de un colaborador que maneje información Altamente Confidencial, el jefe inmediato deberá notificar a los Responsables de Soporte TI, Recursos Humanos, Administración y Seguridad de la Información esta decisión a fin de retirarle los accesos físicos y lógicos correspondientes de inmediato.

4. INCUMPLIMIENTO

- a. El incumplimiento de esta política puede generar la materialización de riesgos de acceso lógico no autorizado a los activos de información de la Cooperativa (sistemas, carpetas compartidas, correo electrónico, servicios), fuga de información altamente confidencial, daños en la reputación de la Cooperativa, entre otros; pudiendo afectar la confidencialidad, integridad y disponibilidad de la información en la empresa.
- b. El incumplimiento de la presente política representa una falta, la cual puede seguir las medidas correspondientes en el Artículo 28 y 29 del Reglamento Interno de Trabajo de “Vale un Perú”.
- c. Las acciones disciplinarias no se limitarán sólo a la pérdida de privilegios de los sistemas de información ya que se podrá considerar la cancelación de contratos u otras acciones apropiadas según lo establecido en el Manual de Funciones y Responsabilidades de la Cooperativa.

POLÍTICA DE USO Y SEGURIDAD EN INTERNET

1. OBJETIVO

La Política de Uso y Seguridad en Internet de “Vale un Perú” tiene por objetivo definir los requerimientos mínimos que garanticen un adecuado uso de los beneficios de Internet, sin que este exponga a la empresa a riesgos de información innecesarios. Cabe resaltar que esta política fue desarrollada de acuerdo a lo contemplado en la ISO/IEC 27001:2014, y en la Circular N° G- 140 - 2009 “Gestión de la seguridad de la información.

2. ALCANCE

Esta política es de estricto cumplimiento de todas aquellas personas que mantienen un vínculo laboral con la empresa, de manera temporal o permanente, bajo todas las modalidades de contrato.

3. DESCRIPCIÓN

- a. El acceso a Internet, deberá ser otorgado únicamente a aquellos colaboradores de “Vale un Perú” que tienen una necesidad justificada por razones empresariales. La capacidad de acceder y de participar en otras actividades de Internet no es un incentivo, al cual todos los colaboradores de “Vale un Perú” tienen derecho.
- b. Los accesos a Internet brindados a los colaboradores son asignados de acuerdo a niveles establecidos donde se les permite o deniega el acceso a páginas de Internet. Los niveles de internet son aprobados por el Encargado de seguridad de información.
- c. Si un empleado de “Vale un Perú” no cuenta con el adecuado acceso a Internet, pero lo necesita para un proyecto en particular, deberá obtener la aprobación de su jefatura y/o gerencia y posteriormente solicitarlo al Encargado de seguridad de información.
- d. Todo acceso a páginas web adicionales que se soliciten deberá ser aprobado por el Encargado de seguridad de información.

3.1. Integridad de la información

- a. Toda la información adquirida de Internet debe considerarse no confiable. Antes de emplear información suministrada gratuitamente por Internet para la toma de decisiones empresariales, los colaboradores de “Vale un Perú” deben corroborar la información consultando otras fuentes.
- b. Todos los archivos descargados de Internet y provenientes de fuentes que no pertenecen a “Vale un Perú”, deben ser examinados con el antivirus antes de usarlos.

- c. Cuando el proveedor externo del software descargado no es confiable, el mencionado software debe probarse en una máquina independiente aislada de la red de “Vale un Perú”, y excluida del ambiente de producción, que haya sido respaldada recientemente.
- d. Los archivos descargados deben descomprimirse antes de ser sometidos a la verificación antivirus. Es recomendable el uso de firmas digitales para verificar que un archivo no ha sido modificado por partes no autorizadas, mas no garantiza que el archivo esté libre de virus u otros códigos maliciosos.

