ACUERDO No. 014 de 2022
MANUAL DE POLÍTICAS DE SEGURIDAD Y CALIDAD DE LA INFORMACIÓN

El Consejo de Administración de la Cooperativa Grancoop, en reunión efectuada el 24 de junio de 2022, según consta en el Acta No. 451; en uso de las atribuciones legales que le confieren los Estatutos de la Cooperativa Grancoop y la Ley Cooperativa.

CONSIDERANDO

1. Que es función del Consejo aprobar las políticas que considere convenientes y necesarias para la dirección, organización de la Cooperativa Grancoop y el cabal logro de sus fines.

2. Que la Cooperativa debe adoptar una política de buenas prácticas en materia de seguridad de la información, que permita identificar, prevenir y minimizar el impacto de los riesgos operativos tecnológicos.

3. Que atendiendo los lineamientos gubernamentales y legales se hace necesario identificar, medir, controlar y monitorear el riesgo operativo al cual se encuentra expuesta la Cooperativa Grancoop en el desarrollo de su objeto social.

4. Que es función del Consejo de Administración fijar las políticas y definir los procedimientos que se aplicaran en la Cooperativa Grancoop y los demás elementos que integran el Sistema de Administración de Riesgo Operativo SARO y Manual de Políticas de Seguridad y Calidad de la Información.

5. Que cumpliendo con sus funciones de la Cooperativa Grancoop revisó y aprobó el Manual de Políticas de Seguridad y Calidad de la Información.

6. Que en reunión del Consejo de Administración efectuada el 24 de junio de 2022 que consta en Acta No. 451 se aprobó el Manual de Políticas de Seguridad y Calidad de la Información.

ACUERDA

PRIMERO: Aprobar el Manual de Políticas de Seguridad y Calidad de la Información, para ser aplicado en la Cooperativa Grancoop.

COOPERATIVA GRANCOOP
MANUAL DE POLÍTICAS DE SEGURIDAD Y CALIDAD DE LA INFORMACIÓN

CONTENIDO

1. INTRODUCCION 4
2. ALCANCE 4
3. TERMINOS Y DEFINICIONES: 4
4. GOBIERNO DE SEGURIDAD DE INFORMACION 8
4.1 ESTRATEGIA DE SEGURIDAD 8
5. POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION 8
5.1 PRINCIPIOS DE SEGURIDAD DE INFORMACIÓN 9
6. RESPONSABILIDADES NORMATIVAS 10
6.2 REPRESENTANTE LEGAL 10
6.3 AUDITORÍA INTERNA O QUIEN EJERZA CONTROL INTERNO 11
6.7 GESTION DE RIESGOS 12
7. SISTEMA DE SEGURIDAD DE LA INFORMACION 13
8. RECURSOS 14
9. POLÍTICAS ESPECÍFICAS 14
9.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 14
9.1.1 ORGANIZACIÓN INTERNA. 15
9.1.2 USO DE DISPOSITIVOS MÓVILES 15
9.2 SEGURIDAD DEL RECURSO HUMANO 17
9.2.1 ANTES DE ASUMIR EL EMPLEO 17
9.2.2 DURANTE LA EJECUCIÓN DEL EMPLEO 18
9.2.3 TERMINACIÓN Y CAMBIO DE EMPLEO. 18
9.3 GESTIÓN DE ACTIVOS QUE CONTIENEN INFORMACION 18
9.3.1 INVENTARIO 19
9.3.2 CLASIFICACIÓN DE LA INFORMACIÓN 22
9.4 CONTROL DE ACCESO 23
9.4.1 REQUISITOS DE LA COOPERATIVA PARA CONTROL DE ACCESO 24
9.4.2 GESTIÓN DE ACCESO DE USUARIOS 26
9.4.3 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES 26

