FACULTAD DE GERENCIA DE SEGURIDAD DE LA INFORMACIÓN

DESARROLLO DEL PROGRAMA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE UNA COOPERATIVA DE AHORRO Y CRÉDITO

Luis Ernesto Farinango Pabón
Edison Patricio Negrete Ricci

2022

FACULTAD DE GERENCIA DE SEGURIDAD DE LA INFORMACIÓN

PROYECTO CAPSTONE: DESARROLLO DEL PROGRAMA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE UNA COOPERATIVA DE AHORRO Y CRÉDITO

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

Luis Ernesto Farinango Pabón
Edison Patricio Negrete Ricci

2022

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaramos que este trabajo es original, de nuestra autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

Edison Patricio Negrete Ricci
1711688901

Luis Ernesto Farinango Pabón
1002525754

Resumen

Este proyecto de Desarrollo del programa del Sistema de Gestión de Seguridad de la Información describe los pasos para estructurar las iniciativas del sistema de gestión de seguridad de la información (SGSI) de una Cooperativa de Ahorro y Crédito (COAC). Se inicia con una matriz de diagnóstico que permite establecer el nivel de madurez del COAC con base en la ISO27002, identificando un puntaje global que permite determinar los dominios del estándar donde la COAC es más débil. Luego, a través de un levantamiento de información, se identifican y clasifican varios activos con información sensible, seleccionando dos activos que; por la importancia de la información, se toman para un análisis de riesgo; determinando para cada activo, las amenazas y vulnerabilidades a las que pueden estar expuestos, utilizando un marco de referencia MAGERIT. Cada una de las amenazas identificadas se han ubicado en términos de riesgos; evaluando la probabilidad e impacto de estos ante una materialización (riesgo inherente).

Para entender el nivel de riesgo residual se han identificado los controles vigentes, los cuales han sido calificados en función de su solidez con respecto a la mitigación que brindan (riesgo residual). Con base en los riesgos residuales, se determinó un valor de riesgo objetivo (apetito definido por la COAC) para aquellos riesgos críticos y se establecieron los planes de acción a implementar para alcanzar el riesgo objetivo propuesto.

La lista de planes de acción, priorizados por esfuerzo y nivel de contribución, constituyen el primer alcance del plan operativo que será la base de la declaración de aplicabilidad del SGSI, el cual ha sido dimensionado en términos de recursos y esfuerzo para un adecuado seguimiento. Finalmente, el documento muestra los detalles de todo el proceso realizado, y que puede ser replicado a los demás activos de información, para mitigar gradualmente el nivel de riesgo institucional a valores aceptables por el COAC. El resultado del diagnóstico mostró que la COAC tiene un bajo nivel de cumplimiento de la norma ISO27002, y mantiene dos activos altamente sensibles, entre ellos la base de datos. Los primeros planes establecidos para el SGSI proporcionarán un importante nivel de mejora en el corto plazo.

Abstract

This Information Security Management System Program Development project describes the steps to structure the initiatives of the information security management system (ISMS) of a Savings and Credit Cooperative (COAC). It begins with a diagnostic matrix that allows establishing the level of maturity of the COAC based on ISO27002, identifying a global score that allows determining the domains of the standard where the COAC is weakest. Then, through an information survey, several sensitive information assets are identified and classified, selecting two assets that; Due to the importance of the information, they are taken for a risk analysis; determining for each asset, the threats, and vulnerabilities to which they may be exposed, using a MAGERIT reference framework. Each of the threats identified have been placed in terms of risks, evaluating the probability and impact of these before a materialization (inherent risk).

To understand the level of residual risk, current controls have been identified, which have been rated in terms of their robustness with respect to the mitigation they provide (residual risk). Based on the residual risks, an objective risk value (appetite defined by the COAC) was determined for those critical risks, and action plans were established to be implemented to reach the proposed objective risk.

The list of action plans, prioritized by effort and level of contribution, constitute the first scope of the operational plan that will be the basis of the declaration of applicability of the ISMS, which has been dimensioned in terms of resources and effort for adequate follow-up. Finally, the document shows the details of the entire process carried out, and that it can be replicated to the other information assets, to gradually mitigate the level of institutional risk to values acceptable by the COAC. The result of the diagnosis showed that the COAC has a low level of compliance with the ISO27002 standard, and keeps two extremely sensitive assets, including the database. The first plans established for the ISMS will provide a significant level of improvement in the short term.

INDICE DEL CONTENIDO

1 Introducción

La Cooperativa de Ahorro y Crédito (en adelante COAC), es una entidad financiera con una amplia trayectoria de vida institucional en prestación de servicios de intermediación financiera, garantizando la seguridad de los recursos de socios, clientes y funcionarios, sin embargo, las organizaciones y sus sistemas están expuestos a un gran número de amenazas, que pueden comprometer la confidencialidad, integridad y disponibilidad de la información. Se trata de los tres pilares básicos de la seguridad de la información y sin los cuales no existe nada seguro, ya que la información es un activo muy importante para la empresa. Actualmente, el índice de ataques a instituciones financieras se ha incrementado considerablemente; el costo de una brecha financiera es en promedio de 3.86 Millones según el Ponemon Institute. Igualmente, según Kaspersky, los ataques en Ecuador se incrementaron en un 75% en el 2021.

Con la finalidad de proteger adecuadamente la información, es necesario implementar un Sistema de Gestión de Seguridad de la información (en adelante SGSI) que, en su primera etapa, permite realizar un diagnóstico actual de los procesos relacionados con la seguridad de la información, para mejorar su gestión a través de la identificación de amenazas, vulnerabilidades y controles. Para iniciar el diagnóstico del SGSI, el enfoque iniciar consiste en realizar un diagnóstico utilizando un marco de referencia internacional, utilizando la familia ISO 27000, así como también en la ley orgánica de protección de datos personales (en adelante LOPDP) emitido por el organismo de control, lo que apoyará para la aplicación de buenas prácticas, así como también la identificación de posibles controles o iniciativas en los ámbitos de tecnología, procesos y personas para proteger la confidencialidad, disponibilidad e integridad de la información. Finalmente nos facilitará establecer un horizonte claro de ejecución de iniciativas de seguridad que permitan enfocar adecuadamente los esfuerzos e inversiones necesarias para la gestión del sistema.

2 Objetivo General del Proyecto

Desarrollar un programa de Sistema de Gestión de Seguridad de la Información (SGSI) mediante el cumplimiento normativo y alineando a los objetivos

estratégicos de la cooperativa para disminuir riesgos asociados a los activos de información.

3 Objetivos Específicos

- Realizar el análisis situacional actual utilizando una metodología de evaluación para determinar las vulnerabilidades en los activos de información.
- Trazar una línea de partida en la gestión de Seguridad de la Información.
- Cumplir con las regulaciones de las normativas actuales.
- Contar con un Sistema de Gestión de Seguridad de la Información definida.

4 Alcance

Conservando el análisis situacional de la COAC, se define el alcance del Programa del Sistema de Gestión de Seguridad de la información en varias fases:

- Fase 1: Diagnóstico se hace una revisión del estado actual de los controles de seguridad en la entidad.
- Fase 2: Clasificación de la Información se hace un listado general de información para determinar qué tipo de información tengo y que nivel de sensibilidad.
- Fase 3: Inventario de Activos de Información se evalúa que activo se requiere un tratamiento especial.
- Fase 4: Análisis de amenazas y vulnerabilidades de activos de información críticos.
- Fase 5: Documentos clave de SGSI, se apoya de políticas de Seguridad de la información.

5 Fase 1

5.1 Diagnóstico

La cooperativa en los últimos años se ha enfocado con gran dedicación en proteger las diversas capas de infraestructura (perimetral, red interna, bases de datos, aplicaciones, etc.) pero no se ha hecho lo mismo con la capa interna donde precisamente existen las amenazas más importantes y de mayor impacto.

En estas capas se encuentran los usuarios internos, exponiendo a la organización a fuga y divulgación no autorizada de la información sensible, sin embargo, la prioridad se ha enfocado más en proteger los activos externos porque estos representan un mayor volumen y sus ataques tienen de mayor impacto.

Una de las oportunidades de mejora, es fortalecer el compromiso con la cultura de seguridad organizacional, mejorar el conocimiento en temas de protección de activos y establecer un modelo de gobierno para la gestión de la seguridad de la información.

Esto es importante porque los ciberataques en Latinoamérica crecen a una tasa de 24% anual y se enfocan de manera importante en instituciones financieras, por lo que asignar los recursos financieros necesarios en los presupuestos para asegurar los objetivos del SGSI, es una decisión importante que deben afrontar las instituciones de este sector.

La Superintendencia de Economía Popular y Solidaria expidió una norma de control para la seguridad de la información con la finalidad de fortalecer los procesos internos y regular los niveles mínimos para la administración de seguridad de la información en las instituciones financieras. Con estos antecedentes entendiendo que la información es un activo generador de valor para las partes interesadas (stakeholders) de la COAC. se definió implementar un programa de Sistema Gestión de Seguridad de la Información – SGSI, esta implementación se apoya en un marco de referencia internacional ISO 27002-2013 que sirve de base para proveer directrices en la gestión de seguridad.

5.1.1 Metodología

Se ha desarrollado un formato de evaluación con el propósito de evidenciar el estado de situación inicial de los controles de seguridad implementados dentro de la institución, lo que permitirá establecer una hoja de ruta de partida.

A través de este formato, se puede identificar el nivel de madurez actual de la COAC, respecto de los objetivos y los dominios que norma la ISO 27002. La valoración de dominios y controles se realizó considerando varios aspectos que suman un total de 100 puntos base, distribuidos de la siguiente manera:

- Madurez de los procesos: 50%

- Madurez de las políticas: 20%
- Madurez del control: 20%
- Nivel de automatización del control o la practica: 10%

Cada uno de los niveles, tiene un valor de puntuación, dependiendo del estado actual de la práctica, para finalmente otorgar una puntuación por cada práctica del dominio. Cada una de las tablas que se muestran a continuación, detallan los valores y su descripción:

Tabla 1
Madurez en el estado del proceso

Procesos y procedimientos	Puntaje	Descripción
Ninguno	0 %	No se ejecuta esta práctica en la organización.
Informal	20 %	Esta práctica se ejecuta en la organización de manera informal, no existe evidencia documentada.
Formalizado	30 %	Esta práctica, se encuentra documentada y formalizada en la organización, pero no ha sido presentada para aprobación en ningún comité.
Documentado y difundido	40 %	El documento ha sido presentado, y aprobado en Consejo de Administración, difundido a la organización.
Mejora continua	50 %	El proceso es maduro y se encuentra en evolución permanente.

Fuente: Elaboración de autores.

Tabla 2
Madurez en la definición de Políticas

Política	Puntaje	Explicación
Ninguno	0 %	No existe una política
Informal	5 %	Se ejecuta como una práctica común, pero no existe evidencia documentada.
Definido	10 %	Existe un documento informal, pero no ha sido difundido en la organización.
Auditado	15 %	El documento existe y ha sido formalizado, el auditor interno se encuentra revisando y probando su cumplimiento.
Incorporado	20 %	El documento está formalizado y difundido, se ajusta de manera anual.

Fuente: Elaboración de autores.

Tabla 3
Madurez del control

Estado	Puntaje	Explicación
Ninguna	0 %	No existe documentación
Informal	5 %	Se hace, pero no hay documentos, no hay registros.
Formal	10 %	Ya está documentada, se hace captura indicadores.
Métricas y reportes	15 %	Se mide los procesos y hay reporte. La situación de la implementación se presenta al comité.
Mejora continua	20 %	Son parte de la organización.

Fuente: Elaboración de autores.

Tabla 4
Nivel de automatización del control.

Automatización	Puntaje	Explicación
Ninguna	0 %	No existe
Parcial	5 %	Alguna parte esta automatizada y otra parte hace la persona.
Completa	10 %	Se encuentra automatizada.
No aplica	10 %	Hay casos que no aplica para automatizar.

Fuente: Elaboración de autores.

5.1.2 Resultados

Una vez realizado la evaluación respectiva de controles implementadas, se evidencia las falencias en algunos controles de seguridad a nivel de 14 dominios, 35 objetivos y 114 controles. El gráfico siguiente ilustra el estado actual de las prácticas de acuerdo con ISO 27002, comparadas con un valor objetivo que permita establecer un apetito adecuado al riesgo.