- **Instalación de Software**

- a. Los colaboradores de “Vale un Perú” no deben instalar software en los equipos de cómputo suministrados por “Vale un Perú”, bien sea que se hayan descargado de la Internet o se hayan obtenido de otro modo, toda instalación debe coordinarse a través de un requerimiento a Soporte TI.
- b. Es necesario considerar en este punto lo contemplado en la “Política de Adquisición, Desarrollo, Instalación, actualización y cambios a los Sistemas Informáticos”.

- **Tecnología de actualización automática**

- a. Queda prohibida la actualización automática de software o de información en los computadores de “Vale un Perú” través de tecnología de actualización automática de Internet, a menos que el sistema del proveedor haya sido aprobado por el Encargado de seguridad de información de “Vale un Perú”.

- **Información del usuario**

- a. Queda prohibido falsear, ocultar o sustituir la identidad de un usuario en Internet, o en cualquier sistema de comunicaciones electrónicas de “Vale un Perú”. El nombre del usuario, la dirección de correo electrónico, la afiliación a la empresa y otros detalles incluidos en los mensajes o transcripciones deben señalar al verdadero autor de estos.
- b. Queda prohibido el redireccionamiento de correo y otras facilidades anónimas. Se prohíbe el uso de conexiones anónimas (FTP, HTTP o exploración de la web) y otros métodos de acceso establecidos, sin los mecanismos de seguridad correspondientes.

Ante la necesidad explícita de negocio u operación se deberá informar al Encargado de seguridad de información para su evaluación.

- c. Se prohíbe realizar monitoreo de red no autorizada que permita conocer la navegación de los usuarios y/o acceder a información altamente confidencial o de uso personal.

3.2 Uso personal

- a. Los colaboradores de “Vale un Perú” con acceso a Internet y que deseen explorarla para propósitos personales, incluyendo juegos, grupos de noticias y las páginas no relacionadas con el negocio, deben hacerlo durante su tiempo libre y no en horario laboral. El uso de los recursos de “Vale un Perú” para propósitos personales se permite siempre y cuando el aumento en el costo por dicho uso sea insignificante, no tenga prioridad sobre las actividades de negocio de “Vale un Perú” y no conlleve la creación de un ambiente de trabajo desfavorable, o un ejemplo de conducta deficiente.

- **Sitios ofensivos de internet**

- a. “Vale un Perú” no es responsable del contenido de los sitios de Internet. Está terminantemente prohibido el ingreso a sitios con contenido censurable, como por ejemplo material violento, sexista, racista, sexualmente explícito, o potencialmente ofensivo.

- **Bloqueo de sitios y filtros de contenido**

- a. Soporte TI es responsable del control de las licencias de software y/o recursos informáticos. En “Vale un Perú”, únicamente está permitido el uso de software licenciado y autorizado por Soporte TI.
- b. La organización deberá establecer mecanismos para prevenir y detectar el ingreso de software malicioso. Los usuarios, desde su incorporación en la Cooperativa, tienen conocimiento del “Reglamento de Uso de PC”, donde se les indica cómo hacer uso eficiente de los recursos informáticos.
- c. Es responsabilidad de Soporte TI la actualización y habilitación del software antivirus en todas las computadoras y servidores de “Vale un Perú”.

- d. Todas las descargas realizadas de Internet, los mails entrantes y los archivos introducidos por cualquier medio en la red de “Vale un Perú” deben ser examinados por el software de antivirus.
- e. Cualquier usuario que identifique la existencia de algún virus deberá comunicar inmediatamente al Encargado de seguridad de información y al Responsable de Soporte TI. Lo mismo aplica a cualquier medida de protección que se considere desactualizada, que no esté funcionando correctamente o cuando se detecte algún comportamiento sospechoso en los sistemas.
- f. La posibilidad de conectarse con un sitio específico de la Internet no implica que se permita que los usuarios de los sistemas de “Vale un Perú” visiten ese sitio. “Vale un Perú” puede restringir o bloquear el acceso a sitios de Internet, así como impedir la descarga de ciertos tipos de archivo, incluyendo los archivos gráficos y de música, que contravengan la presente política.
- g. El Encargado de seguridad de información deberá aprobar los requerimientos de accesos a páginas de internet, donde se evaluará la necesidad de los accesos, la seguridad de la página, entre otros factores. El requerimiento deberá estar aprobado previamente por la jefatura y/o gerencia del usuario solicitante.

