

UNIVERSIDAD NACIONAL DE CAJAMARCA
FACULTAD DE INGENIERÍA

ESCUELA ACADÉMICO PROFESIONAL
DE INGENIERÍA DE SISTEMAS



TESIS

**“DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA
INFORMACIÓN (SGSI) PARA EDPYME CREDIVISIÓN, BASADO EN
LA NORMA ISO 27001:2013”**

PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTOR:

Bach. JORGE BURGA SEGOVIA

ASESOR:

Dr. Ing. EDWIN ALBERTO VALENCIA CASTILLO.

CAJAMARCA – PERÚ

2022

AGRADECIMIENTO

A mis padres y hermanos, por su trabajo y sacrificio que hicieron durante todos estos años y por alentarme a seguir adelante en cada etapa de mi vida.

A mi esposa e hijas quienes son mi motivación, brindando su apoyo en cada momento y poder cumplir un objetivo más.

A mi tía Ermila y su familia, quienes me apoyaron durante mi etapa universitaria.

A mi asesor y a todos los maestros que me enseñaron, gracias por sus conocimientos compartidos.

DEDICATORIA

Este trabajo realizado con mucho esfuerzo y sacrificio
está dedicado a mis hijas: Celeste y Camila
quienes son mi mayor motivación para seguir adelante y
poder llegar a ser un ejemplo para ellas.

CONTENIDO

CAPÍTULO I. INTRODUCCIÓN	11
CAPÍTULO II. MARCO TEÓRICO.....	14
2.1. ANTECEDENTES TEORICOS.....	14
2.1.1. Antecedentes Internacionales	14
2.1.2. Antecedentes Nacionales	15
2.2. BASES TEÓRICAS	16
2.2.1 Seguridad de la información.....	16
2.2.2 Estándares de Seguridad de la Información.....	17
2.2.2.1. Publicación especial del NIST 800	17
2.2.2.2. Cobit 5	18
2.2.2.3. Familia ISO	19
2.2.3 Metodologías de Gestión de Riesgos	20
2.2.4 Familia ISO 27000.....	25
2.2.5 ISO/IEC 27002 y su relación ISO/IEC 27001	32
2.2.6 Análisis de brechas de la seguridad de información.....	34
2.2.7 Gestión de riesgos en la seguridad de información.....	35
2.2.8 Política de seguridad	37
2.3. DEFINICIÓN DE TÉRMINOS BÁSICOS.....	37
CAPÍTULO III. MATERIALES Y MÉTODOS.....	40
3.1. PROCEDIMIENTO.....	40
3.1.1 Fase 1: Planificación.....	41
3.1.1.1. Plan de inicio del Proyecto.....	41
3.1.1.2. Registro de Interesados	43
3.1.2 Fase 2: Análisis.....	43
3.1.2.1. Análisis de la situación actual	43
3.1.2.2. Contexto de la empresa	54
3.1.2.3. Definir el alcance.....	59
3.1.3 Fase 3: Diseño.....	59
3.1.3.1. Política de la seguridad de información.....	59
3.1.3.2. Estructura Organizacional del SGSI.....	60
3.1.3.3. Metodología de evaluación de riesgos	62
3.1.3.4. Elaborar el plan de tratamiento de riesgos.....	75
3.1.3.5. Declaración de aplicabilidad (SOA).....	76
3.1.3.6. Plan de capacitación y concientización	77
3.1.3.7. Elaborar un plan de continuidad de negocio.....	82

3.1.3.8.	Elaborar un acuerdo de confidencialidad.....	82
3.1.3.9.	Elaborar el manual del SGSI.....	82
3.1.4	Fase 4: Pruebas.....	83
3.1.5	Fase 5: Cierre.....	83
3.2.	TRATAMIENTO Y ANÁLISIS DE DATOS Y PRESENTACIÓN DE RESULTADOS.....	83
3.2.1	Contrastación de la Hipótesis.....	84
3.2.2	Análisis de datos.....	87
3.2.3	Descripción de los métodos de validación para los objetivos.....	90
3.2.4	Descripción y ejecución de pruebas a realizar.....	92
3.2.2.1.	Prueba para indicador 1, según Objetivo Específico 1.....	92
3.2.2.2.	Prueba para indicador 2, según Objetivo Específico 2.....	97
3.2.2.3.	Prueba para indicador 3, según Objetivo Específico 3.....	100
3.2.2.4.	Prueba para indicador 4, según Objetivo Específico 4.....	103
3.2.2.5.	Prueba para indicador 5, según Objetivo Específico 5.....	106
3.2.5	Plan de Mejoras.....	109
CAPITULO IV.	ANÁLISIS Y DISCUSIÓN DE RESULTADOS.....	110
	DE LOS OBJETIVOS PLANTEADOS.....	110
	DE LOS ANTECEDENTES.....	111
CAPITULO V.	CONCLUSIONES Y RECOMENDACIONES.....	112
	CONCLUSIONES.....	112
	RECOMENDACIONES.....	113
ANEXOS.....		118
Anexo 1.	Alcance del SGSI.....	118
Anexo 2.	Políticas y Objetivos SGSI.....	119
Anexo 3.	Enfoque de análisis, evaluación y tratamiento de riesgos.....	120
Anexo 4.	Análisis, Evaluación y tratamiento de riesgos.....	121
Anexo 5.	Enunciado de Aplicabilidad.....	122
Anexo 6.	Plan de tratamiento de Riesgos.....	123
Anexo 7.	Carta de Autorización.....	124
Anexo 8.	Acta de constitución.....	125
Anexo 9.	Inventario de Activos de Información.....	126
Anexo 10.	Análisis de Riesgos.....	148
Anexo 11.	Tratamiento de riesgos.....	150
Anexo 12.	Declaración de Aplicabilidad.....	153
Anexo 13.	Plan de continuidad de negocio.....	162
Anexo 14.	Acuerdo de confidencialidad.....	168

Anexo 15. Manual del SGSI	171
Anexo 16. Valoración de los Expertos	177
Anexo 17. Evaluación de Encuestas.	181
Anexo 18. Análisis de Brechas.....	186

INDICE DE FIGURAS

Fig. 1 Integridad, Confidencialidad y Disponibilidad	17
Fig. 2 Principios de COBIT 5	19
Fig. 3 Ciclo de Deming	27
Fig. 4 Relación de Ciclo de Deming con ISO 27001	28
Fig. 5 Actividades del modelo PDCA.....	29
Fig. 6 Clausulas de la ISO 27001:2013.....	30
Fig. 7 Número de controles por cada Dominio del anexo A.....	33
Fig. 8 Cronograma de Actividades	42
Fig. 9 Análisis de Brechas por Dominio.....	53
Fig. 10 Nivel de Madurez de controles	54
Fig. 11 Organigrama Edpyme CREDIVISIÓN.....	55
Fig. 12 Etapas de desarrollo de un crédito.....	56
Fig. 13 Estructura Organizacional del SGSI	60
Fig. 14 Metodología de Riesgos	62
Fig. 15 Gráfico de Hipótesis	86
Fig. 16 Estado de Cumplimiento Inicial vs Estado Final	89
Fig. 17 Nivel de Madurez vs Controles.....	94
Fig. 18 Cumplimiento vs Capítulos	95
Fig. 19 Cumplimiento vs Clausulas.....	96
Fig. 20 Requisitos y Controles	96
Fig. 21 Activos de Información vs Porcentaje.....	99
Fig. 22 Riesgos Críticos vs Total.....	102
Fig. 23 Variación de Riesgos.....	105
Fig. 24 Personal con capacitación vs sin capacitación	108
Fig. 25 Personal aprobado vs desaprobado	108

INDICE DE TABLAS

Tabla N°1 Partes Interesadas	43
Tabla N°2 Nivel de madurez de Cobit.....	44
Tabla N°3 Personal Encuestado.....	45
Tabla N°4 Resultado de las Encuestas.....	45
Tabla N°5 Estado Actual de cumplimiento de Controles	52
Tabla N°6 Valorización de Activos	65
Tabla N°7 Dimensiones de la información	65
Tabla N°8 Valorización de Confidencialidad	66
Tabla N°9 Valorización de Integridad	66
Tabla N°10 Valorización de Disponibilidad	66
Tabla N°11 Valorización Total del Activo	67
Tabla N°12 Rango Aritmético para decimales.....	67
Tabla N°13 Tipo de Amenazas.....	69
Tabla N°14 Degradación de Confidencialidad.....	71
Tabla N°15 Degradación de Integridad.....	71
Tabla N°16 Degradación de Disponibilidad.....	72
Tabla N°17 Impacto del Riesgo	72
Tabla N°18 Riesgo Operacional.....	73
Tabla N°19 Valores de Probabilidad	73
Tabla N°20 Matriz de Riesgos.....	73
Tabla N°21 Valor de Matriz de Riesgos	74
Tabla N°22 Tratamiento de Riesgos	75
Tabla N°23 Costo Aproximado	76
Tabla N°24 Tiempo Aproximado.....	76
Tabla N°25 Cantidad de Controles Aplicables	77
Tabla N°26 Los recursos, competencias y concientización	78
Tabla N°27 Fases de entrenamiento.....	78
Tabla N°28 Plan de Capacitación	81
Tabla N°29 Procesamiento de datos	85
Tabla N°30 Cálculo de rangos	85
Tabla N°31 Cumplimiento Inicial de Clausulas	87
Tabla N°32 Nivel de Madurez Inicial de Controles.....	88
Tabla N°33 Cumplimiento Final de Clausulas	88
Tabla N°34 Nivel de Madurez Inicial de Controles.....	88
Tabla N°35 Valoración de expertos	89

Tabla N°36 Objetivos e indicadores de logro	90
Tabla N°37 Objetivo Específico 1	92
Tabla N°38 Objetivo Específico 2	97
Tabla N°39 Objetivo Específico 3	100
Tabla N°40 Resultados ALE.....	102
Tabla N°41 Objetivo Específico 4	103
Tabla N°42 Objetivo Específico 5	106
Tabla N°43 Fases de la Continuidad del Negocio	164

RESUMEN

El presente trabajo de tesis tiene como objetivo Diseñar un Sistema de Gestión de Seguridad de Información (SGSI) asociado al proceso de Créditos de la Edpyme CREDIVSIÓN, para el diseño se utiliza los procedimientos y lineamientos indicados en la norma internacional ISO/IEC 27001 en su versión 2013 y los controles de seguridad asociados en el Anexo A de la misma. Se detallan actividades para una correcta implementación del antes mencionado Sistema para la referida empresa. Se destaca la priorización de la sensibilización de su recurso humano en la importancia de salvaguardar la información que manejan en sus diferentes actividades laborales. El diseño del referido Sistemas identifica 226 activos de información, y 106 activos críticos que interactúan en el proceso de créditos; también, se identifican por cada activo sus amenazas y vulnerabilidades y los agentes que lo provocan. En base la matriz de riesgos se identifican 23 riesgos críticos para lo que se propone plan de tratamiento de riesgos tomando como base la declaración de aplicabilidad (SOA) del anexo A, para tal caso se identifican 93 controles que aplican y reducen la probabilidad y el impacto del riesgo alineados a los objetivos de negocio, para la mejora de la disponibilidad, confidencialidad e integridad del proceso de créditos. Para contrastar la hipótesis se utiliza la prueba T Wilcoxon cuyos resultados son: 4.5355, valor mayor que la toma decisión:1.645, concluyendo así que el diseño de un sistema de gestión de la seguridad de la información basado en la Norma ISO 27001:2013 aplicado a Edpyme CREDIVSIÓN permite mejorar la confidencialidad, integridad y disponibilidad en el proceso de créditos.

Palabras Clave: Sistema de Gestión de Seguridad de Información; activos de información; proceso de créditos; plan de tratamiento de riesgo; ISO/IEC 27001.

ABSTRACT

The objective of this thesis work is to Design an Information Security Management System (ISMS) associated with the Credit process of Edpyme CREDIVSIÓN, for the design the procedures and guidelines indicated in the international standard ISO/IEC 27001 are used in its version 2013 and the associated security controls in Annex A thereof. Activities are detailed for a correct implementation of the aforementioned System for the aforementioned company. The prioritization of the awareness of its human resources on the importance of safeguarding the information they handle in their different work activities is highlighted. The design of the aforementioned Systems identifies 226 information assets, and 106 critical assets that interact in the credit process; Also, their threats and vulnerabilities and the agents that cause them are identified for each asset. Based on the risk matrix, 23 critical risks are identified for which a risk treatment plan is proposed, based on the statement of applicability (SOA) of annex A, for this case, 93 controls are identified that apply and reduce the probability and risk. risk impact aligned to business objectives, to improve the availability, confidentiality and integrity of the credit process. To contrast the hypothesis, the Wilcoxon T test is used, the results of which are: 4.5355, a value greater than the decision making: 1.645, thus concluding that the design of an information security management system based on the ISO 27001:2013 Standard applied Edpyme CREDIVSIÓN improves confidentiality, integrity and availability in the credit process..

Keywords: Information Security Management System; information assets; credit process; risk treatment plan; ISO/IEC27001.

CAPÍTULO I. INTRODUCCIÓN

El trabajo remoto evidencia la gran dependencia tecnológica que se tiene en la actualidad. Sin embargo, existen empresas poco preparadas a nivel técnico que carecen de una infraestructura TI de calidad o, por el contrario, cuentan con las mejores herramientas de seguridad, pero no capacitan a sus empleados en un uso seguro y correcto de las soluciones a disposición. Sin duda se debe llegar a un equilibrio en donde el elemento humano en la seguridad cibernética sea tan importante como el técnico. [1]. Los bancos, con el cierre y la limitación de algunos canales físicos, se han visto obligados a mejorar sus canales digitales como alternativas para llevar a cabo acciones mientras garantizan la calidad del servicio, refuerzan la seguridad de la información, evitan saturaciones o caídas en los sistemas como consecuencia del aumento en banca en línea. [2]

Según precisó la SBS, el sistema financiero cuenta con 54 empresas que son supervisadas hace 90 años y que incorpora a múltiples empresas financieras, cajas municipales, cajas rurales y Edpyme. La superintendente detalló que el 97.5% del sistema financiero está representado por estas empresas supervisadas. [3]. La SBS supervisa mediante la Circular G-140-2009, cuya finalidad es establecer criterios mínimos para una adecuada gestión de la seguridad de la información; la cual resulta necesario actualizar la normativa sobre gestión de seguridad de la información vía la aprobación de un reglamento, complementario al Reglamento para la Gestión del Riesgo Operacional, tomando en cuenta los estándares y buenas prácticas internacionales sobre seguridad de la información, entre los que se encuentran los publicados por el National Institute of Standards and Tecnología y la familia de estándares ISO/IEC. La SBS aprueba el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, que entra en vigencia el 1 de julio de 2021, fecha en la que se deroga la Circular G 140-2009, con excepciones que se complementan en el año 2022 [4]

La EDPYME CREDIVISIÓN ha sido creada por iniciativa de dos entidades de desarrollo: World Visión International WVI y la Asociación para el Desarrollo Económico del Perú ASODECO PERU. Mediante Resolución SBS No.413-2000 del 13 de junio del 2000 se autoriza el funcionamiento como una empresa del Sistema Financiero y luego inició sus operaciones el 17 de Julio del mismo año. Mediante Resolución SBS N° 5905-2013, el 27 de setiembre de 2013 se aprobó el aumento de capital social de EDPYME CREDIVISIÓN, siendo el capital social a favor de VisionFund International 96.1% y a favor de Asodeco 3.9%. [5]. La Edpyme cuenta con un sistema Core llamado SISGO, que es un sistema integrado de gestión que abarca entre los procesos importantes: créditos y personal, donde se guarda

información de clientes y del personal, sin embargo, no cuenta con los controles de acceso y medidas de procedimientos de seguridad necesarios para resguardar sus activos de información, estando expuestos a diversas amenazas.

Según auditoría realizada en noviembre del 2021 a EDPYME CREDIVISIÓN y con la finalidad de dar cumplimiento a las actividades programadas requeridas por la SBS, el resultado del informe fue: **Deficiencia en la Gestión de Seguridad de la Información y Ciberseguridad**. Indicando deficiencias tales como:

- i. Políticas y Lineamientos no vigentes para el SGSI
- ii. Inventario de Activos de Información desactualizado y no clasificado.
- iii. No cuenta con la definición de la segregación de funciones y áreas de responsabilidad para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.
- iv. La política de control de accesos de la compañía no considera el requisito de una evaluación previa de seguridad de la información para los casos de modificación de accesos de usuarios y está desactualizada al año 2017.
- v. Inadecuado procedimiento de gestión de bajas de usuarios, se mantiene las cuentas activas de colaboradores cesados por un plazo mayor a lo recomendado.
- vi. No cuenta ni ejecuta controles de monitoreo periódico de la gestión de accesos (cuentas activas, altas, bajas y modificaciones) sobre las cuentas nominales y privilegiadas en el sistema, base de datos y sistemas operativos para el periodo en revisión
- vii. No ha definido políticas y procedimientos para la seguridad de la información en las comunicaciones

La Edpyme CREDIVISIÓN presenta deficiencia en sus procesos en cuanto a los principios de seguridad de la información (confidencialidad, integridad y disponibilidad), además no está cumpliendo con la circular G-140, que es una directiva de la Superintendencia SBS, la cual establece requisitos mínimos de seguridad de la información

Ante el problema mencionado surge el presente proyecto de investigación, que trata de determinar ¿Cómo mejorar la gestión de la Seguridad de la información mediante un SGSI aplicando la ISO 27001:2013 en la Edpyme Credivisión?, con la finalidad de contestar a ésta pregunta se plantea el objetivo general del proyecto que propone un diseño de un Sistema de Gestión de Seguridad de la Información para la EDPYME CREDIVISIÓN, basado en la norma ISO 27001:2013, que permita asegurar la confidencialidad, integridad y disponibilidad

de los procesos; así mismo se plantean los objetivos específicos: valorizar los activos de información que soportan el proceso de créditos de la institución, identificar los riesgos de seguridad de la información que afectan al proceso de créditos, elaborar un plan que permita realizar un adecuado tratamiento de los riesgos, determinar el estado de cumplimiento actual de la empresa con respecto al anexo A de la norma ISO 27001:2013 y elaborar un plan que permita desarrollar e implementar los requisitos y controles de la norma ISO 27001:2013. A través del presente proyecto de investigación se pretende demostrar la hipótesis de que el diseño de un sistema de gestión de la seguridad de la información basado en la Norma ISO 27001:2013 aplicado a la Edpyme Credivisión, permitirá mejorar la confidencialidad, integridad y disponibilidad de los procesos.

La presente investigación se justifica ante la necesidad de mejorar la gestión de la seguridad de la información que según la auditoria ultima es deficiente en la Edpyme Credivisión, y además no está alineada con la circular G-140 -2009. En base a las deficiencias señaladas, se ha considerado necesaria la adopción de un diseño de Sistema de Gestión de la Seguridad de la Información (SGSI), base de la norma ISO/IEC 27001 :2013 para la Edpyme. El cual dentro de sus procedimientos y lineamientos internos permitan asegurar la confidencialidad, integridad y disponibilidad de la información de esta.

El proyecto se encuentra estructurado en cinco capítulos de la siguiente manera: el Capítulo I, se realiza una introducción del proyecto donde se menciona el problema, hipótesis general y específicas y la justificación o importancia de la investigación; el Capítulo II, describe las investigaciones que anteceden a la presente investigación y ayudarán a justificarla, además se conceptualizan las bases teóricas que respaldan el proyecto de investigación, asimismo se encontrará la definición de términos básicos que ayudan a entender la terminología utilizada; el Capítulo III, describe la ubicación donde se realizó la investigación; así como el procedimiento, tratamiento, análisis de datos y presentación de resultados; en el Capítulo IV, se muestra el análisis y discusión de los resultados obtenidos mediante el diseño del sistema de gestión de seguridad de la información que sirven para realizar la contrastación de la hipótesis y por el ultimo el Capítulo 5, se menciona las conclusiones y recomendaciones a las que se llega al finalizar el presente proyecto de tesis.

CAPÍTULO II. MARCO TEÓRICO

2.1. ANTECEDENTES TEORICOS

2.1.1. Antecedentes Internacionales

- ✓ Carlos Alberto Guzmán Silva en su proyecto de grado “Diseño de Un Sistema de Gestión de Seguridad de la Información” para una entidad financiera de segundo piso, menciona que la norma ISO/IEC 27001:2013, es una herramienta de gran ayuda que permite identificar los diferentes aspectos que se deben tener en cuenta cuando las organizaciones deciden establecer un modelo de seguridad de la información, ya que si las organizaciones logran cumplir al pie de la letra lo establecido, podrán llegar a forjar en el tiempo un adecuado y sostenible Sistema de Gestión de Seguridad de la Información, aunque dicha labor depende del tamaño y naturaleza de la entidad y de la cultura de la misma en torno a la seguridad de la información. Esta labor debe comenzar con el compromiso demostrable de la alta directiva y partes interesadas donde tienen un interés alto (82%) y un grado de motivación alta (70%) en que la entidad tenga un adecuado sistema de gestión de seguridad para así proteger la información del negocio y de sus clientes. El apoyo de la alta directiva, es indispensable para poder concebir un modelo de Seguridad de la Información que realmente apoye y apalanque la misión y visión de la organización, el cual es fundamental que se tenga antes de comenzar a diseñar un Sistema de Gestión de Seguridad de la Información, ya que si éste no se logra conseguir, es casi seguro que cualquier iniciativa de seguridad que se pretende adelantar, no alcancen los resultados esperados y si por el contrario, genere el rechazo o el poco apoyo o interés por parte de la organización. [6]

- ✓ Luis Paolo Tapia Montoya en su proyecto de Maestría “Metodología para la integración de la norma ISO/IEC 27001:2013 en una empresa industrial naviera” en la Universidad Nacional de Buenos Aires, afirma para el inicio del proyecto de implementación de un SGSI, es necesario el apoyo integral de la Gerencia General y el compromiso del personal responsable de los activos de información, una vez que el SGSI es implementado en el proceso de negocio, resulta aconsejable extenderlo a los demás procesos de la empresa, en función de su criticidad para el negocio, para incrementar el nivel de defensa de la organización frente a posibles amenazas internas y externas. Se recomienda

fuertemente la revisión periódica del SGSI y la incorporación de nuevos controles, en función a la adquisición de nuevas plataformas o componentes de hardware y software, así como su evaluación y mantenimiento periódicos. Se debe preservar toda evidencia y hallazgos sobre los riesgos informáticos para conservar el historial de gestión y responder ante una auditoría externa del SGSI, además se debe implementar un plan de continuidad del negocio y adiestrar al personal, tanto de aquel que se encargará de la operación informática como del resto de los empleados de la organización que se encuentren involucrados en el proceso. En otras palabras, resulta necesario un programa corporativo de capacitación en seguridad en la información que involucre a todo el personal e incluya también a terceros vinculados a los procesos de la empresa. [7]

2.1.2. Antecedentes Nacionales

- ✓ Jaime Fernando Vásquez Escalante, en su proyecto de tesis “Implementación del sistema de gestión ISO 27001:2013, para proteger la información en los procesos de TI” de la Universidad Nacional de San Marcos, plantea que se debe revisar periódicamente las políticas de seguridad de la información para verificar que estén alineadas a los objetivos del negocio, además se deben realizar pruebas periódicas para identificar los controles que aplicarían antes posibles escenarios que atenten contra la información. Se recomienda contar con una bitácora para almacenar los eventos, riesgos e incidentes de seguridad de la información a fin de recolectar evidencias (lecciones aprendidas), en el cual se describan las acciones tomadas y mejoras en los mismos, con el objetivo de prevenir que dichos sucesos vuelvan a ocurrir. Menciona que el sistema de gestión de seguridad de la información no solo aplica para organización que brinden servicios de TI, sino para cualquier empresa (grande o pequeña) y de cualquier rubro (pesquero, industria, público, privado, etc.) que quiera implementar controles para proteger su información. La implementación depende de las necesidades de la organización y del análisis GAP (Brechas) con un cumplimiento inicial de las cláusulas y controles en un 46%, luego de la implementación de controles preventivos, correctivos y/o detectivos se obtuvo una mejora significativa del 86%. Cabe resaltar que la norma ISO/IEC 27001:2013 te indican que es aquello que se debe controlar, pero no indica el cómo; por lo que esto depende de la organización. Todas las empresas que

cuenten con un SGSI implementado, se les recomienda que el enfoque de su SGSI se encuentre alineado con las necesidades y objetivos del negocio. [8]

2.2. BASES TEÓRICAS

Se ha realizado un estudio de los conceptos relacionados con la gestión de seguridad de la información y los marcos legales que ayudan a proteger los activos de información de las organizaciones que serán de utilidad para el desarrollo del tema mencionado.

2.2.1 Seguridad de la información

La seguridad de la información es el conjunto de medidas y técnicas utilizadas para controlar y salvaguardar todos los datos que se manejan dentro de la organización y asegurar que los datos no salgan del sistema que ha establecido la organización. Es una pieza clave para que las empresas puedan llevar a cabo sus operaciones, ya que los datos que maneja son esenciales para la actividad que desarrollan. El principal fin que persigue la norma ISO 27001 es la protección de los activos de información, es decir, equipos, usuarios e información, la cual cuenta con tres aspectos fundamentales Integridad, confidencialidad y disponibilidad, ver figura 1. [9]

Integridad: Es decir, que la información se muestra tal y como fue concebida, sin alteraciones o manipulaciones que no hayan sido autorizadas de forma expresa.

Confidencialidad: La confidencialidad garantiza que solo las personas o entidades autorizadas tendrán acceso a la información y datos recopilados y que estos no se divulgarán sin el permiso de forma correspondiente.

Disponibilidad: En este aspecto se garantiza la información que se encuentra disponible en todo momento para todas las personas o entidades autorizadas para su manejo y conocimiento. [9]



Fig. 1 Integridad, Confidencialidad y Disponibilidad

2.2.2 Estándares de Seguridad de la Información

2.2.2.1. Publicación especial del NIST 800

La serie NIST SP 800 es un conjunto de documentos de libre descarga que se facilita desde el gobierno federal de los estados unidos, que describe las políticas de seguridad informática, procedimientos y directrices, que son publicadas por el Instituto Nacional de Estándares y Tecnología, que contiene 130 documentos.

Para realizar la evaluación de los riesgos, la serie SP 800 tiene un conjunto de documentos que han sido creados utilizando la metodología de riesgo en seis pasos:

- i. **Categorizar:** se debe dar prioridad a los sistemas de información que se basan en la evaluación del impacto. El detalle se encuentra en el documento SP 800-60.
- ii. **Seleccionar:** se deben definir los controles que se deben aplicar, en base a la evaluación del impacto y las bases de SP 800-53, siendo un documento de referencia para este paso.
- iii. **Poner en práctica:** implementar los controles y la elaboración de los documentos. El detalle se encuentra en el documento SP 800-160.
- iv. **Evaluar:** la confirmación de que los controles se implantan de forma correcta, operar según lo previsto, y producir los resultados deseados. El detalle se puede encontrar en el documento SP 800-53.

- v. **Autorizar:** la aceptación del escenario de riesgo, y la autorización para la operación de los sistemas de información y utilización. El detalle se encuentra en el documento SP 800-37.
- vi. **Monitorear:** se acompaña de forma continua de los sistemas de información y el entorno operativo para establecer la eficiencia y el cumplimiento de los controles. El detalle se encuentra en el documento SP 800-137. [10]

2.2.2.2. Cobit 5

COBIT fue creado para ayudar a las organizaciones a obtener el valor óptimo de TI manteniendo un balance entre la realización de beneficios, la utilización de recursos y los niveles de riesgo asumidos. COBIT 5 posibilita que TI sea gobernada y gestionada en forma holística para toda la organización, tomando en consideración el negocio y áreas funcionales de punta a punta, así como los interesados internos y externos. COBIT 5 se puede aplicar a organizaciones de todos los tamaños, tanto en el sector privado, público o entidades sin fines de lucro. [11]

Este marco de trabajo cuenta con cinco principios que una organización debe seguir para adoptar la gestión de TI, según figura 2:

- i. **Satisfacción de las necesidades de los accionistas:** se alinean las necesidades de los accionistas con los objetivos empresariales específicos, objetivos de TI y objetivos habilitadores. Se optimiza el uso de recursos cuando se obtienen beneficios con un nivel aceptable de riesgo.
- ii. **Considerar la empresa de punta a punta:** el gobierno de TI y la gestión de TI son asumidos desde una perspectiva global, de tal modo que se cubren todas las necesidades corporativas de TI. Esto se aplica desde una perspectiva "de punta a punta" basada en los 7 habilitadores de COBIT.
- iii. **Aplicar un único modelo de referencia integrado:** COBIT 5 integra los mejores marcos de Information System Audit and Control Association (ISACA) como Val IT, que relaciona los procesos de COBIT con los de la gerencia requeridos para conseguir un buen valor de las inversiones en TI. También se relaciona con Risk IT, lanzado por ISACA para ayudar a organizaciones a equilibrar los riesgos con los beneficios.
- iv. **Posibilitar un enfoque holístico:** los habilitadores de COBIT 5 están identificados en siete categorías que abarcan la empresa de punta a punta.

Individual y colectivamente, estos factores influyen para que el gobierno de TI y la gestión de TI operen en función de las necesidades del negocio.

- v. **Separar el gobierno de la gestión:** COBIT 5 distingue con claridad los ámbitos del gobierno de TI y la gestión de TI. Se entiende por gobierno de TI las funciones relacionadas con la evaluación, la dirección y el monitoreo de las TI. El gobierno busca asegurar el logro de los objetivos empresariales y también evalúa las necesidades de los accionistas, así como las condiciones y las opciones existentes. [12]



Fig. 2 Principios de COBIT 5

COBIT es empleado en todo el mundo por quienes tienen como responsabilidad primaria los procesos de negocio y la tecnología, aquellos de quien depende la tecnología y la información confiable, y los que proveen calidad, confiabilidad y control de TI. COBIT 5 se basa en el gobierno de TI y el gobierno Corporativo. [11]

2.2.2.3. Familia ISO

Las normas ISO se constituyen en una serie de Estándares que se agrupan por familias, según los distintos aspectos relacionados con la calidad. Aunque existen más de 18000 normas publicadas por ISO, se resaltan las más importantes en cuanto a su aplicación y relevancia de los sectores. [13]

Estas normas tienen carácter voluntario y están enfocadas a coordinar la gestión de la empresa. Entre las principales se tienen:

- i. **ISO 9000** normativa sobre calidad y gestión de la calidad. ISO 9001 es la norma certificable de la familia de normas 9000
- ii. **ISO 14000** normas sobre gestión de medio ambiente que fomenta y cuida la producción minimizando los posibles impactos ambientales. ISO 14001
- iii. **ISO 31000** normas sobre gestión del riesgo.
- iv. **ISO 27001** seguridad de la Información.
- v. **ISO 45001** normas sobre prevención de riesgos laborales y seguridad en el trabajo.
- vi. **ISO 22000** normas sobre la seguridad alimentaria enfocadas hacia la inocuidad de los alimentos.

Las normas ISO pretenden estandarizar las normas de productos y servicios y fueron elaboradas con el objetivo principal de aportar orientación, coordinación y unificación de criterios a las empresas y organizaciones. Implantando los sistemas de gestión correspondientes, dependiendo del sector, las empresas pueden minimizar costes y potenciar la productividad. [14]

2.2.3 Metodologías de Gestión de Riesgos

Existen muchas metodologías para poder analizar los riesgos de seguridad asociados con pérdidas, modificación e interrupción de la información utilizada por la organización. A continuación, se mencionarán algunos de las metodologías de gestión de riesgos usadas en el mercado.

2.2.3.1. ISO 27005

Es el estándar internacional que se ocupa de la gestión de riesgos de seguridad de información. La norma suministra las directrices para la gestión de riesgos de seguridad de la información en una empresa, apoyando particularmente los requisitos del sistema de gestión de seguridad de la información definidos en ISO 27001.

ISO-27005 es aplicable a todo tipo de organizaciones que tengan la intención de gestionar los riesgos que puedan complicar la seguridad de la información de su organización. No recomienda una metodología concreta, dependerá de una serie de factores, como el alcance real del Sistema de Gestión de Seguridad de la Información (SGSI), o el sector comercial de la propia industria.

Los usuarios elijen el método que mejor se adapte para, por ejemplo, una evaluación de riesgos de alto nivel seguido de un análisis de riesgos en profundidad sobre las zonas de alto riesgo. Las secciones de contenido son:

- ✓ Prefacio.
- ✓ Introducción.
- ✓ Referencias normativas.
- ✓ Términos y definiciones.
- ✓ Estructura.
- ✓ Fondo.
- ✓ Descripción del proceso de ISRM.
- ✓ Establecimiento Contexto.
- ✓ Información sobre la evaluación de riesgos de seguridad (ISRA).
- ✓ Tratamiento de Riesgos Seguridad de la Información.
- ✓ Admisión de Riesgos Seguridad de la información.
- ✓ Comunicación de riesgos de seguridad de información.
- ✓ Información de seguridad Seguimiento de Riesgos y Revisión.
- ✓ Anexo A: Definición del alcance del proceso.
- ✓ Anexo B: Valoración de activos y evaluación de impacto.
- ✓ Anexo C: Ejemplos de amenazas típicas.
- ✓ Anexo D: Las vulnerabilidades y métodos de evaluación de la vulnerabilidad.
- ✓ Enfoques ISRA: Anexo E.

Se trata de un estándar que cuenta con una parte principal concentrada en 24 páginas, también cuenta con anexos en los que se incluye ejemplos y más información de interés para los usuarios.

En estos anexos se encuentran tabulados amenazas, vulnerabilidades e impactos, lo que puede resultar útil para abordar los riesgos relacionados con los activos de la información en evaluación. [15]

2.2.3.2. NIST SP 800-30

La clave de dicha metodología es el uso de categorías para clasificar la información según el nivel de riesgo y estándares para asegurar la información apropiada a su nivel. Este método nació en el Instituto Nacional de Estándares y Tecnología. Fue fundado para evaluar los riesgos de seguridad de la información especialmente en sistemas TI (Tecnología de la Información) con

el objetivo de apoyar a las organizaciones con todo lo relacionado a Tecnología. [16]

Los procesos de gestión del riesgo introducen:

- ✓ Estructura del riesgo
- ✓ Evaluación del riesgo
- ✓ Responder a los riesgos
- ✓ Seguimiento de los riesgos

Para los procesos de análisis de riesgos, la metodología NIST SP800-30 está compuesta por nueve fases:

- i. **Caracterización del sistema:** nos permite establecer el alcance y los límites operacionales de la evaluación de riesgos en la empresa.
- ii. **Identificación de amenazas:** es donde se definen las diferentes fuentes de motivación de éstas. Para ello, se debería revisar el historial de ataques, datos de agencias de inteligencia, datos de medios de comunicación. Aquí se busca introducción de virus en los sistemas, corrupción de datos o incumplimientos legales intencionados.
- iii. **Identificación de vulnerabilidades:** para su identificación se desarrolla una lista de defectos o debilidades para conocer las posibles intrusiones de una amenaza. Un ejemplo puede ser: personal sin la adecuada información, la inexistencia de software antivirus, falta de políticas de restricciones de personal para uso de licencias de software.
- iv. **Análisis de controles:** analizar controles actuales y controles planificados, además de elaborar la lista correspondiente. Para entenderlo mejor, un ejemplo de esto puede ser: el control del número de personas que tiene acceso al equipo informático diariamente, registro de información confidencial para la que se requiere uso de contraseñas, etc.
- v. **Determinación de probabilidades.** Conocer a través del estudio cuales son las motivaciones para los ataques, capacidad de las amenazas, naturaleza de las vulnerabilidades... así poder elaborar el ranking de probabilidades de que materialice la amenaza.
- vi. **Análisis del impacto.** En dicha fase de determinación del riesgo, se pretende evaluar el riesgo real en el sistema de información, recomendaciones de control donde se proporcione qué controles se podrían mitigar el riesgo identificado disminuyendo hasta un nivel aceptable.

- vii. **Determinación del riesgo.** Para hacer un plan completo se debe conocer qué probabilidad de explotación de las amenazas, magnitud de los impactos, adecuación de los controles actuales y planificados se encuentra con dicho análisis estableceremos qué nivel de riesgo tiene la organización pudiendo ser: bajo, medio o alto.
- viii. **Recomendación de controles.** Para tener un sistema seguro se debe realizar revisiones de las políticas de seguridad, actualizaciones periódicas del antivirus, un cambio de contraseñas periódicas, instalación de firewalls o en caso de incumplimiento de la normativa vigente, sanciones.
- ix. **Documentación de resultados:** Según los riesgos de la organización proceder a la elaboración de un informe detallado de valoración de los riesgos. [16]

La finalidad de la metodología NIST SP800-30 es: suministrar una base para el desarrollo de la gestión del riesgo y suministrar información acerca de controles de seguridad en función de la rentabilidad del negocio.

2.2.3.3. Magerit

Es una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para de esta forma implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados. Además de esto, cuenta con todo un documento que reúne técnicas y ejemplos de cómo realizar el análisis de riesgos.

Puntualmente MAGERIT se basa en analizar el impacto que puede tener para la empresa la violación de la seguridad, buscando identificar las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas.

Lo interesante de esta metodología, es que presenta una guía completa y paso a paso de cómo llevar a cabo el análisis de riesgos.

Esta metodología está dividida en tres libros.

- ✓ **El primero** de ellos hace referencia al Método, donde se describe la estructura que debe tener el modelo de gestión de riesgos. Este libro está de acuerdo con lo que propone ISO para la gestión de riesgos.
- ✓ **El segundo** libro es un Catálogo de Elementos, el cual es una especie de inventario que puede utilizar la empresa para enfocar el análisis de riesgo. Es así como contiene una división de los activos de información que deben considerarse, las características que deben tenerse en cuenta para valorar los activos identificados y además un listado con las amenazas y controles que deben tenerse en cuenta.
- ✓ **Finalmente, el tercer** libro es una Guía de Técnicas, lo cual lo convierte en un factor diferenciador con respecto a otras metodologías. En esta tercera parte se describen diferentes técnicas frecuentemente utilizadas en el análisis de riesgos. Contiene ejemplos de análisis con tablas, algoritmos, árboles de ataque, análisis de costo beneficio, técnicas gráficas y buenas prácticas para llevar adelante sesiones de trabajo para el análisis de los riesgos.

Esta metodología es muy útil para aquellas empresas que inicien con la gestión de la seguridad de la información, pues permite enfocar los esfuerzos en los riesgos que pueden resultar más críticos para una empresa, es decir aquellos relacionados con los sistemas de información. Lo interesante es que al estar alineado con los estándares de ISO es que su implementación se convierte en el punto de partida para una certificación o para mejorar los sistemas de gestión. [17]

2.2.3.4. Metodología de Análisis de Riesgos que Aplicar

Para el desarrollo de la metodología se utilizó la misma metodología que usa la Edpyme la cual cumple con los lineamientos de la ISO/IEC 27001:2005 (artículo 4.2.1 c, d, e, f, y g), donde indica que se debe contemplar la identificación de activos, su importancia, las amenazas, vulnerabilidades, probabilidad e impacto, además de definir los criterios de riesgos aceptables.

La metodología de Gestión del Riesgo está dividida en 4 partes:

- i. Inventario de Activos de Información.
- ii. Análisis del Riesgo (al que están expuestos los activos de información).
- iii. Evaluación del Riesgo.
- iv. Opción de Tratamiento del Riesgo.

La información es recopilada usando la metodología de Delphi (talleres y encuestas).

2.2.4 Familia ISO 27000

Son un conjunto de estándares creados y gestionados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrónica Internacional (IEC). Ambas organizaciones internacionales están participadas por multitud de países, lo que garantiza su amplia difusión, implantación y reconocimiento en todo el mundo. Las series 27000 están orientadas al establecimiento de buenas prácticas en relación con la implantación, mantenimiento y gestión del Sistema de Gestión de Seguridad de la Información (SGSI).

Estas guías tienen como objetivo establecer las mejores prácticas en relación con diferentes aspectos vinculados a la gestión de la seguridad de la información, con una fuerte orientación a la mejora continua y la mitigación de riesgos. Comprende: [18]

- **ISO 27001**

Especifica los requerimientos necesarios para implantar y gestionar un SGSI. Esta norma es certificable.

- **ISO 27002**

Define un conjunto de buenas prácticas para la implantación del SGSI, a través de 114 controles, estructurados en 14 dominios y 35 objetivos de controles.

- **ISO 27003**

Proporciona una guía para la implantación de forma correcta un SGSI, centrándose en los aspectos importantes para realizar con éxito dicho proceso.

- **ISO 27004**

Proporciona pauta orientadas a la correcta definición y establecimiento de métricas que permitan evaluar de forma correcta el rendimiento del SGSI.

- **ISO 27005**

Define como se debe realizar la gestión de riesgos vinculados a los sistemas de gestión de la información orientado en cómo establecer la metodología a emplear.

- **ISO 27006**

Establece los requisitos que deben cumplir aquellas organizaciones que quieran ser acreditadas para certificar a otras en el cumplimiento de la ISO/IEC-27001. Entre otros [18]

2.2.4.1. ISO 27001

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

A la hora de implementar un Sistema de Gestión de Seguridad de la Información basado en el estándar internacional ISO 27001, se utiliza el ciclo PDCA (siglas en inglés) o PHVA (siglas en español); como se muestra en la figura 3.



Fig. 3 Ciclo de Deming

Planificar: Consiste en planificar acciones para hacer frente a los riesgos e identificar las oportunidades, para posteriormente evaluarlas y gestionarlas.

- ✓ Definir las políticas de seguridad de la información
- ✓ Establecer el alcance del SGSI
- ✓ Realizar el análisis de riesgo
- ✓ Seleccionar los controles de seguridad
- ✓ Definir competencias
- ✓ Establecer el mapa de riesgos
- ✓ Definir autoridades y responsabilidades

Actuar: Indica que la organización debe de disponer los recursos necesarios para establecer, implementar y mantener el SGSI, además de dar a conocer las políticas de seguridad de la información del SGSI.

- ✓ Poner en marcha el Plan de gestión de riesgos establecido
- ✓ Se implanta el SGSI
- ✓ Se establecen los controles de seguridad

Verificar: Se debe tener procedimientos y rutinas establecidos para medir el desempeño del proceso y políticas del SGSI, informando los resultados para su pronta revisión.