Gráfico 1. Nivel de madurez de la COAC

Se realiza una síntesis de los resultados que se detallan por cada dominio.

- Dominio 5: Políticas de Seguridad.

Tabla 5

DOMINIO EVALUADO	SCORE	OBJETIVO
Políticas de seguridad	80,00 %	80,00 %

Fuente: Elaboración de autores.

Análisis: Del diagnóstico realizado, cuenta con múltiples políticas escritas y difundidas en materia de Seguridad de la Información, lo que se refleja en la calificación de dominio más alta, siendo una fortaleza de línea base para la cultura de la seguridad, ya que el desarrollo de la seguridad se ha centrado de manera principal en identificar todas las necesidades básicas de Seguridad a nivel de políticas.

- Dominio 6: Organización de la seguridad de la información.

Tabla 6

DOMINIO EVALUADO	SCORE	OBJETIVO
Aspectos organizativos de la seguridad de la información	35,25 %	60,00 %

Fuente: Elaboración de autores.

Análisis: La COAC es una institución mediana, que hace apenas un par de años, ha tomado conciencia de la necesidad de implementar y fortalecer una estructura de Seguridad de la información conforme marcos de referencia internacionales y de acuerdo con la disponibilidad de recursos en el mercado. En este dominio, se encuentra en etapa inicial (apenas 35,25%) donde ha designado un responsable de seguridad de la información, quien está creando la primera versión del SGSI, sin contar por el momento con un equipo de apoyo en la función, sin existir tampoco segregación de funciones entre tecnología y la nueva área. Dentro de las expectativas organizacionales, existe la necesidad

de llevar a la empresa a nivel repetible, a través de una estructura que administre y monitoree los principales controles que sean definidos para Seguridad de la información.

- Dominio 7: Seguridad y Recursos humanos.

Tabla 7

DOMINIO EVALUADO	SCORE	OBJETIVO
Seguridad asociada a los recursos humanos	65,28 %	70,00 %

Fuente: Elaboración de autores.

Análisis: El área de Recursos Humanos ligada especialmente a la Seguridad se observa que falta un porcentaje mínimo para alcanzar el objetivo deseado en primera instancia, sin embargo se debería ir mejorando en las contrataciones y aplicar rigurosamente las verificaciones de antecedentes ya que ellos serán quienes tendrán accesos al consumo de las informaciones sensibles, entre otros, así como también hacer conocer desde un principio Responsabilidades y Obligaciones a la no divulgación de la información.

- Dominio 8: Gestión de activos de información.

Tabla 8

DOMINIO EVALUADO	SCORE	OBJETIVO
Gestión de activos	20,56 %	50,00 %

Fuente: Elaboración de autores.

Análisis: En la gestión de activos la COAC. tiene mucha debilidad, de llevar responsabilidades en los clasificados de los activos, inventario de estos, y la protección de la información. Esta debilidad podría ser atacada a la fuga de la información siendo un fraude interno del personal. Al contar con la gestión de activos permite entregar información de manera ordenada, organizada y controlar los accesos a los activos esenciales protegiendo en las tres

dimensiones de la triada de la Seguridad.

- Dominio 9: Control de accesos.

Tabla 9

DOMINIO EVALUADOS	SCORE	OBJETIVO
Control de accesos.	66,88 %	70,00 %

Fuente: Elaboración de autores.

Análisis: Aplica buenas prácticas de manera formal, sin embargo, se observa que existe personal con controles de accesos totales a las herramientas e informaciones del giro del negocio que son agregadores claves o de valor, se apega al objetivo trazado lo que permite mantener alertado al evidenciar asignaciones de cuentas privilegiados y/o super - usuario.

- Dominio 10: Cifrado de datos.

Tabla 10

DOMINIO EVALUADO	SCORE	OBJETIVO
Cifrado.	35,00 %	40,00 %

Fuente: Elaboración de autores.

Análisis: Aplica parcialmente los controles de seguridad en el portal de transferencia, lo que resalta la necesidad de aplicar controles criptográficos cuyo fin es alcanzar los distintos niveles de seguridad, confidencialidad, integridad y la disponibilidad, dando como resultado de maximizar beneficios y minimizar riesgos.

- Dominio 11: Seguridad física y ambiental.

Tabla 11

DOMINIO EVALUADO	SCORE	OBJETIVO

Seguridad física y ambiental.	64,72 %	70,00 %

Fuente: Elaboración de autores.

Análisis: Uno de los controles de seguridad que aplica, son las áreas seguras de los accesos a manipulación de equipos críticos, lo que ha demostrado un porcentaje alto como proteger físicamente (huella digital, sistema de alarmas), y se cuenta formalmente socializado acceso restringido, adicional se verifica controles en las salidas de los equipos que debe ir a la par con los controles debidamente documentado mediante bitácoras actualizadas de las responsabilidades y asegurados.

- Dominio 12: Seguridad en las operaciones.

Tabla 12

DOMINIO EVALUADO	SCORE	OBJETIVO
Seguridad en las operaciones.	50,25%	50,00 %

Fuente: Elaboración de autores.

Análisis: La gestión en seguridad operativa mantiene en nivel medio del objetivo deseado lo que se evidencia que aún existe concienciar en temas de seguridad de parte de los colaboradores sobre el tratamiento, respaldos, procedimiento de cambios, entre otros que afecte la operatividad de los procesos. De la misma manera se ha evidenciado iniciativas de buenas prácticas en algunos controles de gestión de cambios, y capacidades, en la separación de ambientes de prueba, desarrollo y operación; así como también de proveer de servidores de espejo para la continuidad de la disponibilidad.

- Dominio 13: Seguridad en las telecomunicaciones.

Tabla 13

DOMINIO EVALUADO	SCORE	OBJETIVO
Seguridad en las telecomunicaciones.	52,08 %	50,00 %

Fuente: Elaboración de autores.

Análisis: Cuenta segmentadas las redes en varias áreas con la finalidad de

aplicar controles de accesos indebidos o ataques a la red intranet lo que comprometería los recursos de la institución, sin embargo, se debe llevar un adecuado monitoreo para permitir la detección de eventos que podrían afectar para la seguridad de la información. Adicional se verifica que aplican un acuerdo de intercambio de información con todas las obligaciones y responsabilidades detallas en acuerdos de confidencialidad.

- Dominio 14: Adquisición, desarrollo y mantenimiento de los sistemas de información.

Tabla 14

DOMINIO EVALUADO	SCORE	OBJETIVO
Adquisición, desarrollo y mantenimiento de los sistemas de información	40,19 %	50,00 %

Fuente: Elaboración de autores.

Análisis: En la adquisición, desarrollo y mantenimiento de los sistemas de información, la COAC cumple con las buenas prácticas a base de procesos y procedimientos correctos, sin embargo, se verifica que esto puede ser o no aplicado evidenciando que se requiere un análisis minucioso de la necesidad para hacer la gestión adecuada, sean estos en la planificación, desarrollo, y entrega de servicio y funcionalidad, así como también llevar un control adecuado de registro de propiedad intelectual de las aplicaciones creadas y principios de reingeniería de software seguro.

- Dominio 15: Gestión de terceros / proveedores.

Tabla 15

DOMINIO EVALUADO	SCORE	OBJETIVO
Relaciones con proveedores.	46,67 %	50,00 %

Fuente: Elaboración de autores.

Análisis: La organización cuenta con varios proveedores de servicios, que ha

permitido mantener en los controles de seguridad sobre el uso y manejo de la información y protección contra la divulgación de la información dando como resultado un porcentaje alto apegado al objetivo definido, por lo que es necesario documentar todos los acuerdos entre la organización y proveedor, se evidencia el acuerdo de confidencialidad aplicado por la COAC.

- Dominio 16: Gestión de incidentes de Seguridad de la información.

Tabla 16

DOMINIO EVALUADO	SCORE	OBJETIVO
Gestión de incidentes en la seguridad de la información.	39.29 %	40,00 %

Fuente: Elaboración de autores.

Análisis: Demuestra el alcance de objetivo trazado los controles de seguridad y monitoreo en la gestión de incidencias, siendo un punto central de cómo actuar y responder frente a estos eventos ocurridos, no se cuenta con una gestión adecuada que maneje asuntos relacionados con los incidentes de la seguridad.

- Dominio 17: Seguridad de la información y continuidad de negocio.

Tabla 17

DOMINIO EVALUADO	SCORE	OBJETIVO
Aspectos de seguridad de la información en la gestión de la continuidad del negocio	50.83 %	50,00 %

Fuente: Elaboración de autores.

Análisis: No se ha evidenciado eventos que paralicen totalmente el negocio, sin embargo, de acuerdo con la evaluación se verifica que aún existe algunos controles que se deben implementar a la hora de presenciar incidentes mayores, no se ha tenido establecido el nivel de seguridad de la información durante la situación adversa.

- Dominio 18: cumplimiento.

Tabla 18

DOMINIO EVALUADO	SCORE	OBJETIVO
Cumplimiento.	42,33 %	50,00 %

Fuente: Elaboración de autores.

Análisis: Actualmente está implementando el cumplimiento a la norma del organismo de control, en este caso a la superintendencia de Economía Popular y Solidaria, quienes establecieron un marco normativo alineado a ISO 27002, señalando la obligatoriedad de la implementación de múltiples controles de seguridad de la información. No obstante, el 42,33% obedece también a que muchos de los controles se hallan en proceso de implementación o han sido implementados con alcances muy limitados.

5.1.3 Conclusiones y recomendaciones

- El diagnóstico de postura de Seguridad de la información utilizando el marco de trabajo ISO 27002, presenta varias oportunidades de mejora a nivel de controles de seguridad, iniciando por una clasificación de los activos con información sensible, para identificar amenazas y vulnerabilidades de los activos y proponer iniciativas que mejoren la puntuación obtenida.
- La evaluación del estado de situación de la seguridad de la información basado en ISO27001, arrojo una puntuación de 49,18% de cumplimiento, resaltando como aspectos importantes de mejora la ausencia de un modelo de gestión de Seguridad de la información, poca gestión de activos de información, no se aplica cifrado, no se gestionan incidentes de Seguridad de la información y debilidades en el cumplimiento normativo
- Los activos más sensibles, requieren un fortalecimiento importante de la postura de seguridad a nivel de sus controles, mismos que pueden realizarse con la implementación de iniciativas de corto plazo, que

mitiguen los riesgos más significativos.

- En el análisis de los activos más sensibles, se encontró que la disponibilidad es el pilar que se encuentra más fortalecido, mientras que la confidencialidad, es el aspecto que presenta mayores oportunidades de mejora.
- Dentro del conjunto de iniciativas planteadas para el SGSI, los controles de mayor impacto en la mitigación están relacionados con el bloqueo de accesos innecesarios, el afinamiento de configuraciones y el monitoreo del estado de salud de los componentes tecnológicos.
- La normativa emitida para el control de las COAC está completamente alineada a ISO 27002, por lo que su cumplimiento, permite apalancar la creación de un adecuado Sistema de Gestión de Seguridad de la información.
- Es necesario implementar un SGSI que permita realizar una adecuada gestión de la información sensible; para que la organización pueda responder de manera efectiva ante los riesgos de ciberataques, desastres naturales y/o incidencias de mayor impacto.

6 Fase 2

6.1 Clasificación de la información

Para una buena gestión de la información es necesario tener identificada toda la información de la COAC, para poder evaluarla en términos de grado de confidencialidad, el nivel de integridad y accesibilidad, y donde se encuentra almacenada la información, al que denominara en posterior como “Activo de información” (que incluye hardware, software, redes, base de datos, información, servicios, documentos físicos, etc.).

Por tal motivo en esta fase de la clasificación de la información se realiza el proceso de levantamiento y la identificación de activos de información con el fin de establecer niveles de protección en las tres dimensiones de la triada de seguridad que son: Integridad, confidencialidad y disponibilidad.

6.1.1 Metodología

En esta fase se aplica el método de encuestas al área de TI y otras áreas competentes que aporte al levantamiento de la información con la finalidad de

identificar qué información tengo y que tipo de sensibilidad, se puede evidenciar tipos de información los cuales son: activos primarios y activos de soporte. Ver Anexo 1.

