FACULTAD DE POSGRADOS

PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) APLICADO A LA INSTITUCIÓN FINANCIERA “COOPELQUINCHE”.

AUTOR

FREDDY PATRICIO AULES PINEIDA

AÑO

2021

FACULTAD DE POSGRADOS

PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) APLICADO A LA INSTITUCIÓN FINANCIERA “COOPELQUINCHE”.

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Magíster en Gestión de la Seguridad de la Información.

Autor

Freddy Patricio Aules Pineida

Año

2021

AGRADECIMIENTOS

A todos los profesores que impartieron sus conocimientos.

A mi esposa Gloria y a mis hijos, por el apoyo, comprensión y paciencia brindada en toda esta etapa.

A Dios y a la Virgen de El Quinche, por derramar sus bendiciones y poder culminar con éxito la maestría.

DEDICATORIA

Este proyecto de titulación va dedicado a mi esposa, a mis padres y a mis hijos, quien siempre están a mi lado para poder seguir adelante y cumplir con éxito este trabajo de titulación.

A mis abuelitos Anselmo y Rosa porque siempre me están regando su bendición.

RESUMEN

La pandemia provocada por el COVID-19, ha conllevado que la información sea uno de los recursos más importantes en las organizaciones. Razón por la cual todas las organizaciones y mucho más las instituciones del sector financiero sin importar el segmento en el cual estén ubicados deberían realizar una apropiada gestión de riesgos.

El identificar y clasificar activos de información, analizar las vulnerabilidades y amenazas a las que se encuentran expuestas ayudara a establecer un plan de acción que permita mitigar los riesgos existentes, donde uno de los principales objetivos es evitar interrupciones en las operaciones que conlleven a generar pérdidas financieras.

Actualmente la Institución financiera “COOPELQUINCHE” tiene deficiencia en cuanto al manejo interno de los activos de información, generando por un lado el desconocimiento de los riesgos a los cuales está expuesta la información que se genera, tramite o almacena en la institución, por lo cual nos hemos propuesto la tarea de ***“Desarrollar un Programa del Sistema de Gestión de Seguridad de la Información”.***

El programa del Sistema de Gestion de Seguridad de la Información ante el incremento considerable de incidentes informáticos presentados en las instituciones del país, nos permitirá identificaremos que tan madura esta la institución basados en el Anexo A de la norma ISO 27001:2013 cubriendo los tres pilares de la información: confidencialidad, integridad y disponibilidad.

ABSTRACT

The pandemic caused by COVID-19, needed that the information be one of the most important resources of the organizations. That is why all the enterprises, especially the ones of the financial sector, without considering its segment where they are located, must do an appropriate risk management.

Identify and classify assets of information, analyze their vulnerabilities and threats that they are exposed will help to establish an action plan that allows mitigating the present risks, where one of the principal objectives is avoid interruptions in the operations that generate financial lost.

Currently the financial Institution called " COOPELQUINCHE" has a deficiency in the internal management in the assets of information, causing an unacknowledged of risks that is exposed the information that is generate or saved in the institution, that is why is *"Developed a system of Information Security Management"*

The program of Information Security Management, in front of the important increase of informatics problems presented in the country's institutions will allowed us identify how mature is the situation according to the Annex A of the standard ISO 27002:2013, covering the three important bases of information: confidentiality, integrity and availability.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La información se ha convertido en uno de los fatores más importantes de una empresa, convirtiéndose como muchos lo mencionan en “las joyas de la corona”. Por lo que esto conlleva a implementar proceso, lineamientos y procedimientos basados en normas y marco de referencia que se ajusten a las instituciones financieras según el grupo económico y segmento al cual correspondan.

El uso de equipos tecnológicos que permitan minimizar los riesgos a los cuales está expuesta la información que se procesa, almaceno o se trasmite obliga a estar a la vanguardia de la tecnología.

El proyecto de titulación parte de la recopilación de información necesaria que permita diagnosticar la situación actual de la cooperativa de ahorro y crédito “COOPELQUINCHE” basado en los requisitos que mencionan las normas ISO 27001 e ISO 27002 con el fin de clasificar y proteger los activos de información.

Ayudados de las normas antes indicadas se elabora un Programa del Sistema de Gestión de Seguridad de la Información en la institución financiera con el fin de establecer políticas y procedimientos que norme la protección de la información tomando muy en cuenta los principios de integridad, confidencialidad y disponibilidad.

Para esto se realiza el análisis de amenazas y vulnerabilidades que permite identificar los riesgos a los cuales está expuesta enfocados en activos de información críticos.

DESARROLLO DEL PROGRAMA

1.1 Objetivo

Desarrollar un Programa del Sistema de Gestión de Seguridad de la Información para la cooperativa de ahorro y crédito “COOPELQUINCHE” utilizando como marco de referencia las normas ISO 27001 y 27002.