9.5 SEGURIDAD FÍSICA Y DEL ENTORNO. 28
9.5.1 ÁREAS SEGURAS 28
9.5.2 EQUIPOS 30
9.6 SEGURIDAD DE LAS OPERACIONES. 32
9.6.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES....32
9.6.2 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS....33
9.6.5 CONTROL DE SOFTWARE OPERACIONAL 35
9.6.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA 35
9.7 ADQUISICIÓN DESARROLLO Y MANTENIMIENTO DE SISTEMAS....36
9.7.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN 36
9.7.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE....38
9.7.3 DATOS DE PRUEBA 39
9.8 RELACIONES CON LOS PROVEEDORES....40
9.8.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES U OTROS TERCEROS....40
10. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN....43
9.9.1 POLÍTICAS DE GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN....46
10. CUMPLIMIENTO 46
10.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES 46
11. DIVULGACIÓN DE INFORMACIÓN 47

1. INTRODUCCION

La Cooperativa Grancoop ha implementado un manual de políticas que busca asegurar y proteger de manera adecuada e idónea la información en cualquier medio en el que se encuentre, para su elaboración se deberá tomar como modelo de referencia el estándar de seguridad de información ISO/IEC 27001:2013- ISO 27000, la cual trata sobre Tecnologías de la información – Resumen y vocabulario.

2. ALCANCE

El alcance de esta política se aplica a toda la Cooperativa Grancoop, a todos los recursos informáticos prioritarios y críticos a proteger, igualmente a todos los empleados y directivos que interactúan con los sistemas de información tanto dentro de las oficinas, las sucursales o desde cualquier otra parte autorizados por las directivas de la Cooperativa para desempeñar sus labores cotidianas, y terceros que presten servicios o tengan algún tipo de relación con la Cooperativa.

3. TERMINOS Y DEFINICIONES:

Cooperativa Grancoop: de ahora en adelante nos referiremos a través de Grancoop.

Acción resolutiva: Acción tomada para evitar la repetición de un incumplimiento mediante la identificación y tratamiento de las causas que la provocaron.

Activo de información: Componente de hardware, software de procesamiento, almacenamiento y comunicaciones, bases de datos, documentos físicos, procesos procedimientos y recursos humanos asociados con el manejo de los datos y la información misional que maneja la Grancoop.

Acuerdo de Confidencialidad: Es un documento en los que los colaboradores de Grancoop, directivos o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la Cooperativa, comprometiéndose a no divulgar, usar, exponer o lucrarse de la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

Amenaza: Factor externo que aprovecha una debilidad en los activos de información y puede impactar en forma negativa en la organización. Es la causal de un potencial incidente.

Asociado: son las personas naturales o jurídicas con quienes Grancoop mantiene un vínculo legal o contractual para el suministro de los productos ofrecidos por la Cooperativa.

Autenticación: Es el proceso que conlleva a la comprobación de la identidad de un usuario o un equipo tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Autenticidad: Aseguramiento de la identidad respecto al origen cierto de los datos o información que circula por la Red.

Centros de cableado: Son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables.

Centro de cómputo: Es un área específica bien puede ser interna o externa para el almacenamiento de múltiples equipos de cómputo para un fin específico, los cuales se encuentran conectados entre sí a través de una red estructurada de datos.

Cifrado: Es la transformación de los datos mediante el uso algoritmos de criptografía para producir datos incomprensibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a las bases de datos que contiene información considerada de alta seguridad para la Cooperativa.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados, y no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Contención: Evitar que el incidente siga ocasionando daños.

Control: Es toda actividad o proceso encaminado a mitigar o evitar un riesgo, Incluye políticas, procedimientos y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Criptografía: Técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes de uso confidencial de la Cooperativa, con el fin de hacerlos difíciles a receptores no autorizados tanto a personal interno como externo.

Disponibilidad: Es la característica, cualidad o condición que se refiere a que la información y los recursos necesarios para su uso estén a disposición ahora y en el futuro para quienes necesiten acceder a ella, ya sean personas, procesos o aplicaciones.

Equipo de cómputo: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Evento de seguridad: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad. [ISO/IEC 27000:2018].