Para la clasificación de la información se realizó una matriz de criterios enfocados los siguientes aspectos principales de confidencialidad, disponibilidad, integridad, cumplimiento normativo y afectación cuantitativa este último está ligado a la valoración de la información desde punto de vista de riesgo operativo que son definidos en la COAC.

Se clasifica de acuerdo las afectaciones que presenciaría la COAC, en los siguientes factores, ver Anexo 2:

- **Catastrófico:** en la triada de seguridad se consideraría este factor cuando la información se encuentra comprometida en la fuga de información sensible, pérdida de credibilidad, demanda de los clientes o pagos indemnización a los terceros que afecten presupuestos mayores a 50%, intervención de ente de control, destrucción de data center que afectaría la paralización de las operaciones al 100% sin capacidad de restaurar respaldos.
- **Mayor:** una afectación mayor se considera cuando en la triada de seguridad la información existe incidente de filtración a la información confidencial y divulgación a sitios estratégicos siendo una afectación al 75% en la paralización de la operatividad, y un porcentaje considerable de no recuperación de datos dando como resultado indisponibilidad de servicio, conocimientos por redes sociales la afectación ocurrida y pago de indemnizaciones a terceros en un valor total o igual al 20%.
- **Moderado:** Se ubica moderado las afectaciones de información al evidenciar accesos no autorizados a la información interna, exfiltración de políticas, lo que ocurriría a una paralización de 15% de servicios, todas las afectaciones de respaldos en esta categoría se pudrían recuperar con los respaldos, y considerando un pago de indemnización a terceros por acciones legales que pueden afectar al presupuesto de la COAC en un mayor o igual al 5%.
- **Menor:** Se considera en la escale menor cuando se encuentra que la

infraestructura afectada es fácilmente reemplazable, cuando la información afectada es recuperable en menos de 30 minutos, así como también cuando existe acceso a la información anonimizada, y en temas de presupuesto los pagos sean en un valor menor o igual al 1%.

- **Insignificante:** las afectaciones de la triada de seguridad se parecieran similar a la anterior, únicamente resaltando afectaciones la variación de 1% a 0,5% por los pagos de indemnizaciones por acciones legales**.**

6.1.2 Resultados

Una vez identificado los tipos de información, se realiza la recopilación o inventario con las descripciones: Entidad o dominio, tipo de información, ubicación, disponibilidad de activos en medios físicos y/o electrónicos, tipo de OS, tipo de aplicación, motor de base de datos.

En la COAC. se identificó dominios como: Clientes, Socios, Empleados, Directivos, proveedores, productos, transacciones.

Tipos de información de estos dominios se encuentran, información general que permita identificar las partes interesadas, los contactos, posición financiera, información legal, actividad económica, información médica, información crediticia, y movimientos financieros.

En esta fase se cuenta ya clasificado la información en los siguientes niveles: Sensible que son considerados criticidad, confidencialidad, de uso interno, y uso público.

En los siguientes gráficos, se puede ver la criticidad de la información clasificado de acuerdo con la triada.

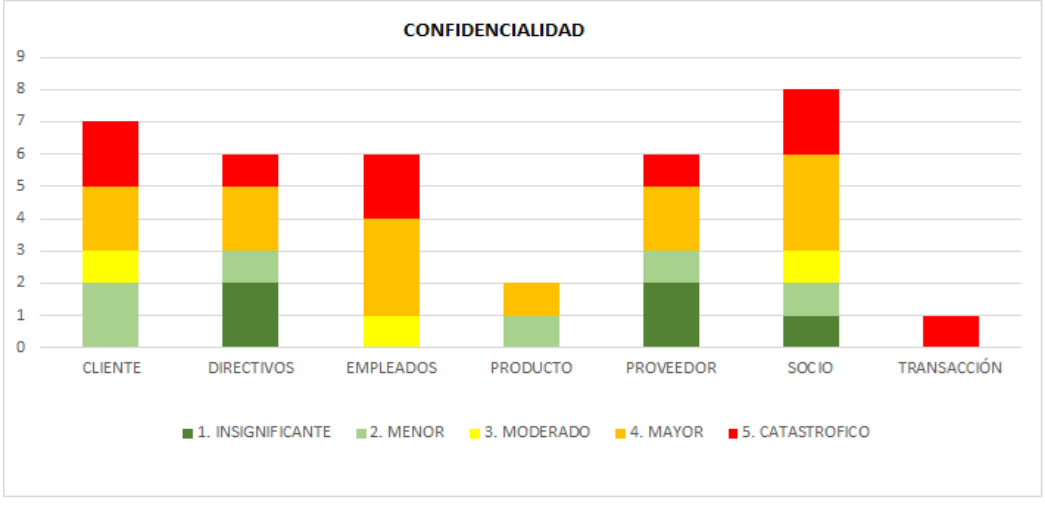

Gráfico 2. Criticidad de la información por confidencialidad.

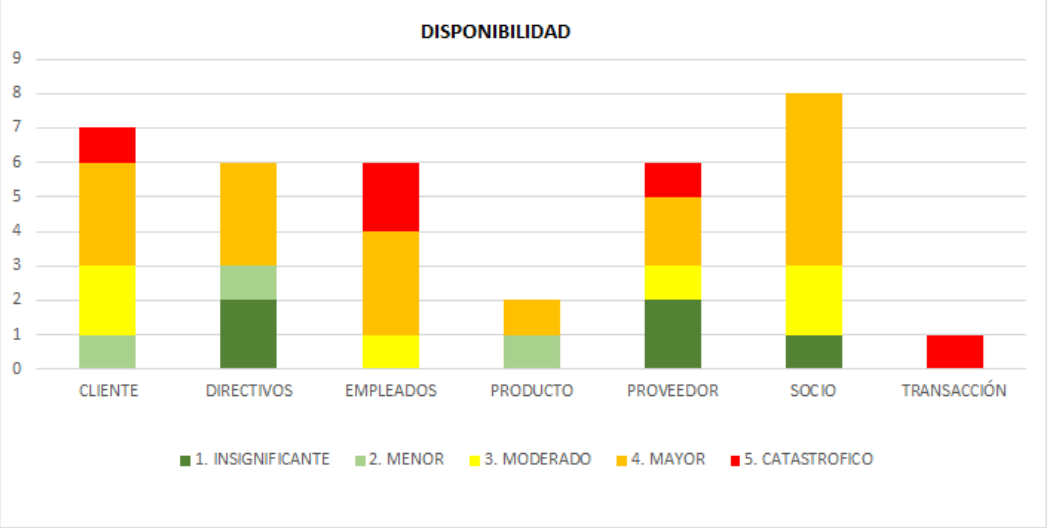

Gráfico 3. Criticidad de la información por disponibilidad.

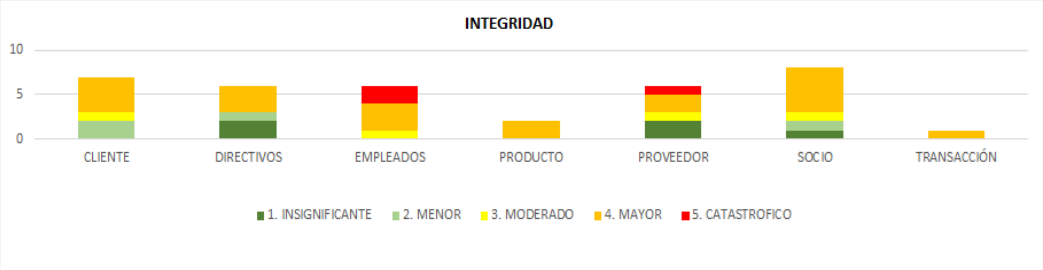

Gráfico 4. Criticidad de la información por Integridad.

6.1.3 Conclusión

- El 61% de la información de la COAC, ha sido clasificada como sensible.
- La información más relevante, está relacionada con datos personales, geo referenciados, financieros y transaccionales de clientes, Información de salarios y Salud ocupacional de empleados e Información de socios y accionistas.
- Es importante entender el contexto y el tipo de información con que cuenta la organización para clasificar la información, lo que nos ayudará a hacer un tratamiento especial y asignar responsables y nivel de accesibilidad autorizada.

7 Fase 3

7.1 Inventario de Activos de Información

7.1.1 Metodología

A través de un levantamiento de información, se identificó y clasificó varios activos de información sensible, lo que permitió contar con un registro de inventario de activos de información que cuenta la COAC. Mediante una matriz de activos se describe lo siguiente:

Tabla 19

Nro.	DESCRIPCIÓN
1	SERVIDOR DE BASE DE DATOS PRINCIPAL: cuenta con un equipo Blade Server HP Proliant 380 generación 10. con OS. Debian versión 11, dispone de un motor de base de datos PostgreSQL v. 11
2	SERVIDOR DE RESPALDOS DE STORAGE: contiene volumen snapshot de sistemas virtuales Gitea, NextCloud (bddMariaDB), servidor spark, vimaforms.
3	SERVIDOR DE APLICACIONES JAVA EE: Es un equipo con las siguientes características generales Proliant DL380, generación 9, contiene aplicaciones Ferp banca online AXXXXXXXS, Reporteador, Monitoreo de facturación, de mensajes de correo y entorno de pruebas.
4	SERVIDOR DE APLICACIONES JAVA EE: Es un equipo con las siguientes características generales Proliant 360, generación 9, OS Debian v. 11, contiene aplicaciones del Core financiero.
5	SERVIDOR DE APLICACIONES: Es un blade con las siguientes características Proliant DL380, generación 8, con OS. Debian v.11: Contiene aplicación. de ATM; App: Cumplimiento, Control Interno y Biblioteca Virtual

6 SERVIDOR DE RESPALDOS DE APLICACIONES: Es un Blade con las siguientes características Proliant DL360, generación 6, con OS. Debian v.11: Contiene repositorio Subversión, Gitea, ambiente de pruebas, NextCloud, EndPoint Eset, Spark, Glpi, vima forms y reporteador.

7 SERVIDOR DE POOL DE CONEXIONES: Es un Blade con las siguientes características Proliant DL360, generación 10, con OS. Debian v.11, con motor de BDD PostgreSQL. Contiene configuraciones del sistema.

8 SERVIDOR ESPEJO DE BASE DE DATOS, Es un Blade Hp Proliant 380, generación 10, con OS Debian v.11, contiene información similar del Activo 1.

9 SERVIDOR BARMAN es un servidor de respaldos que realiza respaldo de información en paquete comprimido, se caracteriza por ser robusta en almacenamiento, es un Blade proliant DL360, generación 10, OS Debianv.11

10 SERVIDOR DE RESPALDOS DE INFORMACIÓN, contiene respaldo de documentos mediante una aplicación DUPLICATTI, se caracteriza de un equipo CPU, con OS Debían .11.

11 SERVIDOR ESPEJO DE BASE DE DATOS, se encuentra alojado en un sitio alterno, se caracteriza por ser un servidor Blade modelo proliant 380 generación 10 con OS Debian v.11

12 SERVIDOR DE RESPALDOS DE CORE FINANCIERO, alojado en un sitio alterno, cuenta con una copia de seguridad de Core financiero.

13 Firewall ASA5520 BUN K9 CISCO

14 Firewall PA-220 PALO ALTO

15 Switch de comunicaciones SW3750E Catalyst CISCO

16 Router de comunicaciones ROU2911 CISCO

17 Router SW3750E Catalyst CISCO para Agencias

18 Switch de comunicaciones SW3750E Catalyst CISCO para pcs

19 Servidor Central telefónica IP (Internet Protocol) GrandStream Isabell

20	Servidor NVR de video grabación 32 channel

Fuente: Elaboración de autores.

Ver Anexo 3

7.1.2 Resultados

De este número de activos se realizó la valoración de la información sensible, tomando en consideración el nivel de confidencialidad, se obtuvo un porcentaje alto de activos que se encuentra con información sensible.