- ✓ Revisar internamente el SGSI
- ✓ Realizar auditorias
- ✓ Se revisan los indicadores y métricas del SGSI

Hacer: Se toman acciones correctivas y preventivas para reaccionar ante amenazas, vulnerabilidades y riesgos, que nos garanticen en todo momento la seguridad y protección de la información, basados en los resultados de la auditoría interna del SGSI.

- ✓ Realizan las acciones correctivas
- ✓ Realizan las acciones preventivas [19]

La siguiente figura 4 se muestra la relación de cada etapa con los puntos de la ISO/IEC 27001.



Fig. 4 Relación de Ciclo de Deming con ISO 27001

Para una implementación exitosa de un SGSI, es necesario hacer un mapeo detallado de las actividades de cada fase del modelo PDCA, además de los entregables exigidos por la norma ISO/IEC 27001:2013, en la figura 5, se especifica las principales actividades que indica las fases del ciclo de Deming.

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

Fig. 5 Actividades del modelo PDCA

Estructura de la Norma ISO/IEC 27001:2013

El anexo A de la norma ISO/IEC 27001 se menciona 10 cláusulas, siendo las cláusulas del 4 al 10 obligatorias para cumplir con la norma, tal como se muestra en la figura 6.

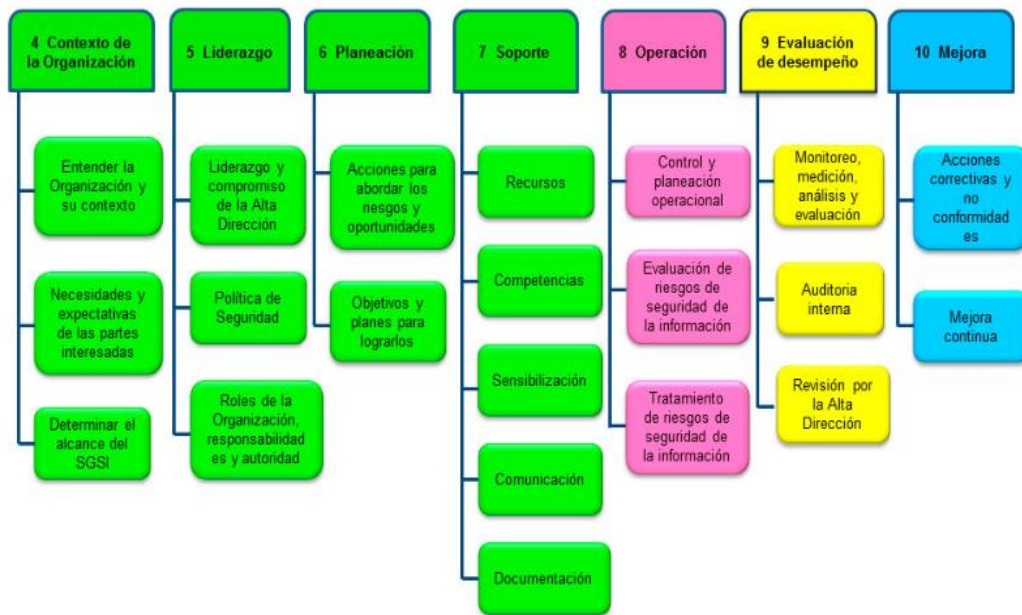


Fig. 6 Cláusulas de la ISO 27001:2013

A continuación, se detalla cada una de las cláusulas: [20]

- **Clausula 4. Contexto de la organización:** En este apartado se hace hincapié en la identificación de los problemas externos e internos que engloban a la empresa.
- **Clausula 5. Liderazgo** Se tiene que ajustar a la relación y la responsabilidad que tiene la alta dirección con respecto al Sistema de Gestión de Seguridad de la Información, por lo que se puede destacar de forma esporádica cómo se debe demostrar el compromiso, por ejemplo:
 - ✓ Garantizar que se cumplan los objetivos del SGSI.
 - ✓ Garantizar la disponibilidad de los recursos.
 - ✓ Garantizar los roles y las responsabilidades.
- **Clausula 6. Planeación:** Esta sección está enfocada para definir los objetivos de seguridad, los cuales deben ser claros y deben contar con planes específicos para conseguirlos. Es necesario presentar grandes cambios durante el proceso de evaluación de riesgos:
 - ✓ El proceso para llevar a cabo la evaluación de riesgos

- ✓ El método utilizado para conseguir el objetivo a la hora de identificar los riesgos que se encuentran asociados
 - ✓ Conocer el nivel de riesgo que se establece como base de la probabilidad de que suceda un riesgo
 - ✓ Se elimina el término propietario del activo y se establece el término propietario del riesgo.
- **Clausula 7. Soporte:** Marca los requisitos de soporte para establecer, implementar y mejorar el Sistema de Gestión de Seguridad de la Información según la norma ISO 27001 2013, en el que se incluye:
 - ✓ Recursos
 - ✓ Personal competente
 - ✓ Conciencia y comunicación de las partes interesadas

Abarca el proceso de documentar, controlar, mantener y conservar la documentación correspondiente al Sistema de Gestión de Seguridad de la Información.

- **Clausula 8. Operación** Establece todos los requisitos necesarios para medir el funcionamiento del Sistema de Gestión de Seguridad de la Información ISO 27001 2013, las expectativas de la dirección y su realimentación, además de cumplir con lo que establece la norma ISO 27001 2013.

Es necesario que las empresas tengan planificadas y controladas las operaciones y los requisitos de seguridad. Los activos, las vulnerabilidades y las amenazas ya no son la base de la evaluación de riesgos. Solo es necesario para identificar los riesgos asociados con la confidencialidad, integridad y disponibilidad.

- **Clausula 9. Evaluación del desempeño** La base de la identificación y medición de la eficiencia y el desempeño del sistema de gestión sigue siendo la auditoría interna y las revisiones que se llevan a cabo en el sistema de gestión.
- **Clausula 10. Mejora:** El principal elemento que se utiliza durante el proceso de mejora son las no conformidades que están identificadas, las cuales tienen

que contabilizarse y compararse con las acciones correctivas para asegurarse de que no se repitan y que las acciones correctivas que se llevan a cabo sean efectivas.

2.2.5 ISO/IEC 27002 y su relación ISO/IEC 27001

Independientemente del contenido de cada una, hay que tener en cuenta un aspecto bastante importante en relación con ambas normas: la ISO 27001 es certificable y la ISO 27002 no lo es ¿Por qué motivo? Se preguntarán. La ISO 27002 no es certificable debido a que no contiene requisitos, es decir, en su contenido no contiene exigencias que toda organización que quiera certificarla debería cumplir. Estos requisitos si están presentes en la ISO 27001.

La ISO 27002 es simplemente una guía de buenas prácticas de cara a implementar los requisitos de la ISO 27001. De hecho, su contenido es una guía de implementación de los 114 controles que recoge el anexo A de la ISO 27001. Por tanto, hay que señalar que la ISO 27002 no se implanta.

En resumidas cuentas, se podría decir que ISO 27001 es el ¿Qué? e ISO 27002 es el ¿Cómo? Se analiza detenidamente el objetivo de cada una:

- La ISO 27001 te indicará que tienes que cumplir con los requisitos “x” y “z” para llevar a cabo el control de un determinado activo de la información de tu organización.
 - Por su parte ISO 27002 señalará que debes hacer en la práctica para poder cumplir con los requerimientos “x” y “z” que indica la ISO 27001 para este punto.
- [21]

Anexo A

Es la serie más conocida de los objetivos de control de seguridad y consiste en un conjunto de 114 controles agrupados en 35 objetivos de control y 14 dominios.

En la figura 7, se detalla el número de controles por cada dominio

Número del Anexo A	Dominio	Número de Controles
A5	Políticas de seguridad	2
A6	Aspectos organizativos de la seguridad de la información	7
A7	Seguridad ligada a los recursos humanos	6
A8	Gestión de activos	10
A9	Control de accesos	14
A10	Cifrado	2
A11	Seguridad física y ambiental	15
A12	Seguridad en la operativa	14
A13	Seguridad en las telecomunicaciones	7
A14	Adquisición, desarrollo y mantenimiento de los sistemas de información	13
A15	Relaciones con suministradores	5
A16	Gestión de incidentes en la seguridad de la información	7
A17	Aspectos de seguridad de la información en la gestión de la continuidad de negocio	4
A18	Cumplimiento	8
Número Total de controles		114

Fig. 7 Número de controles por cada Dominio del anexo A

A continuación, se detalla los catorce dominios ya mencionados:

- **A.5: Políticas de Seguridad de la Información:** hace referencia a los controles sobre cómo escribir y revisar políticas de seguridad.
- **A.6: Organización de la Seguridad de la información:** los controles se encargan de establecer responsables. Al mismo tiempo también se centra en dispositivos móviles y situaciones como la de teletrabajo.
- **A.7: Seguridad de los Recursos Humanos:** controles para las situaciones previas y posteriores referentes a la contratación y finalización de contrato de personal.
- **A.8: Gestión de Recursos:** establecidos para realizar inventario, clasificación de información y manejo de los medios de almacenamiento.
- **A.9: Control de Acceso:** control del acceso tanto a la información como a aplicaciones u otro medio que contenga información.

- **A.10: Criptografía:** controles para gestionar encriptación de información.
- **A.11: Seguridad física y ambiental:** controles para garantizar factores externos, seguridad de equipo y medios que puedan comprometer la seguridad.
- **A.12: Seguridad Operacional:** controles relacionados con gestión de la protección de malware o vulnerabilidades.
- **A.13: Seguridad de las comunicaciones:** Control sobre la seguridad de las redes, transmisión de información, mensajería.
- **A.14: Adquisición, desarrollo y mantenimiento de Sistemas:** controles que establecen los requisitos de seguridad en desarrollo y soporte.
- **A.15: Relaciones con los proveedores:** incluye lo necesario a la hora de realizar contratos y seguimiento a proveedores.
- **A.16: Gestión de Incidentes en Seguridad de la Información:** sirven para reportar eventos las debilidades, así como procedimientos de respuesta.
- **A.17: Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio:** referidos a la planificación de continuidad de negocio.
- **A.18: Cumplimiento:** control relacionado a la hora de identificar regulaciones relacionadas con seguridad de la información y hacer que se cumplan. [22]

2.2.6 Análisis de brechas de la seguridad de información

El análisis de brechas es un proceso que se debe realizar antes de iniciar la implementación del sistema. Permite revisar los requisitos de la norma para determinar el estado de cumplimiento de cada uno en la organización y los vacíos existentes para la conformidad del sistema.

Aunque el análisis de brechas no es un requisito obligatorio en la ISO 27001, es una herramienta estratégica para la seguridad de la información que es adoptada en las

organizaciones como una práctica conveniente a la hora de iniciar con la implementación de esta norma.

El principal propósito del análisis de brechas es evaluar el rendimiento del sistema de información actual de la organización con los requisitos de la ISO 27001 y determinar el grado de cumplimiento existente.

Esta herramienta es de gran utilidad para establecer el “donde estamos” y el “donde queremos llegar” de una organización que busca proteger sus datos, en otras palabras, define el punto de partida para implementar la norma y la cantidad de recursos y esfuerzos necesarios para este propósito. [23]

Este diagnóstico se basa teniendo en cuenta los controles y dominios del anexo A de la norma ISO/IEC 27001:2013.

2.2.7 Gestión de riesgos en la seguridad de información

Es el proceso de identificar, comprender, evaluar y mitigar los riesgos y sus vulnerabilidades subyacentes y el impacto en la información, los sistemas de información y las organizaciones que dependen de la información para sus operaciones. Además de identificar los riesgos y las medidas de mitigación del riesgo, un método y proceso de gestión del riesgo ayudará a:

- ✓ Identificar los activos críticos de información. Un programa de gestión de riesgos puede ampliarse para identificar también a personas críticas, procesos de negocio y tecnología.
- ✓ Comprender por qué los activos críticos escogidos son necesarios para las operaciones, la realización de la misión y la continuidad de las operaciones.

2.2.7.1. Fases y ciclo de la gestión de riesgos

Existen algunas fases de gestión de riesgos que marcan la pauta a seguir para el desarrollo de un proyecto, estas son:

- ✓ Inventario de Activos de Información.
- ✓ Análisis del Riesgo
- ✓ Evaluación del Riesgo.

- ✓ Opción de Tratamiento del Riesgo.

2.2.7.2. Análisis y evaluación de riesgos

En el análisis de riesgos se identifican amenazas y vulnerabilidades que exponen los activos de información más importantes, así como los controles existentes que se tienen para proteger a los activos de estas amenazas. Con esta data se estiman la degradación del activo y se determina un nivel de exposición, luego se identifica probabilidad; con estos resultados se determina el nivel de riesgo.

Los activos de Información que son analizados son los resultados del Inventario de Activos, los cuales pasan a la fase de Análisis de Riesgos. Por cada activo de información, se genera la siguiente información:

- Por cada activo de información, se listan las Amenazas a las que está expuesta y se intenta identificar algún Agente específico que la genere, y la causa de éste.
- Por cada amenaza, se listan las vulnerabilidades que expone el activo y que podrían ser aprovechadas por la amenaza, así como los controles existentes para prevenir la materialización de la amenaza, disuadir al agente, detectar la amenaza o corregir el daño sufrido.

2.2.7.3. Tratamiento de riesgos

Una vez realizado el análisis y evaluación de riesgos, se debe decidir qué acciones tomar con esos activos que están sujetos a riesgos, siendo como objetivo primordial, describir las actualizaciones que se van a realizar para disminuir los riesgos a niveles aceptables.

Técnica para el tratamiento de riesgos

Para reducir el riesgo identificado se hará uso del SOA - Declaración de aplicabilidad (SOA por las siglas en inglés de Statement of Applicability). Es un documento con los controles de seguridad establecidos en el Anexo A de la ISO/IEC 27001:2013, estos a su vez contienen un conjunto de 114 controles agrupados en 35 objetivos de control y 14 dominios.

Los controles ya mencionados son necesarios para definir la aplicación de los controles de seguridad que hayan sido seleccionados y que no han sido

implementados. El propósito principal del SOA, es adoptar mejores prácticas para que permita crear una lista de verificación según lo recomendado por el Anexo A de la ISO 27001:2013, con ella se obtiene una documentación sobre los controles establecidos.

2.2.8 Política de seguridad

Las políticas de seguridad de información son requeridas para toda la organización no solamente para algún sector. Las políticas deben estar establecidas y aprobadas por la máxima autorización, debe ser documentada y distribuida a todas las partes interesadas tanto internas y externas, estas políticas deben cumplir con los objetivos de la organización y su marco de trabajo tiene que establecer un compromiso con la seguridad de información.

2.3. DEFINICIÓN DE TÉRMINOS BÁSICOS

Proceso

Es una serie de tareas interrelacionadas que, juntas transforman las entradas en salidas. Estas pueden ser realizadas por personas, la naturaleza o máquinas utilizando diversos recursos. [24]

Activos de información

Los activos de información son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección. [25]

ISO

La Organización Internacional de Normalización (llamada en ocasiones: Organización Internacional de Estandarización; conocida por el acrónimo ISO) es una organización para la creación de estándares internacionales compuesta por diversas organizaciones nacionales de normalización. [26]

Controles

Un control es un conjunto de medidas o acciones tomadas para gestionar el riesgo y aumentar la probabilidad de que se logren los objetivos establecidos. [27]

Riesgos

El riesgo se define como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas. Los factores que lo componen son la amenaza y la vulnerabilidad. [28]

Anexo A

El Anexo A es un documento normativo que sirve como guía para implementar los controles de seguridad específicos de ISO 27001. Todos estos controles están dirigidos a mejorar la Seguridad de la información de nuestra organización. Está compuesto por 114 controles de seguridad agrupados en 14 secciones. [29]

Mejora Continua

Un proceso de mejora continua es la actividad de analizar los procesos que se usan dentro de una organización o administración, revisarlos y realizar adecuaciones para minimizar los errores de forma permanente. [30]

SBS

La Superintendencia de Banca, Seguros y AFP es el organismo encargado de la regulación y supervisión de los Sistemas Financiero, de Seguros y del Sistema Privado de Pensiones, así como de prevenir y detectar el lavado de activos y financiamiento del terrorismo. Su objetivo primordial es preservar los intereses de los depositantes, de los asegurados y de los afiliados al SPP. [31]

Información:

Conjunto de datos, ya procesados y ordenados para su comprensión, que aportan nuevos conocimientos a un individuo o sistema sobre un asunto, materia, fenómeno o ente determinado [32]

PDCA

Son las iniciales de las palabras en inglés: Plan, Do, Check y Act (Planificar, Hacer, Verificar y Actuar), Es una metodología describe los cuatro pasos esenciales que toda empresa debe llevar a cabo de forma sistemática para lograr la mejora continua de la calidad. [33]

Estándar

Son acuerdos documentados que contienen especificaciones técnicas u otros criterios precisos para ser usados consistentemente como reglas, guías o definiciones de

características para asegurar que los materiales, productos, procesos y servicios cumplan con su propósito". [34]

Metodología

Conjunto de procedimientos racionales utilizados para alcanzar el objetivo o la gama de objetivos que rige una investigación científica, una exposición doctrinal o tareas que requieran habilidades, conocimientos o cuidados específicos. [35]

Inventario

El inventario es una relación detallada, ordenada y valorada de los elementos que componen el patrimonio de una empresa o persona en un momento determinado [36]

Mitigar

Es el proceso de desarrollo de opciones y acciones que, al ser implementadas, mejorarán las oportunidades y reducirán el impacto negativo o la probabilidad de ocurrencia de un evento en particular. [37]

Alcance

Nos ayuda a describir la extensión y los límites del Sistema de Gestión de Seguridad de la Información, por lo que se pueden definir todos los términos de los activos de información, la ubicación física, las unidades organizacionales, actividades o procesos de gran importancia para la organización, es decir, se trata de la selección de los elementos críticos que se deben proteger. [38]

Correctivo

Son un conjunto de tareas técnicas destinadas a reparar o sustituir los equipos que sufren una avería. Este tipo de mantenimiento corrige los fallos existentes en los activos que requieren una intervención para volver a su función inicial. [39]

Preventivo

Previene los fallos en los equipos. Este tipo de mantenimiento se realiza sistemáticamente, es decir, los activos se inspeccionan incluso si no han presentado ninguna manifestación de avería. De este modo, se evita cualquier fallo del equipo lo que garantiza el correcto funcionamiento y la seguridad de los activos. [39].

Activo

Cualquier cosa que tiene valor para la organización. [40]

CAPÍTULO III. MATERIALES Y MÉTODOS

La presente investigación se realizó en la Edpyme CREDIVISIÓN los datos fueron tomados íntegramente de sus procesos y del personal que labora en el área de Negocios para realizar el diagnóstico, análisis, muestra, procesamiento y resultados. Toda la información sirvió como base para el diseño del sistema de gestión de seguridad información en la relación a la ISO 27001:2013

La Edpyme CREDIVISIÓN, se encuentra ubicado en el distrito de San Juan de Miraflores, provincia y departamento de Lima, y la investigación se hizo durante un periodo de siete meses, iniciando el mes de febrero del 2022 hasta agosto del 2022.

3.1. PROCEDIMIENTO

Se diseñó teniendo en cuenta los requerimientos establecidos en la normativa ISO 27001:2013, se definieron 5 fases para el desarrollo del proyecto, los cuales comprenden: planificación, análisis, diseño, pruebas y cierre.

Fase 1: Planificación: Comprende:

- 1.1. Plan de inicio del Proyecto
- 1.2. Registro de Interesados

Fase 2: Análisis: Comprende:

- 2.1. Análisis de la situación actual
- 2.2. Contexto de la empresa
- 2.3. Definir el alcance

Fase 3: Diseño: Comprende:

- 3.1. Política de la seguridad de información
- 3.2. Estructura Organizacional del SGSI
- 3.3. Metodología de evaluación de riesgos
- 3.4. Elaborar el plan de tratamiento de riesgos
- 3.5. Declaración de aplicabilidad (SOA)
- 3.6. Plan de capacitación y concientización
- 3.7. Elaborar un plan de continuidad de negocio.
- 3.8. Elaborar un acuerdo de confidencialidad.
- 3.9. Elaborar el manual del SGSI

Fase 4: Pruebas

- 4.1. Plan de pruebas
- 4.2. Ejecución
- 4.3. Resultados de las pruebas
- 4.4. Plan de mejoras

Fase 5: Cierre

- 5.1. Acta de cierre y entrega del proyecto

3.1.1 Fase 1: Planificación

3.1.1.1. Plan de inicio del Proyecto

El 07 de febrero de 2022 se dio inicio al proyecto del diseño del Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para proteger adecuadamente los activos de información asociados al proceso de créditos, por lo cual se obtuvo el compromiso de la alta dirección.

Adicionalmente, a este compromiso también se obtuvo una carta de autorización que permite utilizar el nombre de Edpyme CREDIVISIÓN para el proyecto de tesis, la misma que se puede apreciar en el formato Carta de autorización (Anexo 7).

a. Acta de constitución del proyecto

Se elaboró el acta de constitución del proyecto para establecer la relación de colaboración que existe entre la Edpyme CREDIVISIÓN y el ejecutor del proyecto, donde se especificó la información general, la descripción del proyecto, los objetivos y el alcance, que fue presentado a la entidad para su aprobación. La misma que se puede apreciar en el formato acta de constitución (Anexo 8).

b. Cronograma

A continuación, en la figura 8, se muestra el cronograma del proyecto de las actividades realizadas:

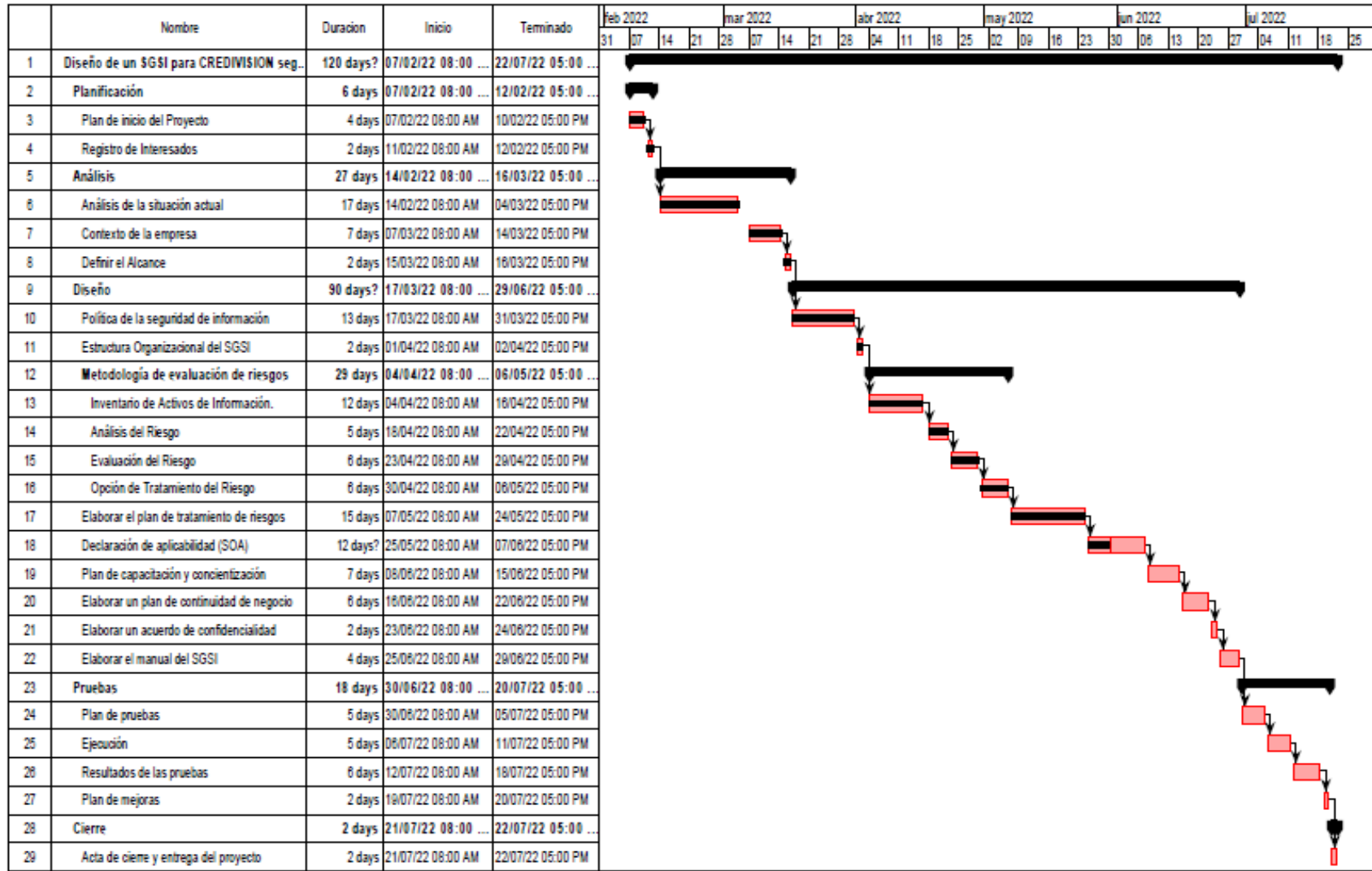


Fig. 8 Cronograma de Actividades

3.1.1.2. Registro de Interesados

Se debe determinar quiénes son las partes interesadas y requisitos de las partes interesadas para la seguridad de la información. A continuación, en la tabla 1, se muestra las partes interesadas y los requisitos de éstas:

Tabla N°1 Partes Interesadas

PARTE INTERESADAS		REQUISITOS DE SGSI
INTERNAS	Accionistas	Maximizar la rentabilidad del negocio
	Gerentes	Maximizar la rentabilidad del negocio
	Colaboradores	Laborar en una empresa sólida y de prestigio.
EXTERNAS	Clientes	Asegurar la confidencialidad, integridad y disponibilidad de su información
	Proveedores	Proteger la continuidad de las operaciones
	Gobierno	Responsabilidad Social

3.1.2 Fase 2: Análisis

3.1.2.1. Análisis de la situación actual

Para poder empezar con el diseño del SGSI es necesario conocer la situación actual en la que se encuentra la empresa, la cual se llevó a cabo mediante el análisis de brechas (GAP - Anexo 18). Los pasos que se realizaron para llegar a este análisis GAP son:

Paso 1: Elaboración de cuestionarios (Anexo 17), aquí se realizaron las siguientes actividades:

- i. Revisión de la norma ISO/IEC 27001:2013.
- ii. Elaboración de preguntas por controles y dominio.
- iii. Definición de niveles y criterios de madurez.

Paso 2: Entrevistas al personal del área de TI y Riesgos, de la Edpyme; se realizaron las siguientes actividades:

- i. Entendimiento de la estructura organizacional.
- ii. Revisión de los perfiles e identificación de los procesos.
- iii. Ejecución de las entrevistas al personal interesado en la empresa.

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

- i. Clasificación del nivel de madurez de los dominios
- ii. Revisión de calificaciones.

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

- i. Cálculo del promedio por dominio.
- ii. Elaboración de gráficas de madurez y brecha.

Para determinar el nivel de madurez de la empresa se definió una escala con seis niveles que se detalla en la tabla 2.

Tabla N°2 Nivel de madurez de Cobit

Nivel Escala	Valor	%	Comentario
Inexistentes	Nivel 0	0%	No hay reconocimiento de la necesidad del control o requisito.
Inicial	Nivel 1	20%	Existe cierto reconocimiento de la necesidad de control interno o requisito. Se aplica para algún problema o tarea específica, no generalizable.
Repetible	Nivel 2	40%	Los controles existen, pero no están documentados.
Definido	Nivel 3	60%	Los controles están en su lugar y están documentados adecuadamente.
Gestionado	Nivel 4	80%	Existe un control interno sobre la aplicación de controles y cumplimiento de requisito.
Optimizado	Nivel 5	100%	Existe un control interno y continuo sobre la aplicación de controles y cumplimiento de requisitos. Se mide la eficacia de los controles estableciendo objetivos de mejora.

A continuación, se muestran los resultados de la encuesta aplicada a los 7 trabajadores de la empresa, tomando como referencia las 10 primeras preguntas de la encuesta, obteniendo los siguientes resultados, que se muestra en la tabla 3.

Tabla N°3 Personal Encuestado

PREGUNTAS	Pregunta1	Pregunta2	Pregunta3	Pregunta4	Pregunta5	Pregunta6	Pregunta7	Pregunta8	Pregunta9	Pregunta10
ENCUESTADOS										
Gerente General	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
Gerente de Riesgos	SI	NO	NO	NO	NO	NO	NO	NO	NO	NO
Jefe de TI	NO	NO	NO	NO	NO	NO	NO	NO	SI	NO
Programador de TI	NO	NO	NO	NO	NO	NO	NO	NO	SI	NO
Desarrollo TI	NO	NO	NO	NO	NO	NO	NO	NO	SI	NO
Analista de Soporte	NO	NO	NO	NO	NO	NO	NO	SI	SI	NO
Administrador de BB.DD	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
TOTAL "SI"	1	0	0	0	0	0	0	1	4	0
TOTAL "NO"	6	7	7	7	7	7	7	6	3	7
% "SI"	14%	0%	0%	0%	0%	0%	0%	14%	57%	0%
% "NO"	86%	100%	100%	100%	100%	100%	100%	86%	43%	100%

Además, para un mejor entendimiento se muestra la tabla 4, el resultado de toda la encuesta en niveles porcentuales, con el fin de determinar el nivel de madurez inicial o actual de la empresa.

Tabla N°4 Resultado de las Encuestas

ITEM	RESULTADOS DE ENCUESTA	SI	NO
A.5	Políticas de seguridad de la información.		
1	¿Existen políticas publicadas para apoyar la seguridad de la información?	14.0%	86.0%
2	¿Las políticas de seguridad de la información son revisadas y actualizadas?	0.0%	100.0%
A.6	Organización de la seguridad de la información		
3	¿Están definidas las responsabilidades de seguridad de la información?	0.0%	100.0%

ITEM	RESULTADOS DE ENCUESTA	SI	NO
4	¿Se han segregado las diversas áreas de responsabilidad sobre la seguridad de la información para evitar accesos indebidos?	0.0%	100.0%
5	¿Existe proceso definido para contactar con las autoridades competentes ante incidentes relacionados con seguridad de la información?	0.0%	100.0%
6	¿Existen contactos definidos con grupos de interés especial?	0.0%	100.0%
7	¿En la gestión de proyectos se consideran aspectos relacionados con seguridad de la información?	0.0%	100.0%
8	¿Existen políticas definidas para el uso seguro de dispositivos móviles?	14.0%	86.0%
9	¿Se aplican criterios de seguridad para el teletrabajo?	57.0%	43.0%
A.7	Seguridad relativa a los recursos humanos		
10	¿La Edpyme realiza verificaciones de antecedentes de los candidatos para los empleos?	0.0%	100.0%
11	¿Existen acuerdos con los empleados y contratistas donde se especifiquen las responsabilidades de seguridad de la información?	0.0%	100.0%
12	¿El cumplimiento de las responsabilidades sobre la seguridad de la información es exigida de forma activa a empleados y terceros?	0.0%	100.0%
13	¿Existen procesos de información, capacitación y concientización sobre la seguridad de la información?	0.0%	100.0%
14	¿Existen acuerdos de responsabilidad de seguridad de la información que siguen siendo válidas después de la finalización del contrato?	0.0%	100.0%
15	¿Existen acuerdos de responsabilidad de seguridad de la información que siguen siendo válidas después de la finalización del contrato?	0.0%	100.0%
A.8	Gestión de activos		
16	¿Se ha realizado un inventario de activos?	29.0%	71.0%
17	¿Se ha identificado al responsable de cada activo?	29.0%	71.0%

ITEM	RESULTADOS DE ENCUESTA	SI	NO
18	¿Se han establecido normas para el uso adecuado de activos?	29.0%	71.0%
19	¿Existe procedimiento para la devolución de activos asignados?	29.0%	71.0%
20	¿Se clasifica la información según su confidencialidad?	0.0%	100.0%
21	¿Existen procedimientos que definan el etiquetado de activos?	29.0%	71.0%
22	¿Existen procedimientos para el manipulado de la información de acuerdo a su clasificación?	14.0%	86.0%
23	¿Existen procedimientos que definen cómo manejar los soportes extraíbles (uso, cifrado, borrado, etc.)?	14.0%	86.0%
24	¿Existen procedimientos para la eliminación de soportes?	29.0%	71.0%
25	¿Son protegidos los soportes físicos con información sensible durante el transporte?	14.0%	86.0%
A.9	Control de acceso		
26	¿Existe una política para definir los controles de acceso a la información según las función o puesto de trabajo?	0.0%	100.0%
27	¿Existen políticas de acceso a las redes y a los servicios de red?	14.00%	86.0%
28	¿Existen procesos de alta y baja de usuarios?	29.0%	71.0%
29	¿Existen procesos para la asignación de perfiles de acceso?	14.0%	86.0%
30	¿Se define un proceso específico para la asignación de permisos privilegiados de administración de accesos?	14.0%	86.0%
31	¿Las contraseñas y otra información de autenticación secreta son proporcionadas de forma segura?	14.0%	86.0%
32	¿Se establecen periodos para renovación de permisos de acceso?	0.0%	100.0%
33	¿Existe un proceso definido para la revocación o reasignación de permisos?	0.0%	100.0%

ITEM	RESULTADOS DE ENCUESTA	SI	NO
34	¿Existen responsabilidades para los usuarios sobre el uso de información secreta de autenticación?	0.0%	100.0%
35	¿El acceso a la información en los sistemas y aplicaciones es restringido según la política de control de acceso?	14.0%	86.0%
36	¿Se han implementado procedimientos de acceso seguro para el inicio de sesión?	14.0%	86.0%
37	¿Cuentan con sistema de gestión de contraseñas?	0.0%	100.0%
38	¿El uso de herramientas de utilidad es controlado y limitado a empleados específicos?	14.0%	86.0%
39	¿Existe procedimiento para el control de acceso al código fuente?	0.0%	100.0%
A.11	Seguridad física y del entorno		
40	¿Se establecen perímetros de seguridad física con barreras de acceso?	14.0%	86.0%
41	¿Existen controles físicos de acceso en áreas restringidas?	14.0%	86.0%
42	¿Se establecen medidas de seguridad para oficinas para proteger la información de pantallas, etc. en áreas accesibles a personal externo?	14.0%	86.0%
43	¿Existen instaladas alarmas, sistemas de protección contra incendios, etc.?	29.0%	71.0%
44	¿Se protegen los equipos de accesos no autorizados?	14.0%	86.0%
45	¿Se protegen los equipos contra fallos de suministro de energía?	14.0%	86.0%
46	¿Existe protección para los cableados de energía y de datos?	14.0%	86.0%
47	¿Se realizan tareas de mantenimiento de los equipos?	29.0%	71.0%
48	¿Existen políticas para proteger o eliminar información de equipos de baja o que van a ser reutilizados?	14.0%	86.0%
49	¿Se establecen reglas de comportamiento para abandonos del puesto de trabajo?	14.0%	86.0%

ITEM	RESULTADOS DE ENCUESTA	SI	NO
50	¿Existen políticas para proteger la información de equipos cuando los usuarios abandonan el puesto de trabajo?	14.0%	86.0%
A.12	Seguridad de las operaciones		
51	¿Se documentan los procedimientos?	0.0%	100.0%
52	¿Se controla que los procedimientos se actualicen constantemente?	0.0%	100.0%
53	¿Se monitorea los recursos para cumplir con la demanda de los usuarios?	14.0%	86.0%
54	¿Existen una separación segura entre los entornos de desarrollo, pruebas y producción?	14.0%	86.0%
55	¿Existen software para la detección de código malicioso?	14.0%	86.0%
56	¿Existe una política de backup definida?	29.0%	71.0%
57	¿Se realiza un registro o logs de eventos?	0.0%	100.0%
58	¿Se ha establecido un sistema de protección para los registros mediante segregación de tareas o copias de seguridad?	14.0%	86.0%
59	¿Se protege de forma segura los accesos de los administradores?	0.0%	100.0%
60	¿Las nuevas instalaciones de software son validadas de forma segura?	14.0%	86.0%
61	¿Se establecen métodos de control para vulnerabilidades técnicas?	0.0%	100.0%
62	¿Existen políticas de restricción en la instalación de software para usuarios finales?	29.0%	71.0%
63	¿La auditoría realiza los controles en los sistemas de información?	14.0%	86.0%
A.13	Seguridad de las comunicaciones		
64	¿Existe controles de red para los elementos conectados?	14.0%	86.0%
65	¿Se verifica la seguridad de los servicios de red?	14.0%	86.0%
66	¿Existe separación de redes tomado en cuenta la información y los recursos?	14.0%	86.0%

ITEM	RESULTADOS DE ENCUESTA	SI	NO
67	¿Existen políticas y procedimientos para el intercambio de información?	0.0%	100.0%
68	¿Se establecen acuerdos de intercambio de información con terceros?	0.0%	100.0%
69	¿Se establecen políticas en mensajería electrónica?	14.0%	86.0%
70	¿Se establecen acuerdos de confidencialidad para el intercambio de información con terceros?	0.0%	100.0%
A.14	Adquisición, desarrollo y mantenimiento de los sistemas de información		
71	¿Se definen los requisitos de seguridad de la información para los nuevos sistemas de información?	0.0%	100.0%
72	¿Se definen requisitos mínimos de seguridad en las aplicaciones para redes públicas?	14.0%	86.0%
A.15	Relaciones con proveedores		
73	¿Existe una política de seguridad de la información para proveedores?	0.0%	100.0%
74	¿Se han definido requisitos de seguridad de la información en contratos con terceros?	0.0%	100.0%
75	¿Se fijan requisitos de seguridad de la información para las comunicaciones y la cadena de suministro?	14.0%	86.0%
76	¿Se controla el cumplimiento de la provisión de servicios por parte de los proveedores?	14.0%	86.0%
A.16	Gestión de incidentes de seguridad de la información		
77	¿Se definen responsabilidades y procedimientos para gestionar los incidentes de la seguridad de la información?	14.0%	86.0%
78	¿Se notifica de forma oportuna los eventos de seguridad de la información?	0.0%	100.0%
79	¿Se corrobora la adecuada notificación de los puntos débiles de la seguridad de la información?	14.0%	86.0%
80	¿Se ha establecido un proceso para gestionar los eventos de seguridad de la información?	0.0%	100.0%
81	¿Existen mecanismos para dar una respuesta a los incidentes de seguridad de la información?	0.0%	100.0%

ITEM	RESULTADOS DE ENCUESTA	SI	NO
82	¿Existe una base de conocimiento de incidentes de seguridad para posteriores soluciones?	0.0%	100.0%
83	¿Se recopila las evidencias de los incidentes en la seguridad de la información?	0.0%	100.0%
A.17	Aspectos de seguridad de la información para la gestión de la continuidad del negocio		
84	¿Se cuenta con un plan de continuidad de seguridad de la información?	14.0%	86.0%
85	¿Se ha implementado las medidas de continuidad en base a la seguridad de la información?	14.0%	86.0%
86	¿Se han verificado y evaluado el plan de continuidad de la seguridad de la información?	14.0%	86.0%
87	¿Existe la disponibilidad de los recursos críticos de la información?	14.0%	86.0%
A.18	Cumplimiento		
88	¿Se tiene conocimiento de la legislación actual?	14.0%	86.0%
89	¿Existe normas de protección de los registros de la organización?	14.0%	86.0%
90	¿Se establecen medidas para la protección de datos personales de acuerdo con la legislación vigente?	0.0%	100.0%
91	¿Se revisan los controles de la seguridad de la información por personal independiente a los responsables de implementar los controles?	14.0%	86.0%
92	¿Se revisa periódicamente el cumplimiento de las políticas y controles de la seguridad de la información?	0.0%	100.0%
93	¿Se realizan evaluaciones sobre el correcto funcionamiento técnico?	0.0%	100.0%

En la tabla 5, se muestra el estado actual de implementación y cumplimiento de los controles del anexo A de la norma ISO/IEC 27001:2013 por parte de la empresa.

Tabla N°5 Estado Actual de cumplimiento de Controles

DOMINIOS		Estado Actual	Estado Estimado	Brecha	Nivel
A.5	Políticas de seguridad de la información.	7.0%	100.0%	93.0%	Inicial
A.6	Organización de la seguridad de la información	10.1%	100.0%	89.9%	Inicial
A.7	Seguridad Relativa a los recursos humanos	0.0%	100.0%	100.0%	Inexistente
A.8	Gestión de activos	21.6%	100.0%	78.4%	Repetible
A.9	Control de acceso	9.1%	100.0%	90.9%	Inicial
A.11	Seguridad física y del entorno	16.7%	100.0%	83.3%	Inicial
A.12	Seguridad de las operaciones	10.9%	100.0%	89.1%	Inicial
A.13	Seguridad de las comunicaciones	8.0%	100.0%	92.0%	Inicial
A.14	Adquisición, desarrollo y mantenimiento de los sistemas de información	7.0%	100.0%	93.0%	Inicial
A.15	Relaciones con proveedores	7.0%	100.0%	93.0%	Inicial
A.16	Gestión de incidentes de seguridad de la información	4.0%	100.0%	96.0%	Inicial
A.17	Aspectos de seguridad de la información para la gestión de la continuidad del negocio	14.0%	100.0%	86.0%	Inicial
A.18	Cumplimiento	7.0%	100.0%	93.0%	Inicial
Promedio de Dominio		9.4%		Inicial	

En la figura 9, se puede apreciar que el dominio con un mayor nivel de madurez es el A.8 “Seguridad física y del entorno”, cuyo resultado de escala nos indica que se encuentra en un “Nivel 2 Repetible”, con un 21.7 % es decir existen los controles, pero no hay documentación alguna de ello. Para el resto de los controles, se puede apreciar que se encuentran por debajo del 16.7% correspondiente a un “Nivel 1 inicial” de madurez.