1.1.1 Objetivos específicos:

- Analizar la situación actual de la institución basado en los 114 controles del anexo A de la norma 27001:2013 y los niveles de madurez de COBIT-2019.
- Identificar y clasificar los tipos de información con los cuales cuenta la institución.
- Elaborar una herramienta que permita Identificar y clasificar los activos de Información críticos, basados en los principios de integridad, confidencialidad y disponibilidad.
- Realizar un análisis de amenazas y vulnerabilidades para un activo de información crítica.
- Promover el uso de marcos de referencia relacionados con seguridad de la información, así como la aplicación de las políticas, roles y responsabilidades de alto nivel identificadas en el trabajo de investigación.

1.2 Metodología

El proyecto pretende evaluar y diseñar un programa de Sistema de Gestión de la Seguridad de la Información que permitirá fortalecer los procedimientos para el uso y manejo de la información. De esta manera permite incrementar la solvencia, estabilidad y el reconocimiento por parte de las partes interesadas.

a) Evaluar los diferentes procedimientos establecidos para tratamiento de la información.
b) Diagnosticar bajo las mejores practicas (ISO 2700-1,2) la situación actual de la organización financiera.
c) Identificar y clasificar los activos de información.
d) Evaluar riesgos identificados.
e) Recomendar planes de acción.

1.3 Fundamentos Teóricos

1.3.1 SGSI

El sistema de seguridad de la información o también conocido como SGSI por sus siglas en inglés (Information Security Management System) tiene como objetivo evaluar todos los riesgos asociados con los datos e información que se manejan dentro de una empresa. (Ambit BST, 2021).

El SGSI es un elemento fundamental de la norma internacional ISO 27001 que persigue asegurar la integridad y confidencialidad de los datos y los sistemas encargados de procesarlos. (Ambit BST, 2021).

La implementación de SGSI está enfocado tanto para grandes como para peñas empresas, debido a los grandes beneficios que se obtiene al implementarlo:

- Identificación de vulnerabilidades
- Reducción de riesgos.
- Reducción de costos.
- Cumplimiento de la normativa vigente
- Incremento de la competitividad.

1.3.2 ISO 27001:2013

La norma ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan, almacenan y trasmiten. (ISOTools Excellence, 2021).

En lo que respecta al SGSI la norma ISO 27001:2013 en la cual se basa el trabajo de investigación permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos. (ISOTools Excellence, 2021).

Estructura de la norma ISO 27001

1. Objeto y campo de aplicación
2. Referencias Normativas
3. Términos y Definiciones
4. Contexto de la Organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación del Desempeño
10. Mejora

1.3.3 COBIT_2019

Cobit 2019 es un marco internacional de prácticas recomendadas para implementar un buen gobierno y una gestión efectiva de las tecnologías de información en las empresas.
COBIT® 2019 asigna un nivel de capacidad a todas las actividades del proceso, permitiendo una clara definición de los procesos con distintos niveles de capacidad. (ISACA, 2018)

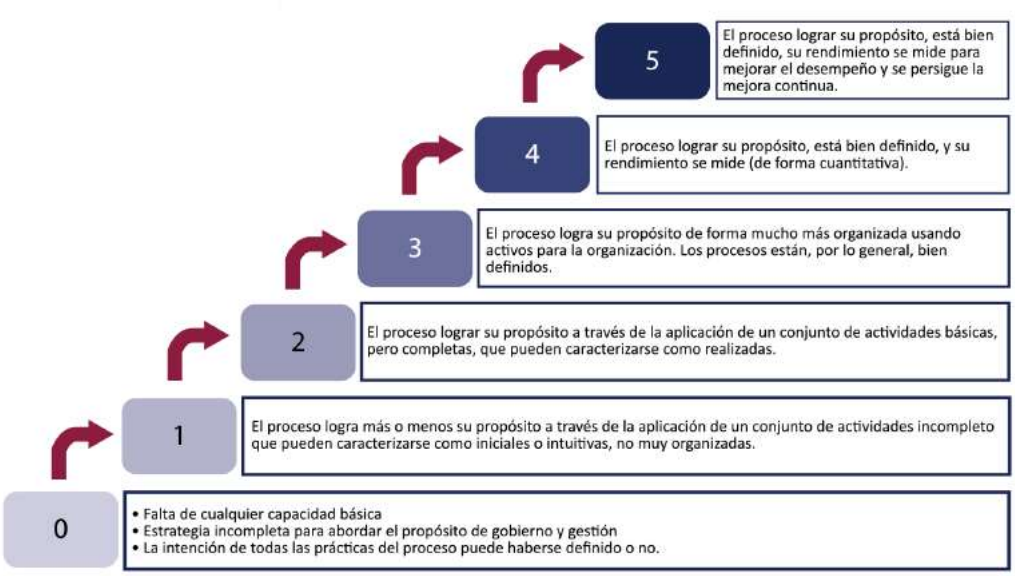

Figura 1 Modelo de Madurez de la Capacidad ® (CMMI)

1.4 Diagnóstico

Las razones que motivan la realización del presente proyecto pretenden dar a conocer el estado actual de la cooperativa de ahorro y crédito “COOPELQUINCHE” relacionado con la aplicación de los 114 controles del anexo A de la norma ISO 27001:2013.