Luego de haber identificado y clasificado los activos de información, se seleccionaron dos activos críticos sensibles, que almacenan la mayor cantidad de información:

1. SRVXXX31 (Servidor de Base de datos): En este servidor, se almacena la información transaccional que incluye los datos de los clientes, socios, empleados, proveedores y directivos, valores de las transacciones, movimientos contables, entre otros. La afectación a este activo en términos de disponibilidad puede generar la paralización de actividades de la COAC. En términos de integridad, los registros transaccionales representan dólares americanos, que podrían ocasionar pérdidas económicas a la institución y en términos de confidencialidad, la fuga de la información almacenada puede generar riesgos reputacionales importantes.
2. SRVXXX112 (Servidor de Respaldos de información): Este servidor se encarga de mantener una copia de seguridad de la información generada por los empleados de la COAC. Dentro de esta información existen desde archivos de estrategia hasta contratos. Toda la información sensible de usuarios es colectada y respaldada por este servidor; y su afectación en términos de disponibilidad, integridad y confidencialidad, es similar a la información transaccional del servidor de base de datos.

7.1.3 Conclusión

- El 50% de la información sensible de la COAC, reside en estos dos activos seleccionados.
- Contar con el inventario de activos de información clasificada nos asegura que la información recibe niveles de protección adecuada en los

tres principios de seguridad Confidencialidad, Disponibilidad e Integridad lo que requiere un tipo de manejo especial.

8 Fase 4

8.1 Análisis de amenazas y vulnerabilidades de activos de información críticos.

8.1.1 Metodología

Luego de ubicar el activo tecnológico, utilizamos MAGERIT como marco de referencia para identificar las amenazas y vulnerabilidades más comunes a los que están expuestos los activos tecnológicos.

El proceso inicia con la identificación de las amenazas mas importantes de cada activo, ubicando las vulnerabilidades de mayor exposición y clasificándolas en términos de probabilidad de ocurrencia e impacto financiero, como se muestra en el siguiente grafico:

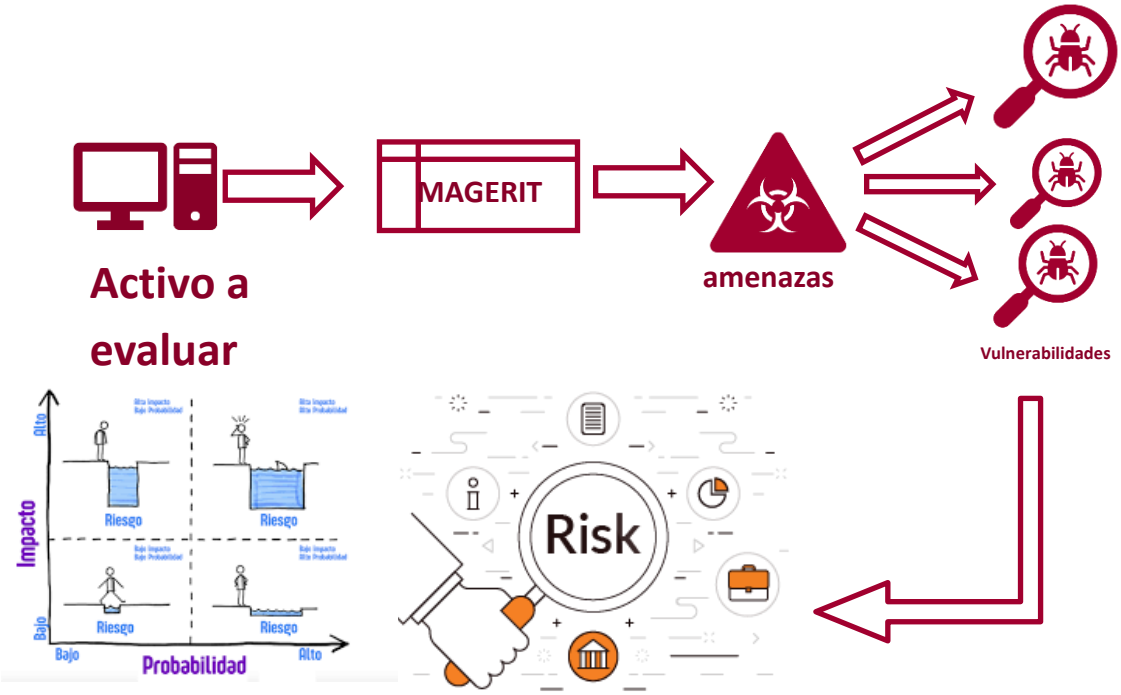

Gráfico 5. Metodología de análisis de Riesgos.

Para el caso del SRVXXX31, se han identificado las amenazas clasificadas por tipo. Ver Anexo 4.

El segundo activo tecnológico para evaluar corresponde al servidor SRVxx112, cuya misión en respaldar de manera centralizada y automática, toda la

información que genera la entidad, mediante un software denominado Duplicati, que, a través de un agente, extrae la información generada en los equipos y la almacena en este servidor; por tanto, este activo ha sido determinado como un activo sensible de información. Ver Anexo 5.

8.1.2 Resultados

Para cada activo se realiza un análisis de los riesgos inherentes que posteriormente aplicados los controles respectivos se obtiene riesgo residual y el riesgo objetivo deseado.

Cada una de estas amenazas, está relacionada a su vez con un conjunto de vulnerabilidades que fueron identificadas. Cada vulnerabilidad, fue valorada en términos de su afectación a la seguridad, sea a la confidencialidad, a la integridad o a la disponibilidad. El gráfico 3, representa la relación entre las amenazas y las vulnerabilidades

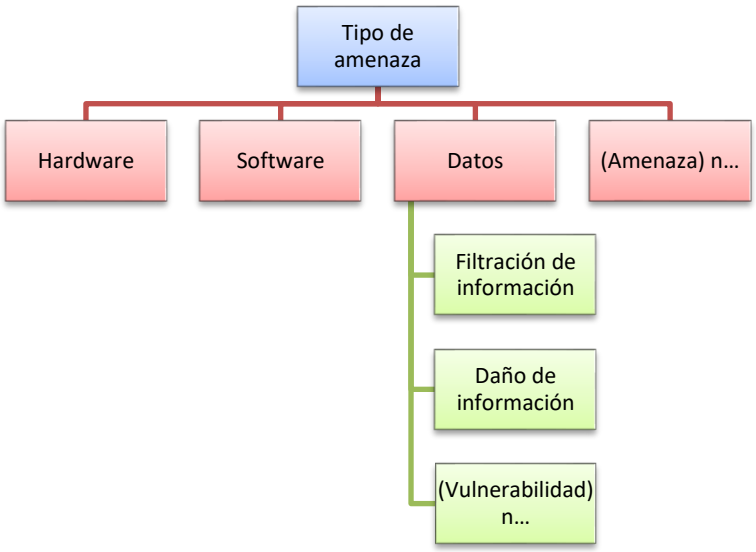

Gráfico 6. Identificación de vulnerabilidades y amenazas

Cada vulnerabilidad representa un riesgo a materializarle, por lo que es importante medir estos riesgos, en términos de probabilidad e impacto.

A nivel de probabilidad, se utilizó una escala cualitativa de 5 niveles, con los valores que se muestran en la tabla 20.

Tabla 20

PROBABILIDAD

NIVELES	%
MUY ALTA	>60%
ALTO	50%
MEDIO	30%
BAJO	15%
POCO PROBABLE	<5%

Fuente: Elaboración de autores.

De la misma manera, se definió una escala de impactos, que establece cualitativamente como se vería impactado el activo, ante la materialización del riesgo. Para estimar el impacto, se tomaron algunas variables, descritas a continuación:

- Pérdidas Financieras, que indican rangos de montos de perdida que puede provocarse ante la materialización del riesgo
- Multas y Sanciones del Organismo de Control, asociadas a lo indicado por la SEPS, que dependen de monto y tipo de COAC.
- Interrupción de Operaciones Parcial / Total, que indica si la paralización de operaciones puede provocarse de manera parcial o total
- Imagen Institucional, que representa la afectación en términos reputacionales de la COAC y los servicios que brinda.

Esta escala cualitativa de impactos se generó también en un modelo de 5 niveles, como se muestra en la tabla 21.

Tabla 21

IMPACTO

Nro.	**NIVELES**	**Pérdidas Financieras**	**Multas y Sanciones del Organismo de Control**	**Interrupción de Operaciones Parcial / Total**	**Imagen Institucional**
5	**CATASTRÓFICO**	> a 200000	Orden de	Cierre de 17	Intervención

			suspensión de las oficinas	Oficinas	a la COAC por parte del ente regulador
4	**MAYOR**	100001 a 200000	10001 a 50000	2 localidades	Comentarios virales en redes sociales >500 tweet
3	**MODERADO**	20001 a 100000	5001 a 10000	10 agencias	Perdida de un 10% clientes
2	**MENOR**	1001 a 20000	1000 a 5000	5 agencias	Clientes molestos se quejan en redes <20 tweet
1	**INSIGNIFICANTE**	1 a 1000	1 a 1000	1 agencia	Clientes se quejan en agencias

Fuente: Elaboración de autores.

En el Anexo 4 se muestra en la pestaña Riesgo ACTIVO 1_Srv.Base Datos, todos los riesgos identificados.

Basado en el análisis de los riesgos, se construye una matriz de riesgo inherente, donde se han identificado 25 Riesgos, ubicados en la matriz de probabilidad e impacto como se muestra en el gráfico 4.

Riesgo Inherente

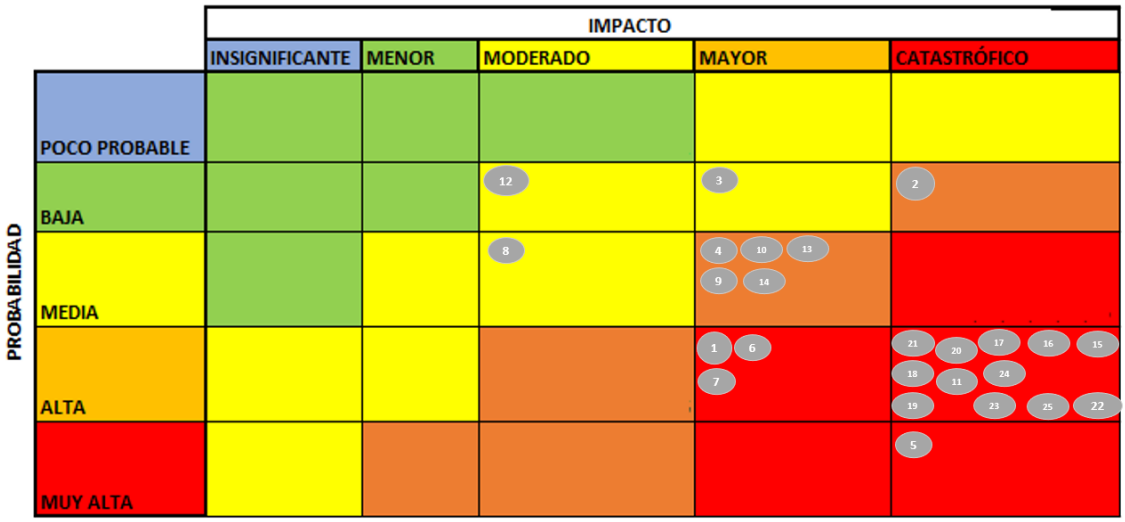

Gráfico 7. Riesgo Inherente activo SrvXXX31

Bajo esta distribución de riesgos, el activo presenta:

- 16 riesgos críticos
- 6 riesgos altos
- 3 riesgos medios

Dentro del foco de acción de los riesgos críticos principalmente, se han aplicado varios controles con la intención de mitigar las amenazas. En los controles se identificaron los objetivos de información CAVR como guías que permiten evaluar si los controles en particular los de procesamiento de información están adecuadamente orientados.

Objetivo	Caracerística	Sigla
Información completa/integra	Completeness	C
Información exacta	Accuracy	A
Información válida	Validity	V
Información protegida	Restricted Acces	R

Gráfico 8. CAVR

No existen riesgos de severidad baja, lo cual concuerda con el diagnostico de madurez de ISO 27002 aplicado a la organización, que obtuvo un nivel de

madurez muy bajo que se refleja justamente sobre la cantidad de riesgos críticos y la falta de riesgos bajos.

Para evaluar la solidez de los controles, se han definido varios criterios que ponderan el resultado final, basado en las escalas que se muestran a continuación.

Oportunidad: Un control puede ser preventivo, detectivo o correctivo. Basado en la oportunidad, los controles preventivos son los que mitigan un riesgo de mejor manera.