Gobierno de seguridad de la información: Sistema por el cual las actividades de seguridad de la información de una organización son dirigidas y controladas.

Impacto: Resultado o consecuencias que produce un incidente de seguridad de la información en cualquiera de sus formas sobre la Cooperativa.

Incidente de seguridad: Cualquier situación o evento que comprometa la operación o cualquier activo de información. Así mismo a cualquier sospecha de violación a las políticas de seguridad de la información de Grancoop.

Información: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. Constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

Integridad: Mantenimiento de la exactitud, precisión, coherencia y completitud de la información y sus métodos de proceso, desde su creación hasta su destrucción. Debe ser inalterada ante accidentes o intentos maliciosos, siempre se debe prevenir modificaciones no autorizadas de la información

Licencia de Software: Es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Log's: Registro de los sistemas de información que permite verificar las tareas o actividades realizadas por determinado usuario o sistema.

Medio Removible: Es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; incluye cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

Nivel de riesgo: Evaluación del riesgo identificando su posible materialización frente al impacto y probabilidad de ocurrencia

Perfiles de Usuario: Son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

Políticas de seguridad: Conjunto de directrices, lineamientos y reglas que permiten velar porque se resguarden los activos de información, aprobados por el consejo de administración.

Probabilidad: Posibilidad que el riesgo se pueda materializar frente a un incidente de seguridad de la información.

Propiedad Intelectual: Es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

Recuperación: Volver el entorno afectado a su estado natural.

Recursos Tecnológicos: Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la Cooperativa.

Responsable por el Activo de Información: Es la persona o grupo de personas, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información que están a su disposición y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Riesgo residual: Es el riesgo que queda después de aplicar los controles al riesgo identificado.

Seguridad de la información: Es el conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información que se almacene, reproduzca o procese en los sistemas informáticos de la organización.

Servicios de computación en la nube: Modelo para permitir un acceso de red conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar y liberar rápidamente con un mínimo esfuerzo de administración o proveedor de servicios**.**

Software Malicioso (Virus): Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal, por lo general su acción es transparente al usuario y este tardo tiempo en descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.

Terceros: Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

Usuario: en el presente documento se emplea para referirse a empleados de la Cooperativa, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red.

Validación: Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.

VPN (Virtual Private Network): es una tecnología de red que permite una extensión segura de la red privada de área local (LAN) sobre una red pública o no controlada como Internet.

Vulnerabilidad: Ausencia o debilidad de un control. Condición que podría permitir que una amenaza se materialice con mayor frecuencia, mayor impacto o ambas. Una vulnerabilidad puede ser la ausencia o debilidad en los controles administrativos, técnicos y/o físicos.

4. GOBIERNO DE SEGURIDAD DE INFORMACION

Grancoop define e implementa el sistema de seguridad de información como un componente integral de las prácticas de buen gobierno, ya que proporciona la dirección estratégica a las actividades de seguridad y garantiza que se alcancen los objetivos y se realice la debida gestión de los riesgos relacionados con seguridad de la información.

El Consejo de Administración designa al Gerente General, Jefe de sistemas, Asistente Administrativa y Administrador de Riesgos como los responsables de la implementación del sistema de seguridad de la información.

4.1 ESTRATEGIA DE SEGURIDAD

El objetivo de la Estrategia de Seguridad de la Información es trazar el camino que nos permita llegar al estado de madurez o capacidad deseado en materia de seguridad de la información. Grancoop ha elaborado una estrategia o plan de implementación (Anexo 1) teniendo en cuenta los requisitos legales y reglamentarios pertinentes. En su elaboración participó la Gerente General, el jefe de sistemas, Asistente administrativa y Administrador de riesgos, y el avance en la ejecución del plan será informado a los miembros del Comité de riesgos y Consejo de Administración.