Dentro los principales puntos de atención a destacar, podemos ver la falta de un política de seguridad de la información documentada, aprobada y difundida, inexistencia de procesos para la identificación de vulnerabilidades y tratamiento de riesgos informáticos, no se han realizado pruebas de la efectividad del proceso de continuidad del negocio, inventario de equipos informativos desactualizado, falta de informes de mantenimientos de equipos, falta de capacitaciones del personal en temas relacionados a seguridad de la información.

1.4.1 Estado actual de la Gestión del SGSI basados en el anexo A de la norma ISO 27001:2013.

Poder identificar en que se está fallando, es uno de los principales factores para la implementación de un programa de la Gestion de Seguridad de la Información exitoso. El estado actual de la cooperativa de ahorro y crédito "COOPELQUINCHE", se evalúa basado en los 14 dominios de la norma ISO 27001:2013 que comprende 35 objetivo de control distribuidos en 114 controles.

Las métricas definidas para evaluar cada uno de los controles están basados en los niveles de capacidad COBIT 2019 adaptados a la realidad de la organización; estas se detallan a continuación:

Tabla 1 Métricas para evaluar el SGSI

Estado	Significado
No aplicable	No evaluado, de acuerdo con el rol de la institución.
Inexistente	No se dispone de ningún componente en el control, no se tiene evidencia de implementación.
Incompleto	No existe un proceso formal para realizarlas, se maneja de manera muy artesanal, no se disponen de apoyo tecnológico y de efectuá eventualmente.
Básico	No se dispone de documentación formal, sin embargo, se realiza actividades al respecto.
Intermedio	Se dispone de procedimientos formales documentados y aprobados, las actividades se realizan en base a los dispuestos en los procedimientos
Administrado	Se basa en mejores prácticas y normas de las SEPS, además utiliza herramientas tecnológicas que permites monitorear y generar una base de conocimiento.
Optimizado	Se ha convertido en un referente dentro del área de conocimiento, y se garantiza su cumplimiento

La evaluación se lo lleva a cabo con ayuda de una matriz elaborada en Microsoft Excel donde se dispone de los 114 objetivos, con los controles que debe cumplir cada uno de estos, además se dispone de una columna llamada *"Estado"* en la cual se pondera según las métricas establecidas, por otro lado, se emite un plan de acción por cada uno de los dominios. El anexo completo se encuentra disponible en medio digital.

APLICACIÓN DE LOS CONTROLES DE SEGURIDAD DE LA INFORMACION PARA LA COOPERATIVA DE AHORRO Y CREDITO "COOPELQUINCHE"

Dominio	Categoría	Descripción	Controles de Seguridad de la Información	Estado	Control	Código_Plan de Acción	Plan_de_Acción
A5 Políticas de seguridad de la información	A5.1 Directrices de gestión de la seguridad de la información	Proporcionar orientación y apoyo a la gestión de seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normas pertinentes.	A5.1.1 Conjunto de políticas para la seguridad de la información	Incompleto	Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.	PA1	Definir y establecer políticas que permitan asegurar la información existente en la institución financiera, basado en integridad, disponibilidad y confidencialidad, así dejar por un lado la revisión y actualización periódica.
			A5.1.2 Revisión de las políticas para la seguridad de la información	Incompleto	Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.		
A6 Organización de la seguridad de la información	A6.1 Organización interna	Establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.	A6.1.1 Asignación de responsabilidades para la SI (Roles y responsabilidades en seguridad de la información)	Incompleto	Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas.	PA2	Establecer instructivos de puesto, para el personal del área de Tecnología, de tal manera que se maneje diferencia con el personal de Gestión de Accesos.
			A6.1.2 Segregación de tareas	Básico	Las funciones y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o uso indebido de los activos de la organización.		
			A6.1.3 Contacto con las autoridades	Intermedio	Deben mantenerse los contactos apropiados con las autoridades pertinentes.		
			A6.1.4 Contacto con grupos de interés especial	Intermedio	Deben mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad.		
			A6.1.5 Seguridad de la información en la gestión de proyectos	No aplicable	La seguridad de la información debe tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.		
	A6.2 Los dispositivos móviles y el teletrabajo	Garantizar la seguridad en el teletrabajo y en el uso de dispositivos móviles.	A6.2.1 Política de dispositivos móviles	No aplicable	Se debe adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.		
			A6.2.2 Teletrabajo	No aplicable	Se debe implementar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.		

Figura 2 Matriz de evaluación

Resultado del examen realizado a la cooperativa de ahorro y crédito "COOPELQUINCHE" se identifica que de un total de 114 controles 18 de estos no aplican evaluación, para los restantes: 30 inexistentes, 33 incompleto, 22 básico, 10 intermedio, 1 Administrado y ninguno es optimizado.