Tabla 22

OPORTUNIDAD DEL CONTROL		**puntaje**
PREVENTIVO	El control evita la materialización de un riesgo	5
DETECTIVO	El control puede detectar el riesgo para gestionar acciones de remediación	3
CORRECTIVO	El control corrige un error o una circunstancia de riesgo materializado	2

Fuente: Elaboración de autores.

Nivel de automatización: para determinar la solidez, un control automático suele ser más efectivo que un control manual

Tabla 23

NIVEL DE AUTOMATIZACIÓN		**puntaje**
AUTOMATICO	El control está automatizado al 100%	5
HIBRIDO	El control tiene una parte automatizada y una parte manual	3
MANUAL	El control es ejecutado por personas	2

Fuente: Elaboración de autores.

Combinando estos criterios, podemos obtener controles fuertes y débiles.

Tabla 24

FORTALEZA DEL CONTROL		**puntaje**
FUERTE	El control cumple a nivel de diseño y eficiencia con el objetivo para el cual fue diseñado	5
DEBIL	El control cumple parcialmente a nivel de diseño y eficiencia con el objetivo para el cual fue diseñado	2

Fuente: Elaboración de autores.

Finalmente, un control puede incidir en disminuir la probabilidad de ocurrencia, el impacto final o reducir tanto la probabilidad como el impacto.

Tabla 25

Afectación del Control	
A LA PROBABILIDAD	El control disminuye la probabilidad de ocurrencia de un riesgo
AL IMPACTO	el control disminuye el impacto del riesgo al ocurrir un evento
A AMBOS	el control reduce tanto probabilidad como impacto

Fuente: Elaboración de autores.

Los mismos riesgos, luego de evaluar la solidez de los controles, permiten visualizar los riesgos residuales de la manera que se muestran en la tabla inferior.

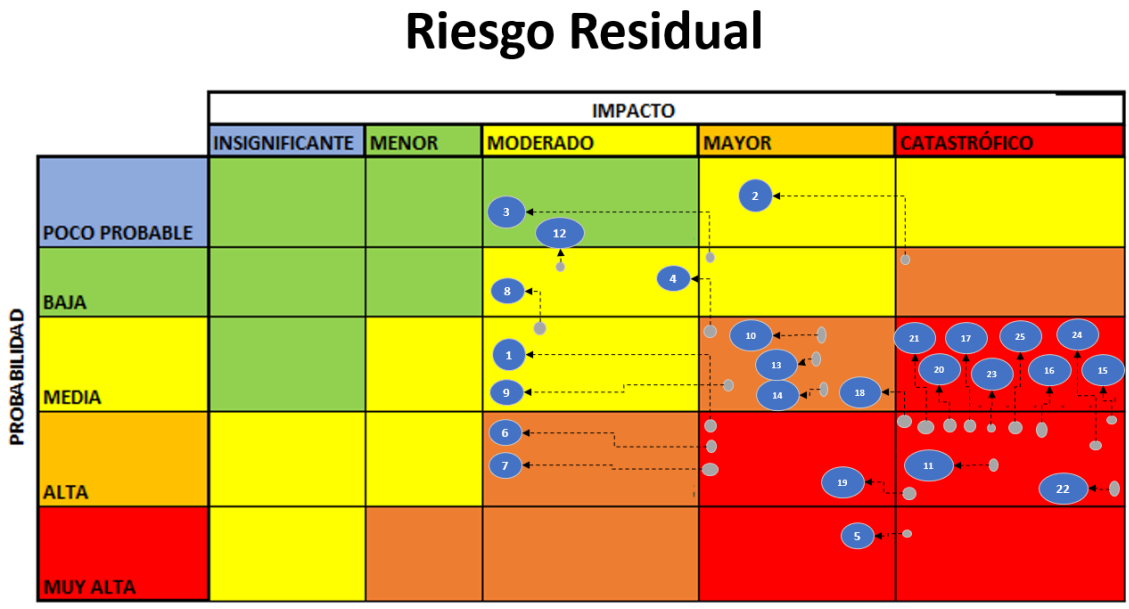

Gráfico 9. Riesgo residual activo SrvXXX31

Luego de evaluar la solidez de los controles, vemos que hay una importante migración de riesgos críticos, generando la siguiente distribución:

- 12 riesgos Críticos
- 6 riesgos altos
- 5 riesgos medios
- 2 riesgos bajos

Se describe riesgo objetivo y priorización de planes de acción; de acuerdo con

el apetito de riesgo de la organización, se ha definido que los riesgos migren su calificación de la siguiente forma:

Tabla 26

Riesgo actual	Riesgo Objetivo
12 riesgos críticos	Transformar en riesgo medio
6 riesgos altos	Transformar en riesgo medio
5 riesgos medios	23 riesgos medios
2 riesgos Bajos	Mantener

Fuente: Elaboración de autores.

Este ejercicio se consigue manteniendo los controles eficientes, e implementando nuevos controles / iniciativas que permitan alcanzar el riesgo objetivo.

El listado de iniciativas se presenta en la matriz, ver Anexo 6.

Para el caso del SRVXX112, se ubicaron 21 amenazas, que han sido identificadas utilizando información de la metodología MAGERIT, misma que a su vez, permite relacionar los tipos de amenaza con vulnerabilidades específicas, tal y como se muestra en el grafico 7.

En términos de probabilidad y severidad, se utilizaron los mismos criterios que para el activo 1, descritos en las tablas: tabla 20 (probabilidad) y Tabla 21 (impacto).

En el Anexo 5 se muestra en la pestaña Riesgo ACTIVO 2_Duplicatti, todos los riesgos identificados. Basado en el análisis de los riesgos, se construyó una matriz de riesgo inherente, donde se han identificado 22 Riesgos, ubicados en la matriz de probabilidad e impacto como se muestra en el gráfico 7.

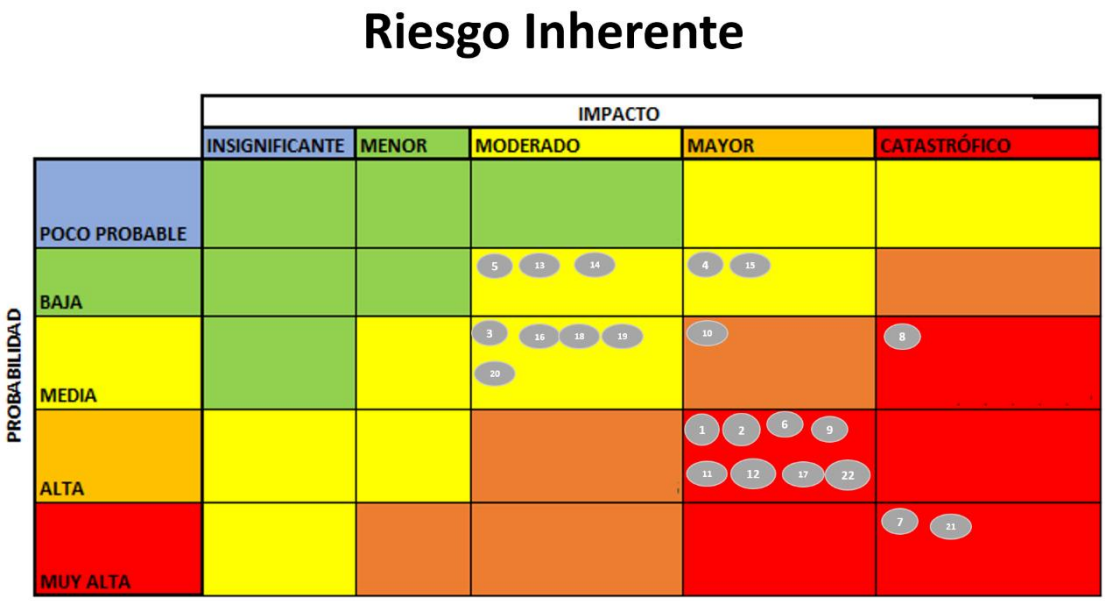

Gráfico 10. Riesgo Inherente activo Srvxx112

Bajo esta distribución de riesgos, el activo presenta:

- 11 riesgos críticos
- 1 riesgo alto
- 10 riesgos medios

Dentro del foco de acción de los riesgos críticos principalmente, se han aplicado varios controles con la intención de mitigar las amenazas. En los controles se identificaron los objetivos de información CAVR como guías que permiten evaluar si los controles en particular los de procesamiento de información están adecuadamente orientados.

Igual que con el activo SRVxxx112, no existen riesgos de severidad baja, lo cual concuerda con el diagnostico de madurez de ISO 27002 aplicado a la organización, que obtuvo un nivel de madurez muy bajo que se refleja justamente sobre la cantidad de riesgos críticos y la falta de riesgos bajos.

Para evaluar la solidez de los controles, se han utilizado los mismos criterios y ponderaciones utilizadas para evaluar el activo SRVXXX112, otorgando un puntaje al control basado en Oportunidad, Nivel de automatización y fortaleza del control.

Finalmente, un control puede incidir en disminuir la probabilidad de ocurrencia,

el impacto final o reducir tanto la probabilidad como el impacto.

Tabla 27

Afectación del Control	
A LA PROBABILIDAD	El control disminuye la probabilidad de ocurrencia de un riesgo
AL IMPACTO	el control disminuye el impacto del riesgo al ocurrir un evento
A AMBOS	el control reduce tanto probabilidad como impacto

Fuente: Elaboración de autores.

Los mismos riesgos, luego de evaluar la solidez de los controles, permiten visualizar los riesgos residuales de la manera que se muestran en el grafico 8.

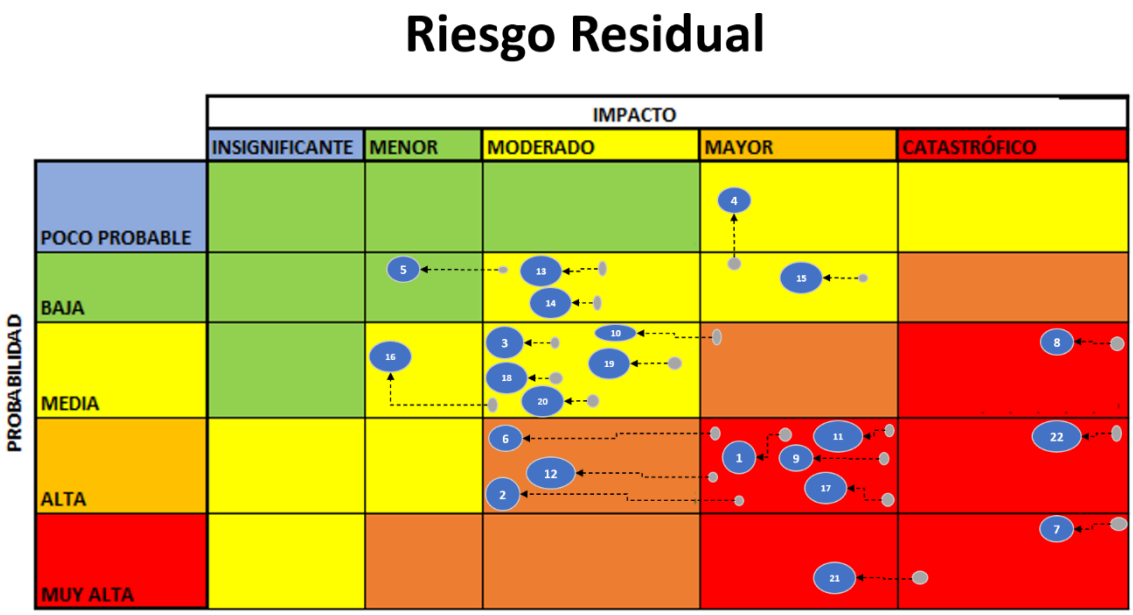

Gráfico 11. Riesgo residual activo Srvxx112

Luego de evaluar la solidez de los controles, vemos que hay una importante migración de riesgos críticos, generando la siguiente distribución:

- 8 riesgos Críticos
- 3 riesgos altos
- 10 riesgos medios
- 1 riesgo bajos

Se identifica el riesgo objetivo y se prioriza planes de acción de acuerdo con el apetito de riesgo de la organización, se ha definido que los riesgos migren su calificación de la siguiente forma:

Tabla 28

Riesgo actual	Riesgo Objetivo
9 riesgos críticos	3 se transforman en Altos 6 se transforman en medios
3 riesgos altos	Transformar en riesgo medio
10 riesgos medios	18 riesgos medios
2 riesgos Bajos	Mantener

Fuente: Elaboración de autores

Este ejercicio se consigue manteniendo los controles eficientes, e implementando nuevos controles / iniciativas que permitan alcanzar el riesgo objetivo.