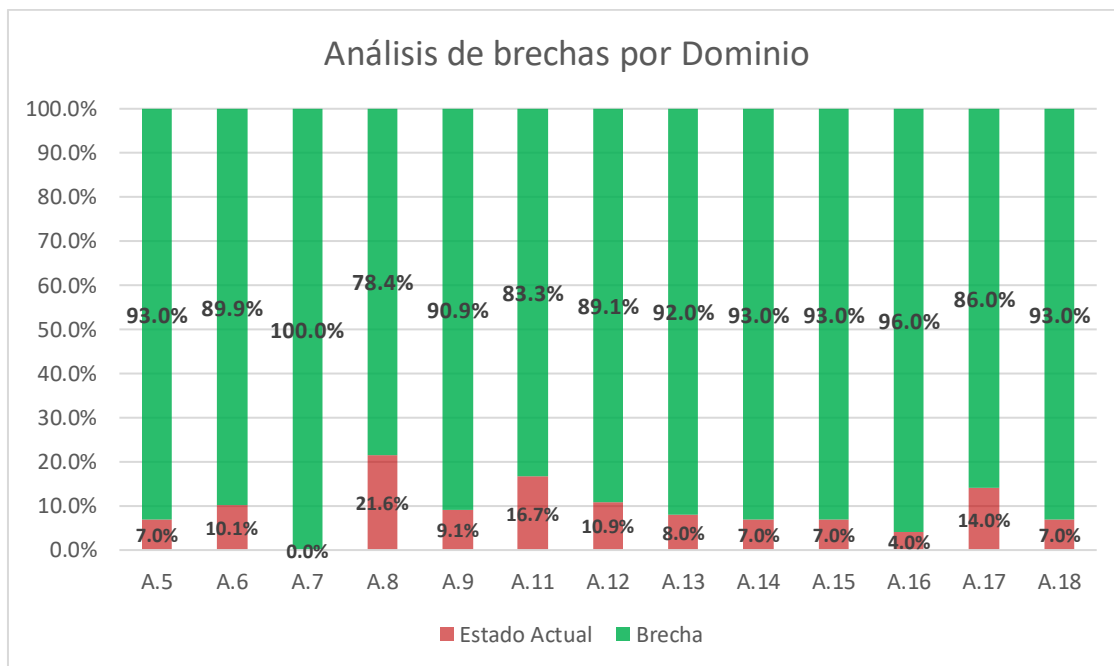


Fig. 9 Análisis de Brechas por Dominio

Finalmente, en la figura 9, se realizó un cuadro estadístico general de todos los controles del anexo A de la norma ISO/IEC 27001:2013. el resultado de escala nos indica:

- ✓ **El “Nivel 0 Inexistentes”** ocupa un 41% del total de controles, es decir no cumplen o no existen controles que se respeten dentro de la empresa.
- ✓ **El “Nivel 1 inicial”**, ocupa un 46 % del total de controles, es decir tienen cierto reconocimiento de la necesidad de un control.
- ✓ **El “Nivel 2 Repetible”**, con un 7 % nos indica que existen los controles, pero no hay documentación alguna de ello. Por lo que se requiere una intervención inmediata dado que el objetivo del proyecto es proteger los activos de información.

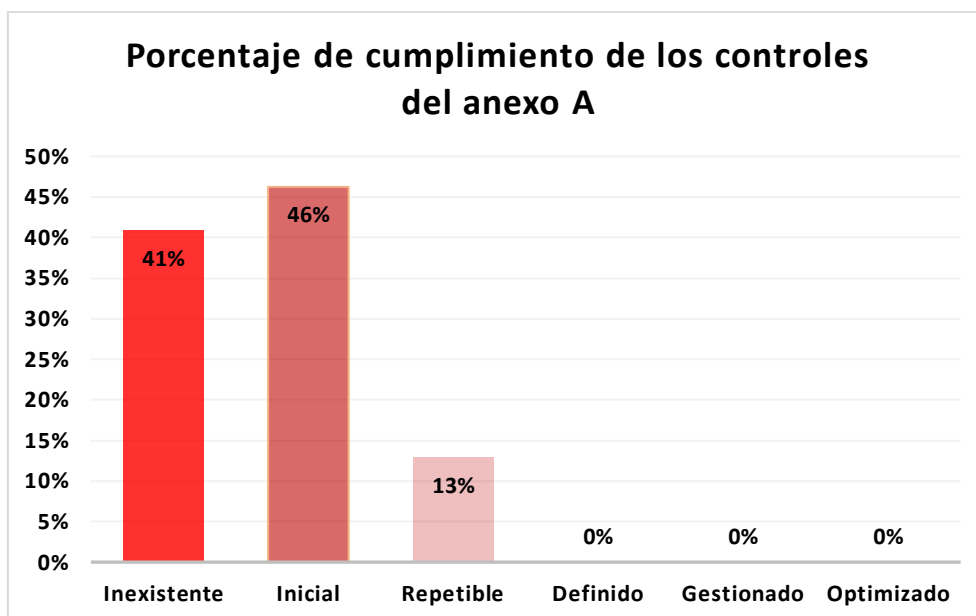


Fig. 10 Nivel de Madurez de controles

3.1.2.2. Contexto de la empresa

2.3.1. Contexto interno

El SGSI debe ser alineado a la cultura organizacional, procesos y la estrategia de la empresa, razón por la cual se ha analizado a la Edpyme Credivisión en los siguientes puntos:

✓ Misión

“Somos una empresa microfinanciera cristiana, que genera oportunidades de desarrollo para los pobres, contribuyendo a la transformación humana, con énfasis en los niños, niñas, adolescentes, a través de servicios financieros y no financieros”.

✓ Visión

“Ser la mejor opción de microfinanzas con enfoque cristiano”

✓ **Organigrama:** La Edpyme cuenta con el siguiente organigrama, ver figura 11

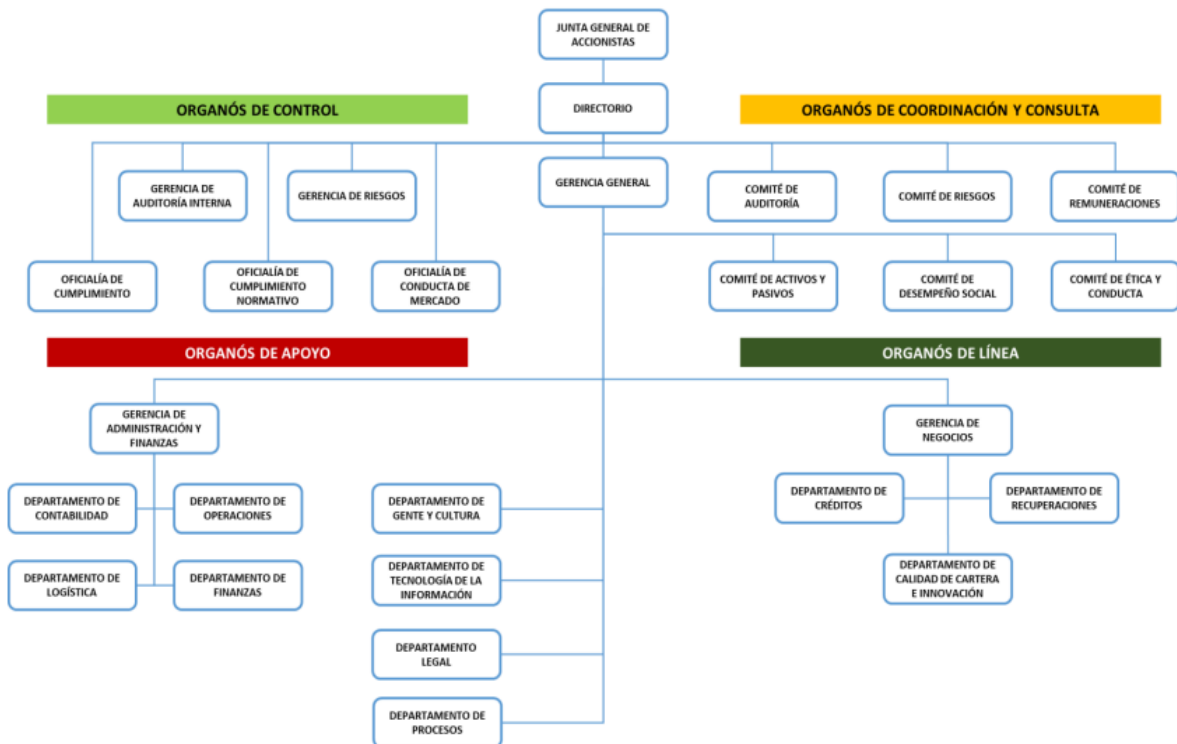


Fig. 11 Organigrama Edpyme CREDIVISIÓN

La Edpyme CREDIVISIÓN, ofrece servicios de préstamos para sus clientes quienes mayormente provienen de sectores como las de las Micro y Pequeña Empresa (MYPES), quienes se asocian con el objetivo de poder acceder a mayores beneficios de financiamiento.

En el desarrollo de un crédito de la EDPYME CREDIVISIÓN. se distinguen dos grandes etapas:

- a. Otorgamiento de Créditos.
- b. Recuperación de Créditos.

Adicionalmente a ello se considera el seguimiento de cartera.

A continuación, en la figura 12 se detallan las etapas del proceso de créditos:

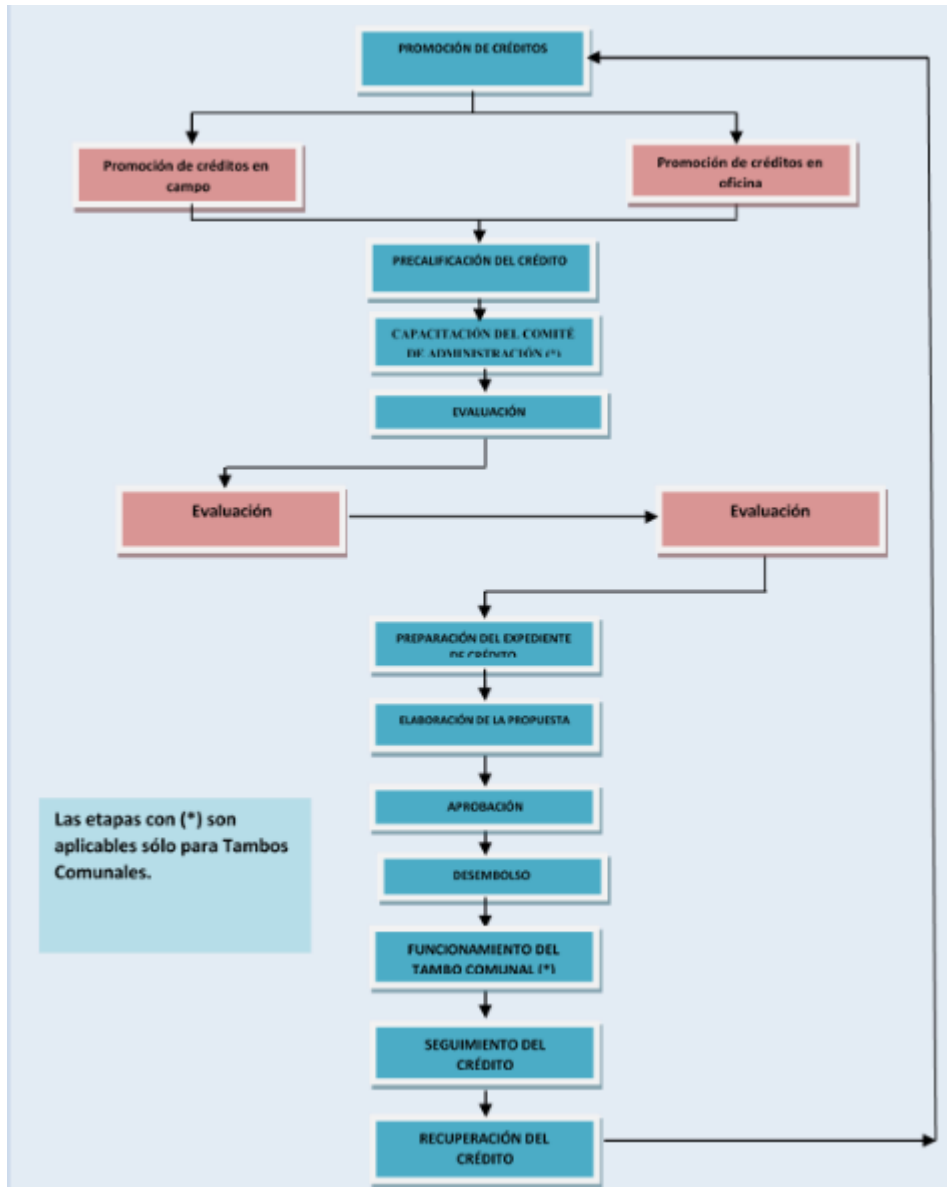


Fig. 12 Etapas de desarrollo de un crédito

Se procede a detallar las funciones y procedimientos que desarrolla cada una de estas etapas:

a. Otorgamiento de Créditos

i. Promoción

Presentar a la EDPYME CREDIVISIÓN ante los clientes potenciales, hacerles conocer los beneficios y características del servicio financiero y estimularlos a solicitar un crédito a la institución.

ii. Precalificación

Determinar la viabilidad del crédito a través de preguntas que nos permitan sondear la capacidad, la voluntad de pago y el destino del crédito pudiendo contar con la información de la central de riesgos de ser posible; en caso de viabilidad del crédito se debe solicitar los documentos necesarios para sustentar la propuesta sin condicionar el llenado de la solicitud a la presentación de éstos. La solicitud debe ser llenada con el DNI original del solicitante.

Debe ser ágil y en caso se cumplan las condiciones debe concluir con el llenado e ingreso de la solicitud al sistema automatizado SISGO.

iii. Capacitación del Comité de Administración

Orientar a la correcta toma de decisiones sobre las funciones, responsabilidades actividades que desarrollarán sus integrantes del tambo durante su período de gestión.

iv. Evaluación

Medir la solvencia del cliente y su negocio desde el punto de vista moral, empresarial y económico financiero, así como también determinar que la operación crediticia cumpla con este Manual y con las Políticas de Crédito de Edpyme CREDIVISIÓN y se encuentre respaldada suficientemente por garantías reales o personales, sean estas solidarias o reales.

v. Preparación del Expediente de Crédito

Mantener en archivo y en forma ordenada toda la documentación que origina el otorgamiento de un crédito, cuidando que la documentación se encuentre disponible para su utilización posterior, especialmente para actividades de seguimiento y control, así como para acciones judiciales u otros reclamos originados por los clientes.

vi. Elaboración de la Propuesta de Crédito

Ordenar la información cualitativa y cuantitativa recopilada en la fase de evaluación de manera que permita tomar una decisión sobre la conveniencia o no de otorgar el crédito con el menor riesgo posible.

vii. Aprobación del Crédito

Evaluar las propuestas de crédito, a través de los comités de Créditos, con la finalidad de aprobarlas o denegarlas de acuerdo con el nivel de aprobación y al tipo de producto.

viii. Desembolso del Crédito

Formalizar la operación crediticia, dándole valor legal a la operación y a las garantías que la respaldan, así como proceder a la entrega de los recursos económicos al cliente.

ix. Funcionamiento del Tambo Comunal

Garantizar la eficiente operatividad del tambo comunal, permitiendo que las socias en sus diferentes roles se empoderen y apropien del tambo comunal, cuidando y garantizando su permanencia indefinida como clientes de Edpyme CREDIVISIÓN.

Esta etapa se iniciará apenas culmina la ceremonia de inauguración. Es el momento en que las socias con el dinero que han recibido como préstamo se dirigirán a realizar sus inversiones. Es necesario tener en cuenta que el primer ciclo es el más importante para el futuro del Tambo por lo que se le debe brindar mayor atención y apoyo.

x. Seguimiento del Crédito

Reducir el riesgo crediticio e identificar a tiempo cualquier cambio en las condiciones del negocio que incrementen el riesgo de la operación y/o para ofrecer nuevos servicios o Créditos.

b. Recuperación del crédito

Recuperar los créditos otorgados a través del pago de cuotas de los clientes, fomentando el pago puntual que garantice una cartera de Créditos, sana y diversificada, que busque la satisfacción y lealtad del cliente y a la vez el fortalecimiento y crecimiento institucional.

La recuperación del crédito se realizará de la siguiente forma:

- En agencias, a través de las ventanillas de caja;
- En agencias de Entidades Financieras (Banco de Crédito del Perú, Banco de la Nación, entre otros) con zonas de atención estarán en función del

convenio firmado con el banco o con depósitos directos en las cuentas que la Edpyme CREDIVISIÓN mantiene en otras instituciones.

Del párrafo anterior se establece que ningún colaborador se encuentra autorizado a recibir el pago de cuotas fuera de las agencias de la Edpyme CREDIVISIÓN, salvo los Analistas de Créditos de tambos comunales. En caso excepcional la Gerencia de Negocios podrá autorizar a otro colaborador la recepción de pago de cuotas fuera de la institución.

3.1.2.3. Definir el alcance

La norma ISO/IEC 27001:2013 indica definir de manera adecuada el alcance del SGSI para poder conocer los límites de acción. Como primera medida la empresa establece el alcance del SGSI, siendo definido de acuerdo con las características del negocio. Para este proyecto el alcance no implica abarcar toda la empresa, sino iniciar con un alcance limitado que involucre el proceso crítico del negocio.

La Edpyme CREDIVISIÓN, de conformidad con la norma ISO/IEC 27001:2013 establece que el alcance del Sistema de Gestión de Seguridad de Información comprende el proceso de créditos que contiene los siguientes subprocesos: 1). Otorgamiento de Créditos y 2). Recuperación de Créditos. Ver Anexo 1

3.1.3 Fase 3: Diseño

En esta fase se realiza la elaboración y recopilación de todo lo mencionado en la norma ISO/IEC 27001:2013, para garantizar la confidencialidad, integridad y disponibilidad asociado al Diseño del Sistema de Gestión de Seguridad de la Información (SGSI).

3.1.3.1. Política de la seguridad de información

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

Edpyme Credivisión, en cumplimiento con las normativas vigentes, y para el ejercicio de sus funciones, se compromete a preservar la confidencialidad, integridad y

disponibilidad de los activos de información y la continuidad de nuestras operaciones, mediante una adecuada gestión de riesgos.

En referencia al punto anterior, se describe las siguientes políticas de seguridad de la información (Anexo 2), basado en los principios seguridad de la información; debiendo ser evaluados periódicamente para una mejora continua y cumplimiento de los objetivos de la empresa.

3.1.3.2. Estructura Organizacional del SGSI

Como lo indica el numeral 5.1 del estándar, el compromiso y la participación que tenga la dirección es esencial para desarrollar y mantener un SGSI efectivo en el tiempo. La dirección ayuda a crear una cultura de seguridad de la información y educar a todos los miembros de la organización.

En la Edpyme, se pensaba que al área de TI o Riesgos pueden tomar el control también de las funciones y acciones relevantes inherentes a la seguridad. Sin embargo, se presentan una serie de inconvenientes, como la no independencia en las funciones de seguridad de la información relacionados con TI y el conflicto de interés al actuar como juez y parte.

Teniendo presente, estos inconvenientes, se propone una estructura como la que se muestra en la figura 13.



Fig. 13 Estructura Organizacional del SGSI

A continuación, se describen los diferentes roles:

➤ **Gerencia General / Directorio**

La Gerencia General y Directorio debe aprobar la política de gestión de seguridad de la Información, asignar los roles en materia de seguridad y coordinar el seguimiento de los planes de la seguridad en la organización.

➤ **Comité de Seguridad de la información**

Son los encargados de planificar y gestionar los recursos y el ambiente para llevar adelante la gestión de riesgos y el establecimiento del SGSI. Asimismo, Planifica y define los documentos y contenidos del SGSI y gestiona la aprobación de directorio. Considera mejoras al SGSI en función de los resultados y métricas. Este comité lleva un rol de liderazgo del SGSI, y debe tener un rol ejecutivo para asegurarse que se cumplan las actividades y etapas requeridas. Conformado por:

- Gerente General.
- Gerente de Administración y Finanzas.
- Gerente de Riesgos.
- Jefe de TI.
- Gerente de Negocios.
- Coordinador del SGSI.

➤ **Coordinador del SGSI**

Es el principal responsable operativo de la implementación, operación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI). Funciones:

- ✓ Elaborar políticas específicas de seguridad de la información manual, procedimientos, planes, instructivos, metodologías, guías, formatos y documentación en general del SGSI.
- ✓ Coordinar el proceso de gestión de riesgos con los respectivos dueños de procesos dentro del alcance del SGSI.
- ✓ Evaluar, coordinar y monitorear la implementación de controles resultantes de la gestión de riesgos de seguridad de la información.
- ✓ Registrar, evaluar y realizar seguimiento de los incidentes de seguridad de la información.
- ✓ Elaborar el plan de concientización en seguridad de la información.
- ✓ Elaborar el programa anual de auditorías del SGSI.

➤ **Representante del proceso**

Responsable de la seguridad del activo de información que está bajo su control, asimismo asume la propiedad del riesgo. Sus funciones específicas son: Función:

- ✓ Tomar medidas para minimizar el riesgo por pérdida o exposición de los activos de información que están bajo su responsabilidad.
- ✓ Asegurar que el personal a su cargo asuma su responsabilidad en el cumplimiento de los controles de seguridad de la información.
- ✓ Apoyar activamente en las actividades de identificación, análisis, evaluación y tratamientos de riesgos de seguridad de la información
- ✓ Brindar información oportuna y pertinente para la elaboración de indicadores y métricas, auditoría, revisión y mejora continua del SGSI.
- ✓ Realizar y mantener actualizado el inventario de activos de información de su proceso.

3.1.3.3. Metodología de evaluación de riesgos

Los resultados del Tratamiento de riesgos serán revisados en un ciclo de mejora continua que se realizará anualmente para coordinación e identificación de cualquier modificación, de tal forma asegurar un control de riesgos de forma aceptable.

La evaluación de riesgos se llevó a cabo según la metodología indicada en la figura 14, la cual permitió asegurar una gestión de riesgos aceptable. Ver Anexo 3.



Fig. 14 Metodología de Riesgos

3.3.1. Inventario de Activos

Se debe iniciar con la elaboración del inventario de activos de información del proceso considerado dentro del alcance del SGSI. Los activos de información identificados serán valorados en base a los criterios de confidencialidad, integridad y disponibilidad sobre los mismos. La decisión de utilizar una escala cuantitativa a una cualitativa es netamente de preferencia organizacional, pues ambos tipos de valoración podrían ser utilizados para el mismo activo.

3.3.1.1. Tipos de Activos de Información

Para agrupar los distintos tipos de activos de información, se define 5 tipo: información, software, tangibles, servicio, y personas.

a. Información

- ✓ **Información Física:** Información que se encuentra impresa o manuscrita, y que se utiliza para ciertas actividades del proceso.
- ✓ **Información Digital:** Información intangible que se genera en el proceso y que se encuentra almacenada en un medio (magnético, óptico, electromagnético, etc.), fuentes (base de datos, cuadro, texto, archivo, documento, etc.) y formatos (pdf, xls, txt, etc.).
- ✓ **Información Audible:** Información producida por la voz humana en una conversación, llamada telefónica, reunión, grabación, etc.

b. Software

Conjunto de programas que puede ejecutar el hardware para la realización de las tareas de computación a las que se destina: Sistemas operativos, aplicativos, utilitarios, módulos, entre otros.

c. Tangibles

Conjunto de elementos materiales (hardware) que componen un equipo informático u otros equipos. Son de dos tipos:

- ✓ **Entorno tecnológico:**
 - Servidores: Servidores Aplicaciones, Servidores Call Center, entre otros.
 - Equipos de comunicación: Router, switch, modem, firewall, appliance, entre otros.

- ✓ **Entorno físico:** Edificios, ambiente, oficina, mobiliario, entre otros, donde se alojan los activos tangibles y los colaboradores.

d. Servicio

Tales como Energía Eléctrica, Agua, Red, Conexión VPN, Telefonía, Servicio de Correo Electrónico. Estos servicios se apoyan generalmente en elementos de hardware (cables, tubos, etc.) y software, pero los usuarios los perciben como servicios.

e. Personas

Personas que componen la EDPYME CREDIVISIÓN y ejecutan tareas propias del negocio.

3.3.1.2. Metodología de Inventario y Valorización de Activos de Información

a. Inventario de Activos de Información

El inventario de los activos de información se obtuvo como parte del alcance del Sistema de Gestión de Seguridad de la Información. Se han definido algunos atributos en función del tipo de activo. Todo activo o grupo de activos tiene un propietario, además de otros atributos que son detallados en los formatos de inventarios de activos de información (Anexo 9)

El principal activo de la información, aunque sea redundante es la misma información, para ello debe tomarse en cuenta el formato en el que se encuentra la información (txt, base de datos, Excel, formato físico preimpreso, etc.). Es necesario considerar que la información es conjunto de datos significativos y pertinentes que describan sucesos o entidades.

b. Valorización de activos para determinar la importancia del activo (CID)

La estimación del valor de importancia de un activo de información está en función a la Confidencialidad-Integridad-Disponibilidad (CID), tomando en cuenta las obligaciones o requisitos del negocio, la parte legal y lo contractual. Esta importancia es definida por el responsable del activo con el apoyo del responsable de seguridad de la información. A continuación, en la tabla 6, se definen estos términos, así como los valores de importancia:

Tabla N°6 Valorización de Activos

ESCALA	VALOR DE IMPORTANCIA
5	MUY ALTO
4	ALTO
3	MEDIO
2	BAJO
1	MUY BAJO

c. **Dimensiones de la Información:** las dimensiones se describen en tabla 7

Tabla N°7 Dimensiones de la información

DIMENSIÓN	DESCRIPCIÓN
Confidencialidad	Acceso a la información por parte únicamente de quienes estén autorizados.
Integridad	Cambio de la información por un agente, por error o en forma deliberada.
Disponibilidad	Asegurar la disponibilidad de la información por parte de los usuarios autorizados en el momento que ellos lo requieran.

Confidencialidad

Estos valores se obtienen de acuerdo a la clasificación del activo, tabla 8:

- ✓ **Información Reservada:** Información con mayor grado de sensibilidad; el acceso a esta información es solo por el propietario o es muy restringido y autorizado caso por caso.
- ✓ **Información Confidencial:** Información sensible que solo será divulgada a aquellos colaboradores que la necesiten para el cumplimiento de sus funciones.
- ✓ **Información de uso Interno:** Datos generados para facilitar las operaciones diarias; serán manejados de una manera discreta.
- ✓ **Información Pública:** Información que es generada específicamente para su divulgación masiva o que no tiene ninguna reserva.

Tabla N°8 Valorización de Confidencialidad

Muy Alto	5 MA	Información Reservada.
Alto	4 A	Información Confidencial.
Medio	3 M	Información Interna.
Bajo	2 B	Información Pública.

Integridad:

¿Qué tan importante es para el negocio de la EDPYME CREDIVISIÓN que este activo mantenga su integridad?, en la tabla 9 se detalla la valorización.

La falta de integridad del activo (por error/adulteración/accidente):

Tabla N°9 Valorización de Integridad

Muy Alto	5 MA	Tiene el potencial de replicarse y afectar el objetivo del proceso.
Alto	4 A	Afecta la integridad de una parte de la información del proceso.
Medio	3 M	Afecta la integridad de la información de una o más actividades medianamente importantes.
Bajo	2 B	Afecta la integridad de una actividad del proceso.
Muy Bajo	1 MB	La integridad del activo tiene poca importancia.

Disponibilidad

¿Qué tan importante es para la Institución que este activo mantenga su disponibilidad? En la tabla 10, muestra la falta de disponibilidad del activo:

Tabla N°10 Valorización de Disponibilidad

Muy Alto	5 MA	Puede paralizar/dificultar el flujo de producción de varios procesos importante de línea.
Alto	4 A	Ocasiona un incumplimiento del negocio, contractual / Afecta la producción de un proceso.

Medio	3 M	Afecta la disponibilidad de información de varias actividades.
Bajo	2 B	Afecta el funcionamiento de una actividad sin importancia.
Muy Bajo	1 MB	La disponibilidad del activo tiene poca importancia.

d. Importancia del Activo (Total)

Para la información, se toma el valor promedio para todos los activos, como se muestra en tabla 11.

VALOR DEL ACTIVO = Promedio (Confidencialidad, Integridad, Disponibilidad)

Tabla N°11 Valorización Total del Activo

PROMEDIO ARITMÉTICO	VALOR DEL ACTIVO	SIGNIFICADO
[5]	5 (MA)	Importancia Muy Alta
[4]	4 (A)	Importancia Alta
[3]	3 (M)	Importancia Media
[2]	2 (B)	Importancia Baja
[1]	1 (MB)	Importancia Muy Baja

Los activos cuya importancia sea Muy Alta pasarán a la fase de Análisis de Riesgos.

En la tabla 12 del Rango Aritmético, para los valores que resulten en números decimales.

Tabla N°12 Rango Aritmético para decimales

Rango Aritmético	Criterio de Valoración
1.3 – 1.4	1
1.5 – 2.4	2
2.5 – 3.4	3
3.5 – 4.4	4
4.5 - 5	5

3.3.2. Análisis de Riesgos

Tomando como base el Anexo 4, se realiza un análisis de riesgos donde se identifican amenazas y vulnerabilidades que exponen los activos de información más importantes (Anexo 10), así como los controles existentes que se tienen para proteger a los activos de estas amenazas. Con esta data se estiman la degradación del activo y se determina un nivel de impacto, luego se identifica probabilidad según tabla 19; con estos resultados se determina el nivel de riesgo según tabla Matriz de Riesgo (Tabla 20)

Los activos de Información que son analizados son los resultados del Inventario de Activos, los cuales pasan a la fase de Análisis de Riesgos Por cada activo de información, se genera la siguiente información:

- a. Por cada activo de información, se listan las Amenazas a las que está expuesta y se intenta identificar algún Agente específico que la genere, y la causa del mismo.
- b. Por cada amenaza, se listan las vulnerabilidades que expone el activo y que podrían ser aprovechadas por la amenaza, así como los controles existentes para prevenir la materialización de la amenaza, disuadir al agente, detectar la amenaza o corregir el daño sufrido.

A. Amenaza, Vulnerabilidades y Controles Existentes

Amenaza es una causa potencial de un incidente no deseado, que puede resultar en un daño para la organización o el sistema. El responsable de Activo debe listar las amenazas que afectan a los activos a su cargo y cuáles son las causas por las cuales se produce la amenaza.

Ejemplos de Amenaza son: Falsificación de documentos presentados por el cliente, fuga de Información que figura en los sistemas de la Edpyme, Incendio, etc.

Es necesario tener en cuenta que entre las amenazas existen dependencias como por ejemplo la denegación de un servicio es causada por una mala operación o por un código malicioso, adicionalmente el código malicioso es una amenaza que es causada por un cracker, el impacto de esta amenaza

esta dado que puede paralizar un servicio y a la vez puede paralizar todo un proceso critico de un negocio.

A.1. Tipo de Amenazas

Si bien las amenazas pueden ser de tipos muy variados, para propósitos de análisis se establecen algunos tipos de amenaza que se van a utilizar tabla 13:

Tabla N°13 Tipo de Amenazas

Cód.	Amenaza	Agente
A1	Fuego	Natural, falla eléctrica, agente externo.
A2	Daños por agua	Baños, tuberías, lluvias
A3	Desastres naturales (terremotos, tormenta, huaico, etc.)	Naturales
A4	Desastres industriales	Empresas cercanas, equipos industriales
A5	Contaminación mecánica (vibraciones, polvo, suciedad, etc.)	Ambiente
A6	Contaminación electromagnética (radio, campos magnéticos, etc.)	Equipos de comunicación
A7	Fallas de los equipos	Fabricación, falta o mal mantenimiento
A8	Falla lógica (fallos en los programas, etc.)	Programador, empresa, control calidad
A9	Corte de suministro eléctrico	Falla cables, tablero, trafo, empresa
A10	Condiciones inadecuadas de temperatura y humedad.	Mala o falla en la ambientación, Natural
A11	Falla de servicios de comunicación	Equipos de comunicación, proveedor, cable

Cód.	Amenaza	Agente
A12	Interrupción de otros servicios y suministros esenciales.	Equipos, empresas
A13	Errores de usuarios	Usuarios no capacitados o incompetentes
A14	Errores de administrador	Administrador no capacitado o incompetente
A15	Errores de monitorización	Falla equipo, incumplimiento de personal
A16	Errores de configuración	Personal no capacitado o incompetente
A17	Fuga de información	Personal interno y/o externo
A18	Alteración de la información	Error humano o deliberado
A19	Destrucción de la información	Falla proceso, deliberado, mal manejo
A20	Errores de mantenimiento	Personal no capacitado o incompetente
A21	Caída de sistemas por agotamiento de recursos	Incumplimiento de especificaciones, saturación
A22	Ausencia del personal	Huelga, enfermedad, vacaciones
A23	Denegación de servicio	Hacker, saturación, mal proceso
A24	Vandalismo	Hacker, personal descontento
A25	Sabotaje	Hacker, personal interno o externo
A26	Código malicioso	Hacker, personal interno, programador
A27	Otros	

Nota: Cuando la amenaza descrita por el entrevistado no encaje en ninguno de los tipos de amenaza listados, utilizar el código AO.

B. Degradación del Activo

De acuerdo con la metodología se valoriza la degradación de la confidencialidad, integridad y disponibilidad considerando las vulnerabilidades y los controles existentes para cada riesgo (se debe tener en cuenta la efectividad de esos controles), luego se va a poner el valor de degradación máximo el cual es asumido como el nivel de impacto de la seguridad de la información.

Luego se define la probabilidad según la tabla 14, el cual nos indica la posibilidad en las condiciones actuales que se llegue a materializar la amenaza.

Con el valor del impacto y la probabilidad de cada riesgo se determina con la matriz de riesgo el nivel muy bajo, bajo, medio, alto y muy alto.

Valores de Degradación

- **Degradación – Confidencialidad**

Tabla N°14 Degradación de Confidencialidad

5 MA	Un activo secreto es fácilmente vulnerado
4 A	Un activo confidencial es vulnerado o un activo secreto es difícilmente vulnerado
3 M	Un activo interno es fácilmente vulnerado o un activo confidencial es difícilmente vulnerado
2 B	Un activo interno es difícilmente vulnerado

- **Degradación – Integridad**

Tabla N°15 Degradación de Integridad

5 MA	Imposible de recuperar la información al 100%.
4 A	Se puede reconstruir con suma dificultad.
3 M	Se puede reconstruir a un costo razonable.
2 B	Se pueden obtener copias, aunque su obtención no es inmediata.
1 MB	Resulta fácil obtener la copia del activo.

- **Degradación – Disponibilidad**

Tabla N°16 Degradación de Disponibilidad

5 MA	Disponible en más de 24 horas o no se puede detectar
4 A	Disponible en más de 4 - 24 horas
3 M	Disponible en 1- 4 horas
2 B	Disponible en menos de 1 hora
1 MB	Disponible en cuestión de minutos

Degradación máxima: Se toma el valor máximo de las 3 degradaciones CID para el posterior cálculo del Impacto. Para el caso de información se determina el valor promedio entre la degradación y el valor del activo cuyo resultado es redondeado a nivel de décimas (r): Ej.: Si la degradación es 3.5 sería 4, si es 2.4 sería 2.

C. Impacto del Riesgo

Para este factor se considera evaluación cualitativa, tabla 17, con base a los siguientes niveles:

IMPACTO = Promedio Aritmético (Degradación y valor del activo)

Tabla N°17 Impacto del Riesgo

Promedio Aritmético	Valor del Impacto	Significado
1 (r)	1 (MB)	IMPACTO MUY BAJO
2 (r)	2 (B)	IMPACTO BAJO
3 (r)	3 (M)	IMPACTO MEDIO
4 (r)	4 (A)	IMPACTO ALTO
5 (r)	5 (MA)	IMPACTO MUY ALTO

Asimismo, cada nivel de impacto se tomará como referencia los valores cuantitativos determinados en la metodología de riesgo operacional tabla 18 (en nuevos soles):

Tabla N°18 Riesgo Operacional

1. Muy Bajo	2. Bajo	3. Medio	4. Alto	5. Muy Alto
<= 8,000	> 8,000 a <= 20,000	> 20,000 a <= 45,000	> 45,000 a <= 150,000	> 150,000

3.3.3. Evaluación de Riesgos

Probabilidad de Ocurrencia del Riesgo

Tabla N°19 Valores de Probabilidad

VALOR	PROBABILIDAD
5	Es probable que ocurra al menos una vez al mes
4	Es probable que ocurra más de una vez al año
3	Es probable que ocurra cada año
2	Es probable que ocurra cada 2 años
1	Es muy poco probable que pase cada 5 años

Valor del Riesgo por Niveles: Según tabla 20:

Tabla N°20 Matriz de Riesgos

PROBABILIDAD	Muy Alto	5	Alto	Alto	Muy Alto	Muy Alto	Muy Alto
	Alto	4	Medio	Alto	Alto	Muy Alto	Muy Alto
	Medio	3	Bajo	Medio	Medio	Alto	Muy Alto
	Bajo	2	Bajo	Bajo	Medio	Medio	Alto
	Muy Bajo	1	Bajo	Bajo	Bajo	Medio	Alto
MATRIZ DE RIESGOS			1	2	3	4	5
			Muy Bajo	Bajo	Medio	Alto	Muy Alto
			IMPACTO				

Los valores del riesgo se definen de acuerdo con la siguiente tabla 21:

Tabla N°21 Valor de Matriz de Riesgos

VALOR	RIESGO	DESCRIPCIÓN	SIGNIFICADO
B	Bajo	El activo vulnerado no causa un efecto en la información de la organización ni en el proceso	Es un riesgo aceptable, cuando el activo se encuentra expuesto a riesgos bajos o moderados, por lo que no amerita que pase al proceso de Tratamiento de Riesgo.
M	Moderado	El activo vulnerado no causa un efecto considerable en la información de la organización, pero si en alguna actividad del proceso.	
A	Alto	El activo vulnerado puede afectar considerablemente la información, ocasionando incumplimiento de metas, pérdidas económicas importantes, teniendo un efecto negativo en el proceso.	Cuando el activo se encuentra expuesto a riesgos altos o extremos que ameritan ser tratados.
E	Extremo	El activo vulnerado puede afectar seriamente la información de la organización, ocasionando incumplimientos críticos de servicio al cliente con pérdidas económicas muy importantes y daño considerable a la imagen de la institución.	

NOTA: Los Riesgos Altos o Extremos pasan a la fase de Tratamiento de Riesgos.

Los Riesgos Bajos o Moderados pasan a una fase de Monitoreo, siendo revisado periódicamente para verificar si permanece en su condición de aceptable.

El valor total resulta de la combinación del valor del riesgo con la cantidad de criterios aplicables. Luego se procede a ordenar los riesgos dándoles un orden de prioridad.

La evaluación del riesgo sirve para darle significancia y para identificar los riesgos que requerirán la aplicación priorizada de su tratamiento.

3.3.4. Tratamiento de Riesgos

En la tabla 22, se determina para cada riesgo a tratar cual va a ser la estrategia:

Tabla N°22 Tratamiento de Riesgos

TRATAMIENTO	DESCRIPCIÓN
Transferir	Transferir a un tercero con capacidad financiera / especialización necesaria para administrar adecuadamente.
Reducir	Esta estrategia consiste en actuar para reducir la probabilidad de ocurrencia o el impacto de un riesgo
Aceptar	Aceptar riesgo en su presente nivel debido a que no es posible realizar un tratamiento, justificando el motivo.
Evitar	El nivel de riesgo de la actividad es inaceptable, además no es posible eliminar las causas del riesgo (agente amenaza)

3.1.3.4. Elaborar el plan de tratamiento de riesgos.

Es elaborado o actualizado de ser el caso en base a las decisiones tomadas por la Gerencia, asimismo será aprobado, para su correspondiente implementación, la misma que contiene una serie de controles y recomendaciones básicas de seguridad que permita disminuir un alto grado de riesgo. Ver anexo 6

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

En el plan de tratamiento de riesgo (Anexo 12), se presentan dos columnas; costo aproximando y tiempo aproximado, los cuales se han estimado como sigue en las tablas 23 y 24 respectivamente.

Costo Aproximado

En la tabla 23, se proyecta una estimación del costo para implementar la función de protección propuesta.

Tabla N°23 Costo Aproximado

4	Mayor a S/.42,000
3	De S/.18.000 a S/.42,000
2	De S/.7.000 a S/. 18,000
1	Menor a S/.7,000
D	Desconocido

Tiempo Aproximado

En la tabla 24, se detalla la estimación del tiempo de implementación de la función de protección propuesta.

Tabla N°24 Tiempo Aproximado

C	Corto plazo (Menor a 3 meses)
M	Corto plazo (de 3 a 12 meses)
L	Largo plazo (Mayor a 12 meses)
D	Desconocido

3.1.3.5. Declaración de aplicabilidad (SOA)

El estándar ISO 27001:2013, exige la preparación de la declaración de aplicabilidad incluyendo controles que deben ser seleccionados. Para ello, se ha tenido en cuenta lo siguiente:

- Resultado del análisis de riesgos: luego de haber identificado los activos de información críticos y los riesgos a los que se encuentran expuestos, se ha tomado conocimiento de qué controles son necesarios para poder mitigar los riesgos.
- Resultado del análisis de brechas: brinda una visión general de qué controles ya se encuentran implementados y su grado de madurez.

Para la elaboración de la Declaración de aplicabilidad se ha hecho uso del detalle de los controles que se encuentran en la ISO 27002:2013. Este entregable se encuentra en el Anexo 12, en el documento de anexos que acompaña al proyecto donde se muestra la siguiente información:

- **Cláusula:** Dominios de seguridad de la información.

- **Objetivo de Control:** Descripción del control, en donde se refiere cada uno de los controles de la norma.
- **Control:** El cual hace referencia a un tema específico al que un riesgo puede estar asociado.
- **Aplicabilidad:** Se indica si el control en mención es aplicable a la organización o si no lo es.
- **Justificación:** La justificación de la aplicabilidad o no aplicabilidad del control.

Se evidencia en la Declaración de Aplicabilidad que para la Edpyme no aplican 21 controles del Anexo 1 de la norma ISO 27001:2013, según tabla 25:

Tabla N°25 Cantidad de Controles Aplicables

Cant.	Estatus	Significado	Contribución %
93	SI	El control SI es aplicable para la empresa	82%
21	NO	El control no es aplicable para la empresa ni para el negocio	18%
114			

3.1.3.6. Plan de capacitación y concientización

En este paso, el área de seguridad de TI evalúa la estrategia de entrenamiento que será desarrollada y aprobada, es importante que el programa de concientización y entrenamiento apoye las necesidades de negocio y sea relevante a la cultura organizacional.