El plan describe:

- Qué se va a hacer
- Qué recursos se requerirán para ejecutar el plan
- Quién será el responsable del plan
- Cuando finalizará la ejecución del plan
- Cómo se evaluarán los resultados logrados

5. POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION

Para la Cooperativa Grancoop es importante proteger la información de los asociados, colaboradores y demás terceros, como parte indispensable para el logro de sus metas u objetivos estratégicos, por ello se compromete a implementar políticas de buenas prácticas en materia de seguridad de información, enmarcado en el cumplimiento de la normatividad vigente y mantener una mejora continua del sistema, garantizando así, que los activos de información se utilicen de forma correcta y responsable, se gestionen y se protejan de amenazas internas o externas, conservando su confidencialidad, integridad y disponibilidad.

Esta política tiene como objetivos:

- Identificar y mitigar los riesgos contra la seguridad de la información y disminuir su impacto adoptando mecanismos de prevención.
- Cumplir con los principios de seguridad de la información.
- Mantener la confianza de los asociados, colaboradores y demás.

- Apoyar la innovación tecnológica y mejora continua del sistema manteniendo un nivel de eficacia.
- Proteger los activos de información y darle el tratamiento correspondiente según su clasificación.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información y mantener su actualización constante.
- Educar y crear una cultura de seguridad de información con el fin de que todos los que tienen relación con la Cooperativa se comprometan, acepten y apliquen las políticas de seguridad de información.
- Gestión de incidentes garantizando la continuidad del negocio.
- Cumplir con todos los requerimientos legales y regulatorios en materia de seguridad y protección de datos.

Esta política se actualizará y se ajustará según las necesidades de la Cooperativa y requerimientos normativos, y deberá cumplirse en un 100% por los colaboradores, directivos, proveedores y terceros.

El Consejo de Administración aprueba esta política en apoyo y compromiso con la implementación de políticas eficientes que garanticen la seguridad de la información.

5.1 PRINCIPIOS DE SEGURIDAD DE INFORMACIÓN

Los principios que deberán respetarse son:

- Privacidad: La información que se maneja en la Cooperativa Grancoop, solamente podrá ser conocida por las personas que, de acuerdo a sus funciones, deben acceder a ella, será utilizada sólo para fines exclusivos de la Cooperativa y su tratamiento será de acuerdo a lo contemplado en la ley 1581 de protección de datos.

- Divulgación: las políticas y responsabilidades frente a la seguridad de la información definidas, serán compartidas, publicadas y aceptadas por cada uno de los colaboradores, directivos, proveedores, y terceros.

- Protección: Grancoop aplicará controles para proteger la información generada, procesada o resguardada por los procesos internos de la Cooperativa, las instalaciones de procesamiento y la infraestructura tecnológica que soporta los procesos críticos con el fin de minimizar impactos financieros, operativos o legales.

- Disponibilidad: Grancoop garantiza la disponibilidad de la información, procesos y la continuidad de las operaciones.

- Legalidad: Se garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

6. RESPONSABILIDADES NORMATIVAS

Cada rol y responsabilidad para la seguridad de información está claramente definido, a cada una de funcionarios o colaboradores se le ha asignado una responsabilidad con el Sistema de Gestión Seguridad de información, la gestión de riesgos y la evaluación de riesgo residual es responsabilidad de los Líderes de procesos con el apoyo de la Oficina de Riesgos.