Para mejorar el nivel de madurez, se diseñaron varios planes de acción que mejoran o incorporan nuevos controles y ajustan el riesgo residual, a niveles aceptados por la organización. En los anexos 4 y 5, se seleccionaron un conjunto de controles que ayudan a disminuir la posición del Riesgo residual. Para poder establecer el programa del SGSI anual, se generaron un conjunto de iniciativas, que agrupan la implementación de uno o varios controles.

El listado de iniciativas se presenta en el siguiente cuadro.

Tabla 29. Iniciativas

Iniciativa	Alcance	Controles	Activos involucrados
Afinamiento operativo	Realizar un afinamiento tecnológico a las plataformas sensibles de la COAC, de acuerdo con los estándares de hardenización definidos, para mejorar la postura de seguridad frente a la disponibilidad, confidencialidad e integridad de la información. El plan incluye el bloqueo de puertos no utilizados, protocolos de acceso seguro, y sistemas de respaldo	Cerrar puertos no utilizados. Utilizar herramienta segura de acceso remoto. Deshabilitar accesos remotos en los servidores. Aplicar la duplicación de disco RAID 5.	BDD Artesanos, Duplicatti BDD Artesanos, Duplicatti BDD Artesanos, Duplicatti BDD Artesanos, Duplicatti

		Implementar un equipo robusto servidor de respaldos	BDD Artesanos, Duplicatti
		Realizar bloqueos de controles USB	BDD Artesanos, Duplicatti
Comunicaciones	Establecer un proceso continuo de gestión y monitoreo de comunicaciones, que permita implementar redundancia de enlaces y balanceo de carga.	Contar con un proveedor de comunicaciones redundantes para balancear carga y segregar servicios.	BDD Artesanos, Duplicatti
		Contar con equipos redundantes de comunicaciones.	BDD Artesanos, Duplicatti
Continuidad de Negocio	Se estructurará un proceso periódico mensual de verificación de respaldos que incorpore las etapas de: extracción de muestras, carga de respaldos en ambiente de pruebas, acceso y verificación funcional y técnico de la información.	Realizar la comprobación frecuencia de efectividad de respaldos.	BDD Artesanos, Duplicatti
		Crea una copia exacta de los datos de las unidades	BDD Artesanos, Duplicatti
Encriptación	Aplicar protocolos seguros de encriptación de información para datos sensibles, tanto a nivel de disco como de canal de comunicaciones.	Encriptar información sensible contra los ataques.	BDD Artesanos, Duplicatti
		Encriptar información sensible contra los ataques para la transportación.	BDD Artesanos, Duplicatti
		Encriptación de la información sensible.	BDD Artesanos, Duplicatti
		Encriptar textos planos en la transportación de información en varias capas.	BDD Artesanos, Duplicatti
Gestión de Accesos	Establecer un equipo de gestión de accesos, que administre la política de accesos, enfocándose en los siguientes aspectos: 1. Menor privilegio 2. gestión de usuarios privilegiados 3. creación de perfiles de acceso a los aplicativos, que dependan del	Se debe monitorear los accesos a procesos críticos.	BDD Artesanos, Duplicatti
		Entregar cuentas de accesos limitados, y llevar registros de autorizaciones a los accesos críticos.	BDD Artesanos, Duplicatti

	rol del empleado en la COAC. 4. Monitoreo de Accesos y comportamiento de usuarios 5. Monitoreo de acciones sensibles sobre sistemas operativos, aplicaciones y motores de datos.	Configuración de alertas y asignación del personal responsable para Monitoreo de servicio.	BDD Artesanos, Duplicatti
		Solicitar reportes periódicos, y llevar un monitoreo de accesos.	BDD Artesanos, Duplicatti
		Segregación de roles y perfiles.	BDD Artesanos, Duplicatti
		Habilitar logs de accesos en la base de datos.	BDD Artesanos
		Número mínimo de usuarios que debe tener acceso a la base de datos.	BDD Artesanos, Duplicatti
		Permisos limitados y los niveles mínimos necesarios para que puedan realizar su trabajo.	BDD Artesanos, Duplicatti
		Acceso a la red con un nivel mínimo de permisos necesarios.	BDD Artesanos, Duplicatti
		Crear usuarios con privilegios limitados.	BDD Artesanos, Duplicatti
		Asignar permisos mínimos de accesos únicamente para la actividad correspondiente	BDD Artesanos, Duplicatti
		Activación de logs y permisos restringidos.	BDD Artesanos, Duplicatti
Gestión de infraestructura	Diseñar e implementar la infraestructura critica de los servidores señalados, en un entorno conectado 100% al cloud, que sirva como contingencia operacional, ahorrando los costos de implementar un centro alterno de procesamiento de datos,	Migración a Cloud	BDD Artesanos, Duplicatti

Gestión de Terceros	Generar cláusulas contractuales estándar respecto a la gestión de proveedores. Dentro de estas cláusulas, se incluirán temas como personal backup (Disponibilidad), Acuerdos de no difusión de información compartida (confidencialidad e integridad), operación de proveedores critico luego de su salida, y responsabilidad por operar de manera dolosa la información.	Firmar acuerdos de cambios de información con los proveedores de servicios.	BDD Artesanos, Duplicatti
		Contar con personal backup del proveedor.	BDD Artesanos, Duplicatti
		Contar con cláusula que obligue al proveedor a operar al menos 60 días luego de notificar su salida.	BDD Artesanos, Duplicatti
Habilidades duras	Gestionar entrenamiento y soporte especializado interno al personal técnico de la COAC, que permita operar de manera adecuada tanto los sistemas de respaldo como los motores de base de datos.	Intervención de personal capacitado responsable.	BDD Artesanos, Duplicatti
		Asignar personal calificado para administración de base de datos.	BDD Artesanos, Duplicatti
Mantenimiento de Servidores	Se establecerá un cronograma de revisión periódica (4 veces al año) con el proveedor de la solución tecnológica que incluya la ejecución de mantenimientos preventivos, actualización de parches, verificación de redundancias eléctricas y afinamiento de configuraciones recomendadas por el fabricante. Cualquier elemento que se requiera repotenciar/reemplazar/eliminar, será analizado en el contexto de esta iniciativa. Cada mantenimiento del activo tecnológico debe concluir con un informe con los cambios realizados y un listado de riesgos identificados por el proveedor que incluyan necesidades de repotenciación, actualización de versiones, configuración de accesos, etc.	Mantener un cronograma de mantenimientos con técnicos especializados.	BDD Artesanos, Duplicatti
		Mantenimientos programados de sistema de ventilación.	BDD Artesanos, Duplicatti
		Llevar una bitácora actualizada de los mantenimientos e informar las novedades encontradas.	BDD Artesanos, Duplicatti
		Contar con respaldos de energía, y llevar registro de eventos.	BDD Artesanos, Duplicatti
		Contar con manual operativo en caso de activar eventos inadecuados.	BDD Artesanos, Duplicatti
		Actualizar equipos que se encuentran descontinuados.	BDD Artesanos, Duplicatti

		Coordinar, analizar equipos con proveedores para cambio y/o reemplazo.	BDD Artesanos, Duplicatti
		Monitoreo y revisión frecuentes de la salud de base (estimación informes mensuales).	BDD Artesanos, Duplicatti
		Supervisión de calidad de datos.	BDD Artesanos, Duplicatti
		Ejecución de parches actualizados.	BDD Artesanos, Duplicatti
		Cambio o reemplazo a equipos actualizados.	BDD Artesanos, Duplicatti
		Llevar un registro actualizado de mantenimientos.	Duplicatti
Sensores y Alertas	Establecer un tablero de indicadores donde se colocará la métrica de alertas de rendimiento de los servidores y componentes asociados. El tablero emitirá alertas cuando los indicadores se encuentren fuera de los umbrales de seguridad establecidos por el fabricante.	Mantener un monitoreo de consumos de recursos.	BDD Artesanos, Duplicatti
		Monitoreo frecuente de la salud de disco duro y realizar actualizaciones de la herramienta.	BDD Artesanos, Duplicatti
		Habilitar logs de accesos en el motor de BDD.	BDD Artesanos
		- Monitoreo automático de notificación en caso de eventos.	Duplicatti
Software Base	Asegurar que los programas de seguridad en punto final (Antivirus, EDR y DLP [Data Loss Prevention]) se mantengan actualizados	Mantener actualizado el software de Antivirus.	BDD Artesanos, Duplicatti

Fuente: Elaboración de autores

8.1.3 Conclusión

Como conclusión, es importante destacar que, si bien existe una mitigación de los riesgos, el activo sigue manteniendo una importante cantidad de riesgos críticos y altos, por lo que algunos de los controles no han resultado efectivos para la mitigación de amenazas.

Los objetivos de reducción de riesgos propuestos por la organización se encuentran enfocados en la reducción de riesgos críticos.

9 Fase 5

9.1 Iniciativas y documentos clave del SGSI

9.1.1 Metodología

En esta fase, se tomaron los objetivos de reducción de riesgo definidos por la organización, considerando 3 aspectos clave:

a) Reducir los riesgos asociados hasta un nivel de riesgo medio
b) Agrupar los planes de acción en iniciativas ejecutables
c) Priorización basada en dependencias e impacto hacia la organización.

Como resultado de este ejercicio, se definió el portafolio de iniciativas, y el mapa de dependencia de estas, que se muestra en el grafico siguiente:

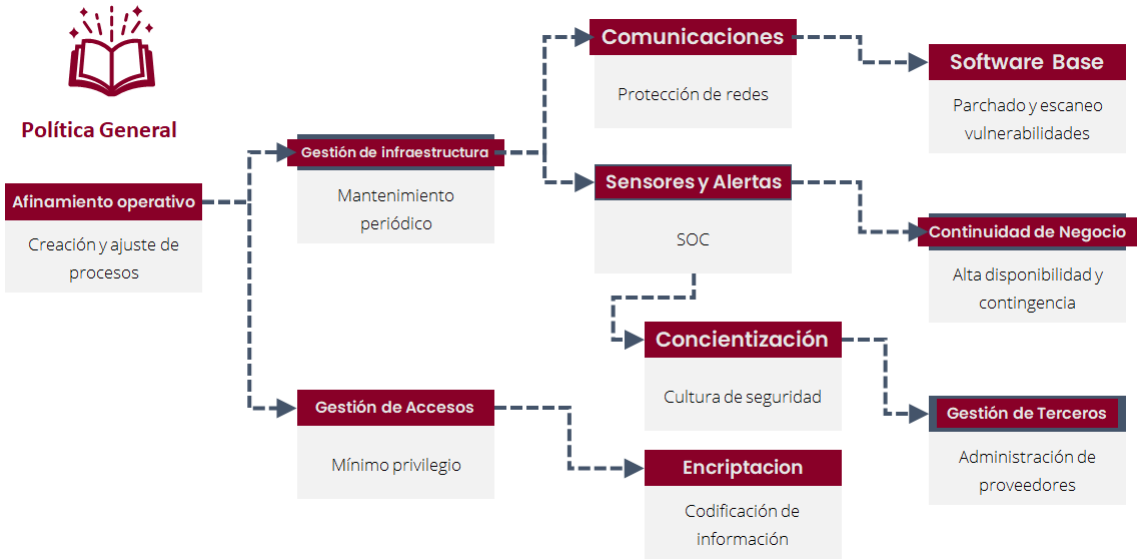

Gráfico 12. Mapa de dependencia de iniciativas.

De esta manera, el programa inicia con la construcción de una política general de Seguridad de la información, basada en los controles del estándar ISO 27002. Ver Anexo 8.

9.1.2 Resultados

Se cuenta con un documento de políticas que es parte fundamental dentro de una empresa, estas normas internas permitirán a las partes interesadas a tomar mayor compromiso en el tratamiento de la información, así como también ayudará al oficial de seguridad de la información basarse como guía para aplicar controles de seguridad y cumplimiento normativo.