Tabla 2 Situación Actual

Estado	# Objetivos	Situación Actual
No aplicable	18	**16%**
Inexistente	30	26%
|Incompleto	33	29%
Básico	22	19%
Intermedio	10	9%
Administrado	1	1%
Optimizado	0	0%
Total	114	100%

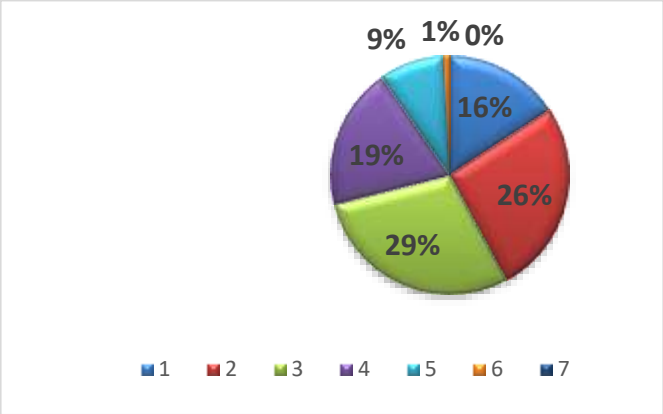

Figura 3 Situación Actual

1.5 Clasificación de los tipos de Información

La información se ha convertido en uno de los principales activos para la cooperativa de ahorro y crédito por lo cual se ve la necesidad de identificar los tipos de información existentes y sobre la cual gira el negocio. Identificar los tipos de información permitirá conocer los activos de información, así como realizar un análisis de riesgos adecuado enfocado principalmente en los activos críticos.

Es importante mencionar que la clasificación de los tipos al igual que las otras etapas que comprenden el análisis de riesgos, es un proceso que se lo debe llevar a cabo de manera constante.

La identificación de las entidades, así como la clasificación de los tipos de información se realiza con la siguiente escala de impacto:

Tabla 3 Escala de Impacto

IMPACTO				
Valor Cuantitativo	**Valor Cualitativo**	**Pérdidas Financieras**	**Interrupción de operaciones parciales y/o totales**	**Multas y Sanciones de los Organismos de Control**
5	Catastrófico	Mayores al 30% del ingreso neto		Mayor a 3 sanciones al año
4	Mayor	Mayores al 15% y menores al 30% del ingreso neto	Mayor a 8 horas y menor a 12 horas.	Mayor a 2 sanciones al año
3	Moderado	Mayores al 8% y menores al 15% del ingreso neto	Mayor a 3 horas y menor a 8 horas	Mayor a 1 sanciones al año
2	Menor	Perdidas mayores al 3% y menores al 8% del ingreso neto	Mayor a 1 horas y menor a 3 horas	
1	Insignificante	Perdidas menores al 3% del ingreso neto	Menor a 1 horas	

Además, utilizaremos un mapa de calor relacionado con la triada CID (confidencialidad, disponibilidad e integridad) en la cual, a más de la escala de impacto, utilizaremos la escala de probabilidad:

Tabla 4 Escala de probabilidad

PROBABILIDAD		
Valor Cuantitativo	**Valor Cualitativo**	**Descripción**
1	Raro	Una vez al año
2	Poco probable	Dos veces al año
3	Posible	Cuatro veces al año
4	Probable	Una vez cada mes
5	Casi Certeza	Dos o más veces cada mes

Tabla 5 Mapa de calor para evaluar los factores CID

MAPA DE CALIFICACIÓN DE SEVERIDAD						
Probabilidad	Raro	BAJO	BAJO	BAJO	MODERADO	ALTO
	Poco probable	BAJO	BAJO	MODERADO	ALTO	ALTO
	Posible	BAJO	MODERADO	MODERADO	ALTO	CRITICO
	Probable	MODERADO	MODERADO	ALTO	CRITICO	CRITICO
	Casi Certeza	MODERADO	ALTO	ALTO	CRITICO	CRITICO
		Insignificante	Menor	Moderado	Mayor	Catastrófico
		Impacto				

Resultado de la evaluación de las identidades y la clasificación de los tipos de información se observa que la información financiera tiene una calificación **"CRITICIDAD = SI"**, por lo que esta será considerada para nuestro estudio en las siguientes fases. El anexo completo se encuentra disponible en medio digital.

Nro.	Entidad	Tipo de Información	Evaluación Impacto Intregridad	Evaluación Impacto Confidencialidad	Evaluación Impacto Disponibilidad	CRITICIDAD
1	Clientes	Personal	MODERADO	BAJO	ALTO	NO
2		Contacto	MODERADO	MODERADO	ALTO	SI
3		Financiera	ALTO	ALTO	ALTO	SI
4		Legal	MODERADO	MODERADO	MODERADO	SI
5	Empleados	Personal	MODERADO	MODERADO	BAJO	NO
6		Financiera	MODERADO	MODERADO	MODERADO	SI
7	Proveedores	Contacto	MODERADO	BAJO	BAJO	NO
8		Legal	MODERADO	BAJO	MODERADO	NO
9		Financiera	MODERADO	MODERADO	ALTO	SI
10	Organización	Contratos	MODERADO	MODERADO	MODERADO	SI

Figura 4 Tipos de información críticos

1.6 Activos de Información críticos identificados y clasificados

Los activos de información críticos dentro de las instituciones se han convertido en un pilar fundamental para el análisis de riesgos tecnológicos, es así como en mucho apartado se los ha catalogado como las “joyas de la corona”.