Las herramientas de soporte del SGSI, exige que se otorguen los recursos pertinentes a fin de poder dar cabal cumplimiento con las fases de establecer, implementar, mantener y mejorar (modelo PHVA). Por ello para las diferentes actividades que se realizan durante el SGSI se han asignado personas, documentos, tecnología, capacitaciones y otras facilidades que son fundamentales para las operaciones.

Los requisitos exigidos por los numerales 7.2 y 7.3, que hacen referencia a las competencias y concientización del personal respectivamente, tienen actividades asociadas a su desenvolvimiento, las cuales han sido definidas en el plan de

capacitación, concientización y evaluación con los siguientes recursos y se muestra en la tabla 26:

Tabla N°26 Los recursos, competencias y concientización

RECURSO	DESCRIPCIÓN	HERRAMIENTAS
Evaluación del personal	Certificar si el personal asignado tiene la capacidad de cumplir con las tareas encomendadas a su cargo mediante evaluaciones según sus roles, sea por tener la educación necesaria o por experiencia adquirida, en caso contrario, deberá tomar un curso de actualización, capacitación según sea el caso	Evaluaciones de personal
Capacitación al personal	La capacitación está dirigida al personal que ha evidenciado deficiencias en su rol dentro de la organización o que es nuevo.	Diapositivas de capacitación
Concientización al personal	Se deben establecer charlas periódicas de concientización al personal, con la finalidad de recordar los diferentes riesgos cotidianos de seguridad de la información que podrán impactar en la organización.	Diapositivas de seguridad de la información
Control	Las capacitaciones y evaluaciones de concientización deben quedar registradas	Registros de capacitación y evaluación

a. Plan de Concienciación

Para ello se propuso las siguientes fases según tabla 27:

Tabla N°27 Fases de entrenamiento

FASE	DURACION
Ataque dirigido	Día 1
Distribución de material	Día 4
Proceso formativo 1	Día 5
Consejos de seguridad	Día 6
Recordatorio de ataque	Día 9
Proceso formativo 2	Día 12
Encuesta y valoración	Día 15

a.1 Ataque dirigido

Se realizó ataques dirigidos con la finalidad de concientizar a los empleados lo vulnerables que son y que deben procurar ser precavidos a la hora de confiar en los archivos que podrían llegar a su bandeja de entrada.

El procedimiento de ataque dirigido fue vía correo electrónico institucional, utilizando un archivo malware.

- Correo electrónico institucional con archivo malware

Para llevar a cabo este tipo de ataque dirigido se creó una cuenta ficticia con un nombre genérico que cuente con el nombre del departamento de la compañía involucrado como por ejemplo en este caso el del departamento de TI, apoyoti@credivisionperu.com.pe, esto con el fin de generar un correo de un área que aporte confianza al usuario y pueda este descargar el email.

Posteriormente se enviaron a las cuentas de correo que formarán parte de esta prueba. Es recomendable que el correo a ser enviado lleve incluido en copia al Gerente de Riesgos, quien debe conocer de las pruebas que se practicarán.

El procedimiento es que, al abrir el archivo mostrará una advertencia al usuario donde se indique que podría ser malicioso para el equipo; esta advertencia nos permitirá observar cual es la decisión del usuario en ese punto donde se da la advertencia de seguridad, al darle clic será abrirá el navegador web y dirigirlo automáticamente a la intranet local donde se mostrará lo peligro que acaba de realizar, así como las precauciones que debería tomar para no causar una infección por parte de algún tipo de malware en la red.

a.2 Distribución de material

Luego de haber realizado los ataques dirigidos, se buscó publicar las imágenes como fondos de pantalla y en la intranet.

Estas imágenes se publicaron y se cambió cada semana con nuevos enunciados para que los colaboradores tengan en cuenta las maneras de evitar peligros en aspectos de seguridad de la información.

a.3 Proceso formativo 1

Consiste es distribuir de forma organizada y espaciada (Videos y presentaciones en PowerPoint), material informativo a los colaboradores para que a través de ellos puedan obtener información útil sobre seguridad de la información, consejos y buenas prácticas.

a.4 Consejos de seguridad

Los consejos son imágenes que serán enviadas por correo electrónico y utilizadas como fondo de pantalla. Se publicará un consejo cada semana

a.5 Recordatorio de ataque

Se realizará una nueva prueba de ataques dirigidos a los empleados con el fin de que los colaboradores recuerden los consejos de seguridad ya explicados. Además, esto nos permitirá evaluar el impacto que este plan está teniendo en ellos con respecto a la concienciación en Seguridad de la Información.

a.6 Proceso formativo 2

Consiste es retroalimentar los términos de seguridad de la información, consejos y buenas prácticas a los colaboradores, utilizando los mismos mecanismos videos y presentaciones en PowerPoint.

a.7 Encuesta y valoración

Una vez terminado el plan de concienciación en la Edpyme CREDIVISIÓN, los colaboradores y jefes de área involucrados, deberán dar su opinión respecto a la experiencia sobre el proceso sensibilización.

Esto servirá de retroalimentación de información continua al equipo que ha implementado este plan para mejoras futuras.

b. Plan de Capacitación

El objetivo del plan es proveer a los colaboradores involucrados (Sistemas y Riesgos) una clara comprensión sobre las tareas que son capaces de resolver en tabla 28, mediante talleres y charlas que se buscará impartirles.

Tabla N°28 Plan de Capacitación

TEMA	DURACIÓN
Inducción a las políticas de seguridad de la información	Día 1
Respaldo de la información	Día 3
Lineamientos generales de la política de SGSI	Día 5
Gestión de incidentes de seguridad	Día 7

b.1 Inducción a las políticas de seguridad de la información

En dicha capacitación se abordará temas de:

- Política de Seguridad de la Información.
- Objetivos de Seguridad de la Información
- Consecuencias de incumplimiento del SGSI
- Beneficios.

Una vez culminada la charla de capacitación se tomará un examen para analizar cuanto conocimiento ha captado el personal y su posterior retroalimentación.

b.2 Respaldo de la información

En dicha capacitación se abordará temas de:

- Como hacer un respaldo
- Métodos para hacer respaldo de información
- Beneficios

Una vez culminada la charla de capacitación se tomará un examen para analizar cuanto conocimiento ha captado el personal y su posterior retroalimentación.

b.3 Lineamientos generales de la política de SGSI

En dicha capacitación se abordará temas como:

- Objetivos
- Alcance
- Responsabilidades
- Principios generales
- Monitoreo y análisis del SGSI

Una vez culminada la charla de capacitación se tomará un examen para analizar cuanto conocimiento ha captado el personal y su posterior retroalimentación.

b.4 Gestión de incidentes de seguridad

En dicha capacitación se abordará temas como:

- Niveles de Incidentes
- Clasificación de incidentes
- Reportar los incidentes a externos
- Evaluación de incidentes de seguridad

Una vez culminada la charla de capacitación se tomará un examen para analizar cuanto conocimiento ha captado el personal y su posterior retroalimentación.

3.1.3.7. Elaborar un plan de continuidad de negocio.

Se elabora los controles globales con el fin de identificar y disminuir todos los riesgos posibles, los resultados de este análisis son utilizados para la toma de decisiones respecto a las estrategias de recuperación. La misma que se visualiza en el formato de Plan de continuidad de negocio (Anexo 13), este documento está definido para ser utilizado en una situación de emergencia para la recuperación de procesos, recursos y acciones específicas a realizar.

3.1.3.8. Elaborar un acuerdo de confidencialidad.

Se elabora un acuerdo o convenio de confidencialidad entre la empresa y el empleado, cuyo objetivo es mantener en secreto cierta información reservada de la empresa durante la relación laboral, evitando que las partes implicadas puedan utilizar la información para sus propios fines. Este documento de acuerdo de confidencialidad (Anexo 14), señala que es una falta grave que amerita el despido, el uso o entrega a terceros de información reservada del empleador, así como la sustracción o la utilización no autorizada de documentos de la empresa.

3.1.3.9. Elaborar el manual del SGSI

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

Este manual se basa en los lineamientos solicitados por la norma ISO/IEC 27001:2013 y tiene como alcance el proceso créditos de la empresa. El contenido del manual aplica a todo el personal de la empresa. Este documento se puede revisar en su totalidad en el manual del SGSI (Anexo 15).

3.1.4 Fase 4: Pruebas

Las pruebas, la ejecución, los resultados y plan de mejoras se detallarán en el siguiente ítem 3.2.

3.1.5 Fase 5: Cierre

Una vez finalizado todas las etapas del proyecto del diseño del Sistema de Gestión Seguridad de la Información, para el proceso de créditos del área de Negocios; y haciendo entrega de la documentación requerida por la parte interesada, se acuerda dar por concluido el presente proyecto con el acta de cierre (Anexo 16).

3.2. TRATAMIENTO Y ANÁLISIS DE DATOS Y PRESENTACIÓN DE RESULTADOS.

La primera fase se desarrollará la planificación de los elementos que serán medidos a través de la descripción de los beneficios de los métodos de validación a aplicar, como estos se encuentran asociados a los objetivos específicos y su vinculación con la validación de los indicadores de logro descritos en el capítulo 1. Asimismo, se identificarán las pruebas que se realizarán mediante la presentación de los indicadores que se han elaborado para dicho fin.

La segunda fase se realizará un análisis de cada uno de las pruebas realizadas y acto posterior, como tercera fase, se procederá a realizar un contraste con los valores característicos de cada indicador, a fin de comparar resultados.

Como última fase, se identificarán qué acciones de mejora habrá que llevar a lugar de acuerdo con los valores obtenidos de cada uno de los indicadores.

3.2.1 Contrastación de la Hipótesis

Hipótesis nula

H₀: El diseño de un sistema de gestión de la seguridad de la información basado en la Norma ISO 27001:2013 aplicado a la Edpyme Credivisión, no permitirá mejorar la confidencialidad, integridad y disponibilidad.

Hipótesis alternativa

H₁: El diseño de un sistema de gestión de la seguridad de la información basado en la Norma ISO 27001:2013 aplicado a la Edpyme Credivisión, permitirá mejorar la confidencialidad, integridad y disponibilidad.

Nivel de significancia

El nivel de significancia será de 5% $\alpha=0.05$

Población

Se ha considerado los 226 activos que interactúan con el proceso de créditos

Muestra

Se ha considerado los 15 activos críticos del proceso de créditos

Instrumentos

Los instrumentos utilizados son los siguientes: Inventario de activos y anexo A de la norma ISO 27001:2013.

Procedimiento

Haciendo uso de la prueba T de Wilcoxon, el primer paso consiste en organizar los datos, luego en asignar el rango correspondiente a los valores absolutos de las diferencias, esto es, la diferencia absoluta menor recibe el rango 1, la que le sigue tiene el rango 2, etcétera sin tomar en cuenta el signo como lo muestra la tabla 29.

Tabla N°29 Procesamiento de datos

N° Activo	Pre SGSI	Pos SGSI	Difere	Rd	R+	R-
1	2	3	-1	3		3
2	3	5	-2	8		8
3	2	5	-3	12		12
4	2	5	-3	12		12
5	2	4	-2	8		8
6	3	4	-1	3		3
7	3	4	-1	3		3
8	3	5	-2	8		8
9	3	5	-2	8		8
10	4	5	-1	3		3
11	3	4	-1	3		3
12	1	5	-4	14.5		14.5
13	2	4	-2	8		8
14	2	5	-3	12		12
15	1	5	-4	14.5		14.5
				Sumas	0	120
				nDif	15	

Para el cálculo se escriben los diferentes valores de las diferencias de menor a mayor, luego se escribe la frecuencia los rangos, según tabla 30.

Tabla N°30 Cálculo de rangos

Diferencia	fi	RanOcupado	RangoAsignado	ei
1	5	1 a 5	3	60
2	5	6 a 10	8	60
3	3	11 a 13	12	12
4	2	14 a 15	14.5	3
			E	135

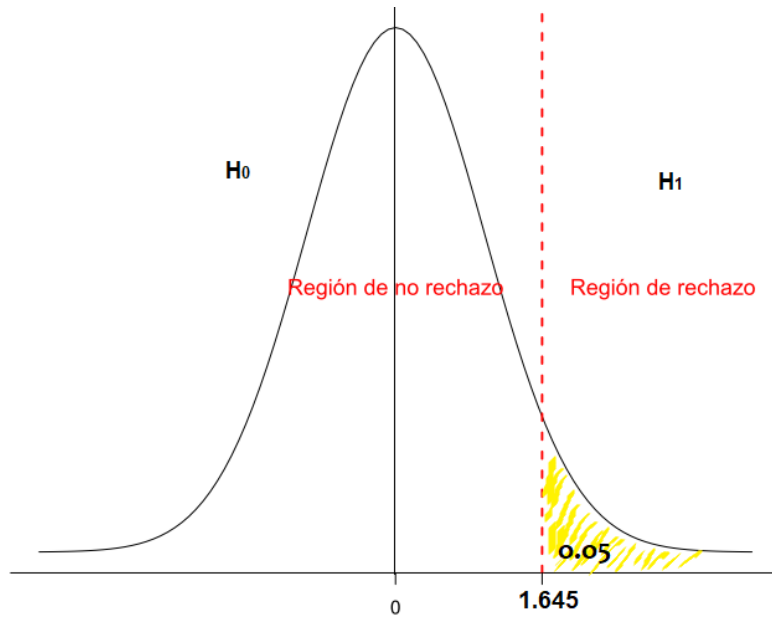


Fig. 15 Gráfico de Hipótesis

Regla de decisión:

- Si $Z_t \leq 1.645$ no se rechaza H_0 .
- Si $Z_t > 1.645$ se rechaza H_0 .

Donde:

$$ei = \frac{fi^3 - fi}{2}$$

$$E = \sum_{i=1}^{i=n} ei$$

N = número de diferencias distinto de cero ($N_{dif} = 15$)

El valor **T de Wilcoxon es 120**, luego se procede a calcular el error estándar:

$$eet = \sqrt{\frac{N(N+1)(2N+1)}{24} - E}$$

$$eet = 13.22875656$$

Se calcula la media de la nuestra distribución:

$$u_T = \frac{N(N + 1)}{4}$$

$$u_T = 60$$

Por último, se calcula la significación del estadístico de contraste Z:

$$Z_T = \frac{T - u_T}{\text{eet}}$$

$$Z_T = 4.5355$$

Conclusión:

Como 4.5355 es mayor a 1.645 se rechaza H_0 y se acepta la hipótesis alternativa H_1 .

3.2.2 Análisis de datos

Se determina el estado de cumplimiento inicial con respecto al anexo A, para saber el porcentaje de cumplimiento de las cláusulas y el nivel de madurez de los controles.

Resultados del estado de cumplimiento inicial

En la tabla 31 y 32 se presenta los resultados iniciales obtenidos a través del análisis GAP.

Tabla N°31 Cumplimiento Inicial de Clausulas

CLAUSULA	% CUMPLIMIENTO
4. CONTEXTO DE LA ORGANIZACIÓN	31%
5. LIDERAZGO	25%
6. PLANIFICACIÓN	30%
7. SOPORTE	32%
8. OPERACIÓN	28%
9. EVALUACION DEL DESEMPEÑO	26%
10. MEJORA	15%
Total	26.7%

Tabla N°32 Nivel de Madurez Inicial de Controles

DOMINIO	% CUMPL.
A.5. Políticas de seguridad de la información	7.0%
A.6. Organización de la seguridad de la informacion	10.1%
A.7. Seguridad relativa a los recursos humanos	0.0%
A.8. Gestion de activos	21.6%
A.9. Control de acceso	9.1%
A.11. Seguridad física y del entorno	16.7%
A.12. Seguridad de las operaciones	10.9%
A.13. Seguridad de las comunicaciones	8.0%
A.14. Adquisición, desarrollo y mantenimiento de los SI	7.0%
A.15. Relaciones con proveedores	7.0%
A.16. Gestión de incidentes de SI	4.0%
A.17. Aspectos de seguridad de la información para la GCN	14.0%
A.18. Cumplimiento	7.0%
Total	9.4%

Resultados del estado de cumplimiento final

En la tabla 33 y 34 se presenta los resultados finales obtenidos través del análisis GAP.

Tabla N°33 Cumplimiento Final de Clausulas

CLAUSULA	% CUMPLIMIENTO
4. CONTEXTO DE LA ORGANIZACIÓN	52%
5. LIDERAZGO	41%
6. PLANIFICACIÓN	43%
7. SOPORTE	43%
8. OPERACIÓN	48%
9. EVALUACION DEL DESEMPEÑO	46%
10. MEJORA	42%
Total	45.0%

Tabla N°34 Nivel de Madurez Inicial de Controles

DOMINIO	% CUMPL.
A.5. Políticas de seguridad de la información	50.0%
A.6. Organización de la seguridad de la informacion	45.0%
A.7. Seguridad relativa a los recursos humanos	34.4%
A.8. Gestion de activos	74.2%
A.9. Control de acceso	74.6%
A.11. Seguridad física y del entorno	74.3%
A.12. Seguridad de las operaciones	58.4%
A.13. Seguridad de las comunicaciones	69.1%
A.14. Adquisición, desarrollo y mantenimiento de los SI	43.0%
A.15. Relaciones con proveedores	40.0%
A.16. Gestión de incidentes de SI	55.1%
A.17. Aspectos de seguridad de la información para la GCN	93.0%
A.18. Cumplimiento	43.0%
Total	58.0%

Comparación de estado inicial vs estado Final

En la figura 16 se hace una comparación del estado inicial vs el estado final.

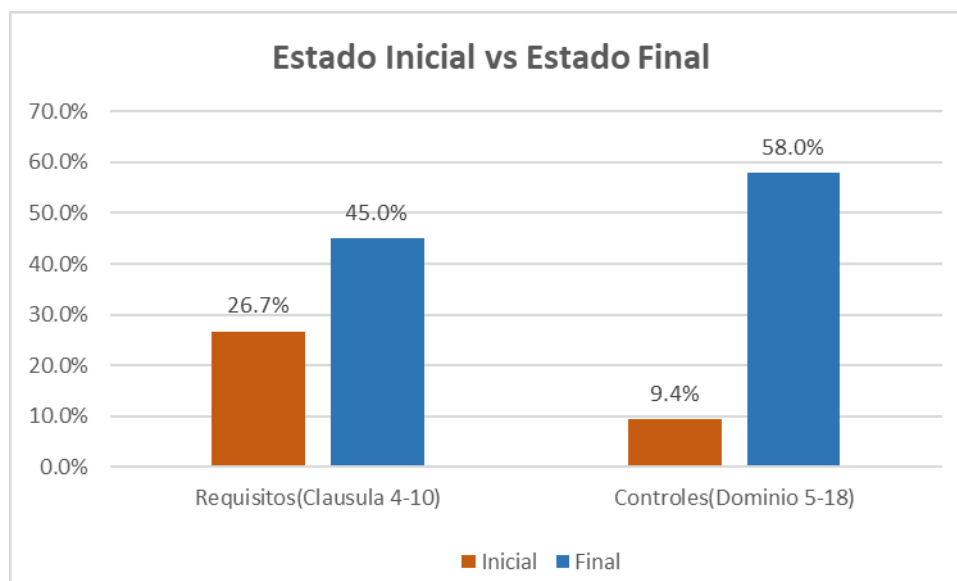


Fig. 16 Estado de Cumplimiento Inicial vs Estado Final

En base a la figura 16, los resultados muestran que en ambos casos se hallaron mejoras porcentuales, **esto conlleva a mejorar la confidencialidad, integridad y disponibilidad** del proceso de créditos.

A. Validación por el juicio de los expertos

Se estructura una ficha de validación con un total de 4 ítems, cada ítem tiene una valoración desde 0 a 5 puntos, obteniéndose un máximo de 20 puntos.

En el ítem 1 los expertos califican si el estado inicial y final calculado es el correcto, en el ítem 2 califican si el SGSI planteado mejora la confidencialidad, en el ítem 3 califican si el SGSI planteado mejoró la integridad y en el ítem 4 califican si el SGSI planteado mejoró la disponibilidad del proceso de créditos.

Para la validación de expertos, se utilizó fichas de observación las mismas que forman parte del anexo 16, donde se obtiene los resultados que se muestran en la tabla 35, que respaldan el proyecto de investigación:

Tabla N°35 Valoración de expertos

EXPERTO	VALORACIÓN (0 a 20)
Ing. Richard Riveros Flores	19
Ing. Eric Antonio Jimenez Mendoza	18

3.2.3 Descripción de los métodos de validación para los objetivos

La intención del presente plan es poder validar el desarrollo y cumplimiento de los objetivos específicos, puesto que se encuentra asociado al éxito del presente trabajo. Es por ello, que se han desarrollado indicadores que podrán:

- **Incrementar la responsabilidad:** Pueden incrementar la responsabilidad pues permiten identificar que controles o procesos no han sido implementados correctamente o no se encuentran implementados.
- **Evidencia de cumplimiento de requisitos:** Provisión documentada de evidencia que ayude a demostrar el cumplimiento de la normativa vigente.
- **Toma de decisiones:** Ayuda a la organización a poder controlar las fallas en inversión de seguridad de la información.

Dichos indicadores serán aplicados para medir la efectividad de cada uno de los indicadores de logro detallados en el presente trabajo, a efectos de validar su desarrollo, cumplimiento y efectividad. Se identifico 5 indicadores que ayuden a evaluar el cumplimiento de las políticas y controles definidos, tales como se muestran en la tabla 36:

Tabla N°36 Objetivos e indicadores de logro

OBJETIVOS DEL SGSI	INDICADORES	MÉTRICAS	META
Valorizar los activos de información, que soportan el proceso de créditos de la institución.	Matriz de valorización de activos de información.	Porcentaje de activos de información críticos	No supere el 70% de la totalidad de activos de información
Identificar los riesgos de seguridad de la información que afectan al proceso de créditos	Matriz de análisis de riesgos y mapa de riesgos	Exposición de pérdida anual en riesgos de seguridad de la información	No mayor al 10% del costo de control
Elaborar un plan que permita realizar un adecuado tratamiento de los riesgos.	Plan de tratamiento de riesgos	Porcentaje de riesgos que sobrepasan el	No mayor al 5% del total de riesgos no tolerables

OBJETIVOS DEL SGSI	INDICADORES	MÉTRICAS	META
	seguridad de la información.	nivel de tolerancia	
Determinar el estado de cumplimiento actual de la empresa con respecto al anexo A de la norma ISO 27001:2013.	Informe de análisis de brechas de seguridad de la información	Porcentaje de cumplimiento de las cláusulas de la normativa ISO 27001:2013	Estado de cumplimiento sea superior al 20%
		Nivel de madurez de los controles aplicables	Sea equivalente a un valor igual o mayor al nivel 4 (Gestionado)
Elaborar un plan que permita desarrollar e implementar los requisitos y controles de la norma ISO 27001:2013.	Plan de Seguridad de la Información	Porcentaje de empleados que han participado en una capacitación de sensibilización del SGSI	Mayor al 85% de la totalidad de empleados
		Porcentaje de empleados que aprobaron el examen del total de Personas que dieron el examen	Mayor al 85% de la totalidad de empleados que dieron examen

Cada uno de los objetivos e indicadores detallados en la tabla anterior contará con los siguientes elementos en su descripción:

- **Definición del indicador:** Declaración de medición, generalmente descrita usando una palabra como "porcentaje", "número", "frecuencia" y "promedio".
- **Objetivo:** Se determina el propósito de la medición.
- **Fórmula de cálculo:** Cómo debería ser evaluada, calculada o puntuado.
- **Características de indicador:** Resultado deseado de la medición.
- **Responsables:** Encargada de recopilar la información y procesar la medida.







- **Fuente:** Posibles fuentes como base de datos, herramientas de seguimiento, organizaciones externas o roles individuales.
- **Frecuencia:** Con qué frecuencia se deben recopilar e informar los datos.
- **Reporte:** Cómo se deben informar estos reportes.

3.2.4 Descripción y ejecución de pruebas a realizar

3.2.2.1. Prueba para indicador 1, según Objetivo Específico 1

Tabla N°37 Objetivo Específico 1

OBJETIVOS DEL SGSI	INDICADORES	MÉTRICAS
Determinar el estado de cumplimiento actual de la empresa con respecto al anexo A de la norma ISO 27001:2013.	Informe de análisis de brechas de seguridad de la información	Porcentaje de cumplimiento de las cláusulas de la normativa ISO 27001:2013
		Nivel de madurez de los controles aplicables

Definición de Indicador	
Nombre	Grado de cumplimiento de las cláusulas de la normativa ISO 27001:2013
Objetivo	Determinar el nivel de madurez de los controles del sistema de seguridad de la información
Cálculo	<p>a. Estado de cumplimiento de los controles = $\frac{(\sum \text{Cantidad de grado de cumplimiento})}{\text{Cantidad de controles aplicables}} \times 100\%$</p> <p>b. Nivel de madurez de controles = $\frac{(\sum \text{Nivel de madurez actual})}{\text{Cantidad de Controles por dominio}} \times 100\%$</p>
Características del indicador	<p style="text-align: center;">  81% - 100 % Nivel 5: Optimizado  61% - 80% Nivel 4: Administrado  41% - 60% Nivel 3: Definido  21% - 40% Nivel 2: Repetible  0% - 20% Nivel 1: Inicial  0% Nivel 0: Inexistente </p> <p> Nivel 5: Nivel óptimo alcanzado, con mejora continua Nivel 4. Nivel deseado, se debe monitorizar y medir Nivel 3: Los controles existen, se encuentran documentados y actualizados Nivel 2: Los controles existen, pero no están documentados ni gestionados Nivel 1: Existe cierto reconocimiento de la necesidad de los controles y no están alineados Nivel 0: No hay reconocimiento de la necesidad del control </p>
Responsables	Coordinador del SGSI
Fuente	Coordinador del SGSI
Frecuencia	Recolección: Semestral Reporte: Semestral
Reporte	Gráfico de barras

El presente indicador hará uso como fuente de información el Informe de análisis de brechas (anexo 3) que fue desarrollado mediante la metodología detallada en el punto 3.6.4., dado que en este se encuentra detallado el nivel de madurez de cada uno de los controles de seguridad de la información. Se hará uso de las evaluaciones al cumplimiento de los capítulos de la normativa 27001:2013 y a las cláusulas de la normativa 27002:2013.

El indicador representará 2 valores, las cuales se detallarán a continuación:

- **Requisitos:** Mide el grado de cumplimiento actual de los capítulos del 4-10 de la normativa.
- **Controles:** Mide el grado de cumplimiento actual de los dominios del 5-18 de la normativa.

Para su cálculo se usará la fórmula descrita en el indicador, a efectos de poder obtener posteriormente una gráfica que nos permita observar el reporte. La revisión de estas métricas deberá ser semestral, dado que esa será la frecuencia con el que será actualizado por parte del coordinador del SGSI.

Pruebas realizadas (a)

Para la realización de esta métrica ha sido necesario realizar una revisión al análisis de brechas de seguridad de la información ubicada en el Anexo 3 del presente trabajo, la cual ha seguido como guía la metodología desarrollada en el Plan Estratégico de Seguridad de la Información en donde se ubica los niveles de madurez. Es así como se ha podido determinar qué cantidad de controles cumplen cierto nivel de madurez siendo el resultado que se detalla:

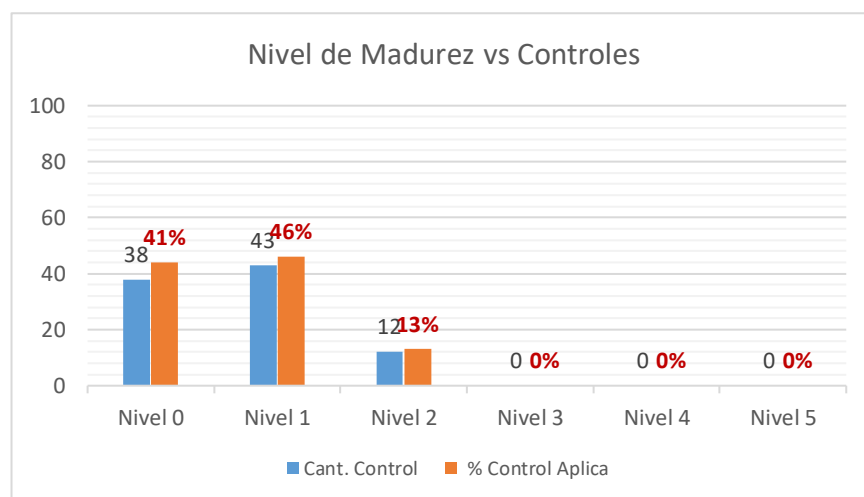


Fig. 17 Nivel de Madurez vs Controles

Según la figura 17, se determina que el nivel de madurez de todos los controles del anexo A de la norma ISO/IEC 27001:2013; teniendo como resultado que el “Nivel 0 Inexistentes” ocupa un 41% y el “Nivel 1 Inicial”, con un 46% de la cantidad de controles.

Resultados (a)

De acuerdo con lo evidenciado se observa que la mayoría de los controles se encuentra con un nivel de madurez entre Inexistente (cero) e inicial (uno) siendo estos los que mayor cantidad se ha podido apreciar. Eso lleva a deducir que de existir procedimientos estos no se encuentran bien definidos por lo que la organización se limita a contar con un nivel muy bajo con respecto a la madurez de sus controles.

Pruebas realizadas (b)

Esta métrica se orienta a validar el nivel de madurez inicial en el que se encuentra a la entidad financiera, se evalúa el nivel de acuerdo con los requerimientos por el Anexo 1 de la norma 27001:2013, así como los requisitos de la misma norma contenidos en las cláusulas del 4 al 10, los cuales son mandatorios. En la figura 18, se puede apreciar el nivel de madurez de acuerdo con cada evaluación.

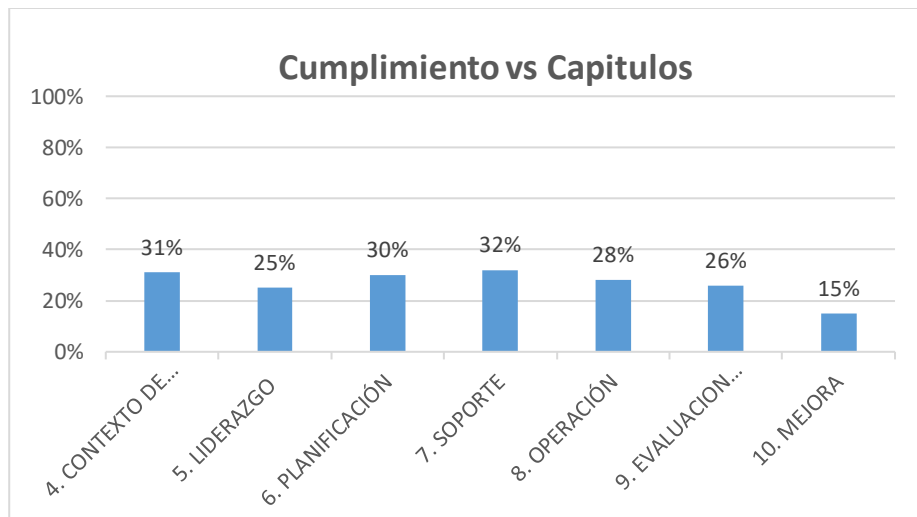


Fig. 18 Cumplimiento vs Capítulos

A efectos de poder conocer el cumplimiento de la normativa 27001, se procedió a evaluar en qué estado se encuentra cada cláusula de tal manera que permita poder conocer el contexto de cada una de ellas. En ese sentido, se puede apreciar que el cumplimiento a nivel general de la Edpyme Credivisión está en nivel 2, es decir que los controles existen, pero no están documentados ni gestionados.

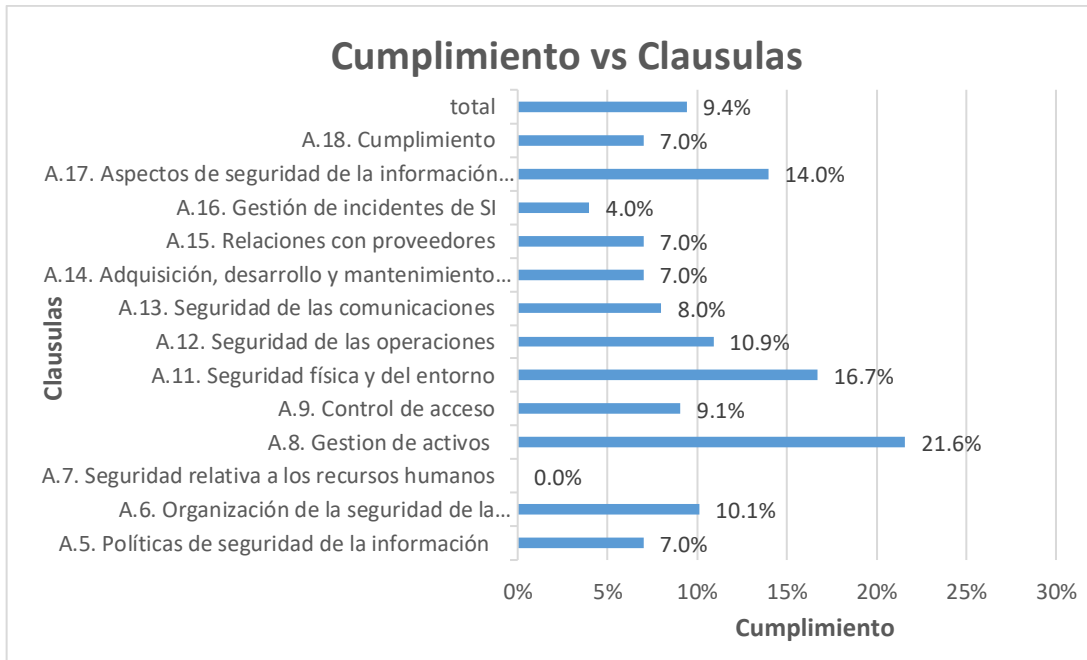


Fig. 19 Cumplimiento vs Clausulas

Asimismo, como se evidencia en la figura 19, se procedió a evaluar cada uno de los dominios de control de la cláusula, con el objetivo de poder determinar el nivel de cumplimiento de cada uno de ellos. En el resultado se puede observar que el nivel más mínimo lo obtienen los aspectos de seguridad relativa a los recursos humanos, gestión de incidentes los cuales cuentan con un cumplimiento igual o inferior al del 4%.

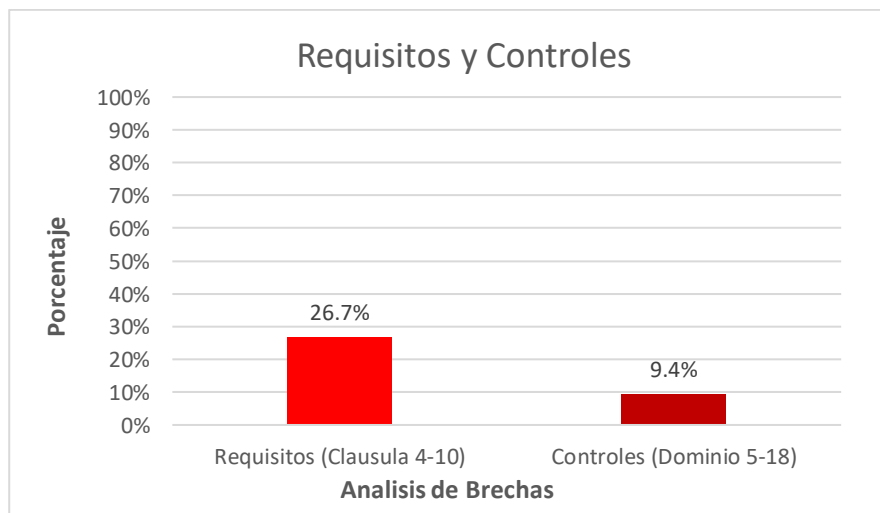


Fig. 20 Requisitos y Controles

Como se observa en la figura 20, la entidad tiene un bajo nivel inicial de madurez, tanto en los capítulos como en los controles de seguridad del Anexo 1 de la norma. Esto es debido a que nunca se ha contado con un estándar de seguridad de la información antes en la entidad.




Resultados

La entidad se posiciona en un estado rojo en el semáforo, pues no representan entre ambos más del 20%. Esto se debe a que no existían políticas, procedimientos y lineamientos de seguridad de la información. Se propone practicar este procedimiento luego de implementar el presente diseño a efectos de evaluar la evolución del sistema de gestión.

3.2.2.2. Prueba para indicador 2, según Objetivo Específico 2

Tabla N°38 Objetivo Específico 2

OBJETIVOS DEL SGSI	INDICADOR	MÉTRICAS
Valorizar los activos de información, que soportan el proceso de créditos de la institución.	Matriz de valorización de activos de información.	Porcentaje de activos de información críticos

Definición de Indicador	
Nombre	Porcentaje de cumplimiento de las cláusulas de la normativa ISO 27001:2013
Objetivo	Determinar la cantidad de activos críticos de información que se han logrado identificar.
Cálculo	$\% \text{ de activos críticos} = \frac{(\text{Cantidad de activos críticos})}{\text{Cantidad total de activos de información}} \times 100\%$
	<p>  Mayor a 60 %  Entre 31% y 60%  Menor a 30% </p> <p> Rojo: La mayoría de los activos de información son críticos. Amarillo: Casi la mayoría de los activos son críticos Verde: Los activos de información críticos son menos </p>
Responsables	Propietario del activo Coordinador de SGSI
Fuente	Inventario de Activos
Frecuencia	Recolección: Mensual (cada 2 meses) Análisis y Reporte: Semestral Revisión de métricas: Anual
Reporte	Gráfico de barras

El presente indicador hará uso como fuente de información el inventario de activos (anexo 5) que fue desarrollado mediante la metodología detallada en el punto 3.4.3., dado que en él se encuentra el registro de cada uno de los activos que maneja la Edpyme Credivisión.

Para obtener el inventario de activos se utilizó entrevistas que fueron dirigida a los trabajadores del área de TI, créditos y riesgos; y con ello se logró determinar cuáles son los activos de información involucrados en dicho proceso.

Posteriormente, se valorizó los activos según su grado de importancia y criticidad en la empresa. Primero, se valoriza la afectación o pérdida que le puede generar a la empresa en los aspectos financieros, legal y de imagen institucional, puesto que si se materializase una amenaza sobre el activo afectará su confidencialidad, integridad y disponibilidad.

El indicador representará básicamente 2 valores, las cuales se detallarán a continuación:

- **Críticos:** Cantidad de activos de información que han sido plenamente identificados críticos de acuerdo a su valor de tasación.
- **Total:** Cantidad de activos de información total plenamente valorizados.

Para el cálculo se usará la fórmula de descrita en el indicador, a efectos de poder obtener posteriormente una gráfica que permita observar el reporte.

La revisión de esta métrica deberá sea anual, dado que esa será la frecuencia con el que será actualizado por parte de los propietarios de información.

Pruebas Realizadas

En la siguiente figura 21, se muestra la cantidad de activos de información que han sido identificados de acuerdo a su valoración, estos datos fueron recopilados mediante el seguimiento al inventario de activos, así como a los riesgos asociados a ellos.

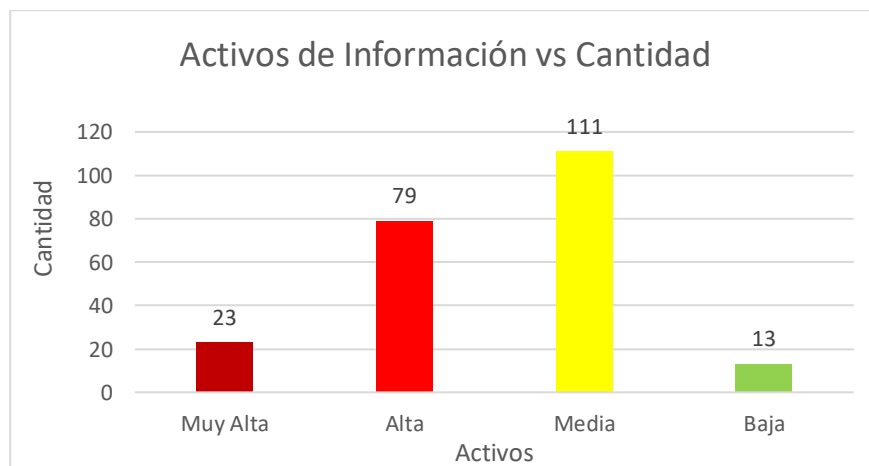


Fig. 21 Activos de Información vs Porcentaje

Como se puede observar en la figura 21, se tiene que los activos de información han llegado a ser valorizados plenamente, obteniendo como producto de tal ejercicio activos de información de carácter crítico (muy alta y alta), medio, bajo y muy bajo. Los activos críticos de información representan el 45.14% del total de los activos identificados debido a que la entidad financiera trabaja más con aquellos activos de información que la comprometen con riesgos financieros de acuerdo con lo requerido por los objetivos de negocio.



Resultados

Comparando estos resultados con los rangos del semáforo especificado para el indicador en evaluación, **este encuentra en un nivel ámbar** puesto que la organización viene pasando por diversas auditorias de la SBS que ayudan a gestionar mejor los activos de información.

3.2.2.3. Prueba para indicador 3, según Objetivo Específico 3

Tabla N°39 Objetivo Específico 3

OBJETIVOS DEL SGSI	INDICADORES	MÉTRICAS
Identificar los riesgos de seguridad de la información que afectan al proceso de créditos	Matriz de análisis de riesgos y mapa de riesgos	Exposición de pérdida anual en riesgos de seguridad de la información

Definición de Indicador	
Nombre	Exposición de pérdida anual en riesgos de seguridad de la información
Objetivo	Determinar la esperanza de pérdida anualizada que produciría en caso de materializarse los riesgos de seguridad más críticos.
Cálculo	Exposición de pérdida anual =Tasa anual de ocurrencia * Esperanza de pérdida única
	 ALE > Control  ALE < Control Verde: Valor no supera el valor del ALE. Rojo: Valor es mayor que valor del ALE.
Responsables	Coordindador de SGSI
Fuente	Matriz de Riesgos
Frecuencia	Recolección: Semestral Análisis y Reporte: Semestral Revisión de métricas: Anual
Reporte	Gráfico de barras

El presente indicador hará uso como fuente de información la matriz de riesgos que se desprende del Informe de gestión de riesgos (Anexo 8) que fue desarrollado a detalle en el punto 3.4 del presente trabajo.

El indicador representará dos barras, las cuales representan lo siguiente:

- **Riesgos Críticos:** riesgos reportados previamente por el área de tecnologías como producto de sus incidentes diarios.
- **Total de riesgos:** riesgos identificados a la fecha, incluyendo a los detectados anteriormente.

