FECHA VIGENCIA:	VERSIÓN
16/07/2024	3.0

PRO-GSI-GIF-02

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

	CARGO	NOMBRE	FIRMA
APROBADO POR:	Gerencia General	Ing. Mónica Nicolalde	Firmado electrónicamente por: MONICA FERNANDA NICOLALDE CASTILLO
REVISADO POR:	Presidente Comité de Procesos	Ing. Iván Quisilema	LUIS IVAN QUISILEMA MARTINEZ — Firmado digitalmente por LUIS IVAN QUISILEMA MARTINEZ Fecha: 2024.07.29 10:41:06 -05'00'
ELABORADO POR:	Oficial de Calidad y Procesos	Ing. Adriana Rosero	ADRIANA IVONNE ROSERO PORTILLA — Digitally signed by ADRIANA IVONNE ROSERO PORTILLA DN: c=EC, sn=ROSERO PORTILLA, givenName=ADRIANA IVONNE, serialNumber=IDCEC-1003550744, cn=ADRIANA IVONNE ROSERO PORTILLA Date: 2024.07.22 16:28:49 -05'00'
	Oficial de Seguridad de la Información	Ing. César Rosero	CESAR ALFONSO ROSERO BALSECA — Firmado digitalmente por CESAR ALFONSO ROSERO BALSECA Fecha: 2024.07.23 13:29:27 -05'00'

TABLA DE CONTENIDO

HISTÓRICO DE CAMBIOS			
RESPONSABLE	**CARGO**	**FECHA DE APROBACIÓN**	**VERSIÓN**
Ing. Carolina Ruiz	Oficial de Seguridad de la Información	2019-04-04	1.0
Ing. Carolina Ruiz	Oficial de Seguridad de la Información	2020-12-11	2.0
Ing. César Rosero	Oficial de Seguridad de la Información	2024-07-16	3.0

1. OBJETIVO

Gestionar incidentes de seguridad de la información incorporando mecanismos para la detección, notificación, evaluación, respuesta, tratamiento y aprendizaje, mediante el análisis y ejecución de acciones preventivas, contención y correctivas, con el propósito de evitar perjuicio a la Cooperativa, a través de un sistema de monitoreo de incidentes de seguridad y la implementación de planes de acción de manera oportuna para minimizar el posible impacto.

2. ALCANCE

Este procedimiento abarca todas las etapas desde la detección hasta la respuesta y aprendizaje de incidentes de seguridad de la información. Inicia con la notificación de alertas o amenazas por parte de clientes, colaboradores o proveedores a través de los canales de comunicación establecidos. Además, incluye la monitorización de plataformas tecnológicas, sistemas, aplicaciones, bases de datos críticas, y amenazas a recursos de infraestructura y redes de comunicación, como equipos de comunicación y herramientas de seguridad. El alcance se extiende a la evaluación, respuesta, tratamiento y ejecución de acciones preventivas, de contención y correctivas para minimizar el impacto potencial, garantizando una protección integral y oportuna a la Cooperativa mediante la implementación por parte del Departamento de Seguridad de la Información, de un sistema de monitoreo de incidentes de seguridad y planes de acción específicos.

3. DUEÑO DE PROCESO / RESPONSABLE OPERATIVO

Oficial de Seguridad de la Información

4. POLÍTICAS

4.1. GENERALES

a) Las políticas de este documento son de aplicación obligatoria para los empleados que estén involucrados en la ejecución de actividades descritas en el presente documento.

b) Este documento se debe aplicar de conformidad al ordenamiento jurídico vigente. Todos los aspectos que no se encuentren normados de forma expresa por este documento y que sean necesarios para su aplicación deberán ser complementados por disposiciones escritas emitidas por el dueño del proceso, las cuales se mantendrán vigentes hasta la siguiente actualización del documento.

c) El Oficial de Seguridad de la Información notificará a la gerencia correspondiente sobre cualquier incidente de seguridad provocado por colaboradores o terceras partes. Estos incidentes deberán ser sancionados de acuerdo con el Reglamento Interno de Trabajo o los contratos establecidos con proveedores y terceros. Las acciones a realizar pueden incluir el retiro de accesos o privilegios.

d) Este procedimiento se actualizará conforme a las mejores prácticas y cambios en las amenazas cibernéticas, asegurando el cumplimiento de normativas y estándares de seguridad relevantes.