3.2. Confidencialidad de la Información

- **Intercambio de Información**

- a. El intercambio de software o de datos por Internet, exceptuando el correo electrónico, entre “Vale un Perú” y cualquier tercero no debe proceder, a menos que se haya suscrito un acuerdo por escrito que especifique los términos del intercambio y la manera en que el software o los datos se van a manejar y proteger.
- b. La información Confidencial de “Vale un Perú” no debe enviarse por Internet, a menos que haya sido cifrada con métodos autorizados por el Comité de Seguridad de la Información de “Vale un Perú” y validados por el Encargado de seguridad de información.
- c. Es necesario considerar en este punto lo contemplado en la “Política de Uso y Seguridad del Correo Electrónico”

- **Exposición de información**

- a. Los colaboradores de “Vale un Perú” no deben colocar información Altamente Confidencial de “Vale un Perú” en ningún computador accesible públicamente por la Internet que soporte FTP anónimos o servicios similares, a menos que la exposición de estos materiales haya sido autorizada por el Encargado de seguridad de información relevante.

- **Parámetros de seguridad**

- a. A menos que se tenga conocimiento confiable de que la conexión está cifrada, los números de tarjetas de crédito, información financiera de clientes, las contraseñas de acceso fijas y otros parámetros de seguridad que puedan emplearse para obtener acceso a bienes y servicios, no deben enviarse por Internet en forma legible.

- **Eliminación de mensajes**

- a. Los mensajes enviados por colaboradores de “Vale un Perú” a los grupos de discusión, a boletines electrónicos y a otros foros públicos de la Internet, que incluyan una afiliación implícita o explícita con “Vale un Perú”, pueden eliminarse por iniciativa de la Gerencia General de “Vale un Perú”, si ésta considera que los mismos no están acordes con los intereses del negocio o con la política vigente de “Vale un Perú”. Se incluyen en esta categoría, las declaraciones políticas y religiosas, el uso de lenguaje grosero o soez, y otras afirmaciones consideradas como hostigamiento a otras personas, basándose en la raza, el credo, el color, la edad, el sexo, las discapacidades físicas o las preferencias sexuales. La decisión de solicitar la eliminación del mensaje, debe tomarla el Encargado de seguridad de información. Cuando sea práctico y viable, los individuos responsables del mensaje serán informados de la decisión y tendrán la oportunidad de eliminar el mensaje ellos mismos.

- **Divulgación de información Confidencial**

- a. Los colaboradores de “Vale un Perú” no deben divulgar públicamente información Altamente Confidencial de la empresa a través de la Internet, si se identifica la publicación de este tipo de información en los medios se procederá con la aplicación de la política de sanciones.

- **Divulgación Involuntaria**

- a. Está prohibida la divulgación de Información Altamente Confidencial en Internet por los colaboradores de “Vale un Perú”.

- **Uso de Redes sociales desde las estaciones de trabajo**

- a. El uso de redes sociales debe ser utilizado responsablemente y en horario no laborable. Se encuentra prohibido divulgar información confidencial o que perjudique la reputación de la empresa en las redes sociales.

4. INCUMPLIMIENTO

- a. El incumplimiento de esta política puede generar la materialización de riesgos de infección de equipos informáticos, fuga o exposición de información altamente confidencial de la Cooperativa, entre otros; pudiendo afectar la confidencialidad, integridad y disponibilidad de la información confidencial de la empresa.
- b. El incumplimiento de la presente política representa una falta, la cual puede seguir las medidas correspondientes en el Artículo 29 del Reglamento Interno de Trabajo de “Vale un Perú”.