La norma ISO27001:2013 menciona que un activo de información es un bien que la organización valora y por esta razón se debe proteger, minimizando sus vulnerabilidades y debilidades. (Estupiñan, Pulido, & Jaime, 2013)

Una vez que en la primera etapa se identificado los tipos de información críticos, se procede a identificar donde se genera, trasmite o reposa la información, de tal manera se pueda identificar los activos de información.

En base a la criticidad de los tipos de información nos enfocamos en calificar los activos para identificar el activo de información más crítico que será evaluado en la siguiente fase. El anexo de la evaluación realizada se adjunta en medio digital.

Activo	Nombre Activo	Formato de Información	Tipo de Información	Propietario	Criticidad Entidad	Aux	Criticidad del Activo
1	Servidor Aplicativo y Base de Datos	Digital	Personal de Cliente	Gerente Financiero	NO	3	CRITICO
			Contacto de Cliente	Gerente Financiero	SI		
			Financiera de Cliente	Gerente Financiero	SI		
			Legal de Cliente	Asesor Legal	SI		
2	Base de datos Sistema RR.HH.	Digital	Personal de empleado	Gerente	NO	1	CRITICO
			Financiera de empleado	Gerente	SI		
3	Carpeta Compartida FTP	Digital	Personal de Proveedor	Gerente Financiero	NO	1	CRITICO
			Legal de Proveedor	Asesor Legal	NO		
			Financiera de Proveedor	Gerente Financiero	SI		
4	Bóveda	Físico	Legal de Cliente	Gerente Financiero	SI	1	CRITICO
5	Archivadores	Físico	Personal de Cliente	Gerente Financiero	NO	2	CRITICO
			Financiera de Cliente	Gerente Financiero	SI		
			Contrados, SLAs de Servicios	Asesor Legal	SI		

Figura 5 Identificación de activos críticos

Resultado de nuestro análisis el servidor de aplicación es el más crítico, además se identifica que este servidor reposa la aplicación y la base de datos de sistema financiero.

1.7 Análisis de amenazas y vulnerabilidades de activos de información críticos

El análisis de amenazas y vulnerabilidades es una etapa crucial para poder identificar los riesgos asociados a los activos de información.

Una vez identificad el activo de información más crítico que será motivo de nuestro estudio, se elaborá una matriz basada en la metodología de MARGERIT-version_3.0 rescatando las taxonomías, salvaguardas y amenazas con el fin de identificar las vulnerabilidades asociadas al activo de información “Base de datos Sistema Core”. Para determinar la severidad de la amenaza utilizamos los factores de la Tabla 3.

Nombre Tipo de Información	Descripción Tipo de Información	Activo de Información	Tipo de Activo	Clasificación Activo	Custodio Activo	Proceso(s)	Componente	Salvaguardas Esperadas	Amenazas
Información Financiera del Cliente	La información aquí almacena hace referencias, a las cuentas de ahorros, prestamos, depositos y retiros.	**Base de datos Sistema Core**	Base de Datos	Crítico	Gerente Sistemas	Captaciones y colocaciones de efectivo	Base de Datos	H.IA Identificación y autenticación H.AC Control de acceso lógico H.ST Segregación de tareas H.IR Gestión de incidencias H.AU Registro y auditoría SW.A Copias de seguridad (backup) PS.AT Formación y concienciación BC.BIA Análisis de impacto (BIA) D.C. Cifrado de la información BC.DRP Plan de Recuperación de Desastres (DRP)	[A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado [A.15] Modificación deliberada de la información [E.19] Fugas de información E.2 Errores del administrador [E.18] Destrucción de información [I.5] Avería de origen físico o lógico [A.3] Manipulación de los registros de actividad (log) [E.24] Caída del sistema por agotamiento de recursos [A.24] Denegación de servicio