9.1.3 Conclusión

- La ejecución del plan de priorización definido permitirá reducir el impacto a niveles controlables por la COAC, los mismos que serán parte integrante del portafolio de iniciativas del SGSI.
- La cooperativa dentro del programa de SGSI debe establecer los lineamientos y requerimientos mínimos de seguridad de la información y debe ser aplicado por todos los colaboradores y proveedores que realizan el intercambio de la información, a través del cumplimiento adecuado de la política general de Seguridad de la información definida.
- Se debe implementar un adecuado modelo de gestión de accesos, considerando el principio de menor privilegio.
- Es necesario generar un programa de iniciativas SGSI, auspiciadas por el Directorio y con los recursos asociados.
- Luego de los análisis, se recomienda incorporar a la Seguridad de la Información como parte del Plan estratégico de la COAC.
- Medir, controlar y reportar al Directorio, el nivel de mitigación de los controles propuestos por el SGSI sobre las vulnerabilidades identificadas.

10 Referencias

ISO/IEC 27002:2013, Information technology. Security Techniques. Code of practice for information security controls.

ISO/IEC 27005, Information technology. Security techniques. Information security risk management.

ISO 31000:2009. Risk management—Principles and guidelines.

https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

https://www.seps.gob.ec/wp-content/uploads/Norma-ISO-27001.pdf

ANEXOS

Anexo 1: Archivo Excel: matriz denominado Clasificación de información, pestañas inventario y clasificación.

Anexo 2: Archivo Excel: matriz denominado Clasificación de información, pestaña Criterios.

Anexo 3: Archivo Excel: matriz denominado Clasificación de información, pestaña Inventario de Activos.

Anexo 4: Archivo Excel: matriz denominado Clasificación de información, pestaña Riesgo ACTIVO 1_Srv.Base Datos.

Anexo 5: Archivo Excel: matriz denominado Clasificación de información, pestaña Riesgo ACTIVO 2_Duplicatti.

Anexo 6: Archivo Excel: matriz denominado Clasificación de información, pestaña Planes de acción Activo 1.

Anexo 7: Archivo Excel: Metodología_evaluacionISO27001

Anexo 8: Política General de Seguridad de la información

CONTROL DE CAMBIOS

versión	**Descripción**	**Elaborado por**	**Firma**
1.0	Versión Inicial	Ernesto Farinango Patricio Negrete	

Objetivo

Establecer los lineamientos y requerimientos mínimos de seguridad de la información para la Cooperativa de Ahorro y Crédito, conocida en adelante como COAC.

Alcance

Aplica de forma obligatoria a todos los colaboradores y proveedores de la COAC que gestionen, almacenen y transmitan información perteneciente a la COAC.

Responsables

Del Cumplimiento

1. Seguridad de la Información
2. Tecnología y Operaciones
3. Área administrativa

4. Dueños de datos e Información
5. Custodios de Datos e Información
6. Colaboradores la COAC y proveedores usuarios de información
7. Auditoría

Seguridad de la Información:

Responsable de:

- Definir y monitorear los controles de seguridad de los datos e información física y digital.
- Diseñar, implementar, evaluar y mejorar periódicamente los controles derivados de la presente política a fin de mantener su efectividad acorde a los desafíos tecnológicos existentes y los cambios en el ambiente de riesgos de seguridad.
- Administrar el Sistema de Gestión de Seguridad de la Información (SGSI).

División de Tecnología y Operaciones

Responsable de:

- Establecer las especificaciones técnicas y parámetros para todo el ciclo de vida de los activos tecnológicos que almacenan datos e información.
- Realizar análisis de capacidad de los medios tecnológicos de almacenamiento de datos e información y gestionar los recursos para garantizar la disponibilidad de los datos a lo largo de su ciclo de vida.
- Verificar y mantener la disponibilidad e integridad de los respaldos de datos e información para los períodos de retención que establece la normativa del SEPS vigente.

División Administrativa

Responsable de:

- Establecer las directrices de gestión documental para el COAC.
- Proveer los repositorios institucionales y los controles ambientales necesarios para el almacenamiento seguro de información física.

Dueños de datos e información

Responsable de:

- Realizar la clasificación de campos de datos de acuerdo con la Metodología de Evaluación establecida por la COAC.
- Validar con el Custodio de Datos que los controles de seguridad de información aplicados al repositorio oficial a su cargo se encuentren operando de acuerdo con la clasificación de la información definida por el mismo.
- Gestionar los riesgos asociados a los activos en su custodia.
- Autorizar los accesos y cambios directos de información contenida en los repositorios oficiales de información a su cargo.

Custodios de datos e información

Responsable de:

- Entender la clasificación de los datos e información asignada por el dueño y los controles de seguridad aplicables de acuerdo con las directrices de seguridad de la información a fin de validar la aplicación oportuna de los mismos sobre la información física o digital que se encuentra bajo su custodia.
- Asesorar al dueño de datos respecto de las solicitudes de accesos o cambios directos de información contenida en los repositorios oficiales.
- Mantener actualizado el detalle de los datos e información que custodia.
- Notificar de manera inmediata posibles eventos o debilidades de seguridad de la información de acuerdo con los canales de comunicación y procedimientos definidos en el COAC.
- Participar en el análisis de riesgos de los activos de información que custodia.
- Participar en las decisiones transversales respecto a la gestión del repositorio de los datos e información que custodia.

Empleados de la COAC y proveedores

Responsable de:

- Mantener la confidencialidad de la información de la COAC, y utilizarla únicamente para los propósitos de la función que se

encuentren autorizados realizar.

- Ingresar información correcta y de calidad a los sistemas tecnológicos y/o archivos físicos.
- Cumplir con políticas, procedimientos y estándares de seguridad de la información definidos por la COAC.
- Comunicar a su línea de supervisión y/o al dueño de los datos e información y a Seguridad de la Información de manera inmediata cuando conozca la divulgación no autorizada de información o posibles eventos o debilidades de seguridad, usando los canales de comunicación y procedimientos definidos por la COAC.

Auditoría

Responsable de:

- Validar el cumplimiento de esta política.

Políticas

Políticas Generales

- La COAC es propietaria de todos los datos e información que se generen a través de sus empleados y proveedores, en cumplimiento de sus labores y/o funciones encomendadas.
- Los datos e información de la COAC deben tratarse con estricto apego y cumplimiento a los principios, derechos y obligaciones establecidas en la Constitución, los instrumentos internacionales, Leyes, Reglamentos y la demás normativa aplicable.
- Los datos e información la COAC deberán clasificarse, conforme a los criterios institucionales, para establecer el grado de sensibilidad y criticidad independiente de que esté:
- Almacenada, en los sistemas o medios portables,
- Transmitida, a través de redes de comunicaciones o entre sistemas,
- Impresa o escrita, en papel.
- El dueño y custodio de datos e información de la COAC se identificarán de acuerdo con los procedimientos establecidos a nivel institucional.
- Los datos e información la COAC que no hayan sido clasificados, deberán tratarse como confidenciales hasta que el dueño de esta

cambie su nivel de clasificación.

- La seguridad de datos e información sensible deberá tomarse en cuenta desde el diseño y por defecto en todos los proyectos e iniciativas.
- Los controles definidos por seguridad de la información deberán priorizar el resguardo de la información sensible de cada proceso.
- El flujo de los datos gestionados en proyectos deberá identificarse mediante diagramas de flujo. (DFD)

Políticas Específicas

Directrices de la Dirección en seguridad de la información.

- El área de seguridad de la información será responsable de definir un conjunto de políticas específicas (cuando sean requeridas), y serán anexadas al cuerpo del presente documento, mismas que entraran en vigor a partir de su aprobación y difusión por los canales oficiales de la COAC (Intranet y correo institucional).
- Las políticas de Seguridad de la información, así como la política general de Seguridad de la información, serán revisadas al menos una vez al año, verificando si aún continúan vigentes, en función de los objetivos institucionales, transformación digital, cambios regulatorios y amenazas nuevas del entorno.
- Todas las políticas generadas por seguridad de la información serán presentadas al directorio y a los comités que establezca el ente de control, para su revisión y aprobación.

Organización interna

- El oficial de seguridad de la información, o quien cumpla ese rol dentro de la COAC, será responsable de:
    - Validar al menos una vez al año, los riesgos identificados sobre la información que afecten la disponibilidad, integridad, confidencialidad y privacidad de esta.
    - Establecer en conjunto con las áreas respectivas, los controles necesarios para asegurar la adecuada mitigación de los riesgos.
    - Evaluar al menos una vez al año, la solidez de los

controles, buscando mejorar aquellos que se presenten como débiles.

- El área de Recursos humanos generara una estructura que permita la segregación de funciones de seguridad de la información.
- El oficial de Seguridad de la información coordinara el contacto con las autoridades de control para presentar avances, descargos y detalles del cumplimiento de la normativa vigente respecto a seguridad de la información.
- El oficial de seguridad de la información realizara acercamientos con grupos de interés de seguridad de la información, tanto de otras cooperativas como de grupos profesionales de seguridad, a fin de establecer una red colaborativa de contactos para intercambiar conocimientos en materia de seguridad de la información.
- El oficial de seguridad de la información participara activamente en la gestión de proyectos, para asegurar que los mismos cuentes con controles que garanticen confidencialidad, disponibilidad, integridad y privacidad en la implementación de estos.

Dispositivos para movilidad y teletrabajo

- El oficial de seguridad de la información definirá en conjunto con las áreas tecnológicas, una política de uso de dispositivos para movilidad que habiliten de manera segura el uso de dispositivos móviles para transportar correos y archivos sensibles.
- El oficial de seguridad de la información trabajará en conjunto con las áreas tecnológicas, para implementar controles que aseguren la portabilidad en jornadas de Teletrabajo, estableciendo el uso de VPNs, antivirus y demás componentes de seguridad en dispositivos corporativos, con el objetivo de proteger la integridad, disponibilidad, confidencialidad y privacidad de la información sensible de la COAC.

Seguridad de recursos humanos

- El área de recursos humanos diseñará controles en los procesos de contratación, que permitan a la COAC:

- Realizar investigación de antecedentes de los cargos sensibles contratados.
- Establecer Términos y condiciones de contratación que incluyan la responsabilidad del empleado en el cuidado y protección de la información a su cargo.
- Establecer normas en el reglamento interno de trabajo, que especifiquen claramente las responsabilidades en su gestión en materia de Seguridad de la información
- Implementar procesos de concienciación, educación y capacitación en seguridad de la información.
- Establecer sanciones por incumplimiento de la política general de seguridad de la información.
- Definir procesos que aseguren la protección de la información sensible, ante el cese o cambio de puesto de trabajo.

Protección de activos de información

- El oficial de seguridad de la información establecerá procedimientos y controles para asegurar que el responsable de los activos tecnológicos realice las siguientes actividades: elaborar un Inventario de activos de información que contenga el nombre del activo, su ubicación, el tipo de activo, el propietario o custodio, el uso aceptable de un activo y las condiciones de devolución de un activo.
- Cada jefe o gerente de área, deberá realizar la clasificación de activos de información, de acuerdo con los procedimientos establecidos por el oficial de seguridad de la información.
- El proceso de clasificación debe contener al menos los siguientes aspectos:
  - Lineamientos para la clasificación de la información
  - Procedimiento de etiquetado y manipulado de la información.
  - Procedimiento para la Manipulación de activos.
- El oficial de seguridad de la información, en conjunto con el responsable de Tecnología, elaborara y mantendrá actualizados los procedimientos para gestionar adecuadamente los soportes de almacenamiento,

dispositivos extraíbles y soportes físicos de información, de manera que aseguren el uso adecuado del soporte, incluyendo procedimientos de eliminación de información sensible y destrucción de medios que contengan información sensible y que deban ser retirados del entrono tecnológico.

Gestión de accesos

- Todos los dispositivos de red, así como las consolas de monitoreo y administración de componentes, deben tener un usuario de administración diferente al que viene por defecto de fábrica.
- El oficial de seguridad de la información implementara controles para la gestión y monitoreo de usuarios, tanto en las aplicaciones como en el directorio activo, incluyendo la definición de perfiles de acceso en función de las actividades que realiza en la COAC.
- Los jefes de cada área revisaran y aprobaran la definición del perfil de acceso de sus empleados, en función de las actividades que realiza, asegurándose que los accesos se corresponden con las tareas y funciones definidas en el documento descriptivo funcional de contratación.
- Los empleados cambiaran periódicamente (al menos cada 2 meses) la contraseña de sus usuarios de acceso a la red y a las aplicaciones, utilizando una longitud mínima de 12 caracteres, que incluyan al menos una letra mayúscula, un número y un carácter alfanumérico especial.
- Esta terminantemente prohibido para cualquier empleado de la COAC, enviar fuera de la organización, copiar, transmitir o enviar a un usuario no autorizado, cualquier contenido identificado como confidencial o sensible.