El objetivo es poder visualizar que tanto se estaría perdiendo en caso se materializarán los riesgos de seguridad de la información más críticos. Dichos riesgos se encuentran asociados al ataque de personal interno.

Para su cálculo se usará la fórmula descrita en el indicador, a efectos de poder obtener posteriormente una gráfica que permita observar el reporte. La revisión de estas métricas deberá ser anual, dado que se realizará una gestión de riesgos nueva cada año.

Pruebas realizadas

La presente métrica se realiza mediante el cálculo del ALE (Exposición de pérdida anual) es una fórmula algebraica que multiplica el valor de un evento discreto de pérdida (expectativa de pérdida individual o SLE) por su expectativa anual de ocurrencia (ARO), es decir, la pérdida monetaria que se puede esperar para un activo debido a la materialización de una o más amenazas en un periodo de un año. Se define a través de la siguiente fórmula:

$$\mathbf{ALE = SLE \times ARO}$$

$$\mathbf{SLE = FE \times VA}$$

Donde:

- ✓ ALE: Expectativa de Pérdida Anual
- ✓ SLE: Expectativa de Pérdida Individual
- ✓ ARO: Tasa de Ocurrencia Anualizada
- ✓ FE: Factor de Exposición
- ✓ VA: Valor del activo

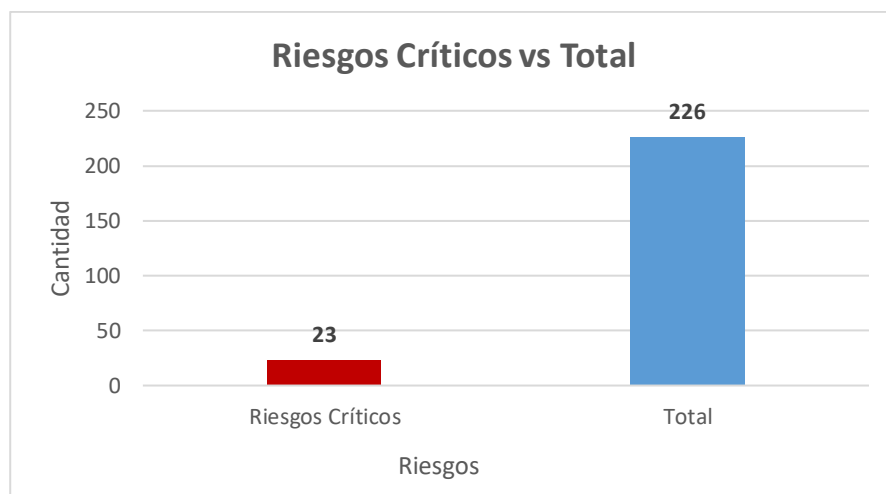


Fig. 22 Riesgos Críticos vs Total

Como se observa la figura 22, como producto de los análisis realizados se ha obtenido una cantidad de riesgos críticos que representan casi la décima parte del total de riesgos de seguridad de la información. Sin embargo, todos estos riesgos críticos se encuentran asociados a acciones por parte de personal malintencionado dentro de la organización.

Resultados

A fin de comparar los resultados obtenidos con los rangos del semáforo especificado para el indicador en evaluación, se ha determinado que el valor del ARO (tasa anual de ocurrencia) va desde entre 40% y 50%. De tal manera el resultado que se obtiene como producto de $ARO \times SLE$ es menor valor a lo que la empresa perdería anualmente en caso se materializara alguno de estos riesgos críticos.

Para efectos del indicador, se observa en tabla 40, el valor no supera los costos que se incurriría en aplicar controles que mitiguen dichos riesgos de acuerdo al valor total del activo expresado en soles.

Tabla N°40 Resultados ALE




Riesgos	Valor S/	ARO	FE	ALE
Créditos mal colocados	S/ 50,000	50%	40%	S/ 10,000
Información errónea de los créditos	S/ 1,000	40%	20%	S/ 80
Error en la generación de pagares	S/ 25,000	50%	10%	S/ 1,250
Demora en la atención de Clientes	S/ 2,000	50%	30%	S/ 300
Pérdidas financieras de Caja	S/ 2,000	50%	30%	S/ 300

Riesgos	Valor S/	ARO	FE	ALE
Demora en la atención e insatisfacción de clientes	S/ 3,000	30%	20%	S/ 180
Indisponibilidad de aprobación de créditos	S/ 3,000	40%	20%	S/ 240
Indisponibilidad de JA para aprobación de Créditos	S/ 3,500	50%	20%	S/ 350
Indisponibilidad de GG para aprobación de Créditos	S/ 15,000	50%	30%	S/ 2,250
Sistemas expuestos a terceros	S/ 1,000	50%	30%	S/ 150
Robo de información de clientes y sus créditos	S/ 10,000	50%	20%	S/ 1,000
Robo de reportes de créditos a personas	S/ 50,000	50%	40%	S/ 10,000
Alteración de la información de clientes, lo cual genera pérdidas financieras.	S/ 70,000	50%	30%	S/ 10,500
Perdida de información e indisponibilidad del sistema	S/ 70,000	50%	20%	S/ 7,000
Demora en atención del Server Aplicaciones	S/ 70,000	50%	30%	S/ 10,500
Perdida de información y financieras	S/ 60,000	50%	30%	S/ 9,000
Pérdida de clientes y reputación	S/ 6,000	50%	20%	S/ 600
Mala reputación de la empresa	S/ 4,000	50%	40%	S/ 800
Indisponibilidad de JT para operatividad del Sistema	S/ 7,000	50%	40%	S/ 1,400
Indisponibilidad de JR para recuperación	S/ 1,000	50%	10%	S/ 50
Pérdidas financieras de Cartera	S/ 3,000	50%	30%	S/ 450
Demora en la evaluación de Créditos	S/ 9,000	50%	20%	S/ 900
Indisponibilidad de GR para evaluación	S/ 3,500	50%	10%	S/ 175

3.2.2.4. Prueba para indicador 4, según Objetivo Específico 4

Tabla N°41 Objetivo Específico 4

OBJETIVOS DEL SGSI	INDICADORES	MÉTRICAS
Elaborar un plan que permita realizar un adecuado tratamiento de los riesgos.	Plan de tratamiento de riesgos de seguridad de la información.	Porcentaje de riesgos que sobrepasan el nivel de tolerancia

Definición de Indicador	
Nombre	Porcentaje de riesgos que sobrepasan el nivel de tolerancia
Objetivo	Evaluar la exposición de la organización a la variación de los riesgos de seguridad de la información.
Cálculo	$\% \text{ de riesgos sobre el límite} = \frac{(\text{Nro Riesgos por encima del apetito de riesgo})}{\text{Nro Riesgos aceptables}} \times 100\%$
	<p>  Menor a 5  Ente 5 y 15  Mayor a 20 </p> <p> Verde: Se requiere revisar los parámetros definidos Amarillo: se requiere observación para evitar llegar a rojo Rojo: se requiere intervención y reevaluación de los riesgos </p>
Responsables	Coordindador de SGSI
Fuente	Registro de Riesgos
Frecuencia	Recolección: Semestral Reporte: Semestral
Reporte	Gráfico de barras

El presente indicador hará uso como fuente de información el plan de tratamiento de riesgos (Anexo 8) que fue desarrollado en base a la evaluación de riesgos que se hizo previamente, trasladando aquellos valores obtenidos bajo la metodología señalada en el punto 3.4.6. Bajo esos parámetros se definen las medidas que se tomaran ante los riesgos identificados.

El indicador representará dos resultados, los cuales se detallarán a continuación:

- **Riesgos aceptables:** Aquellos que luego de la aplicación del tratamiento de riesgos tienen como resultado una valoración aceptable.
- **Riesgos no aceptables:** Aquellos que luego de la aplicación del tratamiento de riesgos no son aceptados por la organización de acuerdo con el apetito de riesgo.

Para el cálculo se usará la fórmula descrita en el indicador, a efectos de poder obtener posteriormente una gráfica que permita observar el reporte.

El resultado permitirá conocer y medir con el tiempo que cantidad de riesgos la organización puede tolerar puesto que ha definido que los riesgos no aceptables no deben superar el cinco por ciento. La revisión de estas métricas deberá ser semestral, dado que esa será la frecuencia con el que será actualizado por parte del coordinador del SGSI.

Pruebas

La métrica se da a partir de que un riesgo aceptable puede cambiar su condición a no aceptable pues tanto el apetito de riesgo como el nivel de tolerancia pueden variar en el tiempo. En consecuencia, es necesario poder medir aquellas desviaciones en los riesgos a efectos de que sirvan de alerta para la entidad financiera. En la siguiente figura, se observa la variación de los datos recopilados.

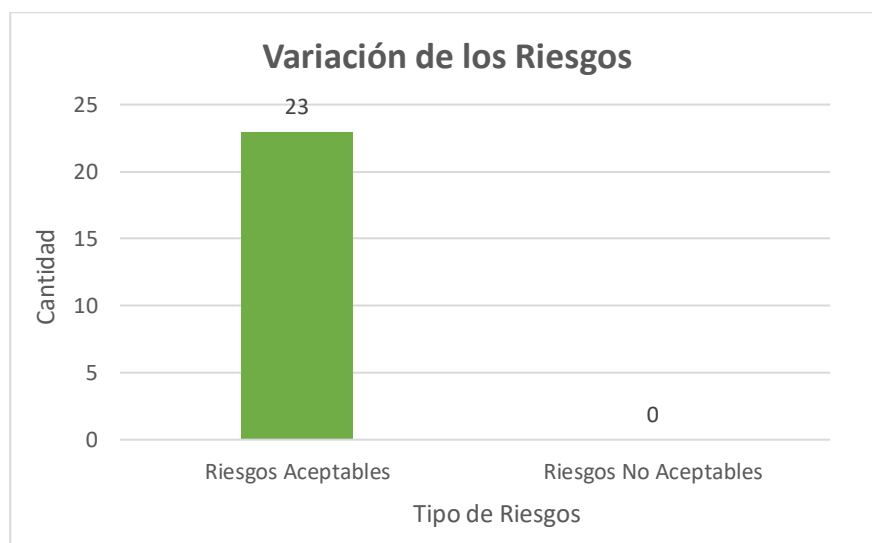


Fig. 23 Variación de Riesgos

Como se puede observar en la figura 23, no se cuenta con riesgo no aceptable que ha cambiado su condición.

Resultados




Comparando los resultados con los rangos del semáforo especificado para el indicador en evaluación se encuentra por encima del valor esperado, eso lo posiciona en un estado verde en el semáforo del indicador con un 0%.

En conclusión, se valida la realización del plan de tratamiento de riesgos de la información

3.2.2.5. Prueba para indicador 5, según Objetivo Específico 5

Tabla N°42 Objetivo Específico 5

OBJETIVOS DEL SGSI	INDICADORES	MÉTRICAS
Elaborar un plan que permita desarrollar e implementar los requisitos y controles de la norma ISO 27001:2013.	Plan de Seguridad de la Información	Porcentaje de empleados que han participado en una capacitación de sensibilización del SGSI
		Porcentaje de empleados que aprobaron el examen del total de Personas que dieron el examen

Definición de Indicador	
Nombre	Porcentaje de empleados que han participado y aprobado una capacitación de sensibilización del SGSI
Objetivo	Medir cuantos empleados han recibido y aprobado la inducción de seguridad de la información.
Cálculo	<p>a. % participantes capacitación= $\frac{(\text{N}^\circ \text{ de empleados que recibió la capacitación del SGSI})}{(\text{N}^\circ \text{ empleados que debe recibir la capacitación del SGSI})} \times 100\%$</p> <p>b. % aprobados capacitación= $\frac{(\text{N}^\circ \text{ de empleados que aprobaron la capacitación del SGSI})}{(\text{N}^\circ \text{ empleados que rindieron la capacitación del SGSI})} \times 100\%$</p>
Características del indicador	<p> Mayor a 81</p> <p> Entre 51 y 80</p> <p> Menor a 50 %</p> <p>Verde: No se requiere ninguna acción Amarillo: Se requiere retroalimentación Rojo: Se requiere intervención inmediata en sensibilización de SGSI</p>
Responsables	Dpto de Gente y Cultura Coordinador del SGSI
Fuente	Fichas de empleados, registro de capacitaciones, lista de participantes.
Frecuencia	Recolección: Mensual Análisis y Reporte: Semestral Revisión de métricas: Anual
Reporte	Gráfico de barras

El presente indicador hará uso como fuente de información el registro de empleados que tiene el departamento de Gente y Cultura, dado que en dicho registro se encuentra el perfil de cada colaborador de la organización que deberá ser capacitado en materias de seguridad de la información. Las charlas se llevarán a cabo durante el horario laboral siguiendo la metodología descrita en el punto 4.1.1., en donde se detalla el Plan de entrenamiento.

El indicador representará dos valores para a, los cuales se detallarán a continuación:

- **Con capacitación:** Personal que ha sido capacitado en prácticas de seguridad de la información.
- **Sin capacitación:** Personal que no ha recibido capacitación en seguridad de la información por diversas razones.

El indicador representará dos valores para b, los cuales se detallarán a continuación:

- **Aprobados:** Personal que aprobó la evaluación de prácticas de seguridad de la información.
- **Desaprobados:** Personal que no aprobó la evaluación de concientización en seguridad de la información.

Para su cálculo se usará la fórmula descrita en el indicador, a efectos de poder obtener posteriormente una gráfica que permita observar el reporte.

La revisión de estas métricas deberá ser anual, dado que permitirá realizar las programaciones para las capacitaciones y evaluaciones anuales por parte del departamento G&C en coordinación con el coordinador del SGSI.

Pruebas realizadas (a)

La presente métrica tiene como objetivo poder medir cuantos empleados han recibido las capacitaciones de inducción en seguridad de la información. En la figura 24, se aprecia cuantos colaboradores recibieron la capacitación.

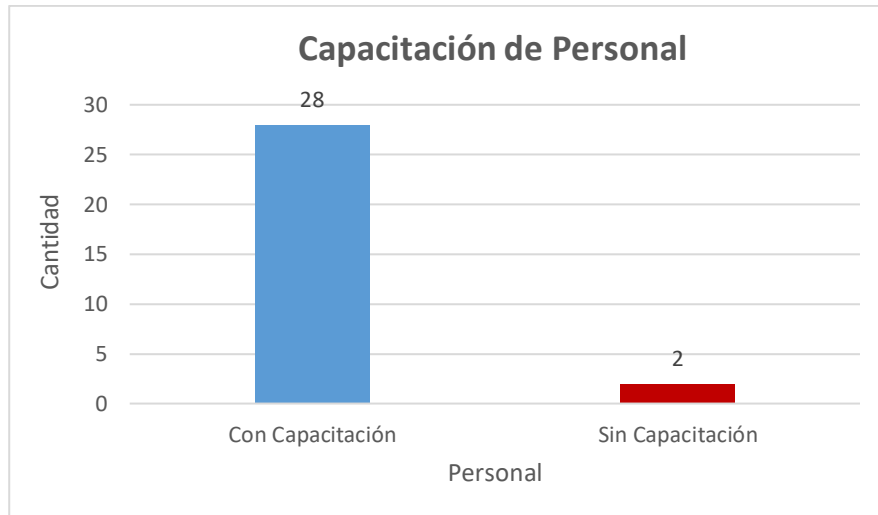


Fig. 24 Personal con capacitación vs sin capacitación

Como se observa, la cantidad de empleados que no recibieron la inducción es de 2 de un total de 30 empleados.

Resultado (a)

La entidad se posiciona en un estado verde debido a que el 93.3% de los colaboradores recibieron las capacitaciones. Las razones por las cuales los 2 trabajadores no hayan podido recibirlas podrían obedecer a vacaciones y permisos por salud.

Pruebas realizadas (b)

La presente métrica tiene como objetivo poder medir cuantos empleados han aprobado satisfactoriamente las capacitaciones de inducción en seguridad de la información. En la siguiente figura se aprecia cuántos colaboradores aprobaron la capacitación.

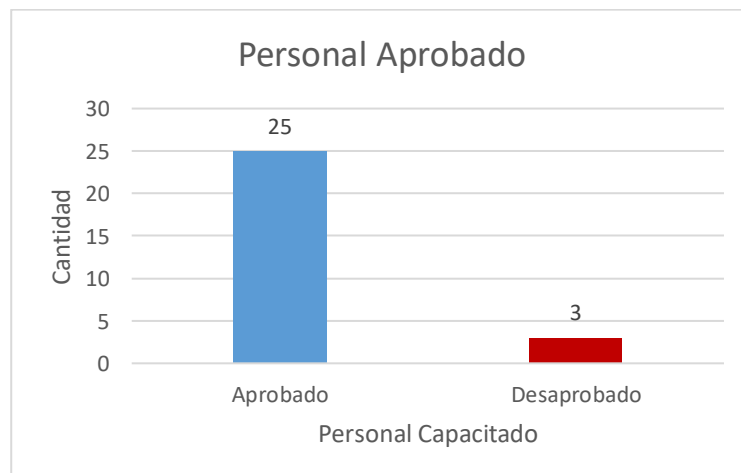


Fig. 25 Personal aprobado vs desaprobado

Como se observa en la figura 25, la cantidad de empleados que no aprobaron la capacitación es de 3 de un total de 28 empleados que fueron capacitados

Resultado (b)

La entidad se posiciona en un estado verde debido a que el 89.3% de los colaboradores aprobaron las capacitaciones.

Se recomienda realizar una retroalimentación a la capacitación a efectos de cumplir a cabalidad con los lineamientos dictados por la entidad financiera.

3.2.5 Plan de Mejoras

Debido a que, el presente proyecto no incluye la implementación del SGSI, más que solo su diseño, este no se incluye mejoras de implementación. Sin embargo, es necesario volver a emplear cada procedimiento descrito anteriormente, luego de haber implementado el diseño propuesto con el fin de evaluar la evolución del Sistema de Gestión de Seguridad de la Información.

CAPITULO IV. ANÁLISIS Y DISCUSIÓN DE RESULTADOS

DE LOS OBJETIVOS PLANTEADOS

- O.1.** En el presente diseño se establecieron lineamientos para determinar el nivel de madurez inicial de los requisitos y controles de la norma ISO 27001:2013 en la Edpyme, generando un resultado final de cumplimiento del 45.0% en los requisitos de los capítulos de la normativa y de 58.0% en los controles de dominio del Anexo A. Esto irá mejorando cada vez a medida que se vayan implementando las acciones definidas en dicho diseño del SGSI.
- O.2.** La valorización total de activos de información para el proceso de créditos en la Edpyme permitió que la entidad pueda identificar aquellos elementos que son críticos para los objetivos de negocio, favoreciendo a poder identificar a los responsables del manejo de los mismos, así como la periodicidad y clasificación. En base a esto, se indica que la financiera mejoró y seguirá mejorando significativamente la gestión de sus activos respecto a su estado inicial, garantizando así una forma efectiva en la gestión de riesgos.
- O.3.** Durante el desarrollo del proyecto, se logró identificar 23 riesgos críticos de un total de 226 riesgos que representa la décima parte del total, en base a la formula ALE, se concluye que en caso se materializarán los riesgos de seguridad de la información más críticos el valor no supera los costos que se incurriría en aplicar controles que mitiguen dichos riesgos de acuerdo al valor total del activo expresado en soles.
- O.4.** Durante el trabajo de investigación se ha elaborado un plan de tratamiento de riesgos de seguridad de información, asegurando el proceso Core y los objetivos de negocio a través de la selección de controles del Anexo A, en base a esto se indica que todos los riesgos críticos son riesgos aceptables.
- O.5.** La capacitación al personal en cuanto a temas de seguridad de la información tiene un alto nivel de concientización resultando con un total de participación del 93.3% de los cuales el 89.3% de los colaboradores aprobaron las capacitaciones. Esto irá mejorando cada vez a medida que se ejecute un plan anual de capacitaciones donde se incluya un proceso de retroalimentación.

DE LOS ANTECEDENTES

En este punto se discute los resultados obtenidos en la presente investigación y los resultados de los autores de las investigaciones tomadas como antecedentes. Esta discusión de resultados se rige a la finalidad de determinar si los objetivos planteados al iniciar esta investigación se cumplieron parcial o totalmente.

En el presente trabajo de investigación se da a conocer que es primordial que la alta gerencia se involucre y dé todo el apoyo para que se cumpla con los lineamientos de la seguridad de la información, caso contrario es difícil tener el apoyo de la organización. Lo mencionado anteriormente coincide con Carlos Alberto Guzmán Silva [6] en cuya investigación considera aspectos similares.

Se da conocer que desde el inicio del diseño del sistema de gestión de seguridad de la información es necesario el apoyo de la alta gerencia e involucrar a los dueños de los activos de información. Además, se considera que la implementación del SGSI se debe empezar por un(os) proceso(s) principales luego replicarlos en los demás procesos de la organización, dicho SGSI se debe revisar periódicamente lo cual conlleva a la incorporación de nuevos controles y activos. Dichos puntos coinciden con Luis Paolo Tapia Montoya [7], en su en su proyecto de Maestría.

Se menciona que un SGSI depende de las necesidades propias de una organización, y que la norma ISO/IEC 27001:2013 indica que es lo que se debe controlar, pero no indica el cómo controlarlo; por lo que depende de las organizaciones alinearlas con sus necesidades y objetivos del negocio. Misma conclusión menciona Jaime Fernando Vásquez Escalante [8], en su proyecto de tesis "Implementación del sistema de gestión ISO 27001:2013, para proteger la información en los procesos de TI".

CAPITULO V. CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Se logró identificar y clasificar 226 activos de información de la Edpyme CREDIVISIÓN que se interactúan en el proceso de créditos, de los cuales se concluye que los activos críticos representan el 45,14% del total, debido a ello, la empresa revisará periódicamente la metodología para lograr mitigar los riesgos encontrados.

Se identificó a través de la metodología ISO 27001:2005, 23 riesgos críticos (10.18% del total), los cuales mediante ALE se concluye que el valor de exposición de pérdida anual de cada riesgo no supera el valor total de cada activo.

Se elaboró un plan de tratamiento de riesgos, tomando como base los 23 riesgos identificados como críticos, estos no sobrepasan el nivel de tolerancia del 5% por lo cual se concluye como valido el plan de tratamiento de riesgos propuesto.

El nivel de cumplimiento en Edpyme Credivisión mejoró, teniendo como estado inicial el 26.7% con respecto a requisitos (clausulas) y 9.4% con respecto a los controles (dominio), mientras que estado final es del 45.0% con respecto a los requisitos (clausulas) y el 58.0% con respecto a los controles (dominio).

Se elaboró un plan que permita desarrollar los requisitos y controles mediante la participación de empleados en capacitaciones, el cual se tuvo una participación del 93.3% de los cuales el 89.3% aprobaron las capacitaciones, por la tanto se concluye que la participación si cumplió el objetivo planteado (más del 85%). Además, la importancia de establecer un plan anual de capacitación, formación y sensibilización en seguridad de la información, con el objetivo de fortalecer la cultura de seguridad en los colaboradores que laboran para la entidad.

RECOMENDACIONES

Se recomienda a la alta gerencia involucrar a todo el personal y difundir las normas de seguridad, estableciendo charlas de capacitación y concientización en toda la empresa, esto debido al poco conocimiento de seguridad de información que existe en la empresa.

La gerencia de riesgos debe realizar un análisis periódico de la brecha de controles, análisis de riesgos y los objetivos con una periodicidad no mayor a un año, y poder verificar el estado de los mismos y la efectividad de los controles existentes hasta que sea una práctica común en la Empresa.

Al finalizar el diseño del SGSI para el proceso de créditos, se recomienda al directorio optar por abarcar los demás procesos de la Edpyme, por tal motivo, es necesario el apoyo de la norma ISO/IEC 27001:2013, para asegurar la información sensible que maneja dicha organización.

REFERENCIAS BIBLIOGRÁFICAS

- [1] D. Abarca, «SeguridadAmerica,» Seguridad America, 30 03 2021. [En línea]. Available: <https://www.seguridadamerica.com/que-importancia-tiene-la-seguridad-de-la-informacion-para-las-empresas/>.
- [2] Prensario, «Prensario TI latin America,» Prensario TI latin America, 14 07 2021. [En línea]. Available: <https://prensariotila.com/29125-la-importancia-de-la-seguridad-bancaria/>.
- [3] M. Ríos, «Gestion,» Gestion, 01 09 2021. [En línea]. Available: <https://gestion.pe/economia/mas-del-7-de-creditos-en-cajas-y-edpymes-no-se-esta-pagando-segun-sbs-socorro-heysen-sistema-financiero-noticia/>.
- [4] E. Peruano, «EL Peruano,» Diario Oficial el Peruano, 19 02 2021. [En línea]. Available: <https://busquedas.elperuano.pe/normaslegales/aprueban-el-reglamento-para-la-gestion-de-la-seguridad-de-la-resolucion-no-504-2021-1929393-1/>.
- [5] Credivision, «Credivision,» Credivision, [En línea]. Available: <http://www.credivisionperu.com.pe/index.php?controlador=pagina&accion=detalle&id=1>.
- [6] C. A. Guzman Silva, «DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA UNA ENTIDAD FINANCIERA DE SEGUNDO PISO,» INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO, Bogota, 2015.
- [7] L. P. T. MONTOYA, «Metodología para la integración de la norma ISO/IEC 27001:2013 en una empresa industrial naviera,» Universidad de Buenos Aires, Buenos Aires, 2020.
- [8] J. F. V. Escalante, «Implementación del sistema de gestión ISO 27001:2013, para proteger la información en los procesos de TI,» Universidad Nacional Mayor de San Marcos , Lima, 2018.
- [9] P. SSI, «PMG SSI,» PMG SSI, 11 03 2021. [En línea]. Available: <https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/>.
- [10] P. SSI, «PMG SSI,» 05 05 2016. [En línea]. Available: <https://www.pmg-ssi.com/2016/05/como-utilizar-serie-sp-800-norma-iso-27001/>.
- [11] Fernando Jiménez, «GeniusIT,» 24 01 2018. [En línea]. Available: <https://geniusitt.com/blog/que-es-cobit-5/>.
- [12] C. ESAN, «ESAN,» 01 07 2016. [En línea]. Available: <https://www.esan.edu.pe/conexion-esan/los-cinco-principios-de-cobit-5>.

- [13] Normas-ISO, «Normas-ISO,» [En línea]. Available: <https://www.normas-iso.com/la-familia-iso/>.
- [14] grupoacms, «grupoacms,» [En línea]. Available: <https://www.grupoacms.com/consultora/cuales-son-los-tipos-de-normas-iso>.
- [15] pmg-ssi, «pmg-ssi,» 31 01 2014. [En línea]. Available: <https://www.pmg-ssi.com/2014/01/isoiec-27005-gestion-de-riesgos-de-la-seguridad-la-informacion/>.
- [16] pmg-ssi, «pmg-ssi,» 26 08 2021. [En línea]. Available: <https://www.pmg-ssi.com/2021/08/metodologia-nist-sp-800-30-para-el-analisis-de-riesgos-en-sgsi/>.
- [17] Camilo Gutiérrez Amaya, «welivesecurity.,» 14 05 2013. [En línea]. Available: <https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/>.
- [18] globalsuitesolutions, «globalsuitesolutions,» globalsuitesolutions, [En línea]. Available: <https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/>.
- [19] seguridadinoperu, «seguridadinoperu,» 02 05 2017. [En línea]. Available: <http://seguridadinoperu.blogspot.com/2017/05/isoiec-270012013-ciclo-de-mejora.html>.
- [20] isotools, «isotools,» [En línea]. Available: <https://www.isotools.com.mx/la-estructura-la-nueva-norma-iso-27001-2013/>.
- [21] pmg-ssi, «pmg-ssi,» 25 04 2019. [En línea]. Available: <https://www.pmg-ssi.com/2019/04/iso-27001-e-iso-27002-quien-fue-antes-el-huevo-o-la-gallina/>.
- [22] pmg-ssi, «pmg-ssi,» 05 04 2020. [En línea]. Available: <https://www.pmg-ssi.com/2020/03/anexo-a-en-iso-27001-objetivos-de-control-y-controles-de-referencia/>.
- [23] Paola, «grupo-fraga/,» [En línea]. Available: <https://grupo-fraga.com/6-pasos-para-realizar-el-analisis-de-brechas-segun-la-iso-27001/>.
- [24] Wikipedia, «Wikipedia,» 06 09 2021. [En línea]. Available: [https://es.wikipedia.org/wiki/Proceso_\(ingenier%C3%ADa\)](https://es.wikipedia.org/wiki/Proceso_(ingenier%C3%ADa)).
- [25] «PMG,» Pmg, 13 02 2017. [En línea]. Available: <https://www.pmg-ssi.com/2017/02/realizar-inventario-activos-de-informacion/#:~:text=Los%20activos%20de%20informaci%C3%B3n%20son,indirectamente%2C%20con%20las%20dem%C3%A1s%20entidades..>
- [26] Wikipedia, «Wikipedia,» Wikipedia, 08 11 2021. [En línea]. Available: https://es.wikipedia.org/wiki/Organizaci%C3%B3n_Internacional_de_Normalizaci%C3%B3n.

- [27] Diligent, «Diligent,» Diligent, 23 02 2022. [En línea]. Available: https://help.highbond.com/helpdocs/highbond/es/Content/projects/planning_projects/defining_risks_controls.htm.
- [28] Ciifen, «Ciifen,» Ciifen, [En línea]. Available: <https://ciifen.org/definicion-de-riesgo/>.
- [29] PMG, «PMG,» PMG, 05 03 2020. [En línea]. Available: <https://www.pmg-ssi.com/2020/03/anexo-a-en-iso-27001-objetivos-de-control-y-controles-de-referencia/#:~:text=El%20Anexo%20A%20es%20un,la%20informaci%C3%B3n%20de%20nuestra%20organizaci%C3%B3n..>
- [30] Wikipedia, «Wikipedia,» 12 10 2021. [En línea]. Available: https://es.wikipedia.org/wiki/Proceso_de_mejora_continua.
- [31] SBS, «SBS,» [En línea]. Available: <https://www.sbs.gob.pe/acercadelasbs>.
- [32] significados, «significados,» [En línea]. Available: <https://www.significados.com/informacion/>.
- [33] ESAN, «ESAN,» 13 08 2019. [En línea]. Available: <https://www.esan.edu.pe/conexion-esan/ciclo-pdca-conoce-de-que-trata-y-por-que-es-importante-para-las-empresas>.
- [34] mintic, «mintic,» [En línea]. Available: [https://mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Preguntas-frecuentes/5236:Estandares-y-Tecnologias#:~:text=Un%20est%C3%A1ndar%20\(como%20lo%20define,servicios%20cumplan%20con%20su%20proposito%22..](https://mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Preguntas-frecuentes/5236:Estandares-y-Tecnologias#:~:text=Un%20est%C3%A1ndar%20(como%20lo%20define,servicios%20cumplan%20con%20su%20proposito%22..)
- [35] wikipedia, «wikipedia,» 21 05 2022. [En línea]. Available: <https://es.wikipedia.org/wiki/Metodolog%C3%ADa>.
- [36] wikipedia, «wikipedia,» 22 11 2021. [En línea]. Available: <https://es.wikipedia.org/wiki/Inventario>.
- [37] escuelaeuropaexcelencia, «escuelaeuropaexcelencia,» 01 06 2021. [En línea]. Available: <https://www.escuelaeuropaexcelencia.com/2021/06/mitigacion-de-riesgos-proceso-de-3-pasos-para-hacer-frente-al-riesgo/#:~:text=La%20mitigaci%C3%B3n%20de%20riesgos%20es%20el%20proceso%20de%20desarrollo%20de,de%20un%20evento%20en%20particular..>
- [38] pmg-ssi., «pmg-ssi.,» 01 08 2019. [En línea]. Available: <https://www.pmg-ssi.com/2019/08/como-definir-el-alcance-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/#:~:text=El%20alcance%20nos%20ayuda%20a,para%20la%20organizaci%C3%B3n%2C%20es%20decir%2C>.

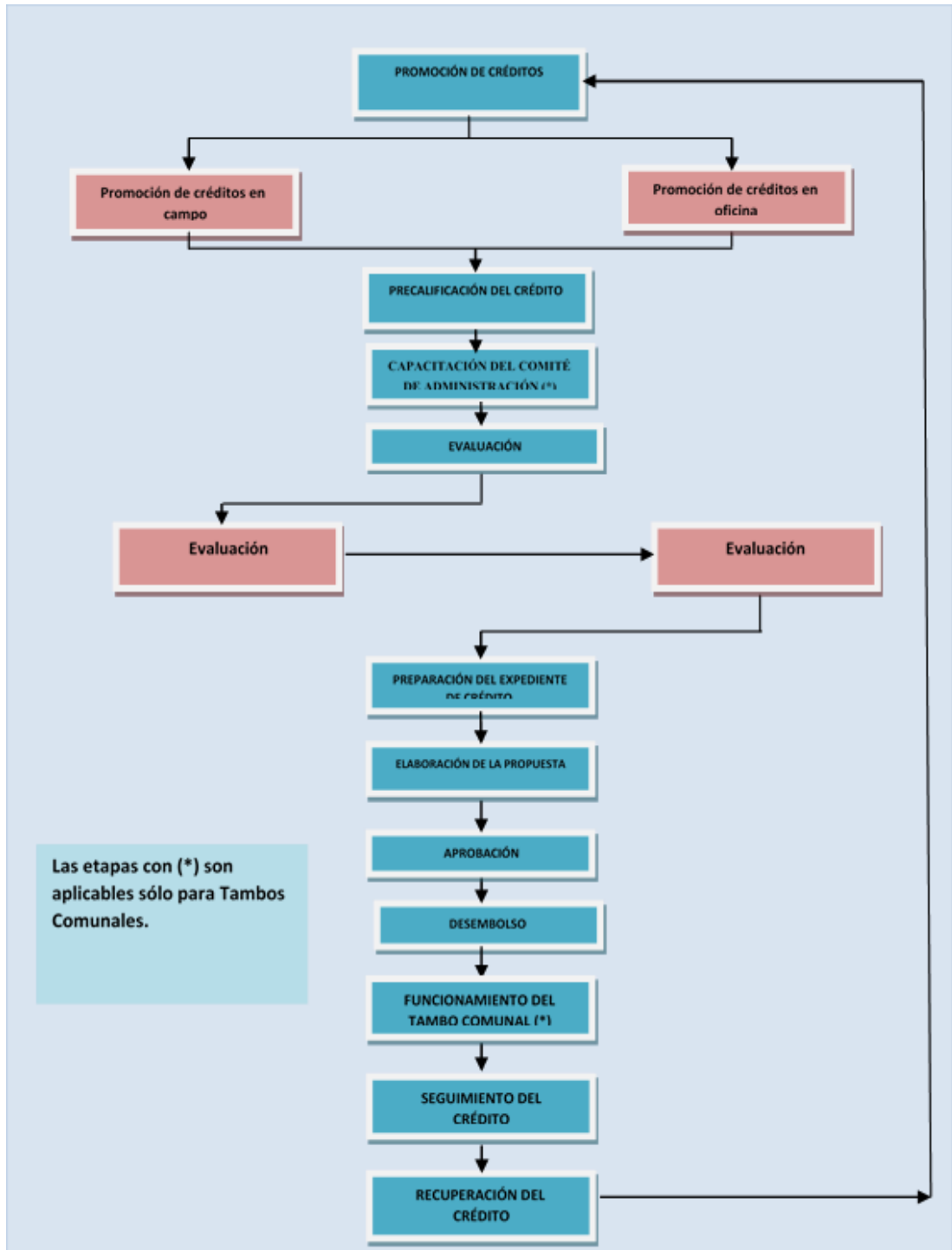
- [39] valuekeep, «valuekeep,» [En línea]. Available: <https://valuekeep.com/es/recursos/blog/mantenimiento-preventivo-y-correctivo/#:~:text=La%20principal%20diferencia%20entre%20estos,para%20prevenir%20fallos%20m%C3%A1s%20complejos.>
- [40] María Camila Arévalo J., «riesgoscero,» 14 02 2020. [En línea]. Available: https://www.riesgoscero.com/blog/las-buenas-practicas-de-la-seguridad-de-la-informaci%C3%B3n?hs_amp=true.
- [41] P. SSI, «PMG SSI,» PMG SSI, 14 08 2013. [En línea]. Available: <https://www.pmg-ssi.com/2013/08/la-nch-iso-27001-origen-y-evolucion/>.
- [42] I. Tools, «Iso Tools,» Iso Tools, 11 12 2013. [En línea]. Available: <https://www.isotools.pe/iso-27001-origen-y-evolucion/>.
- [43] P. SSI, «PMG SSI,» PMG SSI, 05 05 2016. [En línea]. Available: <https://www.pmg-ssi.com/2016/05/como-utilizar-serie-sp-800-norma-iso-27001/>.
- [44] Soportetic, «Soportetic,» Soportetic, 27 03 2021. [En línea]. Available: <https://soportetic.net/comparacion-de-estandares-y-marcos-de-seguridad-de-ti/>.
- [45] Nextech, «Nextech,» Nextech, 12 05 2021. [En línea]. Available: <https://nextech.pe/que-es-cobit-y-para-que-sirve/>.
- [46] ESAN, «ESAN,» ESAN , 01 06 2016. [En línea]. Available: <https://www.esan.edu.pe/apuntes-empresariales/2016/06/los-cinco-principios-de-cobit-5/>.
- [47] normaiso27001.es, «normaiso27001.es,» [En línea]. Available: <https://normaiso27001.es/#h1>.
- [48] D. Kosutic, «Advisera,» Advisera, [En línea]. Available: <https://advisera.com/27001academy/es/que-es-iso-27001/>.
- [49] heflo, «heflo,» [En línea]. Available: <https://www.heflo.com/es/blog/pdca/ciclo-pdca-concepto/>.

ANEXOS

Anexo 1. Alcance del SGSI

Formará parte del Alcance del Proyecto SGSI el proceso de créditos de la Edpyme Credivisión. El proceso de Créditos abarca a subprocesos:

- Otorgamiento de Créditos y
- Recuperación de Créditos.



Anexo 2. Políticas y Objetivos SGSI

OBJETIVOS

- Proteger, conservar y asegurar la información de la empresa y las herramientas tecnológicas utilizadas para su generación, procesamiento y disposición, con el fin de preservar la confidencialidad, integridad y disponibilidad frente a amenazas internas o externas, deliberadas o accidentales.
- Implementar y fortalecer los controles para la protección de los activos críticos.
- Educar y concientizar al personal para lograr servidores públicos competentes y comprometidos con una cultura de seguridad de la información reflejada en la aceptación y aplicación de las directrices de seguridad.
- Implementar una metodología de gestión de riesgos de seguridad de la información como herramienta para actuar proactivamente ante la presencia de situaciones que puedan afectar la continuidad, confidencialidad e integridad de la información de la empresa.

POLITICAS

- Asegurar la preservación de la confidencialidad, integridad y disponibilidad de los activos de información y la continuidad de nuestras operaciones, mediante una adecuada gestión de riesgos.
- Proteger la seguridad y salud de nuestros clientes, visitantes, colaboradores y proveedores; mediante la evaluación y control proactivo de los peligros y riesgos inherentes a nuestras operaciones.
- Notificar al encargado de seguridad y a mis jefes inmediatos, en caso de verificar el mal uso de los recursos por parte de algún otro empleado interno o externo al proceso de créditos.
- Participar de la capacitación y evaluación periódica del personal en temas referentes a la seguridad de la información
- Mantener un comportamiento ético, profesional, e independiente, desarrollando permanentemente nuestras habilidades y competencias técnicas.

Anexo 3. Enfoque de análisis, evaluación y tratamiento de riesgos

Riesgo por niveles

PROBABILIDAD	Muy Alto	5	Alto	Alto	Muy Alto	Muy Alto	Muy Alto
	Alto	4	Medio	Alto	Alto	Muy Alto	Muy Alto
	Medio	3	Bajo	Medio	Medio	Alto	Muy Alto
	Bajo	2	Bajo	Bajo	Medio	Medio	Alto
	Muy Bajo	1	Bajo	Bajo	Bajo	Medio	Alto
MATRIZ DE RIESGOS			1	2	3	4	5
			Muy Bajo	Bajo	Medio	Alto	Muy Alto
			IMPACTO				

La evaluación del riesgo sirve para darle significancia y para identificar los riesgos que requerirán la aplicación priorizada de su tratamiento.

Tratamiento del riesgo

TRATAMIENTO	DESCRIPCIÓN
Transferir	Transferir a un tercero con capacidad financiera / especialización necesaria para administrar adecuadamente.
Reducir	Esta estrategia consiste en actuar para reducir la probabilidad de ocurrencia o el impacto de un riesgo
Aceptar	Aceptar riesgo en su presente nivel debido a que no es posible realizar un tratamiento, justificando el motivo.
Evitar	El nivel de riesgo de la actividad es inaceptable, además no es posible eliminar las causas del riesgo (agente amenaza)

Anexo 4. Análisis, Evaluación y tratamiento de riesgos

La metodología de Gestión del Riesgo se ha dividido en 4 partes:

- i. Inventario de Activos de Información.
- ii. Análisis del Riesgo.
- iii. Evaluación del Riesgo.
- iv. Opciones de Tratamiento del Riesgo.

Por cada activo de definió:

- Código
- Proceso al que pertenece
- Nombre
- Tipo
- Propietario

Con el valor del impacto y la probabilidad de cada riesgo se determina con la matriz de riesgo el nivel muy bajo, bajo, medio, alto y muy alto.

El riesgo es la combinación de la probabilidad de una amenaza se materialice y las consecuencias que acarrea dicho ataque (Impacto). La fórmula es la siguiente:

$$\text{RIESGO} = (\text{Impacto} + \text{Probabilidad}) / 2$$

El criterio de aceptación del riesgo se detalla en:

Los Riesgos Altos o Extremos pasan a la fase de Tratamiento de Riesgos.

Los Riesgos Bajos o Moderados pasan a una fase de Monitoreo, siendo revisado periódicamente para verificar si permanece en su condición de aceptable.

Anexo 5. Enunciado de Aplicabilidad

- Seleccionar los controles adecuados que permitan mitigar los riesgos detectados en el análisis de riesgos del proceso de créditos.
- elaborar un enunciado de aplicabilidad que proporciona un resumen de las decisiones referentes con el tratamiento del riesgo.
- Justificar las exclusiones y proporcionar una comprobación para asegurar que ningún control haya sido omitido inesperadamente.