Figura 6 Salvaguardas asociadas

Amenazas	Posibles Vulnerabilidades	Impacto	IMPACTO	PROBABILIDAD	SEVERIDAD
[A.6] Abuso de privilegios de acceso	- Contraseñas predeterminadas no modificadas. - Asignación de privilegios inadecuada. - Falta de análisis de perfiles por cargo. - Auditoria no activas en el la base de datos.	Perdidas Financiera Multas y Sanciones de los Organismos de Control	MAYOR	POCO PROBABLE	ALTO
[A.11] Acceso no autorizado	Inadecuada segregación de funciones.	Perdidas Financiera	MODERADO	POCO PROBABLE	MODERADO
[A.15] Modificación deliberada de la información	- Falta de formación y conciencia sobre seguridad. - Falta validación de los datos procesados. - Falta controles adecuados para afectaciones directas.	Perdidas Financiera Multas y Sanciones de los Organismos de Control	CATASTRÓFICO	PROBABLE	CRÍTICO
[E.19] Fugas de información	- Falta de formación y conciencia sobre seguridad. - Información sensible (cuentas, saldos, id) en texto claro. - Asignacion incorrecta de roles y permisos.	Multas y Sanciones de los Organismos de Control	MODERADO	PROBABLE	ALTO
E.2 Errores del administrador	- Mantenimiento inadecuado. - Respaldo de configuraciones aplicadas.	Perdidas Financiera Interrupción de operaciones parciales y/o totales	MAYOR	POSIBLE	MODERADO
[E.18] Destrucción de información	- Falta de redundancia de servidores. - Copia única de información.	Perdidas Financiera Interrupción de operaciones parciales y/o totales Multas y Sanciones de los Organismos de Control	CATASTRÓFICO	POSIBLE	CRÍTICO
[I.5] Avería de origen físico o lógico	- Sensibilidad del equipo a los cambios de voltaje. - Sensibilidad del equipo a la humedad, temperatura o contaminantes.	Interrupción de operaciones parciales y/o totales	MODERADO	POSIBLE	MODERADO
[A.3] Manipulación de los registros de actividad (log)	- Exposición del log propio del motor de base de datos. - Falta de control sobre los datos de entrada y salida.	Interrupción de operaciones parciales y/o totales Multas y Sanciones de los Organismos de Control	CATASTRÓFICO	POSIBLE	CRÍTICO
[E.24] Caída del sistema por agotamiento de recursos	- Inadecuada gestión de capacidad del sistema. - Falta de indicadores o reportes de rendimiento.	Perdidas Financiera Interrupción de operaciones parciales y/o totales	MAYOR	PROBABLE	ALTO
[A.24] Denegación de servicio	- Inexistencias de proceso de parchado. - Inadecuada gestión de red. - Equipos con firmware desactualizado	Perdidas Financiera Interrupción de operaciones parciales y/o totales Multas y Sanciones de los Organismos de Control	MAYOR	RARO	MODERADO

Figura 7 Amenazas y vulnerabilidades

Resultado del análisis realizado se pude observar que [A.6] Abuso de privilegios de acceso, [E.19] Fugas de información y [E.24] Caída del sistema por agotamiento de recursos son las amenazas que preocupan y serán analizadas en la siguiente etapa. (MAGERIT, 2012).

1.8 Evaluación de riesgos

La evaluación del riesgo tecnológico es una de las actividades más relevantes que acompañan al programa del sistema de gestión de seguridad de la información, ya que de este depende los planes de acción que se deben ejecutar de manera priorizada.

El Riesgo Tecnológico se define como la probabilidad de sufrir daños o pérdidas económicas, ambientales y humanas como consecuencia del funcionamiento deficiente o accidente de una tecnología aplicada en una actividad humana. (Bosque Sendra, y otros, 2004).

Debido al cambio constante de los procesos y la tecnología que los apalancan el análisis de riesgo debe cumplir con una metodología que permita ejecutar de manera constante este análisis. En esta etapa se parte de las amenazas

existente y para este caso partiremos de las amenazas criticas identificadas anteriormente.

Activo	Riesgo	Objetivos del Control	Controles	Tipo de Control	Control Clasificacion	Frecuencia del Control	Fortaleza de Control
Base de datos Sistema Core	[A.6] Abuso de privilegios de acceso	Mitigar posibles perdidas financieras. Mitigar posibles sanciones de entidades reguladoras	- Establecer un proceso adecuado de acceso lógico. - Identificar transacciones inusuales en la base de datos. - Activar los logs de auditoria en la base de datos.	Manual/ Automático	Preventivo/ Detectivo	Mensual	Alto
	[A.15] Modificación deliberada de la información	Mitigar posibles perdidas financieras Mitigar posibles sanciones de entidades reguladoras	- Identificar si las actividades realizadas sobre la base de datos cuentan con un control de cambios aprobado. - Validación y aprobación para modificación de los datos.	Manual	Preventivo Detectivo	Mensual	Alto
	[E.19] Fugas de información	Mitigar posibles sanciones de entidades reguladoras	- Concientización sobre temas relacionados con seguridad de la información y ciberseguridad. - Ofrustramiento de datos sensibles. - Establecer un proceso adecuado de acceso lógico.	Manual /Automático	Preventivo	Mensual	Alto
	[E.18] Destrucción de información	Mitigar las interrupciones parciales o totales por fallas en el aplicativo Mitigar posibles perdidas financieras Mitigar posibles sanciones de entidades reguladoras	- Identificar si las copias de seguridad se efectúan sin errores. - Validar la existencia de replicas o redundancia de la base de datos.	Automático	Preventivo Detectivo	Mensual	Alto
	[A.3] Manipulación de los registros de actividad (log)	Mitigar las interrupciones parciales o totales por fallas en el aplicativo Mitigar posibles sanciones de entidades reguladoras	- Identificar las seguridades establecidas en los repositorios del log. - Verificar la integridad de los logs del motos de base de datos.	Manual	Preventivo Detectivo	Mensual	Alto
	[E.24] Caida del sistema por agotamiento de recursos	Mitigar posibles perdidas financieras Mitigar las interrupciones parciales o totales por fallas en el aplicativo	- Existencia de reportes de monitore del rendimiento en para el servidor y base de datos. - Verificar si el centro de computo cuenta con las adecuaciones razonables para su correcto funcionamiento.	Automático /Manual	Preventivo Detectivo	Mensual	Alto