6.1. CONSEJO DE ADMINISTRACIÓN

a) Aprobar la política de seguridad de la información y sus modificaciones.
b) Definir y promover la dirección estratégica para la seguridad de la información.
c) Proporcionar los recursos para la adecuada implementación de la seguridad de la información.
d) Proporcionar, velar y apoyar la implementación y asignación del Sistema de Seguridad de Información.
e) Autorizar, facilitar e integrar la puesta en operación del sistema de seguridad de la información, mediante la definición de mecanismos y la supervisión e integración por parte de cada líder de proceso.
f) Velar por el cumplimiento de las obligaciones regulatorias en materia de seguridad de la información.
g) Velar por la disponibilidad de los recursos y su uso apropiado.
h) Designar los responsables de la implementación del sistema de seguridad de la información.
i) Pronunciarse y hacer seguimiento a los informes trimestrales que presente el representante legal, dejando constancia en las actas de las reuniones respectivas.
j) Aprobar las evaluaciones de riesgo de seguridad de la información resultantes.
k) Revisar que la estrategia de seguridad de la información se encuentre alineada con los objetivos de la Cooperativa.
l) Revisar y aprobar las actualizaciones al Sistema de Gestión de Seguridad de la Información (SGSI), para garantizar su continua conveniencia, idoneidad y efectividad.
m) Establecer las prioridades de los proyectos e iniciativas relacionadas con la seguridad de la información.
n) Uso con responsabilidad de los recursos de información de la Cooperativa.

6.2 REPRESENTANTE LEGAL

Sin perjuicio de las funciones asignadas en otras disposiciones al representante legal, frente al sistema de seguridad de la información le corresponde:

a) Velar por el desarrollo de los objetivos estratégicos para la seguridad de la información, definidos por el consejo de administración.
b) Velar por la implementación de la política de seguridad de la información.
c) Facilitar la integración entre los diferentes líderes de procesos de negocio para lograr la implementación del modelo de seguridad de la información.
d) Velar por la disponibilidad de los recursos y su uso apropiado.
e) Velar por la correcta aplicación de los controles de seguridad para reducir el riesgo de seguridad de la información

f) Velar por la designación de los responsables de la implementación de la política de seguridad de la información.
g) Presentar un informe periódico, como mínimo trimestral, al Consejo de Administración sobre la evolución y aspectos relevantes de la seguridad de la información incluyendo, entre otros, las acciones preventivas y correctivas implementadas o por implementar, seguimiento y resultados de mediciones y cumplimiento de objetivos de seguridad de la información.
h) Uso con responsabilidad de los recursos de información de la Cooperativa.

6.3 AUDITORÍA INTERNA O QUIEN EJERZA CONTROL INTERNO

Sin perjuicio de las funciones asignadas en otras disposiciones a la auditoría interna, o quien ejerza el control interno, ésta debe:

a) Tener conocimiento apropiado en materia de seguridad de la información y de esta normativa en particular.
b) Evaluar periódicamente la efectividad y cumplimiento de todas y cada una de las etapas y los elementos clave del sistema de seguridad de la información, con el fin de determinar las deficiencias y sus posibles soluciones.
c) Informar los resultados de la evaluación de la seguridad de la información al consejo de administración.
d) Se designa al jefe de sistemas y al Administrador de Riesgos como responsables de realizar una verificación mínima anual al cumplimiento de las políticas aquí establecidas.

6.4 ADMINISTRADOR DE RIESGOS

Liderar la generación de lineamientos para gestionar la seguridad de información y asesorar en la implementación de controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad.

Actualizar las Políticas de Seguridad Digital con frecuencia anual, con sus roles y responsabilidades.

Socializar las políticas de seguridad de información con periodicidad mínima anual.

6.5 TODO EL PERSONAL Y DEMAS USUARIOS

Los funcionarios y todo el personal provisto por terceras partes que realicen labores en o para la Cooperativa Grancoop, tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de información aquí establecidos.

6.6 RESPONSABILIDADES Y RECURSOS

En el presente manual de políticas de seguridad de información está definido los cargos asociados a la seguridad de la información, respecto a las funciones y responsabilidades en la seguridad de la información.
Adicionalmente, los colaboradores y directivos son capacitados, al momento de su vinculación y durante la permanencia en la Cooperativa, y constantemente el área de riesgos comparte información referente a la seguridad de la información con el objeto de concientizar y educar sobre la seguridad de la información, dichas capacitaciones incluyen:

a) Toda la información a los funcionarios sobre la postura, estrategias y políticas de seguridad de la información de la organización.

b) Proceso disciplinario para incidentes de seguridad de la información, violaciones a la privacidad, piratería informática, fraude y espionaje industrial, por parte de los trabajadores.

c) Nuevos roles, responsabilidades y prácticas de trabajo.