Anexo 6. Plan de tratamiento de Riesgos

- Definir acciones de gestión de acuerdo con el marco normativo del SGSI del proceso de créditos, en relación con los controles seleccionados del Anexo A de la ISO 27001.
- Desarrollar un cronograma para la implementación del marco normativo del SGSI del proceso de créditos donde se definan los tiempos y los responsables de la ejecución.
- Desarrollar un cronograma para la ejecución de actividades que mitigaran los riesgos detectados en el análisis de riesgo según la declaración de aplicabilidad y las opciones del tratamiento de riesgos.

Anexo 7. Carta de Autorización



Lima, 17 de marzo del 2022

Carta N° 032-2022/GG-ECV

Señor:
Jorge Burga Segovia
Analista de TI

Presente -

Referencia: Solicitud de fecha 18.02.2022

De mi mayor consideración,

Es grato saludarlo, y al mismo tiempo dar respuesta a su solicitud de fecha 18.02.2022, mediante la cual solicita permiso para realizar estudio de investigación para su proyecto de tesis "Diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI) para Edpyme CrediVision, basado en la Norma ISO 27001:2013", y así obtener el título de Ingeniero de Sistemas, precisando que cualquier resultado y/o conclusión al que pueda llegar como resultado de la investigación quedará en poder de Edpyme CrediVisión S.A

Al respecto, y luego de la evaluación efectuada, le comunicamos que hemos aprobado su solicitud, debiendo coordinar con el Jefe del Departamento de TI, el proceso y desarrollo de la investigación; y con el Departamento de Gente & Cultura la suscripción de un Acuerdo de Confidencialidad.

Sin otro particular y agradeciendo la atención a la presente, me despido.

Atentamente,

A handwritten signature in blue ink, appearing to read "Carlos Tamayo Caparó".

Carlos Tamayo Caparó
Gerente General



OFICINA PRINCIPAL
Av. Cesar Canevaro 133
San Juan de Miraflores, Lima
Telf.: (01) 224-5909

Anexo 8. Acta de constitución

ACTA DE CONSTITUCIÓN DEL PROYECTO

I. Información General

a. Nombre del Proyecto:

Diseño de un Sistema de Gestión de Seguridad de Información para la empresa Edpyme Credivisión basado en la norma ISO/IEC 27001:2013

b. Fecha: 18/02/2022

c. Preparado por: Jorge Burga Segovia

d. Revisado por: Richard Riveros Flores

e. Autorizado por: Carlos Tamayo Caparó

II. Descripción del Proyecto

En el proyecto de investigación se diseña un SGSI basado en la norma internacional ISO/IEC 27001:2013, que protege adecuadamente los activos de información de la empresa Edpyme CREDIVISIÓN

III. Necesidad del Proyecto

Proteger adecuadamente los activos de información de la empresa Edpyme CREDIVISIÓN.

IV. Objetivos del Proyecto

- Valorizar los activos de información, que soportan el proceso de créditos de la institución.
- Identificar los riesgos de seguridad de la información que afectan al proceso de créditos.
- Elaborar un plan que permita realizar un adecuado tratamiento de los riesgos.
- Determinar el estado de cumplimiento actual de la empresa con respecto al anexo A de la norma ISO 27001:2013.
- Elaborar un plan que permita desarrollar e implementar los requisitos y controles de la norma ISO 27001:2013.

V. Alcance del Proyecto

La Edpyme, de conformidad con la norma ISO/IEC 27001:2013 establece que el alcance del Sistema de Gestión de Seguridad de Información comprende el proceso de créditos que contiene los siguientes subprocesos: 1). Otorgamiento de Créditos y 2). Recuperación de Créditos

Anexo 9. Inventario de Activos de Información

INVENTARIO DE ACTIVOS - NEGOCIOS

ACTIVO: INFORMACIÓN

Código	Proceso	Nombre del Activo	Descripción	Propietario	Copropietario	C	I	D	Valor	Nivel
ICM-001	Promoción	Data de Clientes Pasivos	Archivo Excel que emite el SISGO que contiene la lista de clientes que no renovaron el crédito.	Jefe de TI	Jefe Zonal	3	4	4	4	Alta
ICM-002	Promoción	Trípticos de presentación	Material promocional para publicidad de los tipos de crédito	Jefe Zonal	Jefe Zonal	2	2	2	2	Baja
ICM-003	Promoción	Tarifario	Archivo en Excel con las tasas de acuerdo al monto y plazo.	Directorio	Jefe Zonal	2	3	5	3	Media
ICM-004	Promoción	Hoja de Ruta diaria	Formato para registrar clientes promocionados	Jefe Zonal	Jefe Zonal	3	3	3	3	Media
ICM-005	Evaluación	Lista de Chequeo - documentos del expediente de crédito	Formato para revisión de documento del expediente de crédito	Gerente General	Jefe Zonal y Gerente de Riesgos	3	3	3	3	Media
ICM-006	Evaluación	Solicitud de crédito	Formato N 1A	Gerente General	Jefe Zonal	5	5	5	5	Muy Alta
ICM-007	Evaluación	Solicitud de crédito Tambo Comunal	formato N 1B	Gerente General	Jefe Zonal	3	4	4	4	Alta
ICM-008	Evaluación	Solicitud de crédito-paralelo recurrente campaña	Formato 1E	Gerente General	Jefe Zonal	3	4	4	4	Alta
ICM-009	Evaluación	Solicitud de crédito Tambo Comunal (Recurrente)	Formato 1F	Gerente General	Jefe Zonal	3	4	4	4	Alta

Código	Proceso	Nombre del Activo	Descripción	Propietario	Copropietario	C	I	D	Valor	Nivel
ICM-010	Evaluación	Solicitud de Refinanciamiento	Formato 1H	Gerente General	Jefe Zonal	3	4	4	4	Alta
ICM-011	Evaluación	Declaración Jurada de Bienes y Patrimonio Familiar	Formato N 3A	Gerente General	Jefe Zonal	3	2	2	2	Baja
ICM-012	Evaluación	Declaración Jurada de Bienes y Patrimonio del Garante	Formato 3B	Gerente General	Jefe Zonal	3	2	2	2	Baja
ICM-013	Evaluación	Propuesta de créditos Tambos Comunales	Reporte que se genera del sistema SISGO	Jefe de TI y Gerente General	Jefe de Agencia	3	5	4	4	Alta
ICM-014	Evaluación	Resumen de comité	Reporte que se genera del sistema SISGO	Jefe de TI y Gerente General	Jefe de Agencia	3	4	3	3	Media
ICM-015	Evaluación	Hojas de trabajo para créditos individuales - BALANCE	Formato N 5	Gerente General	Jefe Zonal	3	5	4	4	Alta
ICM-016	Evaluación	Hoja de trabajo	Formato N 5A	Gerente General	Jefe Zonal	3	5	4	4	Alta
ICM-017	Evaluación	Hoja de trabajo de ventas	Formato 5B	Gerente General	Jefe Zonal	3	5	4	4	Alta
ICM-018	Evaluación	Hoja de trabajo de inventarios	Formato físico	Gerente General	Jefe Zonal	3	5	4	4	Alta
ICM-019	Evaluación	Hoja de trabajo de costos de producción	Formato Físico	Gerente General	Jefe Zonal	3	5	4	4	Alta
ICM-020	Evaluación	Hoja de recopilación de información	Formato 5	Gerente General	Jefe Zonal	3	5	4	4	Alta
ICM-021	Evaluación	Formulario de supervisión de créditos	Formato N8	Gerente General	Jefe Zonal	3	5	3	4	Alta
ICM-022	Evaluación	Supervisión a tambos comunales	Formato N 6G	Gerente General	Jefe Zonal	5	5	4	5	Muy Alta

Código	Proceso	Nombre del Activo	Descripción	Propietario	Copropietario	C	I	D	Valor	Nivel
ICM-023	Evaluación	Reglamento interno del tambo comunal	Documento del reglamento del Tambo	Gerente General	Jefe Zonal	3	3	3	3	Media
ICM-024	Aprobación	Expediente de créditos Tambo Comunal - documentos del tambo comunal	Acta de constitución, convenio del tambo, relación de socios vigentes, resúmenes de los estados financieros, hoja de cuenta interna, historia crediticia	Analista de Créditos	Asistente Administrativo	4	4	4	4	Alta
ICM-025	Aprobación	Manual de normas y procedimiento de créditos	Documento normativo	Gerente General	Jefe Zonal	3	4	4	4	Alta
ICM-026	Aprobación	Política de Créditos	Documento normativo	Gerente General	Jefe Zonal	3	4	5	4	Alta
ICM-027	Aprobación	Póliza de seguro de desgravamen	Formulario del asegurador	Gerente General	Asistente Legal	4	5	3	4	Alta
ICM-028	Desembolso	Pagarés	Título valor	Asistente Administrativo	Jefe de Agencia	4	5	5	5	Muy alta
ICM-029	Desembolso	Hoja de resumen informativo	Anexo de contrato	Asistente Administrativo	Jefe de Agencia	2	3	5	3	Media
ICM-030	Desembolso	Contrato multiproducto	Documento contractual	Asistente Administrativo	Jefe de Agencia	2	3	5	3	Media
ICM-031	Desembolso	Cronograma de pagos	Anexo de contrato	Asistente Administrativo	Jefe de Agencia	4	4	5	4	Alta
ICM-032	Desembolso	Váucher de desembolso	Comprobantes de desembolso	Asistente Administrativo	Jefe de Agencia	4	2	4	3	Media
ICM-033	Recuperación	Váucher de pago	Comprobantes de pago	Asistente Administrativo	Jefe de Agencia	4	2	4	3	Media
ICM-034	Recuperación	Seguimiento de cartera	Formato 6A	Analista de Créditos	Jefe de Agencia	3	3	3	3	Media
ICM-035	Recuperación	Seguimiento de crédito refinanciado	Formato 6C	Analista de Créditos	Jefe de Agencia	3	3	3	3	Media

Código	Proceso	Nombre del Activo	Descripción	Propietario	Copropietario	C	I	D	Valor	Nivel
ICM-036	Recuperación	Seguimiento a clientes con riesgo de sobreendeudamiento	Formato 6H	Analista de Créditos	Jefe de Agencia	3	4	3	3	Media
ICM-037	Recuperación	Informe de seguimiento para créditos agropecuarios	Formato 6F	Analista de Créditos	Jefe de Agencia	3	4	4	4	Alta
ICM-038	Recuperación	Libro de actas del Tambo Comunal	Libro legalizado	Analista de Créditos	Jefe de Agencia	3	3	3	3	Media
ICM-039	Recuperación	Libretas de ahorro	Cuadernillo de control	Analista de Créditos	Jefe de Agencia	4	3	3	3	Media
ICM-040	Recuperación	Notificaciones de cobranza titular	Requerimiento de pagos	Analista de Créditos	Jefe de Agencia	3	3	3	3	Media
ICM-041	Recuperación	Notificaciones de cobranza aval	Requerimiento de pagos	Analista de Créditos	Jefe de Agencia	3	3	3	3	Media
ICM-042	Gestión de Créditos	Reporte de avance diario	Archivo de avance de metas	Jefe Zonal	Jefe Zonal	3	3	3	3	Media
ICM-043	Gestión de Créditos	Reporte de avance por semana	Archivo de avance de metas	Jefe Zonal	Jefe Zonal	3	3	3	3	Media
ICM-044	Gestión de Créditos	Reporte de avance por agencia	Archivo de avance de metas	Jefe Zonal	Jefe Zonal	3	3	3	3	Media
ICM-045	Recuperación	Tendencia por analista mensual	Evaluación de desempeño al Analista	Jefe Zonal	Jefe Zonal	3	4	4	4	Alta
ICM-046	Recuperación	Módulos de crédito con educación	Material de capacitación a Tambos	Jefe Zonal	Jefe Zonal	3	3	3	3	Media
ICM-047	Gestión de Créditos	Plan de trabajo anual	Cronograma de actividades	Jefe Zonal	Jefe Zonal	4	4	3	4	Alta
ICM-048	Gestión de Créditos	Formato de metas mensuales y desembolso semanal por agencia	Formato para el establecimiento de las metas por agencia	Jefe Zonal	Jefe Zonal	3	3	3	3	Media

ACTIVO: SOFTWARE

Código	Proceso	Nombre del Activo	Descripción	Propietario	Copropietario	C	I	D	Valor	Nivel
SCM-001	Gestión de Créditos	SISGO-Modulo de Créditos: Simulador - Créditos	Módulos y opción del SISGO	Jefe de TI	Jefe Zonal	3	1	1	2	Baja
SCM-002	Gestión de Créditos	SISGO-Modulo de Créditos-Reporte Del Módulo Créditos: Central de Riesgo	Módulos y opción del SISGO	Jefe de TI	Jefe Zonal	3	1	1	2	Baja
SCM-003	Gestión de Créditos	SISGO-Modulo de Créditos: Consulta estado de cuenta del Cliente	Módulos y opción del SISGO	Jefe de TI	Jefe Zonal	3	4	4	4	Alta
SCM-004	Gestión de Créditos	SISGO-Modulo de Créditos: Ingreso Solicitud de Créditos	Módulos y opción del SISGO	Jefe de TI	Jefe Zonal	5	5	5	5	Muy Alta
SCM-005	Evaluación	SISGO-Módulo de Mantenimiento de personas - Mantenimiento de personas naturales	Módulos y opción del SISGO	Jefe de TI	Jefe Zonal	3	5	5	4	Alta
SCM-006	Evaluación	SISGO-Módulo de Mantenimiento de personas - Mantenimiento de Empresas o Jurídicas	Módulos y opción del SISGO	Jefe de TI	Jefe Zonal	3	5	5	4	Alta
SCM-007	Evaluación	SISGO - Módulo de Créditos -Mantenimiento condiciones crédito	Módulos y opción del SISGO	Jefe de TI	Jefe Zonal	3	5	5	4	Alta
SCM-008	Evaluación	SISGO - Módulo de Créditos - Mantenimiento de Tambos	Módulos y opción del SISGO	Jefe de TI	Jefe Zonal	3	5	5	4	Alta

Código	Proceso	Nombre del Activo	Descripción	Propietario	Copropietario	C	I	D	Valor	Nivel
SCM-009	Evaluación	SISGO - Módulo de Créditos -Generación de créditos de Tambo	Módulos y opción del SISGO	Jefe de TI	Jefe Zonal	3	5	5	4	Alta
SCM-010	Aprobación	SISGO - Módulo de Créditos - Reporte Excel Negocios	Módulos y opción del SISGO	Jefe de TI	Jefe Zonal	3	4	4	4	Alta
SCM-011	Aprobación	SISGO - Módulo de Créditos - Reporte del módulo de créditos	Módulos y opción del SISGO	Jefe de TI	Jefe Zonal	3	3	3	3	Media
SCM-012	Aprobación	SISGO - Módulo de Caja/Tesorería (Operaciones) - Ingreso/Egreso de caja	Módulos y opción del SISGO	Jefe de TI	Jefe Zonal	5	5	5	5	Muy Alta
SCM-013	Aprobación	SISGO - Módulo de Cobranzas y Recuperaciones - Proceso de Notificaciones	Módulos y opción del SISGO	Jefe de TI	Jefe Zonal	3	3	3	3	Media
SCM-014	Aprobación	SISGO - Módulo de Cobranzas y Recuperaciones - Reportes de Recuperaciones y Normalización - Acta de cobranza Judicial	Módulos y opción del SISGO	Jefe de TI	Jefe Zonal	3	5	5	4	Alta
SCM-015	Aprobación	SISGO - Módulo de Cobranzas y Recuperaciones - Reportes de Recuperaciones y Normalización	Módulos y opción del SISGO	Jefe de TI	Jefe Zonal	3	5	5	4	Alta

ACTIVO: INTANGIBLES

Código	Proceso	Nombre del Activo	Función	Propietario	Copropietario	C	I	D	Valor	Nivel
TCM-001	Promoción	Fotocheck del colaborador	Identificación del colaborador	Cada colaborador	Cada Colaborador	2	2	1	2	Baja
TCM-002	Promoción	Celular	Soporte para comunicaciones	Cada colaborador	Cada Colaborador	4	4	5	4	Alta
TCM-003	Promoción	Computadora Estacionaria	Soporte tecnológico	Cada colaborador	Cada Colaborador	3	3	4	3	Media
TCM-004	Promoción	Moto Lineal	Transporte	Cada colaborador	Cada Colaborador	3	3	3	3	Media
TCM-009	Evaluación	Sello de posfirma	Validación de información	Cada colaborador	Cada Colaborador	4	3	3	3	Media
TCM-010	Evaluación	Impresora	Impresión	Cada colaborador	Cada Colaborador	3	5	5	4	Alta
TCM-011	Evaluación	Escáner	Soporte tecnológico	Cada colaborador	Cada Colaborador	3	5	5	4	Alta
TCM-012	Evaluación	Laptop	Soporte tecnológico	Cada colaborador	Cada Colaborador	4	5	5	5	Muy alta
TCM-013	Desembolso	Impresora térmica	Impresión	Cada colaborador	Cada Colaborador	4	4	4	4	Alta
TCM-014	Desembolso	Sello de Caja	Validación de información	Cada colaborador	Cada Colaborador	4	3	3	3	Media
TCM-015	Desembolso	Módulo de caja	Soporte físico	Cada colaborador	Cada Colaborador	3	4	3	3	Media

ACTIVO: SERVICIOS

Código	Proceso	Nombre del Activo	Descripción	Propietario	Copropietario	C	I	D	Valor	Nivel
ECM-001	Promoción y Evaluación	Central de Riesgos de Experian	Servicio para consultas sobre el comportamiento de pago e	Credivisión	Jefe Zonal	3	4	4	4	Alta

Código	Proceso	Nombre del Activo	Función	Propietario	Copropietario	C	I	D	Valor	Nivel
			historial crediticio del cliente/posible cliente.							
ECM-002	Promoción y Evaluación	Central de Riesgos de la SBS	Servicio para consultas sobre el comportamiento de pago e historial crediticio del cliente/posible cliente.	Credivisión	Jefe Zonal	3	5	5	4	Alta
ECM-003	Promoción y Evaluación	Consulta en Línea RENIEC	Servicio para consultas sobre la identidad del cliente/posible cliente.	Credivisión	Jefe Zonal	4	3	3	3	Media
ECM-004	Gestión del Crédito	Correo Institucional	Soporte de comunicación interna	Credivisión	Jefe Zonal	5	5	5	5	Muy Alta
ECM-005	Gestión del Crédito	Intranet	Servicio de publicación de normativas	Credivisión	Jefe Zonal	3	2	2	2	Baja
ECM-006	Gestión del Crédito	Página web	Servicio de publicación de información y normativas	Credivisión	Jefe Zonal	2	2	2	2	Baja
ECM-007	Desembolso	Logística	Servicio de soporte de materiales y recursos para las operaciones.	Asistente de Logística	Jefe Zonal	3	4	4	4	Alta

ACTIVO: PERSONAS

Código	Proceso	Nombre del Activo	Número	Jefe Directo	C	I	D	Valor	Nivel
PCM-001	Gestión del Crédito	Analista de crédito individual - SJM	4	Jefe de Agencia	4	3	3	3	Media
PCM-002	Gestión del Crédito	Analista de crédito Tambo Comunal - SJM	2	Jefe de Agencia	4	3	3	3	Media
PCM-003	Gestión del Crédito	Jefe de Agencia - SJM	1	Jefe Zonal	5	5	5	5	Muy Alta
PCM-004	Gestión del Crédito	Asistente Administrativo - SJM	1	Jefe de Operaciones	4	3	3	3	Media

PCM-005	Gestión del Crédito	Recibidor Pagador - SJM	1	Jefe de Operaciones	4	3	3	3	Media
PCM-006	Gestión del Crédito	Coordinador de Créditos	1	Gerente General	4	3	3	3	Media
PCM-007	Gestión del Crédito	Jefe Zonal	1	Gerente General	4	3	3	3	Media
PCM-008	Gestión del Crédito	Gerente General	1	Directorio	5	5	5	5	Muy alta

INVENTARIO DE ACTIVOS - TI

ACTIVO: INFORMACIÓN

Código	Proceso	Nombre del Activo	Descripción	Propietario	Copropietario	C	I	D	Valor	Nivel
ITI-001	Gestión TI	Relación de Accesos	Información concerniente a los usuarios y sus claves, desarrollado en formato Word	Analista de Soporte	Analista de Soporte	4	5	3	4	Alta
ITI-002	Gestión TI	Inventario de Backup	Relación de Backup de personal	Analista de Soporte	Analista de Soporte	4	3	3	3	Mediana
ITI-003	Gestión TI	Archivo Backup de configuración de red	Documento en formato txt con la configuración de cada enlace de red por sucursal.	Analista de Soporte	DBA y Analista de Soporte	5	5	5	5	Muy Alta
ITI-004	Gestión TI	Bitácora de atención a usuarios	Detalle de las atenciones a los usuarios dentro del mes	Jefe de TI	Analista de Desarrollo I	4	5	3	4	Alta
ITI-005	Gestión TI	Archivo CREDIPAGO BCP	Relación de pagos realizados y por enviar para el cobro de clientes con dicho banco	Jefe de TI	Analista de Desarrollo I	4	5	3	4	Alta
ITI-006	Gestión TI	Archivo BANCO DE LA NACIÓN	Relación de pagos realizados y por enviar para el cobro de clientes con dicho banco	Jefe de TI	Analista de Desarrollo I	4	5	3	4	Alta
ITI-007	Gestión TI	Archivo RCC	Reporte Crediticio Consolidado de clientes a nivel Perú enviado por la SBS de forma mensual	Jefe de TI	Analista de Desarrollo I	5	5	5	5	Muy Alta

ITI-008	Gestión TI	Archivo RCD	Reporte Crediticio Deudores de Edpyme CREDIVISIÓN que se envía a la SBS de forma mensual	Jefe de TI	Analista de Desarrollo I	4	4	4	4	Alta
ITI-009	Gestión TI	Archivo Desgravamen RIMAC	Archivo con detalle del desgravamen cobrado a clientes al desembolso	Jefe de TI	Analista de Desarrollo I	4	4	4	4	Alta
ITI-010	Gestión TI	Archivo Sepelio VALLE DEL RECUERDO	Archivo con detalle del sepelio cobrado a clientes.	Jefe de TI	Analista de Desarrollo I	3	3	4	3	Medi a
ITI-011	Gestión TI	Manuales SISGO	Manuales técnicos de los distintos módulos del SISGO	Jefe de TI	Analista de Desarrollo I	4	4	4	4	Alta

ACTIVO: SOFTWARE

Código	Proceso	Nombre del Activo	Descripción	Propietario	Copropietario	C	I	D	Valor	Nivel
STI-001	Gestión de TI	SISGO	Sistema de gestión de operaciones (sistema principal)	Jefe de TI	Analista de Desarrollo y jefe de TI	3	5	5	4	Alta
STI-002	Gestión de TI	PVE	Programa de Validación Externa brindada por la SBS para el cruce del RCD con el Balance Contable	Jefe de TI	Analista de Desarrollo y jefe de TI	4	3	3	3	Media
STI-003	Gestión de TI	Oracle Form Developer	Programa para programación y desarrollo de formularios.	Jefe de TI	Analista de Desarrollo I y jefe de TI	4	4	3	4	Alta
STI-004	Gestión de TI	Oracle Report Developer	Programa para programación y desarrollo de reportes.	Jefe de TI	Analista de Desarrollo y jefe de TI	4	4	3	4	Alta
STI-005	Gestión de TI	Windows 10 Professional	Sistema operativo para PC's	Jefe de TI	Analista de Soporte y jefe de TI	3	2	3	3	Media

Código	Proceso	Nombre del Activo	Descripción	Propietario	Copropietario	C	I	D	Valor	Nivel
STI-006	Gestión de TI	Microsoft Office 2016	Paquete de herramientas que permiten hacer ciertas operaciones	Jefe de TI	Analista de Soporte y jefe de TI	3	2	2	2	Baja
STI-008	Gestión de TI	Windows server Standar 2012 R2	Sistema operativo para servidores	Jefe de TI	Analista de Soporte, ABD y jefe de TI	3	4	5	4	Alta
STI-009	Gestión de TI	Oracle	Base de Datos Versión 11G donde se almacena la data de la empresa	Jefe de TI	Analista de Soporte, DBA y jefe de TI	4	5	5	5	Muy alta
STI-010	Gestión de TI	Toad	Programa de acceso directo a la Base de Datos	Jefe de TI	Analista de Desarrollo, DBA y jefe de TI	4	4	3	4	Alta

ACTIVO: INTANGIBLES

Código	Proceso	Nombre del Activo	Función	Propietario	Copropietario	C	I	D	Valor	Nivel
TTI-001	Gestión de TI	Servidor de Base de Datos (PRODUCCIÓN)	Almacena toda la información de todo el negocio.	Jefe de TI	Jefe de TI y Analista de Soporte	5	5	5	5	Muy alta
TTI-002	Gestión de TI	Servidor de Virtualización	Almacena la información del personal	Jefe de TI	Jefe de TI y Analista de Soporte	5	5	5	5	Muy alta
TTI-003	Gestión de TI	Servidor de Aplicación (PRODUCCIÓN)	Almacena todos los programas fuentes y ejecutables del SISGO	Jefe de TI	Jefe de TI y Analista de Soporte	5	5	5	5	Muy alta
TTI-004	Gestión de TI	Servidor de Base de Datos (DESARROLLO)	Almacena toda la información de todo el negocio.	Jefe de TI	Jefe de TI y Analista de Soporte	3	3	3	3	Media
TTI-005	Gestión de TI	Servidor de Aplicación (DESARROLLO)	Almacena todos los programas fuentes y ejecutables del SISGO	Jefe de TI	Jefe de TI y Analista de Soporte	3	3	3	3	Media
TTI-006	Gestión de TI	Router	Enrutador de servicios	Jefe de TI	Jefe de TI y Analista de Soporte	3	3	3	3	Media

Código	Proceso	Nombre del Activo	Función	Propietario	Copropietario	C	I	D	Valor	Nivel
TTI-007	Gestión de TI	Switch	Conexión de varios dispositivos a la misma red	Jefe de TI	Jefe de TI y Analista de Soporte	3	3	3	3	Media
TTI-009	Gestión de TI	UPS	Brindar energía a los servidores en caso de corte de fluido eléctrico por al menos 6 horas.	Jefe de TI	Jefe de TI y Analista de Soporte	4	4	4	4	Alta
TTI-010	Gestión de TI	Baterías para el UPS	Brindar energía a los servidores en caso de corte de fluido eléctrico por al menos 6 horas.	Jefe de TI	Jefe de TI y Analista de Soporte	4	4	4	4	Alta
TTI-011	Gestión de TI	Laptop	Manejo y procesamiento de data	Jefe de TI	Jefe de TI	4	4	4	4	Alta
TTI-012	Gestión de TI	Laptop	Manejo y procesamiento de data	Jefe de TI	Analista de desarrollo	4	4	4	4	Alta
TTI-013	Gestión de TI	Laptop	Manejo y procesamiento de data	Jefe de TI	Analista de Soporte	4	3	3	3	Media
TTI-016	Gestión de TI	Celular	Comunicación y soporte a usuarios	Analista de Soporte	Analista de Soporte	3	3	3	3	Media
TTI-017	Gestión de TI	Impresora	Impresión, copia y escaneo	Jefe de TI	TI	3	3	3	3	Media
TTI-018	Gestión de TI	Centro de Cómputo (Sala de Servidores)	Área que concentra los principales equipos de cómputo y comunicaciones de la empresa	Jefe de TI	TI	5	5	5	5	Muy alta

ACTIVO: SERVICIOS

Código	Proceso	Nombre del Activo	Descripción	Propietario	Copropietario	C	I	D	Valor	Nivel
ETI-001	Gestión de TI	Soporte de FIREWALL	Servicio de soporte para cualquier función o modificación en Sophos	Movistar	Jefe TI, ASI y ADB	4	4	4	4	Alta
ETI-002	Gestión de TI	Internet	Servicio de navegación	Movistar	Jefe TI, ASI y ADB	5	5	5	5	Muy Alta
ETI-003	Gestión de TI	Enlaces VPN	Servicio de interconexión de central con sedes	Movistar	Jefe TI, ASI y ADB	3	4	5	4	Alta
ETI-004	Gestión de TI	Info Internet	Servicio de internet para el sistema SISGO	Movistar	Jefe TI, ASI y ADB	5	5	5	5	Muy Alta
ETI-005	Gestión de TI	Antivirus	Servicio de soporte	Net	TI	4	3	3	3	Media
ETI-006	Gestión de TI	Alquiler de Dominio	Servicio para alojar nuestra página en la web	Red Científica Peruana	TI	4	3	3	3	Media
ETI-007	Gestión de TI	Correo Office 365	Sistema operativo para PC's	Movistar	TI	3	3	2	3	Media
ETI-008	Gestión de TI	Microsoft Office 2013	Paquete de herramientas que permiten hacer ciertas operaciones	Jefe de TI	Analista de Soporte	3	2	2	2	Baja
ETI-009	Gestión de TI	Radmin	Programa para control remoto	Jefe de TI	Analista de Soporte	3	2	1	2	Baja
ETI-010	Gestión de TI	Windows Server Standar 2012 R2	Sistema operativo para servidores	Jefe de TI	Analista de Soporte y ABD	4	4	5	4	Alta
ETI-011	Gestión de TI	Servicio de Administración de Base de Datos	Personal Externo cuya función es DBA	Jefe de TI	TI	5	4	4	4	Alta

ACTIVO: PERSONAS

Código	Proceso	Activo	Jefe Directo	C	I	D	Valor	Nivel
PTI-001	Gestión de TI	Analista de Soporte	Jefe de TI	4	4	4	4	Alta

PTI-002	Gestión de TI	Analista de Desarrollo	Jefe de TI	4	4	4	4	Alta
PTI-003	Gestión de TI	Jefe de TI	Gerente General	4	5	5	5	Muy alta
PTI-002	Gestión de TI	Analista de Desarrollo	Jefe de TI	4	4	4	4	Alta

INVENTARIO DE ACTIVOS – RIESGOS

ACTIVO: INFORMACIÓN

Código	Proceso	Nombre del Activo	Descripción	Propietario	Copropietario	C	I	D	Valor	Nivel
IRI-001	Gestión de Riesgos	Plantilla de opinión de riesgos	Formato en Word que incluyen los factores de evaluación de un crédito.	Gerente de Riesgos	Analista de Riesgos	4	4	4	4	Alta
IRI-002	Gestión de Riesgos	Informe de Calidad de Cartera	Formato en Word que contiene variables para medir la calidad de las colocaciones, nivel producto, agencia, sector económico.	Gerente de Riesgos	Analista de Riesgos	5	5	5	4	Muy Alta
IRI-003	Gestión de Riesgos	Plantilla de calidad de cartera	Formato en Excel	Gerente de Riesgos	Analista de Riesgos	4	5	4	4	Alta
IRI-004	Gestión de Riesgos	Plantilla de créditos fallidos	Formato en Excel	Gerente de Riesgos	Analista de Riesgos	4	5	4	4	Alta
IRI-005	Gestión de Riesgos	Informe de Análisis de Cosechas	Formato en PPT que muestra las cosechas consolidadas, por agencia, producto; así como el FPD.	Gerente de Riesgos	Analista de Riesgos	4	5	4	4	Alta
IRI-006	Gestión de Riesgos	Informe de riesgo de sobreendeudamiento	Formato en Word que muestra la gestión del riesgo de sobreendeudamiento, ex ante y ex post	Gerente de Riesgos	Analista de Riesgos	4	5	4	4	Alta
IRI-007	Gestión de Riesgos	Informe de Visita a Agencia	Formato en PPT que muestra los resultados de la vista a agencias	Gerente de Riesgos	Analista de Riesgos	4	5	4	4	Alta

Código	Proceso	Nombre del Activo	Descripción	Propietario	Copropietario	C	I	D	Valor	Nivel
IRI-008	Gestión de Riesgos	Plantilla de Información de Entorno Externo	Formato en Excel	Gerente de Riesgos	Analista de Riesgos	3	4	4	4	Alta
IRI-009	Gestión de Riesgos	Informe Anual IASC	Formato en Excel y Word	Gerente de Riesgos	Analista de Riesgos	4	5	4	4	Alta
IRI-010	Gestión de Riesgos	Informe Anual de Prueba de Estrés	Formato en Excel y Word	Gerente de Riesgos	Analista de Riesgos	4	5	4	4	Alta

ACTIVO: SOFTWARE

Código	Proceso	Nombre del Activo	Descripción	Propietario	Copropietario	C	I	D	Valor	Nivel
SRI-001	Gestión de Riesgos	SISGO: Modulo de Riesgos y Cartera de Créditos - Evaluación y Clasificación de Cartera	Submódulo del sistema SISGO para el acceso a los integrantes de la Unidad de Riesgos.	Jefe de TI	Área de Riesgos	4	3	3	3	Media
SRI-005	Gestión de Riesgos	SISGO: Modulo de Riesgos y Cartera de Créditos - Control de Desemb. y Limites Etc. por Agencia	Submódulo que permite controlar los límites de excepciones por agencia	Jefe de TI	Área de Riesgos	4	3	3	3	Media
SRI-006	Gestión de Riesgos	Macro de Cosechas	Aplicativo Excel	Gerente de Riesgos	Área de Riesgos	4	5	3	4	Alta
SRI-007	Gestión de Riesgos	Macro de Cosechas por rango de desembolso	Aplicativo Excel	Gerente de Riesgos	Área de Riesgos	4	5	3	4	Alta
SRI-008	Gestión de Riesgos	Macro de FPD	Aplicativo Excel	Gerente de Riesgos	Área de Riesgos	4	5	3	4	Alta
SRI-009	Gestión de Riesgos	Aplicativo de Riesgo de Sobreendeudamiento	Aplicativo Excel	Gerente de Riesgos	Área de Riesgos	4	5	3	4	Alta

ACTIVO: TANGIBLES

Código	Proceso	Nombre del Activo	Función	Propietario	Copropietario	C	I	D	Valor	Nivel
TRI-001	Gestión de Riesgos	Laptop	Soporte para actividades de información digital.	Analistas de Riesgos	Analistas de Riesgos	3	4	3	3	Media
TRI-003	Gestión de Riesgos	Laptop	Soporte para actividades de información digital.	Gerente de Riesgos	Gerente de Riesgos	5	5	5	5	Muy Alta
TRI-004	Gestión de Riesgos	Celular Gerente de Riesgos	Soporte para actividades de comunicación.	Analistas de Riesgos	Analistas de Riesgos	3	3	3	3	Media
TRI-005	Gestión de Riesgos	Celular de Analista de Riesgos	Soporte para actividades de comunicación.	Analistas de Riesgos	Analistas de Riesgos	3	3	3	3	Media

ACTIVO: SERVICIOS

Código	Proceso	Nombre del Activo	Descripción	Propietario	Copropietario	C	I	D	Valor	Nivel
ERI-001	Gestión de Riesgos	SUCAVE	Aplicable de la SBS para envío de información	SBS	Gerencia de Riesgos	3	2	4	3	Media

ACTIVO: PERSONAS

Código	Proceso	Nombre del Activo	Jefe Directo	C	I	D	Valor	Nivel
PRI-001	Gestión de Riesgos	Analista de Riesgo Operacional	Gerente de Riesgos	3	4	3	3	Media
PRI-003	Gestión de Riesgos	Gerente de Riesgos	Directorio/Gerencia General	5	5	5	5	Muy Alta

INVENTARIO DE ACTIVOS – RECUPERACIONES

ACTIVO: INFORMACIÓN

Código	Proceso	Nombre del Activo	Descripción	Propietario	Copropietario	C	I	D	Valor	Nivel
IRE-001	Recuperación de crédito	Plantilla de Avance de Recuperaciones CONTINGENCIA	Archivo en Excel sobre monitoreo de avance de recuperación de cartera de 1-30 días de mora.	Jefe de Recuperaciones	Jefe de Recuperaciones	3	4	3	3	Media
IRE-002	Recuperación de crédito	Plantilla de Avance de Recuperaciones TRAMO 2	Archivo en Excel sobre monitoreo de avance de recuperación de cartera de 31-60 días de mora.	Jefe de Recuperaciones	Jefe de Recuperaciones	3	4	3	3	Media
IRE-007	Recuperación de crédito	Plantilla de Informe mensual de Recuperaciones	Archivo en Word que se envía a la Gerencia General detallando la gestión de recuperación.	Jefe de Recuperaciones	Jefe de Recuperaciones	3	3	3	3	Media
IRE-009	Recuperación de crédito	Plantilla de Reporte de la gestión de los 10+	Archivo en Excel sobre los 10 clientes con los créditos más críticos asignados a los Gestores de Cobranza, jefes de Agencia, jefe Comercial y jefe de Recuperaciones.	Jefe de Recuperaciones	Jefe de Recuperaciones	3	4	3	3	Media
IRE-010	Recuperación de crédito castigado	Plantilla de Avance de Recuperación de Cartera Castigada	Archivo en Excel sobre la recuperación de la cartera castigada	Jefe de Recuperaciones	Jefe de Recuperaciones	3	4	3	3	Media
IRE-011	Recuperación de crédito castigado	Acuerdos Extrajudiciales	Documento sobre acuerdos de pago de clientes en mora.	Gestor de Cobranza	Gestor de Cobranza	3	2	2	2	Baja

ACTIVO: SOFTWARE

Código	Proceso	Nombre del Activo	Descripción	Propietario	Copropietario	C	I	D	Valor	Nivel
SER-002	Recuperación de Créditos	SISGO-Módulo de Cobranzas y Recuperaciones: Control y Administración de Créditos	Módulos y opción del SISGO	Jefe de TI	Departamento de Recuperaciones	3	3	4	3	Media
SER-008	Recuperación de Créditos	SISGO-Módulo de Cobranzas y Recuperaciones-Reportes de Recuperaciones/Normalización: Hoja Ruta para Gestión de Campo	Módulos y opción del SISGO	Jefe de TI	Departamento de Recuperaciones	3	3	4	3	Media
SER-009	Recuperación de Créditos	SISGO-Módulo de Cobranzas y Recuperaciones-Control y Seguimiento de la MORA	Módulos y opción del SISGO	Jefe de TI	Departamento de Recuperaciones	3	3	4	3	Media
SER-010	Recuperación de Créditos	SISGO-Módulo De Créditos: Ingreso de Solicitud de Créditos	Módulos y opción del SISGO	Jefe de TI	Departamento de Recuperaciones	3	3	4	3	Media
SER-011	Recuperación de Créditos	SISGO-Módulo De Créditos: Generación de ANEXOS	Módulos y opción del SISGO	Jefe de TI	Departamento de Recuperaciones	3	3	4	3	Media
SER-012	Recuperación de Créditos	SISGO-Módulo De Créditos: REPORTE EXCEL NEGOCIOS	Módulos y opción del SISGO	Jefe de TI	Departamento de Recuperaciones	3	3	4	3	Media
SER-013	Recuperación de Créditos	SISGO-Módulo De Procesos en General: Transferencias	Módulos y opción del SISGO	Jefe de TI	Departamento de Recuperaciones	3	3	4	3	Media

ACTIVO: TANGIBLES

Código	Proceso	Nombre del Activo	Función	Propietario	Copropietario	C	I	D	Valor	Nivel
TRE-001	Recuperación de Créditos	Laptop	Soporte tecnológico	Jefe de Recuperaciones	Jefe de Recuperaciones	4	3	3	3	Media
TRE-002	Recuperación de Créditos	Celular	Soporte de comunicación	Jefe de Recuperaciones	Jefe de Recuperaciones	4	2	3	3	Media

Código	Proceso	Nombre del Activo	Función	Propietario	Copropietario	C	I	D	Valor	Nivel
TRE-003	Recuperación de Créditos	Celular	Soporte de comunicación	Gestores de Cobranza	Gestores de Cobranza	4	2	2	3	Media
TRE-004	Recuperación de Créditos	Desktop	Soporte tecnológico	Gestores de Cobranza	Gestores de Cobranza	3	3	3	3	Media
TRE-005	Recuperación de Créditos	Archivadores para acuerdos extrajudiciales	Almacenamiento de documentos	Gestores de Cobranza	Gestores de Cobranza	3	3	3	3	Media

ACTIVO: SERVICIOS

Código	Proceso	Nombre del Activo	Descripción	Propietario	Copropietario	C	I	D	Valor	Nivel
ERE-001	Recuperación de Crédito	Experian	Brinda información online sobre el récord crediticio del cliente	Credivisión	Departamento de Recuperaciones	3	2	3	3	Media
ERE-002	Recuperación de Crédito	RENIEC	Información de identidad del cliente	Credivisión	Departamento de Recuperaciones	3	2	4	3	Media
ERE-003	Recuperación de Crédito	COFOPRI	Brinda Información gratuita sobre el registro de propiedades inmuebles de los clientes	COFOPRI	Departamento de Recuperaciones	3	2	3	3	Media
ERE-004	Recuperación de Crédito	SUNARP	Brinda Información del registro de propiedades inmuebles de clientes	Credivisión	Departamento de Recuperaciones	3	2	3	3	Media
ERE-005	Recuperación de Crédito	SBS	Brinda información online sobre el récord crediticio del cliente	Credivisión	Departamento de Recuperaciones	3	2	3	3	Media

ACTIVO: PERSONAS

Código	Proceso	Nombre de Activo	Jefe Directo	C	I	D	Valor	Nivel
PRE-001	Recuperación de Créditos	Jefe de Recuperaciones	Gerente General	5	5	5	5	Muy Alta
PRE-002	Recuperación de Créditos	Gestor de Cobranza	Jefe de Recuperaciones	3	2	3	3	Media
PRE-003	Recuperación de Créditos	Gestor de Cobranza	Jefe de Recuperaciones	3	2	3	3	Media
PRE-004	Recuperación de Créditos	Gestor de Cobranza	Jefe de Recuperaciones	3	2	3	3	Media