Figura 8 Análisis de Riesgos

Activo	Riesgo	Objetivo	Codificación	Políticas de Alto Nivel	Calificacion
Base de datos Sistema Core	Abuso de privilegios de acceso	Garantizar que la asignación de privilegios de acceso en la base de datos este de acorde a las funciones que los usuarios.	A.6.1	Establecer un proceso adecuado de acceso lógico.	Alto
			A.6.2	Identificar transacciones inusuales en la base de datos.	Alto
			A.6.3	Activar los logs de auditoria en la base de datos.	Alto
	Modificación deliberada de la información	Garantizar que información almacenada en las tablas no sean alteradas	A.15.1	Identificar si las actividades realizadas sobre la base de datos cuentan con un control de cambios aprobado.	Alto
			A.15.2	Validación y aprobación para modificación de los datos.	Alto
	Fugas de información	Garantizar que el acceso a información que reposa en la base de datos, este debidamente protegida y restringida para los usuarios no autorizados.	E.19.1	Concientización sobre temas relacionados con seguridad de la información y ciberseguridad.	Alto
			E.19.2	Ofrustramiento de datos sensibles.	Alto
			E.19.3	Establecer un proceso adecuado de acceso lógico.	Alto
	Destrucción de información	Establecer mejoras que garanticen la disponibilidad de la información en caso de suscitarse averías en los disco o cintas magnéticas donde reposa la información.	E.18.1	Identificar si las copias de seguridad se efectúan sin errores.	Alto
			E.18.2	Validar la existencia de replicas o redundancia de la base de datos.	Alto
	Manipulación de los registros de actividad (log)	Garantizar que la información generada y almacena por los logs del motor de base de datos, este debidamente custodiada y restringida ante modificaciones.	A.3.1	Identificar las seguridades establecidas en los repositorios del log.	Alto
			A.3.2	Verificar la integridad de los logs del motos de base de datos.	Alto
	Caida del sistema por agotamiento de recursos	Garantizar el correcto funcionamiento y rendimientos de la base de datos. (RAM, DISCO y CPU)	E.24.1	Existencia de reportes de monitore del rendimiento en para el servidor y base de datos.	Alto
			E.24.2	Verificar si el centro de computo cuenta con adecuaciones físicas y lógicas razonables para su correcto funcionamiento.	Alto

Figura 9 Políticas de Alto Nivel

1.9 Modelo Operacional del SGSI

El alcance del proyecto de investigación realizado no contempla la fase de implementación debido a la complejidad y tiempo que tomaría realizar esta, sin embargo, ante la importación de establecer un modelo operacional en la implantación y mantenimiento del sistema de gestión de seguridad de la

información en la “COOPELQUNCHE” se plantea seguir las siguientes fases propuestas.

Basado en la aplicación de ciclo de Deming, se ajusta las fases establecidas de acuerdo con la realizada de la institución.

1. **Diagnosticar:** conocer la situación actual.
2. **Planificar:** Bosquejo de la solución, objetivos y vulnerabilidades que serán resueltas.
3. **Hacer:** Establecer los controles planeados.
4. **Verificar:** Comparar los resultados obtenidos con los objetivos definidos.
5. **Actuar:** Reajustar y establecer acciones correctivas.

Figura 10 Fases de Implementación

1.10 Roadmap de Planes de Acción

El programa de sistema de gestión de seguridad de la información nos permite identificar las debilidades existentes en la cooperativa de ahorro y crédito “COOPELQUINCHE”. Los resultados obtenidos se presentan en una reunión con el Gerente General, Gerente de sistemas y el Analista de Riesgo, quienes ven la importancia de contar con un SGSI ajustado a las necesidades de la institución.

La importancia de contar con una hoja de ruta donde se muestren los planes de acción a realizar, con los responsables y el tiempo en el cual se van ejecutar es no permite estar listo para la implantación del Sistema de Gestion de Seguridad de la Información que si bien esta etapa no está dentro del alcance del proyecto, se ve la necesidad de estar listos para la implementación.

Se elabora una matriz en la cual se define el plan de acción, responsable, dificultad del plan de acción, tiempo de implementación y el estado; este último nos permitirá realizar un el seguimiento.