POLÍTICA DE USO Y SEGURIDAD DEL CORREO ELECTRÓNICO

1. OBJETIVO

La política de Uso y Seguridad de Usuarios del Correo Electrónico de “Vale un Perú” tiene por objetivo definir los requerimientos mínimos acordes con la política de Seguridad de la Información de “Vale un Perú” que garanticen un adecuado uso del correo electrónico corporativo, sin que este exponga a la empresa a riesgos de información innecesarios.

2. ALCANCE

Esta política es de cumplimiento de todos los colaboradores de “Vale un Perú” de Lima y Provincias y de todas aquellas personas que mantienen un vínculo laboral con la empresa de manera temporal o permanente y bajo cualquier modalidad de contrato.

3. MARCO LEGAL

- ISO/IEC 27001:2014.
- Circular N° G- 140 -2009 - Gestión de la seguridad de la información.
- Normas internas que correspondan.

4. DESCRIPCIÓN

4.1. Gestión de usuarios Responsabilidad del usuario

- a. En caso de recibir mensajes con asuntos sospechosos y/o de origen desconocido, una cantidad excesiva de mensajes no deseados de una organización externa en particular, o de una dirección de correo electrónico, los colaboradores destinatarios de “Vale un Perú” deberán reenviar el mail al Encargado de seguridad de información. Por ningún motivo se debe responder directamente al remitente.
- b. Para impedir el acceso de partes no autorizadas a las comunicaciones electrónicas de la empresa, las contraseñas generadas por los usuarios deben tener una complejidad adecuada, la cual es la misma utilizada para el acceso a la red. Los usuarios no deben incluir en la contraseña, palabras que se encuentren en diccionarios, datos personales, nombres o algún otro término relacionado con las actividades laborales. Para este punto, se debe tener en cuenta lo contemplado en la “Política de gestión de acceso de usuarios”.
- c. Todos los usuarios son responsables de la información tratada desde su cuenta de correo electrónico. Cualquier opinión expresada en los mensajes pertenece únicamente al autor remitente, y no representa la opinión de “Vale un Perú”. La

divulgación, difusión, copia y/o adulteración de un correo electrónico de la empresa se encuentra estrictamente prohibida.

- d. Toda información proveniente de Internet se debe considerar no confiable hasta que haya sido respaldada y/o confirmada por una fuente confiable. Los colaboradores que utilicen los sistemas de correo electrónico de “Vale un Perú” deben acatar los siguiente:
 - ✓ Reenviar o reproducir material después de obtener el permiso de la fuente correspondiente.
 - ✓ Citar material de distintas fuentes sólo si éstas se logran identificar adecuadamente.
 - ✓ No revelar información interna de “Vale un Perú”.
- e. Los colaboradores de “Vale un Perú” no deben usar frases irreverentes, palabras obscenas y/o comentarios peyorativos en los mensajes de correo electrónico destinado a los colaboradores, clientes, competidores u otras personas, debido a que estos pueden tener implicancias legales negativas para la empresa. Las comunicaciones electrónicas de “Vale un Perú”, deben utilizarse por parte de los colaboradores, únicamente para asuntos relacionados con el negocio. Como parte de las buenas prácticas que rige el negocio, todas las comunicaciones realizadas, deben adherirse a las normas convencionales de conducta, de ética y de cortesía.
- f. Cuando un correo electrónico contiene información confidencial de la compañía, éste se debe almacenar en un espacio diferente. Los usuarios deben trasladar con regularidad los archivos adjuntos con información confidencial a carpetas compartidas (acceso a un grupo limitado de personas) o en su respectiva Pc. La bandeja de entrada del correo electrónico no debe utilizarse para el almacenamiento de información Confidencial.
- g. Todos los mensajes que se transmitan a través del activo correo electrónico son de propiedad de “Vale un Perú”. El Reglamento Interno de Uso de Computadoras personales es de conocimiento de todos los usuarios, forma parte del File Personal y es firmado al ingreso de cada nuevo colaborador a la organización. Los usuarios deberán cumplir con procesos disciplinarios que se indican en el Reglamento Interno de Trabajo.
- h. Todo documento de carácter confidencial que se transmita a través del correo electrónico deberá protegerse mediante una contraseña de apertura para evitar la