ACTIVO: INFORMACIÓN

Código	Proceso	Nombre del Activo	Descripción	Propietario	Copropietario	C	I	D	Valor	Nivel
IFI-001	Gestión Económica Financiera	Plantilla de Estados Financieros por producto	Plantilla en Excel que muestra la rentabilidad por producto de manera mensual.	Gerente de Administración y Finanzas	Analista de Finanzas	4	4	3	4	Alta
IFI-002	Gestión Económica Financiera	Plantilla de Reporte 12	Formato en Excel de estado de adeudos	Gerente de Administración y Finanzas	Analista de Finanzas	3	4	3	3	Media
IFI-004	Gestión Económica Financiera	Acta Comité ALCO	Documento en Word con información de los acuerdos tomados por el comité	Gerente de Administración y Finanzas	Analista de Finanzas	4	3	2	3	Media
IFI-005	Gestión Económica Financiera	Informe confraternidad	Archivo en Excel que muestra la situación de la cartera y otros indicadores, mensualmente	Gerente de Administración y Finanzas	Analista de Finanzas	3	4	4	4	Alta

ACTIVO: SOFTWARE

Código	Proceso	Nombre del Activo	Descripción	Propietario	Copropietario	C	I	D	Valor	Nivel
SFI-001	Gestión Económica Financiera	SISGO: Módulo de Contabilidad General	Opciones que Genera el Balance de Comprobación	Jefe de TI	Analista de Finanzas	4	4	3	4	Alta

ACTIVO: TANGIBLES

Código	Proceso	Nombre del Activo	Función	Propietario	Copropietario	C	I	D	Valor	Nivel
TFI-001	Gestión Económica Financiera	Computadora estacionaria	Soporte informático	Analista de Finanzas	Analista de Finanzas	4	3	3	3	Media
TFI-002	Gestión Económica Financiera	Celular	Medio de comunicación	Analista de Finanzas	Analista de Finanzas	4	2	3	3	Media
TFI-003	Gestión Económica Financiera	Laptop	Medio de comunicación	GAF	GAF	4	2	3	3	Media
TFI-004	Gestión Económica Financiera	Celular	Soporte informático	GAF	GAF	4	3	3	3	Media

ACTIVO: SERVICIOS

Código	Proceso	Nombre del Activo	Descripción	Propietario	Copropietario	C	I	D	Valor	Nivel
EFI-001	Gestión Económica Financiera	SUNAT	Servicio web para verificar tipo de cambio	SUNAT	Analista de Finanzas	2	4	4	3	Media

EFI-002	Gestión Económica Financiera	BCP	Servicio web para movimientos de dinero	BCP	Analista de Finanzas	4	4	4	4	Alta
EFI-003	Gestión Económica Financiera	BANCO DE LA NACIÓN	Servicio web para movimientos de dinero	BN	Analista de Finanzas	4	4	4	4	Alta
EFI-004	Gestión Económica Financiera	BANBIF	Servicio web para movimientos de dinero	BANBIF	Analista de Finanzas	4	4	4	4	Alta

ACTIVO: PERSONAS

Código	Proceso	Nombre del Activo	Jefe Directo	C	I	D	Valor	Nivel
PFI-001	Gestión Económica Financiera	Analista de Finanzas	GAF	4	2	2	3	Media
PFI-002	Gestión Económica Financiera	GAF	Gerente General	4	3	3	3	Media

Anexo 10. Análisis de Riesgos

Cód.	Nombre del Activo	Vulnerabilidad	Amenaza	Copropietario	Valor	Nivel	DM	Impacto	Probab.	Valor Riesgo
ICM-007	Solicitud de crédito	Falta de control de acceso	Acceso no autorizado	Jefe Zonal	5	Muy alta	5	5	4	Muy Alto
ICM-022	Formulario de supervisión de créditos	Falta de control de acceso	Acceso no autorizado	Jefe Zonal	5	Muy alta	3	4	2	Medio
ICM-037	Pagarés	Falta de control de acceso	Acceso no autorizado	Jefe de Agencia	5	Muy alta	4	5	1	Alto
SCM-004	SISGO - Modulo de Créditos: Ingreso Solicitud de Créditos	No hay control de Acceso en la interfaz del modulo	Acceso no autorizado	Jefe Zonal	5	Muy alta	5	5	3	Muy Alto
SCM-012	SISGO - Módulo de Caja/Tesorería - Ingreso/Egreso de caja	No hay control de Acceso en la interfaz del modulo	Acceso no autorizado	Jefe Zonal	5	Muy alta	5	5	3	Muy Alto
TCM-017	Laptop	Susceptible a daños o pérdida del activo por constante uso fuera de agencia	Pérdida del activo	Cada Colaborador	5	Muy alta	5	3	2	Medio
ECM-004	Correo Institucional	No evidencia	No evidencia	Jefe Zonal	5	Muy alta	3	4	2	Medio
PCM-003	Jefe de Agencia - SJM	Susceptible a enfermedad o evento externo	Enfermedad, error en el uso de activos	Jefe Zonal	5	Muy alta	5	5	2	Alto
PCM-008	Gerente General	Susceptible a enfermedad o evento externo	Enfermedad, error en el uso de activos	Directorio	5	Muy alta	5	5	3	Muy Alto
ITI-003	Archivo Backup de configuración de red	Acceso limitado a personal autorizado, que puede incurrir en error y eliminar archivo	Personal con acceso al archivo	DBA y AS	5	Muy alta	4	5	3	Muy Alto

Cód.	Nombre del Activo	Vulnerabilidad	Amenaza	Copropietario	Valor	Nivel	DM	Impacto	Probab.	Valor Riesgo
STI-009	Oracle	No se cuente con personal con capacidades	Fuga de información	AS, DBA y jefe de TI	5	Muy alta	5	5	4	Muy Alto
TTI-001	Servidor de Base de Datos (PRODUCCIÓN)	Susceptible a daños por temperatura	Cambios de temperatura y humedad	Jefe de TI	5	Muy alta	5	5	3	Muy Alto
TTI-002	Servidor de Virtualización	Susceptible a daños por temperatura	Cambios de temperatura y humedad	Jefe de TI	5	Muy alta	5	5	2	Alto
TTI-003	Servidor de Aplicación (PRODUCCIÓN)	Susceptible a daños por temperatura	Cambios de temperatura y humedad	Jefe de TI	5	Muy alta	5	5	3	Muy Alto
TTI-018	Centro de Cómputo (Sala de Servidores)	Uso inadecuado o descuido del control de acceso físico a las edificaciones	Destrucción de equipo o medios, inundación	Jefe de TI	5	Muy alta	5	5	3	Muy Alto
ETI-002	Internet	Falla de servicios de comunicación	Saturación	Jefe TI, ASI y ADB	5	Muy alta	5	5	2	Alto
ETI-004	Info Internet	Caída de sistemas por agotamiento de recursos	Saturación	Jefe TI, ASI y ADB	5	Muy alta	5	5	4	Muy Alto
PTI-003	Jefe de TI	Ausencia del personal, entrenamiento insuficiente en seguridad de la información	Enfermedad, evento externo	Gerente General	5	Muy alta	5	5	4	Muy Alto
IRI-002	Informe de Calidad de Cartera	Es editable y acceso limitado	Colaborador con acceso a la carpeta compartida.	Analista de Riesgos	5	Muy alta	5	5	3	Muy Alto
TRI-003	Laptop	Mantenimiento insuficiente	Fallas de los equipos	Gerente de Riesgos	5	Muy alta	4	5	2	Alto

Anexo 11. Tratamiento de riesgos

Cod.	Descripción Riesgo	Activo	Responsable	Acción	Control propuesto	Costo	Tiempo	Impacto	Prob.	R. Residual
R01-ICM	Créditos mal colocados	Solicitud de crédito	Jefe Zonal	Reducir	9.4.1 Restricción del acceso a la información	1	M	1	3	3
R02-ICM	Información errónea de los créditos	Formulario de supervisión de créditos	Jefe Zonal	Reducir	9.4.1 Restricción del acceso a la información	1	M	1	1	1
R03-ICM	Error en la generación de pagares	Pagarés	Jefe de Agencia	Reducir	9.1.1 Política de control de accesos.	1	C	1	1	1
R04-SCM	Demora en la atención de Clientes	SISGO - Modulo de Créditos: Ingreso Solicitud de Créditos	Jefe Zonal	Reducir	9.1.1 Política de control de accesos.	1	C	1	3	3
R05-SCM	Pérdidas financieras de Caja	SISGO - Módulo de Caja/Tesorería - Ingreso/Egreso de caja	Jefe Zonal	Reducir	9.1.1 Política de control de accesos.	1	C	1	1	1
R06-TCM	Demora en la atención e insatisfacción de clientes	Laptop	Cada Colaborador	Reducir	11.2.4 Mantenimiento de los equipos.	1	M	1	1	1
R07-ECM	Indisponibilidad de aprobación de créditos	Correo Institucional	Jefe Zonal	Reducir	12.2.1 Controles contra el código malicioso. 13.2.3 Mensajería electrónica.	1	M	1	1	1
R08-PCM	Indisponibilidad de JA para aprobación de Créditos	Jefe de Agencia - SJM	Jefe Zonal	Reducir	6.1.2 Segregación de tareas.	1	M	2	1	2

Cod.	Descripción Riesgo	Activo	Responsable	Acción	Control propuesto	Costo	Tiempo	Impacto	Prob.	R. Residual
R09-PCM	Indisponibilidad de GG para aprobación de Créditos	Gerente General	Directorio	Reducir	6.1.2 Segregación de tareas.	1	M	2	1	2
R10-ITI	Sistemas expuestos a terceros	Archivo Backup de configuración de red	DBA y AS	Reducir	9.1.1 Política de control de accesos. 9.1.2 Acceso a las redes y los servicios de red	1	M	2	1	2
R11-ITI	Robo de información de clientes y sus créditos	Archivo RCC	Analista de Desarrollo	Reducir	9.1.1 Política de control de accesos. 9.1.2 Acceso a las redes y los servicios de red	1	M	2	1	2
R12-STI	Robo de reportes de créditos a personas que no participan en solicitudes de crédito.	Oracle	AS, DBA y jefe de TI	Reducir	9.4.1 Restricción del acceso a la información. 9.4.5 Control de acceso al código fuente de los programas.	1	M	2	1	2
R14-TTI	Perdida de información e indisponibilidad del sistema	Servidor de Virtualización	Jefe de TI	Reducir	13.1.3 Segregación de redes. 12.3.1 Copias de seguridad de la información	1	M	1	3	3
R17-ETI	Pérdida de clientes y reputación	Internet	Jefe TI, ASI y ADB	Reducir	15.2.1 Control y revisión de la provisión de servicios del proveedor	1	L	1	1	1

Cod.	Descripción Riesgo	Activo	Responsable	Acción	Control propuesto	Costo	Tiempo	Impacto	Prob.	R. Residual
R18-ETI	Mala reputación de la empresa	Info Internet	Jefe TI, ASI y ADB	Reducir	15.2.1 Control y revisión de la provisión de servicios del proveedor	1	L	1	2	2
R19-PTI	Indisponibilidad de JT para operatividad del Sistema	Jefe de TI	Gerente General	Reducir	6.1.2 Segregación de tareas.	1	M	2	1	2
R20-PRE	Indisponibilidad de JR para recuperación de Créditos	Jefe de Recuperaciones	Gerente General	Reducir	6.1.2 Segregación de tareas.	1	M	1	1	1
R21-IRI	Pérdidas financieras de Cartera	Informe de Calidad de Cartera	Analista de Riesgos	Reducir	9.4.1 Restricción del acceso a la información.	1	M	1	1	1
R22-TRI	Demora en la evaluación de Créditos	Laptop	Gerente de Riesgos	Reducir	11.2.4 Mantenimiento de los equipos.	1	M	1	1	1
R23-PRI	Indisponibilidad de GR para evaluación de Créditos	Gerente de Riesgos	Directorio/Gerencia General	Reducir	6.1.2 Segregación de tareas.	1	M	1	1	1

Anexo 12. Declaración de Aplicabilidad

N°	CONTROL	APLICA	JUSTIFICACIÓN
5.1	Directrices de la Dirección en seguridad de la información.		
5.1.1	Conjunto de políticas para la seguridad de la información.	SI	Definir un conjunto de las políticas de seguridad de la información de acuerdo a las necesidades identificadas en el análisis de riesgos, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
5.1.2	Revisión de las políticas para la seguridad de la información.	SI	Se debe revisar de forma periódica las políticas de seguridad de la información para mantenerlas actualizadas, o si ocurren cambios significativos
6.1	Organización interna.		
6.1.1	Asignación de responsabilidades para la seguridad de la información.	SI	Los roles y responsabilidades estén definidas y asignadas a los participantes en el modelo de seguridad establecido por Edpyme CREDIVISIÓN.
6.1.2	Segregación de tareas.	SI	Las áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada de la información, o por el uso indebido de los activos de la organización.
6.1.3	Contacto con las autoridades.	SI	Mantener los contactos apropiados con las autoridades pertinentes, que pueden apoyar a solucionar conflictos en cuanto a la seguridad de la información.
6.1.4	Contacto con grupos de interés especial.	SI	Debe ser conveniente mantener contactos apropiados con grupos de interés especial y asociaciones profesionales especializadas en seguridad.
6.1.5	Seguridad de la información en la gestión de proyectos.	SI	Durante la planeación de los proyectos debe participar el Analista de Seguridad de la información como generador de recomendaciones en la evaluación de los riesgos inherentes con dichos proyectos.
6.2	Dispositivos móviles y el teletrabajo.		
6.2.1	Política de dispositivos móviles	SI	El uso de dispositivos móviles debe estar autorizado de forma explícita por la dependencia respectiva, en conjunto con la Gerencia de Riesgos.

N°	CONTROL	APLICA	JUSTIFICACIÓN
6.2.2	Teletrabajo.	SI	Se debe proteger la información a la que se tiene acceso, que es procesada o almacenada en lugares en los que se realiza teletrabajo.
7.1	Antes del empleo		
7.1.1	Investigación de antecedentes.	SI	Los nuevos empleados que ingresen a Edpyme CREDIVISIÓN, deben pasar por un proceso de investigación de antecedentes, con el fin de mitigar los riesgos en el uso de la información.
7.1.2	Términos y condiciones de contratación.	SI	Los contratos de los empleados deben incluir cláusulas que especifiquen las responsabilidades y los cuidados que deben tener con la información.
7.2	Durante el empleo.		
7.2.1	Responsabilidades de gestión.	SI	Edpyme CREDIVISIÓN debe proveer los mecanismos necesarios para asegurar que sus empleados cumplan con sus responsabilidades en Seguridad de la Información desde su ingreso hasta su egreso.
7.2.2	Concienciación, educación y capacitación en seguridad de la información	SI	Edpyme CREDIVISIÓN debe establecer un programa permanente de creación de cultura en seguridad de la información para los empleados y terceros.
7.2.3	Proceso disciplinario.	SI	Las normas y procedimientos que se generen y soporten el Sistema de Gestión de Seguridad de la Información son de obligatorio cumplimiento.
7.3	Finalización del empleo o cambio en el puesto de trabajo.		
7.3.1	Responsabilidades ante la finalización o cambio	SI	Se debe informar a los empleados, las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato, los cuales deben cumplir.
8.1	Responsabilidad sobre los activos.		
8.1.1	Inventario de activos.	SI	CREDIVISIÓN debe mantener un inventario de activos de información. Los dueños de la información deben clasificar la información basados en su valor, sensibilidad, riesgo de pérdida
8.1.2	Propiedad de los activos.	SI	El área responsable del proceso debe realizar el debido control y mantenimiento al inventario de activos de información, para establecer responsabilidad sobre la tenencia de estos y la información sobre éstos.

N°	CONTROL	APLICA	JUSTIFICACIÓN
8.1.3	Uso aceptable de los activos.	SI	Independientemente de donde se encuentre cada activo de información, éstos deben ser clasificados por el dueño de la información, mediante el estándar de clasificación establecido.
8.1.4	Devolución de activos.	SI	Todos los empleados y usuarios externos deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo. Debe quedar un acta de dicha devolución, firmada por ambas partes.
8.2	Clasificación de la información.		
8.2.1	Clasificación de la información.	SI	Los dueños de la información deben clasificar los niveles de sensibilidad de la misma, de acuerdo a criterios que permitan velar por la seguridad de la información.
8.2.2	Etiquetado de la información.	SI	Los dueños de la información deben etiquetar los niveles de sensibilidad de la misma, de acuerdo a criterios que permitan velar por la seguridad de la información
8.2.3	Manipulado de la información	SI	Cada responsable de área debe realizar el proceso de clasificación de información, inventariando la información utilizada por su área.
8.3	Manipulación de los soportes		
8.3.1	Gestión de soportes extraíbles.	SI	No está permitida la conexión a la red cualquier dispositivo que se considere removible, de uso personal de los funcionarios, sin la debida autorización del personal de TI.
8.3.2	Eliminación de soportes.	SI	Se debe efectuar Backup de toda la información considerada confidencial y que se encuentre contenida en los equipos de la Entidad. En especial se debe asegurar el respaldo de información cuando termine el vínculo laboral del empleado, así como cuando se vaya a dar de baja un activo o equipo.
8.3.3	Soportes físicos en tránsito.	SI	Durante el transporte fuera de la organización, los soportes que contengan información deben estar protegidos contra accesos no autorizados, usos indebidos o deterioro.
9.1	Requisitos de negocio para el control de accesos		

N°	CONTROL	APLICA	JUSTIFICACIÓN
9.1.1	Política de control de accesos.	SI	El uso de la información debe ser controlado para prevenir accesos no autorizados. Los privilegios sobre la información deben ser otorgados y mantenidos de acuerdo con las necesidades de la operación
9.1.2	Acceso a las redes y los servicios de red	SI	El acceso a la red debe ser otorgado solo a usuarios autorizados, previa definición, verificación y control de los perfiles y roles para el acceso en los diferentes sistemas de información
9.2	Gestión de acceso de usuario.		
9.2.1	Registro y baja de usuario.	SI	Procedimientos para cubrir todas las etapas del ciclo de vida del acceso de los usuarios, desde del registro inicial de los nuevos usuarios hasta su baja cuando ya no sea necesario su acceso a los sistemas.
9.2.2	Provisión de accesos de usuario	SI	Se deben establecer mecanismos de control de acceso físico y lógico para los usuarios, con el fin de asegurar que los activos de información.
9.2.6	Retirada o reasignación de los derechos de acceso	SI	Todos los usuarios que acceden la información deben disponer de un medio de identificación y el acceso debe ser controlado a través de una autenticación personal, la cual puede ser modificada cuando se presente un cambio de funciones del empleado o se retire definitivamente
9.3	Responsabilidades del usuario.		
9.3.1	Uso de información secreta de autenticación.	SI	Cada usuario es responsable por sus acciones mientras usa cualquier recurso de información. Por lo tanto, cada usuario debe ser las prácticas de la organización en el uso de la información
9.4	Control de acceso a sistemas y aplicaciones.		
9.4.1	Restricción del acceso a la información.	SI	El acceso a la información de la Edpyme y a las funciones de los sistemas de las aplicaciones, será restringido de acuerdo con la política de control de acceso.
9.4.2	Procedimientos seguros de inicio de sesión.	SI	Se debe concienciar y controlar que los usuarios sigan buenas prácticas de seguridad en la selección, uso y protección de contraseñas, las cuales constituyen un medio de validación de la identidad del usuario
9.4.3	Sistema de gestión de contraseñas	SI	Las contraseñas deben poseer algún grado de complejidad y no deben ser palabras comunes, ni tener información personal.

N°	CONTROL	APLICA	JUSTIFICACIÓN
10.1	Controles criptográficos.		
10.1.1	Política de uso de los controles criptográficos.	NO	Dentro del alcance del SGSI no se contempla
11.1	Áreas seguras.		
11.1.1	Perímetro de seguridad física.	SI	La seguridad física de la Entidad debe basarse en perímetros y áreas seguras, las cuales serán protegidas por medio de controles circundantes apropiados.
11.1.2	Controles físicos de entrada.	SI	Todas las entradas a las áreas físicas de Edpyme CREDIVISIÓN deben tener un nivel de seguridad acorde con el valor de la información que se procesa.
11.1.5	El trabajo en áreas seguras.	NO	Dentro del alcance del SGSI no se contempla
11.2	Seguridad de los equipos.		
11.2.1	Emplazamiento y protección de equipos.	SI	Los recursos informáticos deben estar físicamente protegidos contra amenazas de acceso no autorizado y amenazas ambientales para prevenir exposición, daño o pérdida de los activos e interrupción de operaciones.
11.2.2	Instalaciones de suministro.	SI	La Edpyme debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos.
11.2.4	Mantenimiento de los equipos.	SI	Se debe realizar los mantenimientos preventivos periódicamente cada seis meses y correctivos cuando se requieran.
11.2.5	Retirada de materiales propiedad de la empresa.	NO	Dentro del alcance del SGSI no se contempla
12.1	Procedimientos y responsabilidades operacionales		
12.1.1	Documentación de procedimientos de operación.	SI	La Entidad debe efectuar, a través de sus funcionarios responsables de los procesos, la actualización de la documentación y los procedimientos relacionados con la operación y administración de la plataforma tecnológica.
12.1.2	Gestión de cambios.	SI	Todo cambio al Sistema deberá estar controlado y será realizado de acuerdo con los procedimientos de gestión de cambios de TI.
12.1.3	Gestión de capacidades.	SI	TI, debe realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados de manera periódica

N°	CONTROL	APLICA	JUSTIFICACIÓN
12.2	Protección contra el software malicioso (Malware)		
12.2.1	Controles contra el código malicioso.	SI	Implementar los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica
12.3	Copias de seguridad.		
12.3.1	Copias de seguridad de la información.	SI	La Edpyme a través del área de TI debe garantizar la generación de Backup de su información crítica.
12.4	Registro y supervisión.		
12.4.1	Registro de eventos.	SI	Realizará monitoreo permanente del uso que da el personal provisto por terceros a los recursos de la plataforma tecnológica y los sistemas
12.4.3	Registros de administración y operación	SI	Edpyme CREDIVISIÓN debe revisar periódicamente los registros de auditoría de los administradores y operadores de las aplicaciones
12.4.4	Sincronización de relojes.	NO	Dentro del alcance del SGSI no se contempla.
12.5	Control del software en explotación.		
12.5.1	Instalación del software en explotación	SI	TI es responsable de establecer procedimientos para controlar la instalación de software operativo, y asegurará la funcionalidad de los sistemas de información.
12.6	Gestión de la vulnerabilidad técnica.		
12.6.1	Gestión de las vulnerabilidades técnicas.	SI	TI y la Gerencia de Riesgos, revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización periódica de pruebas de vulnerabilidades.
12.6.2	Restricciones en la instalación de software.	SI	La instalación de software en los computadores suministrados por la Entidad es una función exclusiva del área de TI
12.7	Consideraciones sobre de las auditorías de los sistemas de información.		
12.7.1	Controles de auditoría de los sistemas de información.	SI	Auditoría debe realizar monitoreo periódicamente para evaluar la conformidad con las políticas de la organización.
13.1	Gestión de la seguridad de redes.		

N°	CONTROL	APLICA	JUSTIFICACIÓN
13.1.1	Controles de red	SI	A través del área de TI, define los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas y minimizar los riesgos de seguridad de la información
13.1.2	Seguridad de los servicios de red.	SI	Identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios de red, cuando estos se contraten externamente.
13.1.3	Segregación de redes.	SI	Responsabilidad de TI mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente
13.2	Intercambio de información con partes externas.		
13.2.1	Políticas y procedimientos de intercambio de información.	SI	Asegurará la protección de la información en el momento de ser transferida o intercambiada con otras entidades y establecerá los procedimientos y controles necesarios para el intercambio de información.
13.2.4	Acuerdos de confidencialidad o no revelación	SI	Establecer Acuerdos de Confidencialidad dejando explícitas las responsabilidades y obligaciones legales
14.1	Requisitos de seguridad en sistemas de información.		
14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	SI	Los requerimientos de seguridad de la información deben ser identificados previos al diseño de los sistemas de tecnología de la información.
14.1.2	Asegurar los servicios de aplicaciones en redes públicas.	SI	Asegurar que los sistemas de información que pasan a través de redes públicas cumplan con las políticas de seguridad de la información.
14.1.3	Protección de las transacciones de servicios de aplicaciones	NO	Dentro del alcance del SGSI no se contempla.
14.2	Seguridad en los procesos de desarrollo y soporte.		
14.2.1	Política de desarrollo seguro de software.	NO	Dentro del alcance del SGSI no se contempla.
14.3	Datos de prueba.		

N°	CONTROL	APLICA	JUSTIFICACIÓN
14.3.1	Protección de los datos utilizados en pruebas.	NO	Dentro del alcance del SGSI no se contempla.
15.1	Seguridad en las relaciones con proveedores		
15.1.2	Requisitos de seguridad en contratos con terceros	SI	Generar un modelo base para los Acuerdos de Niveles de Servicio y requisitos de Seguridad de la Información
15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones.	SI	Elaborar Acuerdos de Confidencialidad y Acuerdos de Intercambio de Información con terceras partes.
15.2	Gestión de la provisión del servicio del proveedor		
15.2.1	Control y revisión de la provisión de servicios del proveedor	SI	Identificar y monitorear los riesgos relacionados con terceras partes o los servicios provistos por ellas, haciendo extensiva esta actividad a la cadena de suministro de los servicios de tecnología.
15.2.2	Gestión de cambios en los servicios	NO	Dentro del alcance del SGSI no se contempla.
16.1	Gestión de incidentes de seguridad de la información y mejoras.		
16.1.1	Responsabilidades y procedimientos.	SI	Disponer responsabilidad y proveer el reporte de incidentes relacionados con la seguridad de la información
16.1.2	Notificación de los eventos de seguridad de la información.	SI	Los propietarios de los activos de información deben informar al área de TI, los incidentes de seguridad que identifiquen o que reconozcan.
17.1	Continuidad de la seguridad de la información.		
17.1.1	Planificación de la continuidad de la seguridad de la información.	SI	Desarrollar, documentar, implementar y probar periódicamente procedimientos para asegurar una recuperación razonable y a tiempo de la información crítica de la Entidad, sin disminuir los niveles de seguridad establecidos.
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	SI	Realizar pruebas periódicas del plan de recuperación ante desastres o continuidad de negocio, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.
17.2	Redundancias.		

N°	CONTROL	APLICA	JUSTIFICACIÓN
17.2.1	Disponibilidad de los recursos de tratamiento de la información.	SI	Proveer una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables.
18.1	Cumplimiento de los requisitos legales y contractuales.		
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	SI	TI debe identificar y velar porque el software instalado en los recursos de la plataforma tecnología cumpla con los requerimientos legales y de licenciamiento aplicables.
18.1.2	Derechos de propiedad intelectual (DPI).	NO	Dentro del alcance del SGSI no se contempla.
18.1.4	Protección y privacidad de la información de carácter personal.	SI	La Entidad, velará por la protección de los datos personales de sus clientes, proveedores y demás terceros de los cuales reciba y administre información.
18.1.5	Regulación de los controles criptográficos.	NO	Dentro del alcance del SGSI no se contempla.
18.2	Revisiones de la seguridad de la información.		
18.2.3	Comprobación del cumplimiento técnico.	SI	Revisar periódicamente los registros de auditoría de los sistemas de información con el fin de identificar el cumplimiento de las políticas de seguridad dispuestas por organización.

Cant.	Status	Significado	Contribución %
93	SI	El control SI es aplicable para la empresa	82%
21	NO	El control no es aplicable para la empresa ni para el negocio	18%
114			

Anexo 13. Plan de continuidad de negocio

I. OBJETIVO

Establecer las políticas para una adecuada Gestión de Continuidad del Negocio de la EDPYME CREDIVISIÓN; así como los lineamientos a seguir para que, ante eventos de interrupción, Edpyme CREDIVISIÓN pueda continuar o recuperar los procesos que soportan a sus servicios y/o productos críticos dentro de sus tiempos objetivos de recuperación.

II. BASE LEGAL

- Circular N° 139-2009 “Gestión de Continuidad del Negocio” - Superintendencia de Banca, Seguros y AFP
- Resolución SBS N° 2116-2009 “Reglamento para la Gestión del Riesgo Operacional”
- Circular N° G-164-2012 Reporte de Eventos de Interrupción Significativa de Operaciones

III. ALCANCE

El ámbito de aplicación de las disposiciones contenidas en el presente manual comprende a toda la estructura organizativa de Edpyme CREDIVISIÓN.

IV. POLÍTICAS PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO (GCN)

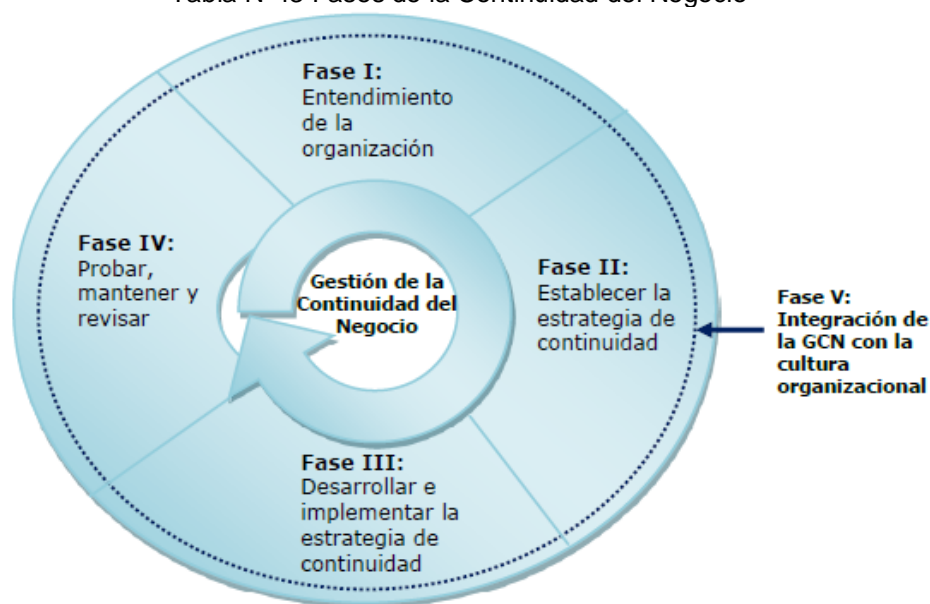
- Edpyme CREDIVISIÓN, realiza una GCN, mediante la implementación de respuestas efectivas para que ante la ocurrencia de eventos que pueden ocasionar una interrupción o inestabilidad en las operaciones de la empresa, la operatividad del negocio continúe de una manera razonable, con el fin de salvaguardar los intereses de sus principales grupos de interés.
- La GCN abarca la identificación de los procesos que requieren contar con una estrategia de continuidad de negocios, considerando los resultados del análisis de impacto y de la evaluación de riesgos.
- Para el análisis que determine el impacto que tendría una interrupción de los procesos que soportan los principales productos, se deberán considerar aspectos como daños a la viabilidad financiera, daños de reputación, incumplimientos regulatorios, y/o de daños al personal o a terceros; estableciendo el período máximo tolerable de interrupción y el tiempo objetivo de recuperación de los procesos.
- El análisis de impacto debe ser actualizado cuando ocurran cambios significativos en la empresa o al menos cada 02 años.

- Desarrollar, probar y mantener los siguientes planes: Plan de Gestión de Crisis, Planes de Continuidad del Negocio, Plan(es) de Emergencia, y Plan de Recuperación de TI.
- Contar con un Comité de Manejo de Crisis conformado por la Gerencia General, Gerente de Administración y Finanzas, Gerente de Negocios, Gerente de Riesgos, jefe de TI, Asistente de Logística y Seguridad y jefe de Agencia.
- Los planes de continuidad deberán ser revisados y probados por lo menos anualmente, las observaciones identificadas durante la ejecución de estas deberán utilizarse para implementar oportunidades de mejora en los planes.
- La incorporación de la GCN a la cultura organizacional de Edpyme Credivisión, se realizará mediante capacitaciones anuales a todos los colaboradores y capacitaciones de inducción al personal nuevo.
- En caso de realizarse cambios significativos en la operatividad de Edpyme Credivisión, se debe realizar evaluaciones de riesgos y análisis del impacto de dichos cambios sobre la continuidad del negocio.
- Edpyme Credivisión contrata seguros como mecanismo de reducción del impacto financiero, ante eventos no deseados, garantizando la seguridad del personal y la protección de los activos y propiedades de la institución, incluyendo los activos de información.
- Las empresas que contrate Edpyme Credivisión para proveer servicios relacionados a la actividad principal de negocios (central de riesgo, internet y comunicaciones), deben contar con planes de continuidad, los cuales deben contar con ejecución de pruebas.
- Garantizar que todas las agencias y oficina principal cuenten con la infraestructura física y un sistema de evacuación que salvaguarden la vida humana y los activos de información en caso de un desastre natural.
- Los colaboradores de Edpyme Credivisión deben participar activamente durante la ejecución de las pruebas de continuidad del negocio, de acuerdo a la función que tenga que realizar.
- Auditoría Interna es el responsable de evaluar el cumplimiento de la gestión de la continuidad del negocio.

V. METODOLOGÍA DE LA GESTION DE CONTINUIDAD DEL NEGOCIO

Contempla cinco (5) fases, desde el entendimiento de la organización hasta la integración de la GCN a la cultura de la organización, como se muestra en tabla 43.

Tabla N°43 Fases de la Continuidad del Negocio



FASE I: Entendimiento de la Organización

Esta fase consiste en conocer los objetivos y metas de Edpyme CREDIVISIÓN a corto y mediano plazo, a fin de que la implementación de la GCN esté alineada a lo establecido por la alta Dirección; para ello, el líder de la Gestión de Continuidad de Negocio tiene acceso al plan estratégico de Edpyme CREDIVISIÓN, a fin de conocer los planes que ayudarán a cumplir los objetivos.

Asimismo, se debe identificar los principales procesos, productos, servicios y proveedores, así como las actividades y recursos requeridos; evaluando los riesgos que podrían causar una interrupción de dichas actividades y el impacto que podría tener dicha interrupción.

Las actividades por desarrollar durante esta fase son dos: i) análisis de impacto en el negocio y ii) evaluación de riesgos.

Fase II: Definición de la estrategia de continuidad

En esta fase, se determinan las estrategias de continuidad que permitirán mantener las actividades y procesos críticos de negocio, dentro del tiempo objetivo de recuperación definido para cada proceso.

Los aspectos para considerar dentro de la estrategia (según sea aplicable para cada proceso), son:

- Seguridad del personal.
- Instalaciones alternas de trabajo.
- Infraestructura alterna de tecnología de información que soporte el proceso.

- Seguridad de la información.
- Equipamiento necesario para el proceso.
- Habilidades y conocimientos asociados al proceso.

Las estrategias seleccionadas y los recursos necesarios para implementarlas serán aprobados por el Comité de Riesgos y ratificados por el Directorio.

Fase III: Desarrollar e Implementar las estrategias de continuidad

Edpyme CREDIVISIÓN debe desarrollar planes de respuesta ante los eventos analizados en las fases previas e implementar un modelo de respuesta flexible que permita cubrir los eventos inesperados y proveer los recursos necesarios, acorde con las estrategias seleccionadas en Fase II, para enfrentar con éxito un evento de interrupción. Para este fin, Edpyme CREDIVISIÓN debe implementar dos tipos de planes:

- Plan de Manejo de Crisis
- Planes de Continuidad del Negocio:

Fase IV: Pruebas y Actualización

Edpyme CREDIVISIÓN deberá realizar ejercicios para validar los planes y procedimientos desarrollados, así como realizar su revisión y mantenimiento de forma periódica y a intervalos definidos.

a) Ejecución de Pruebas:

El alcance de las pruebas debe ser consistente con el alcance de los planes de continuidad del negocio. Cada prueba debe tener objetivos definidos y un reporte que resuma los resultados alcanzados y recomendaciones. Esta información debería ser usada para mejorar los planes de continuidad del negocio en forma oportuna. Pueden aplicarse diferentes tipos de prueba, desde las pruebas de escritorio hasta las simulaciones completas de escenarios de interrupción de operaciones.

Tal como está establecido en las políticas, Edpyme CREDIVISIÓN deberá asegurarse que sus principales proveedores de servicios cuenten con planes de continuidad y que éstos cumplan con lo señalado en el presente numeral.

b) Actualización de los Planes:

Revisará y actualizará los planes de gestión de la continuidad del negocio cada vez que exista un cambio que impacte a la empresa (ya sea interno o externo) a nivel de continuidad.

Los cambios significativos que ocurran en los procesos, en las personas y/o en los sistemas de la empresa serán informados al Oficial de Continuidad del Negocio a través del Analista de Procesos, jefe de TI, según corresponda. El responsable de velar por que los planes se encuentren actualizados es el Oficial de Continuidad del Negocio.

Fase V. Integración de la GCN con la Cultura Organizacional

El proceso para desarrollar e incorporar de forma sostenida la GCN en la cultura de la organización es fruto de los siguientes tres pasos:

- a) Evaluación del grado de conocimiento sobre la gestión de continuidad:
- b) Desarrollo y mejora de la cultura de continuidad:
- c) Monitoreo permanente

VI. PROCEDIMIENTOS

Edpyme CREDIVISIÓN, debe informar a la Superintendencia todo evento que implique las siguientes acciones:

- a) Suspensión de la atención al público por un tiempo mayor al tiempo objetivo de recuperación (RTO) de cuatro (4) horas de interrupción.
- b) Todo evento que implique invocar al Plan de Manejo de Crisis.
- c) Falla del computador principal o de su sistema operativo, entre los cuales se encuentran el SISGO, Intranet, Base de Datos.
- d) Falla de la red de comunicaciones. Lo cual podría generar por ejemplo un corte de los correos electrónicos internos de Edpyme CREDIVISIÓN.
- e) Inhabilitación o imposibilidad de acceso a la oficina principal u oficinas administrativas de la empresa.
- f) Interrupción de operaciones en toda la red de agencias o en una parte significativa de la red (medida como el mayor porcentaje de colocaciones realizadas).
- g) Falla de proveedores de servicios críticos que impacten sobre las operaciones de Edpyme CREDIVISIÓN; tales como central de riesgo y servicio de internet.
- h) Huelgas o paralizaciones del personal.

Plazo de Comunicación a la Superintendencia y Presentación del Informe

Edpyme CREDIVISIÓN, deberá informar a la Superintendencia de Banca, Seguros y AFP's en cuanto tome conocimiento del evento y como plazo máximo al día siguiente hábil de la ocurrencia de éste.

Esta comunicación debe incluir una descripción general del evento ocurrido y deberá ser enviada al correo electrónico: continuidad@sbs.gob.pe a cargo del responsable de Gestión de Continuidad del Negocio de Edpyme CREDIVISIÓN.

Edpyme CREDIVISIÓN deberá mantener informada a la Superintendencia respecto a las medidas tomadas frente a dicho evento para asegurar la continuidad de sus operaciones, hasta que se restablezca el funcionamiento normal de sus procesos.

Posteriormente, transcurridos los diez (10) días hábiles siguientes a la ocurrencia del evento, el responsable de Gestión de Continuidad del Negocio de la Edpyme deberá remitir un informe detallado en que se explique los siguientes aspectos:

- a. Las razones de la falla
- b. La duración del evento
- c. Las líneas de negocio, productos y procesos operativos afectados, según sea el caso.
- d. Las medidas tomadas para superar el evento
- e. La situación existente a la fecha de reporte y si éste ha sido completamente superado.

Anexo 14. Acuerdo de confidencialidad

ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN

Conste por el presente documento, el Acuerdo de Confidencialidad y No Divulgación (en adelante, el ACUERDO) que celebran:

ENTIDAD DE DESARROLLO DE LA PEQUEÑA Y MICROEMPRESA CREDIVISION, identificada con RUC N° 20429417865, con domicilio legal en Av. César Canevaro N° 133 Coo. Viv. Valle Sharon Pampas, distrito de San Juan de Miraflores, provincia y departamento de Lima, representada por su Gerente General, señor **CARLOS TAMAYO CAPARO**, identificado con DNI N° 23862921, según poderes inscritos en la Partida Electrónica N° 11118805 del Registro de Personas Jurídicas de Lima, y por su Gerente de Administración y Finanzas, señor **CARLOS ALBERTO CRUZ CRUZ**, identificado con DNI N° 03662092, según facultades otorgadas mediante Acuerdo N° 060-2021-D-ECV del Directorio, de la Sesión Ordinaria N° 06-2021, de fecha 25 de junio de 2021, a quien en adelante se denominará **CREDIVISION**; y de la otra parte, **JORGE BURGA SEGOVIA**, identificado con DNI N° 44639145, con domicilio en Calle Ontario 275, Distrito de Chorrillos, Provincia y Departamento de Lima, a quien en lo sucesivo se le denominará **EL CONFIDENTE**, conforme a los términos y condiciones siguientes:

En el presente Acuerdo a **EL CONFIDENTE** y **CREDIVISION** se les denominará conjuntamente **LAS PARTES**.

CLÁUSULA PRIMERA: ANTECEDENTES

LAS PARTES del presente Acuerdo están conformadas por las siguientes personas:

- 1.1. **EL CONFIDENTE**, es trabajador de **CREDIVISION**, quien viene desempeñándose en la actualidad en el cargo de **Analista de Soporte Informático**.
- 1.2. **CREDIVISION** es una **EDPYME**, que brinda servicios financieros a la Micro y Pequeña Empresa, con valores cristianos, que contribuyen al desarrollo transformador sostenible de empresarios de bajos recursos.

CREDIVISION ha evaluado colaborar y aceptar que **EL COMITENTE** desarrolle su tesis de investigación, referida al *"Diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI) para Edpyme Credivision, Basado en la Norma ISO 27001:2013"* (en adelante, **EL PROYECTO**), el cual permitirá establecer una mejora en la seguridad de la información en los procesos de **CREDIVISION**.

LAS PARTES dejan constancia que cualquier resultado y/o conclusión al que pueda llegar como parte del desarrollo de la investigación quedará en poder de **CREDIVISION**. Asimismo, y en caso el vínculo laboral fuese, **EL CONFIDENTE** culminará su tesis de investigación, no generando dependencia laboral directa o indirecta con **CREDIVISION**.

CLÁUSULA SEGUNDA: OBJETO DEL CONVENIO

El objeto del presente **ACUERDO** es establecer los compromisos relativos a la confidencialidad y no divulgación que **EL COMITENTE** asume respecto de la información que brindará a **CREDIVISION** para el desarrollo de **EL PROYECTO**. En caso **EL PROYECTO** requiera la entrega de materiales, se deberá suscribir el respectivo Acuerdo de Transferencia de Materiales, sin perjuicio de que tales materiales se encuentren comprendidos en el alcance del presente Acuerdo bajo el concepto de información confidencial.