4.2. ESPECIFICAS

4.2.1. DE LA PREPARACIÓN

a) El Oficial de Seguridad de la Información es responsable de la preparación, identificando todos los contactos internos y externos, eventos, fuentes e información necesaria para la gestión de un incidente de seguridad.

b) El Oficial de Seguridad de la Información deberá realizar una validación periódica de los puntos de acceso inalámbricos documentados por el Departamento de TI de forma trimestral para detectar puntos de acceso inalámbricos no autorizados y mitigar incidentes de seguridad que pudieren presentarse en la Cooperativa.

c) El Oficial de Seguridad de la Información validará la información referente a notificaciones y reportes emitidos por entidades de seguridad sobre amenazas existentes a nivel mundial, y comunicará esta información a los encargados de implementar acciones preventivas y correctivas.

4.2.2. DE LA DETECCIÓN Y ANÁLISIS

a) El Oficial de Seguridad de la Información será responsable de gestionar el monitoreo de eventos de seguridad de la información, revisando y verificando diariamente las alertas, sucesos e incidentes identificados como anómalos, de acuerdo con el FOR-GSI-GIF-02-02 CATALOGO INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN, en las consolas de los sistemas y aplicaciones, así como en los reportes, notificaciones e informes emitidos por los proveedores de servicio, colaboradores y socios-clientes de la Cooperativa.

b) El Oficial de Seguridad de la Información durante la revisión y verificación diaria, puede confirmar que varios sucesos, alertas, sucesos o incidentes anómalos son

amenazas para la confidencialidad, integridad y disponibilidad de los activos de información de la Cooperativa. Los criterios de revisión incluyen determinar si el suceso es un incidente, se convierte en un ataque cibernético, se identifica una vulnerabilidad en un incidente o en la ejecución de análisis de vulnerabilidades, o si el suceso no es un incidente.

c) El Oficial de Seguridad de la Información determinará si el tipo de incidente se identifica como un incidente provocado por un ataque cibernético para activar el PROCEDMIENTO PRO-GSI-GIF-11 RESPUESTA ANTE ATAQUE CIBERNÉTICOS

d) El Oficial de Seguridad de la Información investigará la causa del incidente y evaluará las acciones preventivas y correctivas a implementar, con el fin de contener y eliminar el incidente anómalo, de acuerdo con los parámetros de probabilidad e impacto del Manual de Gestión de Riesgos de Seguridad de la Información.

4.2.3. DE LA CONTECCIÓN, ERRADICACIÓN Y RECUPERACIÓN

a) El Oficial de Seguridad de la Información de acuerdo con la gravedad del impacto, podrá solicitar la participación y apoyo de los jefes departamentales que considere necesario, formando así un equipo de respuesta (temporal).

b) El Oficial de Seguridad de la Información deberá gestionar con las demás áreas la implementación de las acciones correctivas correspondientes (controles, medidas de protección, sanciones, etc.) para contener el incidente y prevenir su recurrencia. Estas actividades pueden incluir el aislamiento de los sistemas, aplicativos o equipos involucrados en el incidente de seguridad del resto de la infraestructura tecnológica de la Cooperativa, con el fin de preservar la información existente en los equipos, sistemas y aplicativos involucrados, siempre que sea técnicamente posible, así como los registros, pistas de auditoría o eventos de las actividades realizadas, ya sean lógicas o no, como capturas de pantalla, registros de eventos, fotos de evidencias y notas escritas. Durante el proceso de contención, se debe considerar que no se puede revelar información confidencial ni detalles técnicos sobre el ciberincidente y sus métodos o herramientas de análisis y solución.

c) Los jefes departamentales serán responsables de aplicar las acciones preventivas y correctivas solicitadas por el Oficial de Seguridad de la Información, para eliminar las causas que provocaron el incidente anómalo.

d) El Oficial de Seguridad de la Información será el responsable de verificar que las acciones ejecutadas son suficientes para contener el incidente de seguridad. De ser necesario, realizará mejoras en las actividades hasta detener la amenaza existente.

e) El Oficial de Seguridad deberá mantener informados a los funcionarios y partes interesadas (internas y externas) sobre nuevas vulnerabilidades, actualizaciones de las plataformas y/o recomendaciones de seguridad informática, que pudieren tener relación con el incidente presentado, a través del medio de comunicación más idóneo para el efecto (SMS, sitio web, intranet, correo, u otros).

f) El Oficial de Seguridad de la Información, una vez aplicadas las acciones correctivas y confirmada la erradicación de la amenaza, notificará al Departamento de Tecnología que se pueden activar los activos involucrados para restablecer el servicio o la infraestructura afectada.