exposición de la información contenida en el archivo, en caso sea accedido por personal no autorizado, esto es responsabilidad del usuario que transmite esta información. Todos los mensajes deben incluir en el asunto su respectiva clasificación, esta etiqueta servirá como recordatorio a los destinatarios acerca de la confidencialidad y privacidad de la información.

- i. Todo archivo adjunto debe ser examinado con un software antivirus autorizado antes de ser abierto o ejecutado. En algunos casos, los archivos adjuntos deben descifrarse o descomprimirse antes de que se realice la verificación de virus. Los colaboradores de “Vale un Perú” deben desconfiar de todos los archivos adjuntos recibidos de terceros aun cuando los conozcan y confíen en ellos.

4.2. Privacidad de la Información

- a. “Vale un Perú” se compromete a respetar los derechos de sus colaboradores incluyendo el respeto a su privacidad, igualmente se responsabiliza de la operación, mantenimiento y protección de sus redes de comunicaciones electrónicas. Asimismo, “Vale un Perú” se reserva el derecho de desactivar y/o deshabilitar cualquier cuenta de correo electrónico que por uso indebido atente contra lo establecido en el presente documento.
- b. En caso estrictamente necesario, “Vale un Perú” cuenta con la potestad de divulgar a las autoridades pertinentes, toda la información requerida que ha sido almacenada en el correo electrónico institucional. Este consentimiento lo brindan los usuarios al hacer uso del sistema de correo electrónico de “Vale un Perú”. Todo proceso de investigación forense que se realice sobre el sistema de correo electrónico deberá ser solicitado al Encargado de seguridad de información y realizado por el equipo de soporte tecnológico o un tercero especializado en el rubro, evidenciando las actividades realizadas a nivel de filtros de búsqueda.
- c. Únicamente cuando se tenga indicios y/o evidencias materiales que el contenido de las comunicaciones electrónicas de los colaboradores de “Vale un Perú” puedan estar comprometiendo las políticas y/o los objetivos de negocio, el Encargado de seguridad de información, previa autorización del Gerente General podrá solicitar las revisiones pertinentes. El Encargado de seguridad de información debe contar con la asesoría y opinión previa de un Abogado.

4.3. Mecanismos de seguridad a nivel de correo electrónico

- a. Para cualquier tipo de acceso al sistema de correo electrónico, ya sea a través de una red externa a la empresa o dispositivos móviles, se deberá realizar el acceso a través de un protocolo seguro (HTTPS/IMAP). Para esto Soporte TI facilita un certificado digital a todos los colaboradores de “Vale un Perú”, este deberá ser instalado en las computadoras desde donde se acceda al correo electrónico.