En este sentido, **LAS PARTES** reconocen que la información, definida en la cláusula siguiente, y por extensión los materiales, de ser el caso, tendrán naturaleza confidencial, por lo que se comprometen a tratarlos según las provisiones del presente acuerdo, a efectos de resguardar su confidencialidad y evitar su divulgación.

EL CONFIDENTE reconoce que la divulgación de la **INFORMACIÓN CONFIDENCIAL**, que comprende los materiales de ser el caso, así como el incumplimiento de su devolución, podría ocasionar daños y



perjuicios a esta, por lo que se obliga a actuar con la debida diligencia y según lo establecido en el presente acuerdo.

CLÁUSULA TERCERA: CONFIDENCIALIDAD Y NO DIVULGACIÓN

- 3.1. **LAS PARTES** acuerdan que toda la información y documentación, así como los materiales a los que **EL CONFIDENTE** pueda acceder de manera directa o indirecta, por cualquier medio (físico, virtual, escrito, oral), que haya sido proporcionada y/o generada por **CREDIVISION** (en adelante, la **INFORMACIÓN CONFIDENCIAL**), en el marco del presente Acuerdo y/o en relación con **EL PROYECTO**, se tratará como confidencial.
- 3.2. La **INFORMACIÓN CONFIDENCIAL** comprende la información y materiales relacionados con **EL PROYECTO** a la que hubiera podido acceder **EL COMITENTE** en las coordinaciones previas a la suscripción del presente acuerdo o durante el desarrollo del **PROYECTO**.
- 3.3. En consecuencia, **EL CONFIDENTE** no podrá entregar la **INFORMACIÓN CONFIDENCIAL** a la que se refiere el presente acuerdo a terceros ni divulgarla de cualquier forma sin autorización expresa y escrita de la otra parte, salvo que se lo ordene una autoridad judicial o administrativa, en cuyo caso **CREDIVISION** deberá informar inmediatamente y por escrito a **EL CONFIDENTE** en un plazo no mayor a tres (3) días hábiles desde que fue notificada con el requerimiento, acompañando copias de dicho requerimiento.
- 3.4. **EL COMITENTE** se compromete a no divulgar, reproducir, transmitir, revelar o emplear la **INFORMACIÓN CONFIDENCIAL** en beneficio propio o de terceros; así como a resguardarla diligentemente, con el mismo nivel de diligencia que aplica para su propia información confidencial y que corresponde a las prácticas comúnmente aceptadas.
- 3.5. **EL COMITENTE** reconoce que los derechos de propiedad intelectual, actuales y futuros, y otros vinculados a la información objeto de este acuerdo pertenecen a **CREDIVISION** y el hecho de revelar la información a **LA INSTITUCIÓN** para el fin mencionado en la cláusula segunda no modifica ni perjudica en forma alguna sus derechos.
- 3.6. **EL CONFIDENTE** se obliga a devolver toda la documentación calificada como confidencial por **CREDIVISION** o a destruirla, así como devolver o destruir los materiales de ser el caso, según lo que requiera **CREDIVISION**, en el supuesto de que la relación entre las partes finalice, ya sea al término del presente Acuerdo o de manera anticipada.

EL CONFIDENTE no podrá realizar ni retener materiales o derivados de estos, copias, fotografías, dibujos ni apuntes o resúmenes de la **INFORMACIÓN CONFIDENCIAL** que le sea confiada.

CLÁUSULA CUARTA: RESPONSABILIDAD DE EL CONFIDENTE

LAS PARTES acuerdan que en caso **EL CONFIDENTE** revele la información confidencial que le sea divulgada por **CREDIVISION** en el marco del presente Acuerdo, directa o indirectamente, de forma dolosa o por falta de diligencia, deberá indemnizar a **CREDIVISION** por los daños y perjuicios que le ocasione, sin perjuicio de las acciones civiles o penales que puedan corresponder a esta última.

CLÁUSULA QUINTA: USO DE SIGNOS DISTINTIVOS DE LA OTRA PARTE

LAS PARTES no podrán usar el nombre, logotipos, emblemas, marcas, ya sea que se encuentren registradas o no, y en general cualquier signo distintivo de la otra parte sin su consentimiento previo y por escrito.

Ninguna de **LAS PARTES** podrá indicar que se encuentra vinculada o relacionada con la otra parte, ni podrá anunciar la existencia de relación alguna, o la realización de **EL PROYECTO**, sin contar con autorización escrita de la otra parte.

CLÁUSULA SEXTA: PROHIBICIÓN DE CESIÓN



LAS PARTES no podrán ceder ni transferir bajo ningún título o modalidad su posición contractual, sin el previo y expreso consentimiento por escrito de la otra parte.

CLÁUSULA SÉPTIMA: SOLUCIÓN DE CONTROVERSIAS Y JURISDICCIÓN

LAS PARTES declaran que celebran el presente Acuerdo conforme a las reglas de la buena fe y de común acuerdo, por lo cual acuerdan que, en caso de producirse alguna discrepancia o controversia en la interpretación, ejecución y/o eventual incumplimiento del presente Acuerdo, será resuelta en forma armoniosa entre **LAS PARTES**.

A tal efecto, la parte que se considere afectada enviará a la otra parte una comunicación escrita, con una relación de los hechos que le afectan, y de ser posible, las medidas que requiere que la otra parte tome para resolver la discrepancia o controversia, otorgándole un plazo no menor de cinco (5) días hábiles para responder por escrito.

De no recibir respuesta o si esta fuera insatisfactoria, la parte agraviada podrá resolver el presente Acuerdo, sin perjuicio de las acciones civiles o penales que puedan corresponder.

CLÁUSULA OCTAVA: PROTECCIÓN DE DATOS PERSONALES

LAS PARTES declaran expresamente que, en el marco del presente Acuerdo, ambas podrán tener acceso a los datos personales de algunos de sus representantes o colaboradores, (en adelante, la **INFORMACIÓN PERSONAL**), por lo que se comprometen expresamente a cumplir con las disposiciones de la Ley 29733 (Ley de Protección de Datos Personales) y su reglamento, aprobado mediante Decreto Supremo 003-2013-JUS, así como de cualquier otra ley, norma y/o disposición que las sustituya, modifique, reglamente o complemente en el futuro.

CLÁUSULA NOVENA: PLAZO, VIGENCIA, COMUNICACIONES y RESOLUCIÓN

El presente **ACUERDO** entrará en vigencia a partir de la suscripción. El **ACUERDO** tendrá un plazo de vigencia de tres (03) meses, contados desde el 17.03.2022 al 16.06.2022. A la conclusión del plazo, **CREDIVISION** deberá indicar a **EL CONFIDENTE** si debe devolver o destruir **LA INFORMACIÓN CONFIDENCIAL**.

LAS PARTES podrán resolver el presente **ACUERDO** en cualquier momento, comunicándolo por escrito a la otra parte con una anticipación no menor a treinta (30) días. En este caso, **EL CONFIDENTE** deberá indicar a **CREDIVISION** si debe devolver o destruir **LA INFORMACIÓN CONFIDENCIAL**.

La devolución o destrucción de **LA INFORMACIÓN CONFIDENCIAL** deberá constar por escrito. La obligación de **EL CONFIDENTE** de mantener la confidencialidad y no divulgar la **INFORMACIÓN CONFIDENCIAL** subsiste incluso después de la conclusión o resolución del Acuerdo, siempre y cuando la información mantenga su carácter confidencial. De igual manera, la información que incluya datos personales goza de protección indefinida.

LAS PARTES suscriben el presente Acuerdo en dos (2) ejemplares de un mismo tenor, a los 17 días del mes de marzo del 2022.




CREDIVISION
CARLOS TAMAYO CAPAND
GERENTE GENERAL


EL CONFIDENTE
JORGE BURGA SECOVIA


CREDIVISION
CARLOS ALBERTO CRUZ CRUZ
GERENTE DE ADMINISTRACIÓN Y FINANZAS

Anexo 15. Manual del SGSI

I. INTRODUCCIÓN

Edpyme CREDIVISIÓN reconoce que la información es uno de los activos más importantes y críticos para el desarrollo de sus funciones. Dado que, en la gestión de los procesos estratégicos, misionales y de soporte, constantemente se está procesando, gestionando, almacenando, transfiriendo e intercambiando valiosa información que debe ser protegida. Es así como la empresa ve la necesidad de implementar un Sistema de Gestión de Seguridad de la Información para establecer los mecanismos y asegurar la confidencialidad, integridad y disponibilidad de la información que se maneja. Asimismo, lograr garantizar que los riesgos de la seguridad sobre los activos de información sean conocidos, gestionados y minimizados.

Para ello, la entidad ha adoptado los lineamientos de la norma ISO/IEC 27001:2013, la cual establece los requisitos para la implementación del SGSI. Es así como en este documento se presentan las políticas, lineamientos y normas de seguridad de la información definidas por la empresa y se convierten en la base para la implementación de los estándares, procedimientos, instructivos y controles que deberán ser implementados.

II. OBJETIVO

El presente manual tiene como objetivo dar a conocer los lineamientos y acciones a seguir para la posterior implementación del Sistema de Gestión de Seguridad de la Información de la empresa.

III. ALCANCE DEL DOCUMENTO

Cumplir con los pilares de seguridad de la información, preservando la confidencialidad, integridad y disponibilidad de la información que se maneja en el área de TI.

IV. TÉRMINOS Y DEFINICIONES

- ✓ **Activo de información.** - En relación con la seguridad de la información, es cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, personas, edificios, etc.) que tenga valor para la organización.

- ✓ **Amenaza.** - Causa potencial de un incidente no deseado que puede provocar daños a un sistema o a la organización.
- ✓ **Análisis de riesgo.** - Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- ✓ **Confidencialidad.** - Propiedad que determina que la información no está disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- ✓ **Disponibilidad.** - Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- ✓ **Gestión de riesgos.** - Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y tratamiento del riesgo.
- ✓ **Impacto.** - Cambio adverso en el nivel de los objetivos del negocio logrado.
- ✓ **Integridad.** - Propiedad de la información relativa a su exactitud y completitud.
- ✓ **Probabilidad.** - Frecuencia o factibilidad de ocurrencia del riesgo.
- ✓ **Riesgo.** - Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
- ✓ **Seguridad de la información.** - Preservación de la confidencialidad, integridad y disponibilidad de la información.
- ✓ **SGSI.** - Sistema de Gestión de Seguridad de la Información.

V. SISTEMA DE GESTION DE SI

5.1. Visión general

La empresa al tener en cuenta la gran dependencia sobre sus sistemas de información y la información que maneja propia y de los contribuyentes, ha decidido adoptar un Sistema de Gestión de Seguridad de la Información bajo los lineamientos de la norma internacional ISO/IEC 27001:2013.

5.2. Alcance

La norma ISO/IEC 27001:2013 indica definir de manera adecuada el alcance del SGSI para poder conocer los límites de acción. Como primera medida la empresa establece el alcance del SGSI, se ha elegido de acuerdo a las características del negocio. Para este proyecto el alcance no implica abarcar toda la empresa, es más recomendable iniciar con un alcance limitado que involucre el corazón del negocio y que trabaje con más información.

Edpyme Credivisión, de conformidad con la norma ISO/IEC 27001:2013 establece que el alcance del Sistema de Gestión de Seguridad de Información comprende el proceso de Créditos que contiene los siguientes subprocesos: 1) Otorgamiento de créditos y 2) Recuperación de créditos.

5.3. Objetivos

- Proteger, conservar y asegurar la información de la empresa y las herramientas tecnológicas utilizadas para su generación, procesamiento y disposición, con el fin de preservar la confidencialidad, integridad y disponibilidad frente a amenazas internas o externas, deliberadas o accidentales.
- Implementar y fortalecer los controles para la protección de los activos críticos.
- Educar y concientizar al personal para lograr servidores públicos competentes y comprometidos con una cultura de seguridad de la información reflejada en la aceptación y aplicación de las directrices de seguridad.
- Implementar una metodología de gestión de riesgos de seguridad de la información como herramienta para actuar proactivamente ante la presencia de situaciones que puedan afectar la continuidad, confidencialidad e integridad de la información de la empresa.

5.4. Gestión de riesgos

La metodología de análisis de riesgos de la seguridad de la información cumple con los lineamientos de la ISO/IEC 27001, donde indica que se debe contemplar la identificación de activos, su importancia, las amenazas, vulnerabilidades, probabilidad e impacto, además de definir los criterios de riesgos aceptables.

La metodología de Gestión del Riesgo está dividida en 4 partes:

- I. Inventario de Activos de Información.
- II. Análisis del Riesgo (al que están expuestos los activos de información).
- III. Evaluación del Riesgo.
- IV. Opción de Tratamiento del Riesgo.

5.5. Criterios para la evaluación de Riesgos

La evaluación del riesgo sirve para darle significancia y para identificar los riesgos que requerirán la aplicación priorizada de su tratamiento.

- La identificación de los riesgos se hará en base al juicio de expertos, es decir el personal que está involucrado en el proceso donde interviene cada activo de información valorizado.
- Personal calificado en seguridad de la información, lo cual da una visión global de los riesgos inminentes sobre los activos de información.
- Documentación y buenas prácticas usadas en el mercado sobre los riesgos de información sobre activos de información. Ello creara conciencia en cuanto a los riesgos que puedan estar sujetos los activos de información y qué medidas adoptar en primera instancia.

Los valores del riesgo se definen de acuerdo a la siguiente escala:

VALOR	RIESGO	DESCRIPCIÓN	SIGNIFICADO
B	Bajo	El activo vulnerado no causa un efecto en la información de la organización ni en el proceso	Es un riesgo aceptable, cuando el activo se encuentra expuesto a riesgos bajos o moderados, por lo que no amerita que pase al proceso de Tratamiento de Riesgo.
M	Moderado	El activo vulnerado no causa un efecto considerable en la información de la organización, pero si en alguna actividad del proceso.	
A	Alto	El activo vulnerado puede afectar considerablemente la información, ocasionando incumplimiento de metas, pérdidas económicas importantes, teniendo un efecto negativo en el proceso.	Cuando el activo se encuentra expuesto a riesgos altos o extremos que ameritan ser tratados.
E	Extremo	El activo vulnerado puede afectar seriamente la información de la organización, ocasionando incumplimientos críticos de servicio al cliente con pérdidas económicas muy importantes y daño considerable a la imagen de la institución.	

Los Riesgos Altos o Extremos pasan a la fase de Tratamiento de Riesgos.

Los Riesgos Bajos o Moderados pasan a una fase de Monitoreo, siendo revisado periódicamente para verificar si permanece en su condición de aceptable.

5.6. Opciones de tratamiento de riesgo

Las opciones de tratamiento de riesgo son:

TRATAMIENTO	DESCRIPCIÓN
Transferir	Transferir a un tercero con capacidad financiera / especialización necesaria para administrar adecuadamente.
Reducir	Esta estrategia consiste en actuar para reducir la probabilidad de ocurrencia o el impacto de un riesgo
Aceptar	Aceptar riesgo en su presente nivel debido a que no es posible realizar un tratamiento, justificando el motivo.
Evitar	El nivel de riesgo de la actividad es inaceptable, además no es posible eliminar las causas del riesgo (agente amenaza)

5.7. Opciones de tratamiento de riesgo

Luego de haber efectuado el análisis de riesgos sobre los activos de información el Comité de Seguridad de la Información, el Oficial de Seguridad de la Información y el área involucrada sobre el riesgo del activo de información deberán reunirse y efectuar un plan de tratamiento de riesgos para los riesgos considerados. Según Anexo 11.

VI. DECLARACION DE APLICABILIDAD

La Declaración de Aplicabilidad o SOA (Statement of Applicability) es un documento basado en el anexo A de la norma ISO/IEC 27001:2013 que contiene los 114 controles en los 14 dominios. A través del SOA la entidad identifica los controles que serán implementados como parte del SGSI y sus excepciones. La declaración de Aplicabilidad del Sistema de Gestión de Seguridad de la Información de la organización se encuentra dentro del presente proyecto en el Anexo 5.

VII. POLÍTICAS DEL SISTEMA DE GESTIÓN DE SI

Las políticas que conciernen al SGSI son de cumplimiento obligatorio para todo el personal de la entidad. Estas tienen el propósito de establecer las acciones necesarias para la protección de la información. Las políticas específicas son:

- Política de control de accesos
- Política de acceso a internet
- Política de escritorio y pantalla limpia
- Política de teletrabajo
- Política de gestión de incidentes de seguridad
- Política de seguridad en las comunicaciones
- Política de seguridad de gestión de incidentes de seguridad de la información

VIII. INCUMPLIMIENTO

El incumplimiento de lo indicado en el presente manual del SGSI tendrá como resultado la aplicación de diversas sanciones de acuerdo con el reglamento interno de la empresa, que serán aplicadas conforme a la naturaleza y gravedad del aspecto no cumplido.

Anexo 16. Valoración de los Expertos

CONSTANCIA DE JUICIO DE EXPERTO

Ing. RICHARD RIVEROS FLORES
ESPECIALISTA EN SEGURIDAD DE LA INFORMACIÓN
DNI: 29726338
CIP: 102830

Mediante la presente hago constar que realice la revisión del proyecto de investigación titulado "DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EDPYME CREDIVISIÓN, BASADO EN LA NORMA ISO 27001:2013" elaborado por el bachiller JORGE BURGA SEGOVIA.

Considero que dicho proyecto reúne los requisitos suficientes y necesarios para ser considerados válidos y confiables por lo tanto aptos para ser aplicados en el logro del objetivo que se planteó en la investigación

Lima, noviembre de 2022



Ing. Richard Riveros Flores

DNI: 29726338

FICHA DE VALIDACIÓN POR EXPERTO

1. REFERENCIA

- 1.1. Experto: Richard Riveros Flores
- 1.2. Especialidad: Seguridad de la información
- 1.3. Cargo actual: Jefe de TI
- 1.4. Grado académico: Maestro en Ingeniería de Sistemas
- 1.5. Lugar y fecha: San Juan de Miraflores, noviembre 2022

2. TABLA DE VALORACIÓN

N°	ITEM	VALORACIÓN					
		5	4	3	2	1	0
1	Cumplimiento inicial y final		X				
2	SGSI con respecto a CONFIDENCIALIDAD	X					
3	SGSI con respecto a INTEGRIDAD	X					
4	SGSI con respecto a DISPONIBILIDAD	X					



Ing. Richard Riveros Flores

DNI: 29726338

CONSTANCIA DE JUICIO DE EXPERTO

Ing. ERIC ANTONIO JIMENEZ MENDOZA
ESPECIALISTA EN SEGURIDAD DE LA INFORMACIÓN
DNI: 42129943
CIP: 159951

Mediante la presente hago constar que realice la revisión del proyecto de investigación titulado "DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EDPYME CREDIVISIÓN, BASADO EN LA NORMA ISO 27001:2013" elaborado por el bachiller JORGE BURGA SEGOVIA.

Considero que dicho proyecto reúne los requisitos suficientes y necesarios para ser considerados válidos y confiables por lo tanto aptos para ser aplicados en el logro del objetivo que se planteó en la investigación

Lima, noviembre de 2022



Ing. Eric A. Jimenez Mendoza

DNI: 42129943

FICHA DE VALIDACIÓN POR EXPERTO

1. REFERENCIA

1.1. Experto: Eric Antonio Jimenez Mendoza

1.2. Especialidad: Seguridad de la información

1.3. Grado académico: Ingeniero de Sistemas

1.4. Lugar y fecha: San Juan de Miraflores, noviembre 2022

2. TABLA DE VALORACIÓN

N°	ITEM	VALORACIÓN					
		5	4	3	2	1	0
1	Cumplimiento inicial y final		X				
2	SGSI con respecto a CONFIDENCIALIDAD		X				
3	SGSI con respecto a INTEGRIDAD	X					
4	SGSI con respecto a DISPONIBILIDAD	X					



Ing. Eric A. Jimenez Mendoza

DNI: 42128943

Anexo 17. Evaluación de Encuestas.

Encuesta de Estado Inicial - CREDIVISION

Descripción del formulario

1. ¿Existen políticas publicadas para apoyar la seguridad de la información? *

Sí

No

2. ¿Las políticas de seguridad de la información son revisadas y actualizadas? *

Sí

No

3. ¿Están definidas las responsabilidades de seguridad de la información? *

Sí

No

4. ¿Se han segregado las diversas áreas de responsabilidad sobre la seguridad de la información para evitar accesos indebidos? *

Sí

No

5. ¿Existe proceso definido para contactar con las autoridades competentes ante incidentes relacionados con seguridad de la información? *

Sí

No

6. ¿Existen contactos definidos con grupos de interés especial? *

Sí

No

7. ¿En la gestión de proyectos se consideran aspectos relacionados con seguridad de la información? *

Sí

No

8. ¿Existen políticas definidas para el uso seguro de dispositivos móviles? *

Sí

No

9. ¿Se aplican criterios de seguridad para el teletrabajo? *

Sí

No

10. ¿La Edpyme realiza verificaciones de antecedentes de los candidatos para los empleos? *

Sí

No

11. ¿Existen acuerdos con los empleados y contratistas donde se especifiquen las responsabilidades de seguridad de la información? *

Sí

No

24. ¿Existen procedimientos para la eliminación de soportes? *

- sí
- No

25. ¿Son protegidos los soportes físicos con información sensible durante el transporte? *

- sí
- No

26. ¿Existe una política para definir los controles de acceso a la información según las función o puesto de trabajo? *

- sí
- No

27. ¿Existen políticas de acceso a las redes y a los servicios de red? *

- sí
- No

28. ¿Existen procesos de alta y baja de usuarios? *

- sí
- No

29. ¿Existen procesos para la asignación de perfiles de acceso? *

- sí
- No

30. ¿Se define un proceso específico para la asignación de permisos privilegiados de administración de accesos? *

- sí
- No

31. ¿Las contraseñas y otra información de autenticación secreta, son proporcionadas de forma segura? *

- sí
- No

32. ¿Se establecen periodos para renovación de permisos de acceso? *

- sí
- No

33. ¿Existe un proceso definido para la revocación o reasignación de permisos? *

- sí
- No

34. ¿Existen responsabilidades para los usuarios sobre el uso de información secreta de autenticación? *

- sí
- No

35. ¿El acceso a la información en los sistemas y aplicaciones es restringido según la política de control de acceso? *

- sí
- No

60. ¿Las nuevas instalaciones de software son validadas de forma segura? *

- Sí
- No

61. ¿Se establecen métodos de control para vulnerabilidades técnicas? *

- Sí
- No

62. ¿Existen políticas de restricción en la instalación de software para usuarios finales? *

- Sí
- No

63. ¿La auditoría realiza los controles en los sistemas de información? *

- Sí
- No

64. ¿Existe controles de red para los elementos conectados? *

- Sí
- No

65. ¿Se verifica la seguridad de los servicios de red? *

- Sí
- No

66. ¿Existe separación de redes tomado en cuenta la información y los recursos? *

- Sí
- No

67. ¿Existen políticas y procedimientos para el intercambio de información? *

- Sí
- No

68. ¿Se establecen acuerdos de intercambio de información con terceros? *

- Sí
- No

69. ¿Se establecen políticas en mensajería electrónica? *

- Sí
- No

70. ¿Se establecen acuerdos de confidencialidad para el intercambio de información con terceros? *

- Sí
- No

71. ¿Se definen los requisitos de seguridad de la información para los nuevos sistemas de información? *

- Sí
- No

72. ¿Se definen requisitos mínimos de seguridad en las aplicaciones para redes públicas? *

- sí
- No

73. ¿Existe una política de seguridad de la información para proveedores? *

- sí
- No

74. ¿Se han definido requisitos de seguridad de la información en contratos con terceros? *

- sí
- No

75. ¿Se fijan requisitos de seguridad de la información para las comunicaciones y la cadena de suministro? *

- sí
- No

76. ¿Se controla el cumplimiento de la provisión de servicios por parte de los proveedores? *

- sí
- No

77. ¿Se definen responsabilidades y procedimientos para gestionar los incidentes de la seguridad de la información? *

- sí
- No

111

78. ¿Se notifica de forma oportuna los eventos de seguridad de la información? *

- sí
- No

79. ¿Se corrobora la adecuada notificación de los puntos débiles de la seguridad de la información? *

- sí
- No

80. ¿Se ha establecido un proceso para gestionar los eventos de seguridad de la información? *

- sí
- No

81. ¿Existen mecanismos para dar una respuesta a los incidentes de seguridad de la información? *

- sí
- No

82. ¿Existe una base de conocimiento de incidentes de seguridad para posteriores soluciones? *

- sí
- No

83. ¿Se recopila las evidencias de los incidentes en la seguridad de la información? *

- sí
- No

Encuesta de Estado Inicial - CREDIVISION

El correo electrónico del destinatario (aborda@credivisionperu.com.pe) se registró al enviar el formulario.

Nombres y Apellidos *

Antonio Borda

Cargo *

Administrador de BBDD

1. ¿Existen políticas publicadas para apoyar la seguridad de la información? *

Si

No

2. ¿Las políticas de seguridad de la información son revisadas y actualizadas? *

Encuesta de Estado Inicial - CREDIVISION

El correo electrónico del destinatario (rriveros@credivisionperu.com.pe) se registró al enviar el formulario.

Nombres y Apellidos *

Richard Riveros Flores

Cargo *

Jefe de TI

1. ¿Existen políticas publicadas para apoyar la seguridad de la información? *

Si

No

2. ¿Las políticas de seguridad de la información son revisadas y actualizadas? *

Si

Anexo 18. Análisis de Brechas

ISO 27002	CONTROL	PREGUNTA	ESTADO ACTUAL	NIVEL DE MADUREZ
5.1	Directrices de la Dirección en seguridad de la información.			
5.1.1	Conjunto de políticas para la seguridad de la información.	¿Existen políticas publicadas para apoyar la seguridad de la información?	Inicial	1
5.1.2	Revisión de las políticas para la seguridad de la información.	¿Las políticas de seguridad de la información son revisadas y actualizadas?	Inexistente	0
6.1	Organización interna.			
6.1.1	Asignación de responsabilidades para la seguridad de la información.	¿Están definidas las responsabilidades de seguridad de la información?	Inexistente	0
6.1.2	Segregación de tareas.	¿Se han segregado las diversas áreas de responsabilidad sobre la seguridad de la información para evitar accesos indebidos?	Inexistente	0
6.1.3	Contacto con las autoridades.	¿Existe proceso definido para contactar con las autoridades competentes ante incidentes relacionados con seguridad de la información?	Inicial	1
6.1.4	Contacto con grupos de interés especial.	¿Existen contactos definidos con grupos de interés especial?	Inexistente	0
6.1.5	Seguridad de la información en la gestión de proyectos.	¿En la gestión de proyectos se consideran aspectos relacionados con seguridad de la información?	Inicial	1
6.2	Dispositivos móviles y el teletrabajo.			
6.2.1	Política de dispositivos móviles	¿Existen políticas definidas para el uso seguro de dispositivos móviles?	Inicial	1

ISO 27002	CONTROL	PREGUNTA	ESTADO ACTUAL	NIVEL DE MADUREZ
6.2.2	Teletrabajo.	¿Se aplican criterios de seguridad para el teletrabajo?	Repetible	2
7.1	Antes del empleo			
7.1.1	Investigación de antecedentes.	¿La Edpyme realiza verificaciones de antecedentes de los candidatos para los empleos?	Inexistente	0
7.1.2	Términos y condiciones de contratación.	¿Existen acuerdos con los empleados y contratistas donde se especifiquen las responsabilidades de seguridad de la información?	Inexistente	0
7.2	Durante el empleo.			
7.2.1	Responsabilidades de gestión.	¿El cumplimiento de las responsabilidades sobre la seguridad de la información es exigida de forma activa a empleados y terceros?	Inexistente	0
7.2.2	Concienciación, educación y capacitación en seguridad de la información	¿Existen procesos de información, capacitación y concientización sobre la seguridad de la información?	Inexistente	0
7.2.3	Proceso disciplinario.	¿Existe un proceso disciplinario donde se comunica a los empleados y terceros las consecuencias de los incumplimientos sobre las políticas de la seguridad de la información?	Inexistente	0
7.3	Finalización del empleo o cambio en el puesto de trabajo.			

ISO 27002	CONTROL	PREGUNTA	ESTADO ACTUAL	NIVEL DE MADUREZ
7.3.1	Responsabilidades ante la finalización o cambio	¿Existen acuerdos de responsabilidad de seguridad de la información que siguen siendo válidas después de la finalización del contrato?	Inexistente	0
8.1	Responsabilidad sobre los activos.			
8.1.1	Inventario de activos.	¿Se ha realizado un inventario de activos?	Repetible	2
8.1.2	Propiedad de los activos.	¿Se ha identificado al responsable de cada activo?	Inicial	1
8.1.3	Uso aceptable de los activos.	¿Se han establecido normas para el uso adecuado de activos?	Inicial	1
8.1.4	Devolución de activos.	¿Existe procedimiento para la devolución de activos asignados?	Repetible	2
8.2	Clasificación de la información.			
8.2.1	Clasificación de la información.	¿Se clasifica la información según su confidencialidad?	Inexistente	0
8.2.2	Etiquetado de la información.	¿Existen procedimientos que definan el etiquetado de activos?	Inicial	1
8.2.3	Manipulado de la información	¿Existen procedimientos para el manipulado de la información de acuerdo a su clasificación?	Inicial	1
8.3	Manipulación de los soportes			
8.3.1	Gestión de soportes extraíbles.	¿Existen procedimientos que definen cómo manejar los soportes extraíbles (uso, cifrado, borrado, etc.)?	Inicial	1
8.3.2	Eliminación de soportes.	¿Existen procedimientos para la eliminación de soportes?	Inicial	1
8.3.3	Soportes físicos en tránsito.	¿Son protegidos los soportes físicos con información sensible durante el transporte?	Inicial	1

ISO 27002	CONTROL	PREGUNTA	ESTADO ACTUAL	NIVEL DE MADUREZ
9.1	Requisitos de negocio para el control de accesos			
9.1.1	Política de control de accesos.	¿Existe una política para definir los controles de acceso a la información según las función o puesto de trabajo?	Inexistente	0
9.1.2	Acceso a las redes y los servicios de red	¿Existen políticas de acceso a las redes y a los servicios de red?	Inicial	1
9.2	Gestión de acceso de usuario.			
9.2.1	Registro y baja de usuario.	¿Existen procesos de alta y baja de usuarios?	Repetible	2
9.2.2	Provisión de accesos de usuario	¿Existen procesos para la asignación de perfiles de acceso?	Inicial	1
9.2.3	Gestión de privilegios de acceso	¿Se define un proceso específico para la asignación de permisos privilegiados de administración de accesos?	Inicial	1
9.2.4	Gestión de la información secreta de autenticación de los usuarios.	¿Las contraseñas y otra información de autenticación secreta son proporcionadas de forma segura?	Inicial	1
9.2.5	Revisión de los derechos de acceso de los usuarios.	¿Se establecen periodos para renovación de permisos de acceso?	Inexistente	0
9.2.6	Retirada o reasignación de los derechos de acceso	¿Existe un proceso definido para la revocación o reasignación de permisos?	Inexistente	0
9.3	Responsabilidades del usuario.			
9.3.1	Uso de información secreta de autenticación.	¿Existen responsabilidades para los usuarios sobre el uso de información secreta de autenticación?	Inexistente	0
9.4	Control de acceso a sistemas y aplicaciones.			

ISO 27002	CONTROL	PREGUNTA	ESTADO ACTUAL	NIVEL DE MADUREZ
9.4.1	Restricción del acceso a la información.	¿El acceso a la información en los sistemas y aplicaciones es restringido según la política de control de acceso?	Inicial	1
9.4.2	Procedimientos seguros de inicio de sesión.	¿Se han implementado procedimientos de acceso seguro para el inicio de sesión?	Inicial	1
9.4.3	Sistema de gestión de contraseñas	¿Cuentan con sistema de gestión de contraseñas?	Inexistente	0
9.4.4	Uso de utilidades con privilegios del sistema.	¿El uso de herramientas de utilidad es controlado y limitado a empleados específicos?	Inicial	1
9.4.5	Control de acceso al código fuente de los programas.	¿Existe procedimiento para el control de acceso al código fuente?	Inexistente	0
10.1	Controles criptográficos.			
10.1.1	Política de uso de los controles criptográficos.	No aplica		
10.1.2	Gestión de claves.	No aplica		
11.1	Áreas seguras.			
11.1.1	Perímetro de seguridad física.	¿Se establecen perímetros de seguridad física con barreras de acceso?	Inicial	1
11.1.2	Controles físicos de entrada.	¿Existen controles físicos de acceso en áreas restringidas?	Inicial	1
11.1.3	Seguridad de oficinas, despachos y recursos.	¿Se establecen medidas de seguridad para oficinas para proteger la información de pantallas, etc. en áreas accesibles a personal externo?	Inicial	1
11.1.4	Protección contra las amenazas externas y ambientales.	¿Existen instaladas alarmas, sistemas de protección contra incendios, etc.?	Repetible	2
11.1.5	El trabajo en áreas seguras.	No aplica		

ISO 27002	CONTROL	PREGUNTA	ESTADO ACTUAL	NIVEL DE MADUREZ
11.1.6	Áreas de acceso público, carga y descarga.	No aplica		
11.2	Seguridad de los equipos.			
11.2.1	Emplazamiento y protección de equipos.	¿Se protegen los equipos de accesos no autorizados?	Inicial	1
11.2.2	Instalaciones de suministro.	¿Se protegen los equipos contra fallos de suministro de energía?	Inicial	1
11.2.3	Seguridad del cableado.	¿Existe protección para los cableados de energía y de datos?	Inicial	1
11.2.4	Mantenimiento de los equipos.	¿Se realizan tareas de mantenimiento de los equipos?	Repetible	2
11.2.5	Retirada de materiales propiedad de la empresa.	No aplica		
11.2.6	Seguridad de los equipos fuera de las instalaciones.	No aplica		
11.2.7	Reutilización o eliminación segura de equipos	¿Existen políticas para proteger o eliminar información de equipos de baja o que van a ser reutilizados?	Inicial	1
11.2.8	Equipo de usuario desatendido.	¿Se establecen reglas de comportamiento para abandonos del puesto de trabajo?	Inicial	1
11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla.	¿Existen políticas para proteger la información de equipos cuando los usuarios abandonan el puesto de trabajo?	Inicial	1
12.1	Procedimientos y responsabilidades operacionales			
12.1.1	Documentación de procedimientos de operación.	¿Se documentan los procedimientos?	Inexistente	0
12.1.2	Gestión de cambios.	¿Se controla que los procedimientos se actualicen constantemente?	Inexistente	0

ISO 27002	CONTROL	PREGUNTA	ESTADO ACTUAL	NIVEL DE MADUREZ
12.1.3	Gestión de capacidades.	¿Se monitorea los recursos para cumplir con la demanda de los usuarios?	Inicial	1
12.1.4	Separación de los recursos de desarrollo, prueba y producción.	¿Existen una separación segura entre los entornos de desarrollo, pruebas y producción?	Inicial	1
12.2	Protección contra el software malicioso (Malware)			
12.2.1	Controles contra el código malicioso.	¿Existen software para la detección de código malicioso?	Inicial	1
12.3	Copias de seguridad.			
12.3.1	Copias de seguridad de la información.	¿Existe una política de backup definida?	Repetible	2
12.4	Registro y supervisión.			
12.4.1	Registro de eventos.	¿Se realiza un registro o logs de eventos?	Inexistente	0
12.4.2	Protección de la información de registro	¿Se ha establecido un sistema de protección para los registros mediante segregación de tareas o copias de seguridad?	Inicial	1
12.4.3	Registros de administración y operación	¿Se protege de forma segura los accesos de los administradores?	Inexistente	0
12.4.4	Sincronización de relojes.	No aplica		
12.5	Control del software en explotación.			
12.5.1	Instalación del software en explotación	¿Las nuevas instalaciones de software son validadas de forma segura?	Inicial	1
12.6	Gestión de la vulnerabilidad técnica.			
12.6.1	Gestión de las vulnerabilidades técnicas.	¿Se establecen métodos de control para vulnerabilidades técnicas?	Inexistente	0
12.6.2	Restricciones en la instalación de software.	¿Existen políticas de restricción en la instalación de software para usuarios finales?	Repetible	2

ISO 27002	CONTROL	PREGUNTA	ESTADO ACTUAL	NIVEL DE MADUREZ
12.7	Consideraciones de las auditorías de los sistemas de información			
12.7.1	Controles de auditoría de los sistemas de información.	¿La auditoría realiza los controles en los sistemas de información?	Inicial	1
13.1	Gestión de la seguridad de redes.			
13.1.1	Controles de red	¿Existe controles de red para los elementos conectados?	Inicial	1
13.1.2	Seguridad de los servicios de red.	¿Se verifica la seguridad de los servicios de red?	Inicial	1
13.1.3	Segregación de redes.	¿Existe separación de redes tomado en cuenta la información y los recursos?	Inicial	1
13.2	Intercambio de información con partes externas.			
13.2.1	Políticas y procedimientos de intercambio de información.	¿Existen políticas y procedimientos para el intercambio de información?	Inexistente	0
13.2.2	Acuerdos de intercambio.	¿Se establecen acuerdos de intercambio de información con terceros?	Inexistente	0
13.2.3	Mensajería electrónica.	¿Se establecen políticas en mensajería electrónica?	Inicial	1
13.2.4	Acuerdos de confidencialidad o no revelación	¿Se establecen acuerdos de confidencialidad para el intercambio de información con terceros?	Inexistente	0
14.1	Requisitos de seguridad en sistemas de información.			
14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	¿Se definen los requisitos de seguridad de la información para los nuevos sistemas de información?	Inexistente	0

ISO 27002	CONTROL	PREGUNTA	ESTADO ACTUAL	NIVEL DE MADUREZ
14.1.2	Asegurar los servicios de aplicaciones en redes públicas.	¿Se definen requisitos mínimos de seguridad en las aplicaciones para redes públicas?	Inicial	1
14.1.3	Protección de las transacciones de servicios de aplicaciones	No aplica		
14.2	Seguridad en los procesos de desarrollo y soporte.			
14.2.1	Política de desarrollo seguro de software.	No aplica		
14.2.2	Procedimientos de control de cambios en los sistemas.	No aplica		
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	No aplica		
14.2.4	Restricciones a los cambios en los paquetes de software.	No aplica		
14.2.5	Principios de ingeniería de sistemas seguros.	No aplica		
14.2.6	Entorno de desarrollo seguro.	No aplica		
14.2.7	Externalización del desarrollo de software.	No aplica		
14.2.8	Pruebas funcionales de seguridad de sistemas.	No aplica		
14.2.9	Pruebas de aceptación de sistemas.	No aplica		
14.3	Datos de prueba.			
14.3.1	Protección de los datos utilizados en pruebas.	No aplica		
15.1	Seguridad de la información en las relaciones con suministradores.			
15.1.1	Política de seguridad de la información en las relaciones con los proveedores	¿Existe una política de seguridad de la información para proveedores?	Inexistente	0
15.1.2	Requisitos de seguridad en contratos con terceros	¿Se han definido requisitos de seguridad de la información en contratos con terceros?	Inexistente	0
15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones.	¿Se fijan requisitos de seguridad de la información para las comunicaciones y la cadena de suministro?	Inicial	1

ISO 27002	CONTROL	PREGUNTA	ESTADO ACTUAL	NIVEL DE MADUREZ
15.2	Gestión de la provisión del servicio del proveedor			
15.2.1	Control y revisión de la provisión de servicios del proveedor	¿Se controla el cumplimiento de la provisión de servicios por parte de los proveedores?	Inicial	1
15.2.2	Gestión de cambios en los servicios provisión del servicio del proveedor.	No aplica		
16.1	Gestión de incidentes de seguridad de la información y mejoras.			
16.1.1	Responsabilidades y procedimientos.	¿Se definen responsabilidades y procedimientos para gestionar los incidentes de la seguridad de la información?	Inicial	1
16.1.2	Notificación de los eventos de seguridad de la información.	¿Se notifica de forma oportuna los eventos de seguridad de la información?	Inicial	1
16.1.3	Notificación de puntos débiles de la seguridad.	¿Se corrobora la adecuada notificación de los puntos débiles de la seguridad de la información?	Inicial	1
16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	¿Se ha establecido un proceso para gestionar los eventos de seguridad de la información?	Inicial	1
16.1.5	Respuesta a incidentes de seguridad de la información.	¿Existen mecanismos para dar una respuesta a los incidentes de seguridad de la información?	Inexistente	0
16.1.6	Aprendizaje de los incidentes de seguridad de la información.	¿Existe una base de conocimiento de incidentes de seguridad para posteriores soluciones?	Inexistente	0
16.1.7	Recopilación de evidencias.	¿Se recopila las evidencias de los incidentes en la seguridad de la información?	Inexistente	0
17.1	Continuidad de la seguridad de la información.			

ISO 27002	CONTROL	PREGUNTA	ESTADO ACTUAL	NIVEL DE MADUREZ
17.1.1	Planificación de la continuidad de la seguridad de la información.	¿Se cuenta con un plan de continuidad de seguridad de la información?	Inicial	1
17.2	Redundancias.			
17.2.1	Disponibilidad de los recursos de tratamiento de la información.	¿Existe la disponibilidad de los recursos críticos de la información?	Inicial	1
18.1	Cumplimiento de los requisitos legales y contractuales.			
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	¿Se tiene conocimiento de la legislación actual?	Inicial	1
18.1.2	Derechos de propiedad intelectual (DPI).	No aplica		
18.1.3	Protección de los registros de la organización.	¿Existe normas de protección de los registros de la organización?	Inicial	1
18.1.4	Protección y privacidad de la información de carácter personal.	¿Se establecen medidas para la protección de datos personales de acuerdo con la legislación vigente?	Inexistente	0
18.1.5	Regulación de los controles criptográficos.	No aplica		
18.2	Revisiones de la seguridad de la información.			
18.2.1	Revisión independiente de la seguridad de la información.	¿Se revisan los controles de la seguridad de la información por personal independiente a los responsables de implementar los controles?	Inicial	1
18.2.2	Cumplimiento de las políticas y normas de seguridad.	¿Se revisa periódicamente el cumplimiento de las políticas y controles de la seguridad de la información?	Inexistente	0
18.2.3	Comprobación del cumplimiento técnico.	¿Se realizan evaluaciones sobre el correcto funcionamiento técnico?	Inexistente	0