					Año divido en trimestres					
Dominio	Categoría	Código_Plan de Acción	Plan_de_Acción	Responsable	3 Trim. 2021	1 Trim. 2022	2 Trim. 2022	3 Trim. 2022	4 Trim. 2022	Estado
A5 Políticas de seguridad de la información	A5.1 Directrices de gestión de la seguridad de la información	PA5	Definir y establecer políticas que permitan asegurar la información existente en la institución financiera, basado en integridad, disponibilidad y confidencialidad; sin dejar por un lado la revisión y actualización periódica.	Oficial de Riesgos	✓					No implementado
A6 Organización de la seguridad de la información	A6.1 Organización interna	PA6	Establecer instructivos de puesto, para el personal del área de Tecnología, de tal manera que se marque diferencia con el personal de Gestión de Accesos.	Recursos Humanos Gerente General		✓				No implementado
	A6.2 Los dispositivos móviles y el teletrabajo									
A7 Seguridad relativa a los recursos humanos	A7.1 Antes del empleo	PA 7	Fortalecer el proceso de capacitación a los colaboradores en temas relacionados con seguridad de la información y ciberdelincuencia.	Recursos Humanos Gerente General		✓				No implementado
	A7.2 Durante el empleo									
	A7.3 Finalización del empleo o cambio en el puesto de trabajo									
A8 Gestión de activos	A8.1 Responsabilidad sobre los activos	PA8	Levantar y analizar los activos de información, de tal manera que permita clasificarlos y definir los propietarios.	Oficial de Riesgos, Gerente de Tecnología				✓		No implementado
	A8.2 Clasificación de la información									
	A8.3 Manipulación de los soportes									
A9 Control de acceso	A9.1 Requisitos de negocio para el control de acceso	PA9	Capacitar al personal de la institución en temas relacionados al manejo y competición de credenciales de acceso.	Recursos Humanos Gerente General		✓				No implementado
	A9.2 Gestión de acceso de usuario									
	A9.3 Responsabilidades del usuario									
	A9.4 Control de acceso a sistemas y aplicaciones									
A10 Criptografía	A10.1 Controles criptográficos	PA10	Establecer procesos de resguardamiento de la información sensible.	Gerente de Tecnología				✓		No implementado

Figura 11 Planes de Acción

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- El estado actual del SGSI de la “COOPELQUINCHE” nos permite identificar que se encuentra en estado inicial e inexistente, hay muy pocos controles que se están trabajando por lo que se presentan algunas oportunidades de mejora.

- La evaluación realizada permite contar con un documento donde se muestren los tipos y activos de información críticos presentes en la institución.

- La triada CID nos permite clasificar de mejor manera a los activos de la información, basados en la confidencialidad, integridad y disponibilidad.

- Promover el uso de marcos de referencia relacionados con seguridad de la información, en la institución permite fortalecer y engrandecer los conocimientos del personal de la institución.

- El cambio de cultura en la institución fue favorable, ya que realizar este ejercicio abre la mente de todo el personal y principalmente de los mandos jerárquicos.

Recomendaciones

- Se recomienda el uso de la norma ISO 27001 de para realizar un análisis de los diferentes controles que deberían evaluados en todas las instituciones y mucho más en las financieras.

- Se sugiere la utilización de metodologías como MAGERIT para el análisis de riesgo enfocados a los activos de información.

- Se recomiendan fortalecer las capacitaciones en todo el personal de la institución en los temas referentes a seguridad de la información y ciberseguridad.

REFERENCIAS

Ambit BST. (14 de 05 de 2021). *¿Para qué sirve un SGSI? Controles y fases*. Obtenido de Ambit BST: https://www.ambit-bst.com/blog/para-qu%C3%A9-sirve-un-sgsi-controles-y-fases

Bosque Sendra, J., Díaz Castillo, C., Díaz Muñoz, M., Gómez Delgado, M., Gónzalez Ferreiro, D., Rodríguez Espinosa, V., & Salado García, M. (2004). Propuesta metodológica para caracterizas las áreas expuestas a riesgos tecnológicos mediante SIG. Aplicación en la Comunidad de Madrid. *www.geo-focus.org*.

ISACA. (2018). Estructura de objetivos de gobierno y gestión de COBIT. En *Marco de Referencia. Introducción y metodología.* (pág. 20). Obtenido de https://issuu.com/: https://issuu.com/sistemas_epuentes/docs/cobit-2019-framework-introduction-and-methodology_/s/10674167

ISOTools Excellence. (2021). *¿Qué es la ISO 27001?* Obtenido de ISOTools Excellence: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Estupiñan, A. d., Pulido, J. A., & Jaime, J. A. (2013). Análisis de riesgos en seguridad de la información. En Ciencia, Innovación Y Tecnología (págs.40-53).

Magerit (2012). Magerit-versión 3.0 Metodología de Análisis Y gestión de Riesgos de los Sistemas de Información, Libro 2-Catalogo de elementos.

ANEXOS

Ejemplo de encuestas realizadas

Anexos digitales

Estado actual del SGSI basados en el anexo A de la norma ISO 27001:2013.

FAules - Herramienta Medir Estado SGSI.xls

Clasificación de los tipos de Información

FAules - Clasificación Tipos de Información.

Activos de Información críticos identificados y clasificados

FAules - Activos de Información.xlsx

Análisis de amenazas y vulnerabilidades de activos de información críticos.

FAules - Amenazas y Vulnerabilidades.xlsx

Evaluación de riesgos

FAules - Analisis de Riesgos.xlsx

Políticas de Alto nivel

FAules - Políticas de Alto Nivel.xlsx