4.2.4. POST INCIDENTE

a) El Oficial de Seguridad deberá registrar todos los incidentes reportados o presentados y los resultados del análisis realizado, en una bitácora que permita evidenciar la recurrencia de estos y el nivel de impacto de cada incidente con el fin de establecer la prioridad de atención. FOR-GIS-GIS-02-01 BITACORA DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**.**

b) El Oficial de Seguridad de la Información entregará un informe del incidente de seguridad, respaldado con información confidencial y la evidencia necesaria que detalle los incidentes identificados hasta su cierre. Este informe se registrará posteriormente en una base de conocimiento. Según la criticidad y el contenido, el informe será clasificado como Restringido, Confidencial, de Uso Interno o Público, con la opción de modificar valores o campos críticos previa autorización, para ser enviado a jefes departamentales involucrados por medios seguros.

c) El Oficial de Seguridad de la Información deberá recopilar y resguardar todas las evidencias encontradas durante la gestión del incidente de seguridad en el repositorio de Seguridad de la Información, para evitar la pérdida o modificación de estas.

d) El Departamento de Seguridad de la Información implementará un sistema de monitoreo continuo para evaluar la gestión y efectividad de las plataformas y

servicios contratados. Se establecerán indicadores clave de rendimiento (KPIs) diseñados para medir la eficacia de estos sistemas.

e) El Oficial de Seguridad de la de la Información será responsable de entregar un informe mensual al Jefe del Departamento de Riesgos. Este informe deberá incorporar todos los elementos presentados en la Gestión de Riesgos de Seguridad de la Información y detallará las acciones, controles y medidas correctivas que deben implementarse en la Cooperativa como respuesta a las alertas y vulnerabilidades reportadas por proveedores o plataformas en relación con la seguridad de la información. Estas acciones incluirán evaluaciones de riesgos, análisis de impacto, y la implementación de parches y actualizaciones de seguridad según sea necesario para mitigar los riesgos identificados. Además, se incluirán recomendaciones para fortalecer las defensas de seguridad de la infraestructura tecnológica de la Cooperativa, garantizando así la protección continua de los activos de información crítica.

f) El Oficial de Seguridad de la Información, junto con su equipo, llevará a cabo capacitaciones internas en la Cooperativa según el Plan de Concienciación y Formación aprobado; y se podrán realizar ejercicios de simulación con la colaboración con los proveedores de servicios de seguridad de la información, con el objetivo de practicar el análisis y la toma de decisiones en dichos escenarios.

g) El Oficial de Seguridad de la Información en conjunto con el Jefe de Tecnología gestionarán capacitaciones técnicas, presenciales o e-learning, al personal clave de Tecnología y Seguridad de la Información, a fin de desarrollar o fortalecer conocimientos en preservación de evidencias, análisis forense y respuesta ante incidentes de seguridad.

5. TÉRMINOS Y DEFINICIONES

Incidente de Seguridad de la Información: Evento que podría afectar la seguridad de la información en su confidencialidad, integridad o disponibilidad, tales como: acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; impedimento al normal funcionamiento de las redes, comunicaciones, sistemas de información o recursos informáticos; o la ejecución de actos que se consideren violación a las Políticas de Seguridad de la Información. Algunos ejemplos de incidentes de seguridad están detallados en el anexo A.

Detección de un incidente de seguridad de la información: Proceso de identificación de cualquier actividad inusual o sospechosa que pudiera comprometer la

seguridad de la información y/o el normal funcionamiento de las operaciones de la Cooperativa.

Equipo de respuesta: Grupo de personas de la Cooperativa (o externos autorizados) que han sido designados para apoyar en la recolección y análisis de información relacionada con los incidentes de seguridad de la información.

Gestión de Incidentes: Capacidad para gestionar de manera efectiva eventos inesperados que podrían perjudicar la seguridad de la información o la operación del negocio la Cooperativa, con el fin minimizar su impacto y mantener o restaurar las operaciones dentro de los tiempos esperados.

Información: Conjunto organizado de datos que comunica o representa conocimiento. Puede presentarse en forma textual, numérica, gráfica, cartográfica, narrativa o audiovisual, y puede residir o transmitirse en cualquier medio sea oral, escrito, visual o electrónico.

Activo de Información: Recurso que participa en la producción, emisión, almacenamiento, procesamiento, comunicación, visualización y recuperación de información.