4.4. Condiciones de Uso del correo electrónico

- a. El sistema de correo electrónico de “Vale un Perú”, debe usarse únicamente para actividades empresariales. Su uso personal, es permitido siempre y cuando sólo consuma una cantidad mínima de los recursos del sistema, no interfiera con la productividad del empleado, y no tenga prioridad sobre otras actividades del negocio. Por otra parte, se restringe su uso para la organización de campañas de recaudación de fondos destinado a obras benéficas, actividades para la defensa de intereses políticos o religiosos, actividades privadas de negocios o entretenimiento personal.
- b. Queda prohibido falsear, confundir, ocultar o sustituir la identidad de algún usuario del sistema de correo electrónico. El nombre del usuario, la dirección de correo electrónico, la afiliación a organizaciones y otros datos relacionados incluidos en los mensajes o anuncios electrónicos deben señalar el verdadero origen de estos.
- c. Es obligatorio el uso de firmas en el envío de correos electrónicos al exterior de “Vale un Perú”, indicando el nombre, cargo, teléfono y dirección.
- d. En caso se requiera una cuenta de uso grupal o genérica, se deberá solicitar el acceso respectivo a Soporte TI y Seguridad de la Información, indicando:
 - ✓ Justificación de uso.
 - ✓ Nombre tentativo de la misma, la cual será evaluada y validada por el Encargado de seguridad de información.
 - ✓ Personas que utilizarán la cuenta.
 - ✓ Responsable de la cuenta de correo (dueño).
- e. La cuenta de correo genérica o de área podrá ser usada para asociarlas a plataformas de servicios cloud que exijan la inscripción con una cuenta de correo, no está permitido asociarlo a cuentas personales de los colaboradores.

Las plataformas de servicio almacenan información en la nube y pueden ser:

 - ✓ Google

- f. Queda prohibido el reenvío y/o redireccionamiento general de los correos electrónicos a terceros fuera de “Vale un Perú”, a menos que se haya obtenido un permiso del Encargado de seguridad de información y el Responsable de Soporte TI de “Vale un Perú”. Los mensajes enviados por terceros que contengan información Confidencial no deben reenviarse a otros terceros a excepción que el remitente tenga un propósito específico y que el envío sea necesario para alcanzar los objetivos laborales. Para el resto de los casos, el reenvío de mensajes enviados por terceros a otros terceros sólo debe realizarse si el remitente está expresamente de acuerdo con dicho reenvío.
- g. Queda prohibida la representación pública de “Vale un Perú” a través de medios de comunicación, página inicial de Internet, foros o boletines electrónicos, mensajes de correo electrónico y mensajes de correo de voz, a excepción de autorización del Comité de Gerencia.

5. INCUMPLIMIENTO

- a. El incumplimiento de esta política puede generar la materialización de riesgos de acceso lógico a los activos de información de la compañía (sistemas, correo electrónico, servicios) pudiendo afectar la confidencialidad, integridad y disponibilidad de la información de “Vale un Perú”.
- b. El incumplimiento de la presente política representa una falta, la cual puede seguir las medidas correspondientes en el Artículo 29 del Reglamento Interno de Trabajo de “Vale un Perú”.

POLITICA GENERAL DE SEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES

“Vale un Perú” es una Cooperativa de Ahorro y Crédito, principalmente enfocada en brindar soluciones financieras como Cuenta a Plazo Fijo, CTS, Cuenta de Ahorro. Con el fin de brindar apoyo a los militares peruanos retirados o en servicio.

“Vale un Perú” reconoce a la información como activo importante para la organización y con la finalidad de mantener su confidencialidad, integridad y disponibilidad, cuenta con un Sistema de Gestión de Seguridad de Información¹ (SGSI). En este sentido, la Gerencia General de “Vale un Perú” considera necesario proteger apropiadamente a los activos asociados a la información, de los posibles escenarios de riesgo dentro de una evaluación permanente de las amenazas a la que se encuentra expuesta. En este sentido, “Vale un Perú” garantiza la seguridad y confidencialidad en el tratamiento de los datos de carácter personal pertenecientes a sus bancos de datos de prospectos, clientes, colaboradores y proveedores; en conformidad con lo dispuesto en la Ley N° 29733, Ley de Protección de Datos Personales, su Reglamento y Directiva de Seguridad. “Vale un Perú” respeta los principios de protección de datos personales:

- ✓ Principio de legalidad
- ✓ Principio de consentimiento
- ✓ Principio de finalidad
- ✓ Principio de proporcionalidad
- ✓ Principio de calidad
- ✓ Principio de seguridad
- ✓ Principio de disposición de recurso
- ✓ Principio de nivel de protección adecuado

El Sistema de Gestión de Seguridad de la Información se basa en los siguientes lineamientos:

- ✓ Todos los colaboradores tienen la responsabilidad de garantizar la integridad, confidencialidad y disponibilidad de la información que producen o utilizan en el marco de sus competencias.
- ✓ Los datos personales (ej. de clientes) se pueden procesar únicamente al otorgar el consentimiento de la persona, quien, al brindarlo, otorga autorización previa, libre, expresa, informada e inequívoca a “Vale un Perú” para realizar el tratamiento y hace uso de la información personal que éste proporcione a “Vale un Perú”.