Controles criptográficos

- La comunicación de los sistemas centralizados y las aplicaciones de usuario deberá realizarse utilizando mecanismos de cifrado definidos como robustos por la institución.

Áreas seguras.

- El área encargada de la seguridad física de la COAC definirá los

espacios definidos como áreas seguras, e implementará controles que permitan garantizar que solo los empleados autorizados, puedan ingresar a dichas áreas.

- El área encargada de la seguridad física colocará lectores de proximidad en las entradas de las áreas seguras, habilitando los accesos en las tarjetas de proximidad de los empleados que se encuentren debidamente autorizados para ingresar a dichas áreas.
- Las áreas definidas como seguras contaran con los siguientes controles:
    - Cámaras de videovigilancia, con capacidad de almacenar hasta 3 meses de video en alta calidad (1080p)
    - Extintores de incendios con polvo Químico Seco (PQS) o de dióxido de carbono según aplique, conforme a los estándares sugeridos para equipos electrónicos, papelería o almacenamiento de sustancias inflamables.
- Los accesos a áreas seguras contaran con una bitácora de acceso y salida de cada persona, quien deberá registrar y firmar tanto la entrada como la salida de dicha área.
- Ninguna persona podrá ingresar a las áreas seguras portando teléfonos celulares, cámaras fotográficas o dispositivos de videograbación o fotografía.
- Para acceder a las áreas seguras, las personas deberán dejar sus pertenencias en los casilleros de entrada y retirarlas a la salida.
- Cualquier excepción a las políticas de acceso a áreas seguras, únicamente puede ser aprobada por el jefe de seguridad y el jefe del área segura.

Seguridad en infraestructura y desarrollo

- El responsable de tecnología en conjunto con el oficial de seguridad de la información, deberán establecer los controles mínimos necesarios para los equipos de usuarios; entre ellos antivirus, encriptación de disco y agentes de prevención de fuga de información.
- Los empleados de la COAC no podrán llevar un activo tecnológico fuera de la oficina, sin una autorización escrita de su línea de supervisión.

- Los computadores asignados a los empleados de la COAC deberán permanecer anclados a los puestos de trabajo a través de los candados, sean estos equipos portátiles o de escritorio.
- Queda restringido el uso de memorias USB o dispositivos removibles, excepto para áreas autorizadas que intercambien información con clientes o entes de control. El área de Riesgo Operativo identificará el riesgo de uso de estos puertos, mismo que será asumido por el responsable del área que solicito el acceso.
- Los escritorios y puestos de trabajo deben permanecer limpios y despejados. Queda prohibido dejar en los escritorios información sensible, post it con contraseñas, pólizas y demás documentos. Luego de cada interacción con un cliente, los documentos deben ser almacenados en los espacios destinados para el efecto, bajo medidas de seguridad.
- Las estaciones de trabajo deben ser bloqueadas por los empleados, cada vez que se retiren de su puesto de trabajo.
- El responsable de tecnología deberá contar con procedimientos documentados respecto a la operación tecnológica.
- Todo cambio, inclusión o eliminación de componentes tecnológicos en los entornos productivos (hardware, software, base de datos), debe venir autorizado a través de un control de cambios que debe estar firmado por las áreas de tecnología, riesgos, negocio y el oficial de seguridad de la información.
- El área de tecnología realizará un análisis de capacidad de los componentes a modificar. El análisis será parte integrante del documento de control de cambios.
- El área de tecnología generara ambientes independientes de desarrollo, pruebas y producción, y se asegurara que los mismos estén aislados.
- Todo control de cambios debe ser probado antes de pasarlo a producción. Por segregación de funciones, la persona que implemento el cambio debe ser diferente de la persona que lo ponga en producción.
- El área de tecnología incorporara dentro de los entornos productivos, protecciones contra código malicioso, validando los estándares con el oficial

de seguridad de la información.

- El área de tecnología debe mantener copias de la información identificada como sensible. Las copias de información deben ser probadas periódicamente (al menos una vez al año) para garantizar su integridad.
- Las copias de seguridad no deben estar en las mismas instalaciones físicas que la información original, y deben ser almacenadas considerando las condiciones óptimas recomendadas por los fabricantes.
- Todas las actividades de los administradores y operadores de los sistemas deben generar logs, con información de la acción, la fecha, la hora y el ejecutor. Esta disposición aplica para directorios activos, bases de datos y aplicaciones.
- La instalación de cualquier aplicación en la COAC debe ser autorizada por el oficial de seguridad de la información, quien emitirá un informe indicando si existen vulnerabilidades, si el software es legítimo y si su uso no genera riesgos de seguridad para la COAC.

Gestión de la seguridad de redes e intercambio de información

- El área de tecnología implementara controles de seguridad en la red como firewall e IPS.
- Las redes deben estar segmentadas por unidad organizativa, región geográfica y canal de servicio.
- El intercambio de información con externos a la organización debe realizarse únicamente si se cuenta con acuerdos de confidencialidad previamente firmados por ambas partes.
- El intercambio de información debe realizarse por solicitud, y únicamente será compartida la porción de información estrictamente necesaria para la actividad realizada con el externo.
- El área de tecnología implementara controles de intercambio seguro de correos con áreas sensibles, como PGP.

Seguridad de proveedores y terceros

- Los proveedores de la COAC, por contrato, deben cumplir con los lineamientos de seguridad de manera obligatoria.

- Todo proveedor de la COAC deberá ser previamente calificado para proporcionar un servicio.
- Los proveedores tecnológicos, deberán además cumplir con lo estipulado en esta política, bajo las mismas condiciones de los empleados de la COAC.
- Ningún proveedor podrá hacer cambios directos, por fuera del proceso de control de cambios.
- Los proveedores que cuentan con credenciales de acceso asignadas a la infraestructura de la COAC no podrán ejecutar actividades diferentes a las que forman parte de su contrato, aun si han sido solicitadas por las áreas tecnológicas.

Gestión de incidentes de Seguridad de la información

- El oficial de seguridad de la información deberá conformar y mantener un modelo de gestión de incidentes documentado y actualizado, que incluya los procesos de: roles y responsabilidades, notificación de eventos y gestión de incidentes de seguridad.
- Cada incidente de seguridad gestionado por la COAC debe ser remitido a riesgo operativo para que sea levantado un riesgo materializado y cuente con un análisis basado en probabilidad e impacto.
- El oficial de Seguridad de la información llevará una bitácora de cada uno de los incidentes detectados y gestionados, que contenga al menos la información básica del evento (fecha, hora, impacto generado, sistemas afectados), así como las acciones realizadas para la contención y recuperación del incidente, asegurándose de recopilar la mayor cantidad de evidencia posible del evento.

Continuidad de negocio

- El área responsable de riesgos debe mantener un plan de continuidad de negocios actualizado de los procesos y servicios críticos, cumpliendo con las disposiciones de la presente política.
- El responsable de tecnología debe garantizar que los componentes de protección de seguridad cuenten con alta disponibilidad o contingencia.
- El responsable de tecnología implementara soluciones de respaldo de

información, para todos aquellos activos tecnológicos que tengan información clasificada como sensible.

Glosario

Para los fines de este documento, los siguientes términos y definiciones aplican.

- **Consentimiento**: toda manifestación expresa de voluntad, libre, inequívoca, específica e informada, emanada por el titular de los datos e información que permiten la recolección y tratamiento de estos.
- **Contenedores externos**: elementos que sirven para almacenar documentación física (cajas, carpetas, sobres etiquetados, mochilas etc.) o información electrónica (sobres de CD, memorias USB, etc.).
- **Control de seguridad de la información:** medios de gestión del riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizacionales, las cuales podrán ser administrativas, técnicas de gestión o de naturaleza jurídica.
- **Criticidad de la Información:** Atributo de la información que establece el nivel de necesidad de la información relacionada a la operación de los procesos de la COAC, a mayor nivel de criticidad, mayor nivel de disponibilidad.
- **Custodio de datos e información**: rol adquirido por un empleado, área, o tercero, que administra el repositorio de la información y por ende debe hacer efectivo el cumplimiento de los requisitos de protección de la información bajo su cargo. En el caso de información almacenada en activos administrados por Tecnología, será esta área la que cumpla el rol de Custodio de Información. Los empleados de la COAC son custodios de la información física o digital almacenada en activos entregados para el desenvolvimiento de sus funciones. (Computador, Celular, Archivador, Escritorio, etc.)
- **Datos**: forma de registro sea este electrónico, óptico, magnético, impreso o en otros medios, susceptible de ser capturado, almacenado, procesado y distribuido.
- **Datos Personales:** Cualquier información relativa a una persona física viva

identificada o identificable. (“¿Qué son los datos personales? | Comisión Europea - European Commission”) Son datos personales la ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria, datos financieros, transaccionales, crediticios, datos biométricos, genéticos, y demás atenientes a la intimidad personal y en especial aquella información cuyo uso púbico atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales.

- **Destrucción de la Información:** eliminación de la información que ha perdido utilidad para la Institución, o de los medios físicos o digitales que la contienen.
- **COAC:** Cooperativa de ahorro y crédito y las filiales o subsidiarias que le pertenecen.
- **Encriptación de Información:** La encriptación de datos o cifrado de archivos es un procedimiento mediante el cual los archivos, o cualquier tipo de documento, se vuelven completamente ilegibles gracias a un algoritmo que desordena sus componentes. Así, cualquier persona que no disponga de las claves correctas no podrá acceder a la información que contiene.
- **Información:** conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- **Información de la COAC**: se considera información de la COAC, a toda aquella generada por sus empleados en cumplimiento de sus labores, por un proveedor en cumplimiento de la relación contractual, o la de los clientes o prospectos de clientes o consumidores financieros de servicios de la COAC que es custodiada y tratada por la COAC o sus proveedores.
- **Información Sensible:** Información de la COAC previamente clasificada como confidencial y sensible.
- **Metadatos:** Sirven para suministrar información sobre los datos producidos, describen el contenido, calidad, condiciones, historia, disponibilidad y otras características de los datos. La COAC utilizara los metadatos para etiquetar documentos digitales de ofimática en base a la sensibilidad.
- **Metodología de Clasificación de información:** Método estándar para

realizar actividades de identificación y clasificación de los datos e información de la COAC en términos de la sensibilidad y criticidad.

- **Modificación de la información:** inserción, eliminación, o actualización de datos contenidos en bases de los sistemas o aplicaciones, o en documentos físicos o digitales oficiales.
- **Niveles de Acceso a la información**: conjunto de perfiles, que se podrá asignar a un usuario para buscar, categorizar, modificar y acceder a la información que se encuentra en un sistema tecnológico: bases de datos, bibliotecas, archivos, Internet, etc. y espacios físicos de almacenamiento: archivadores, bodegas, etc.
- **Repositorio de Información:** Activo de información que almacena datos e información física o digital.
- **Respaldo de Información:** o conocido también como copia de seguridad, es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. Se puede respaldar información física como digital.
- **Restauración de Información:** Leer y grabar parte o la totalidad de información desde una copia de respaldo en la ubicación original u otra alternativa.
- **Retención de información:** período de tiempo que un documento estará 'vivo' o 'accesible' para ser usado.
- **Sensibilidad de la Información:** Atributo de la información que establece el nivel de acceso a la información a fin de que sea conocida solo por el personal autorizado, a mayor nivel de sensibilidad, mayor nivel de confidencialidad. La COAC ha definido como información sensible aquella etiquetada como confidencial o sensible.
- **Titular de los datos**: es la persona natural a quien hace referencia la información. Pueden ser clientes, empleados, prospectos de clientes o proveedores de la COAC.
- **Proveedor**: Toda persona natural o jurídica (por ejemplo, pero sin limitarse a contratistas, terceros, socios de negocio, etc.) que tengan acceso a activos de información de la COAC.