Amenaza: Cualquier objeto, sustancia, ser humano, suceso que es capaz de actuar contra un activo de información de manera que pueda ocasionar un perjuicio. También se considera una amenaza a cualquier cosa que pueda aprovechar una vulnerabilidad y sea una causa potencial de un incidente de seguridad.

Vulnerabilidad: Es una debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad provocando un incidente de seguridad.

Confidencialidad: Característica o propiedad de la información que está disponible para el uso o es revelada exclusivamente a individuos, entidades, o procesos autorizados. Sólo los individuos, entidades o procesos calificados y autorizados tendrán acceso a la información bajo el principio del "mínimo privilegio".

Integridad: Característica o propiedad de la información que es exacta, completa y válida de acuerdo con los valores y las expectativas de Cooperativa Internacional y regulaciones externas.

Disponibilidad: Característica o propiedad de la información que permanece accesible para su uso cuando lo requiera un individuo, entidad o proceso autorizado. El aseguramiento de esta característica minimiza la posibilidad de interrupción del negocio y preserva la continuidad de la operatoria normal pues implica el resguardo de la información de alta criticidad y la recuperación de los procesos en tiempo y forma.

6. INDICADORES

COD	INDICADOR	FORMULA	DESCRIPCION	FUENTE DE INFORMACIÓN	FREC.DE MEDICION
IND-GSI-GIF-02-01	Porcentaje de atención a incidentes de Seguridad de la Información	(Número de incidentes reportados y gestionados / Número total de incidentes reportados)	Nos da la relación entre el número de incidentes solucionados sobre los reportados.	Reporte de incidentes	Mensual

7. REFERENCIAS A DOCUMENTOS UTILIZADOS

CÓDIGO	NOMBRE
MNL-GSI-02	Manual Gestión Riesgo Seguridad Información
Norma ISO 27035	Norma de Gestión de Incidentes de Seguridad
PRO-GSI-GIF-11	Procedimiento de respuesta ante ataques cibernéticos

8. REGISTROS

REGISTRO	METODOLOGIA	RESPONSABLE
Bitácora de eventos de incidentes de seguridad de la información	Se lleva un registro de los eventos e incidentes detectados para mantener una base de conocimiento y soluciones oportunas	Oficial de Seguridad de la Información

9. RIESGOS

TIPO DE RIESGO	FACTOR DE RIESGO	TIPO DE EVENTO DE RIESGO	DESCRIPCIÓN DEL RIESGO POTENCIAL	CONTROLES DEL RIESGO	FRECUENCIA	RESPONSABLE
Operacional	Personas	Deficiencias en la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros	La no confidencialidad de las claves de acceso por parte de los usuarios podría generar fuga, manipulación y perdida de datos confidenciales	1.- Legalización del acuerdo de confidencialidad por parte del personal de Talento Humano al personal nuevo que ingresa de forma permanente	Eventual (Cada que exista nuevo personal)	Talento Humano
Operacional	Personas	Deficiencias en la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros	La demora en la notificación de la desvinculación del personal hacia el área de seguridad de la información podría ocasionar fuga o manipulación de la información	1.- Notificación automática en la herramienta Sistema de Gestión de accesos para la desvinculación del personal y desactivación de claves	Eventual (Cada que exista desvinculación del personal)	Talento Humano
Operacional	Personas	Deficiencias en la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros	Roles inadecuados al personal según sus funciones podría ocasionar una mala manipulación en los datos de los socios	1.- Depuración mensual de roles y perfiles por parte del analista de seguridad de la información utilizando las herramientas tecnológicas y un cruce manual	Mensual	Analista de Seguridad de la Información
Tecnología	Tecnología de la Información	Interrupciones del negocio por fallas en la tecnología de la información	Existencia de vulnerabilidades en sistemas y redes que podrían ser explotadas para acceder de manera no autorizada a la información.	1.- Implementación periódica de escaneos de vulnerabilidades y actualizaciones de parches según los resultados.	Anual	Seguridad de la Información.
Cumplimiento	Procesos	Deficiencias en la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros	Incumplimiento de normativas y estándares de seguridad establecidos, lo que podría resultar en sanciones legales y pérdida de confianza de los clientes.	1.- Auditorías regulares de cumplimiento para evaluar y corregir cualquier vulnerabilidad	Anual	Seguridad de la Información.

10. DIAGRAMA DE FLUJO