- ✓ Cada área en coordinación con el Encargado de seguridad de información debe proponer, diseñar y coordinar la implementación de los controles eficaces en sus procesos y actividades, manteniendo un equilibrio entre la productividad y la seguridad de la información.
- ✓ “Vale un Perú” ha adoptado las medidas técnicas, organizativas y legales necesarias que garanticen la seguridad y eviten la alteración, pérdida y tratamiento o acceso no autorizado a los datos personales.
- ✓ “Vale un Perú”, garantiza el ejercicio de los derechos de información, acceso, actualización, inclusión, tratamiento objetivo, rectificación, supresión, cancelación, oposición y revocación del consentimiento de los datos personales, los cuales serán ejercidos por el titular de los datos personales, en los términos establecidos en la Ley. Es decir, en cualquier momento, los clientes, colaboradores, prospectos y proveedores tendrán el derecho a solicitar a “Vale un Perú” el ejercicio de los derechos que le confiere la Ley.
- ✓ La Gerencia General debe aprobar los lineamientos del sistema de gestión de seguridad de la información, proveer los recursos necesarios para su implementación y verificar su efectividad.
- ✓ El encargado de seguridad de información debe supervisar la implementación y ejecución de los controles y políticas de seguridad de la información. Asimismo, gestionar los incidentes, así como capacitar y sensibilizar periódicamente al personal de la “Vale un Perú” en temas, métodos y herramientas de seguridad de la Información.

INSTRUCTIVO DE GESTIÓN DE ALTAS, MODIFICACIONES Y BAJAS DE ACCESOS

1. OBJETIVO

Definir las actividades, frecuencia, roles y responsables involucrados en los procedimientos de altas, modificaciones y bajas de accesos de los colaboradores de “Vale un Perú”.

2. ALCANCE

Considera la revisión de la correcta ejecución de los procedimientos de ingresos de colaboradores, las modificaciones de accesos a un colaborador de “Vale un Perú” (por modificaciones de puesto) y las bajas correspondientes al cese de vínculo laboral.

3. RESPONSABILIDADES

3.1. Encargado de seguridad de información:

- Autorizar los accesos a servicios de red y/o aplicaciones, carpetas compartidas, base de datos, accesos de conexión remota, entre otros.
- Revisar y validar cuentas asociadas con acceso a sistemas y/o carpetas compartidas de los usuarios activos y cesados.
- Solicitar las autorizaciones necesarias a los propietarios de los sistemas y/o carpetas compartidas.

3.2. Responsable de Recursos Humanos:

- Informar a las áreas responsables la lista de personal de ingreso de nuevos colaboradores y lista de personal cesado.
- Informar a las áreas responsables los cambios de puestos (movimientos internos o ascensos).

3.3. Responsable de Soporte TI:

- Generar la creación de cuentas de usuarios y contraseñas.
- Generar la baja de cuentas de usuarios.
- Bloquear las cuentas de usuario por inactividad, incidentes de seguridad u otros.
- Modificar el perfil de las cuentas de usuarios.
- Notifica término de atención de ticket al personal autorizado.

3.4. Operador TI:

- Genera ticket de requerimiento.
- Comunica el registro de ticket de requerimiento a Seguridad de la Información.

3.5. Gestor del Servicio:

- Comunicar su requerimiento a Mesa de Ayuda adjuntando los formatos correspondientes para solicitar los accesos.
- Valida atención del requerimiento solicitado.

4. DESCRIPCIÓN

4.1. GESTIÓN DE ALTAS

Proceso para las solicitudes de creación de cuentas para los nuevos colaboradores administrativos (personal con fines operativos).

I. Gestión de Alta Administrativa

- El Responsable de Recursos Humanos, envía comunicación vía correo electrónico al Operador TI para informar acerca del ingreso del nuevo colaborador adjuntando la Ficha de Alta de Accesos necesaria para la asignación de los accesos.
- Operador TI, recibe comunicación por parte del Responsable de Recursos Humanos y valida que la Ficha de Alta de Accesos este completa para proceder con la creación del ticket de requerimiento de alta de usuario en el Sistema de Administración de Requerimientos e Incidentes (iTop), posterior solicitará la aprobación por parte del Encargado de seguridad de información.
- Seguridad de la Información, valida en el ticket de requerimiento los datos conforme del nuevo colaborador para confirmación de Rol de Accesos. La aprobación del requerimiento tiene un plazo máximo de 1 día hábil después de haber sido asignado al Encargado de seguridad de información. Luego será derivado al Responsable de Soporte TI para su ejecución.
- Soporte TI, verifica la aprobación y accesos que debe tener el nuevo colaborador de acuerdo con el Rol de Accesos indicado en el requerimiento y procede a la creación de los accesos, finalizada la tarea comunica al jefe inmediato.

4.2. GESTIÓN DE MODIFICACIONES

Proceso para atención de las solicitudes de modificación de cuentas para los colaboradores en los siguientes escenarios:

I. Modificación de Usuario:

La modificación de usuario aplica en caso de asignación y/o retiro de roles y perfiles en sistemas, carpetas compartidas, entre otros para colaboradores activos en “Vale un Perú”.

- El Gestor de Usuario envía comunicación vía correo electrónico al Operador TI indicando las modificaciones de asignación o retiro de roles y perfiles, adjuntando el formato “Solicitud de Autorización de Accesos a Sistemas”.
- El Operador TI, recibe comunicación por parte de responsable y valida que el formato adjunto este completo para proceder con la creación del ticket de requerimiento de modificación de usuario en el Sistema de Administración de Requerimientos e Incidentes, posterior solicitará la aprobación por parte del área de Seguridad de la Información.
- Seguridad de la Información, valida el formato adjunto para solicitar las aprobaciones por parte de los propietarios de los sistemas, carpetas compartidas, entre otros. Posterior a la autorización por parte de los propietarios, el área de Seguridad de la Información aprueba el requerimiento. Cabe resaltar, que la aprobación tiene un plazo máximo de 3 día hábil después de haber sido asignado al área de Seguridad de la Información. Por último, el requerimiento es asignado al Responsable de Soporte TI.
- Soporte TI, valida los accesos que debe tener el usuario final que se desea modificar según el formato adjunto. Procede a la modificación de los accesos, finalizada la tarea comunica al personal responsable.

4.3. GESTIÓN DE BAJAS

Proceso de atención para las solicitudes de desactivación de cuentas de los colaboradores cesados.

I. Baja Definitiva:

- El Responsable de Recursos Humanos, envía comunicación vía correo electrónico al Operador TI con copia a las diferentes áreas involucradas incluido al Encargado de seguridad de información para comunicar acerca del cese del colaborador con el cuadro de datos necesarios para realizar la baja del usuario.
- Operador TI, recibe comunicación por parte del Responsable de Recursos Humanos y valida que la información este completa para proceder con la creación del ticket de requerimiento de baja parcial en el Sistema de Administración de Requerimientos e Incidentes, posterior asignará el requerimiento al Responsable de Soporte TI.

- Soporte TI, valida la cuenta de red y correo electrónico del colaborador cesado y ejecuta la desactivación de los accesos e informa la baja al Responsable de Recursos Humanos e Interesados.