6.7 GESTION DE RIESGOS

En pro de minimizar las vulnerabilidades y posibilidad de materializarse riesgos de pérdida de información, que a su vez afectan la economía y reputación de la Cooperativa, se ha definido un plan de tratamiento de riesgos de seguridad de información (Anexo 2), que permitirá:

a) Tener comprensión de las amenazas, las vulnerabilidades, y el perfil de riesgo de la Cooperativa.

b) Tener entendimiento de la exposición al riesgo y las posibles consecuencias para el negocio.

c) Crear conciencia de las prioridades de la gestión de riesgos con base en las posibles consecuencias de materialización.

d) Definir e implementar estrategias organizacionales adecuadas para la mitigación de riesgos para obtener consecuencias aceptables.

e) Fijar la atención organizacional con base en un entendimiento de las posibles consecuencias del riesgo residual.

f) Conservar información documentada del proceso de gestión de riesgos de seguridad de la información.

La gestión de riesgos consiste en la identificación, medición de riesgo inherente, establecimiento de controles y medición de efectividad de los mismos, calculo de riesgo residual y seguimiento a los eventos de riesgos y planes de acción para la mitigación de riesgos. A través de una matriz de riesgo y mapa de calor, se compara la evolución del perfil de riesgo inherente, riesgo residual y se observa la efectividad de los controles diseñados.

6.7.1 Nivel aceptable de riesgo

Grancoop determina aceptar los riesgos identificados en el Sistema de gestión de seguridad de información, una vez aplicados los controles existentes, presenten un nivel de riesgo residual que se encuentren en la escala entre Moderado y bajo, aquellos riesgos cuyo nivel de riesgo residual sea Alto o Extremo se deberá definir como fortalecer el control existente o determinar un nuevo control con el objeto de disminuir el nivel de riesgo. Sin embargo, aquellos que se encuentren en nivel moderado es importante establecer plan de acción con el fin mitigar la probabilidad de afectar la disponibilidad, integridad y confiabilidad de la información.

7. SISTEMA DE SEGURIDAD DE LA INFORMACION

El sistema de seguridad de la información de Grancoop cuenta con los siguientes puntos:

Políticas de seguridad de la información que identifica e incorpora temas propios de seguridad, normativa aplicable, tipo de información sensible, identificación de la clasificación de la información, responsables y niveles de autorización.

Con periodicidad anual se llevará a cabo un proceso de revisión al cumplimiento de las políticas de seguridad de información, los resultados y hallazgos de esta verificación serán socializados a todo el personal como actividad de retroalimentación y así alinearnos cada vez con los objetivos de la organización solidaria.

Estas políticas de seguridad de información e instrucciones son aprobadas por el Consejo de Administración y deberán ser revisadas por lo menos una vez al año.

Una vez aprobadas se publican a través de los medios de comunicación usados habitualmente y acompañarlo con una socialización a todos y cada uno de los integrantes de la Cooperativa.

En la socialización de las políticas de seguridad de información se realizarán evaluaciones de conocimiento al personal, para garantizar que han sido leídas y que se aplican de acuerdo a lo establecido.

Como proceso de mejora, se aplicarán controles de seguridad bajo parámetros previamente establecidos para su medición, que deben generar como resultado los aspectos a corregir, los cambios que se deben realizar o, la identificación de nuevos riesgos, para ello será necesario los resultados obtenidos de la revisión periódica anual, que evidencien el recurrente incumplimiento a las políticas, con base a ello se tomarán decisiones de actualización de dichas políticas, sugerencias por las partes interesadas y la oportunidad de cambios tecnológicos.

8. RECURSOS

La Cooperativa cuenta con los recursos necesarios para el establecimiento e implementación del Sistema de Seguridad de la Información, considerando lo siguiente:

- Presupuesto de recursos económicos: el jefe de sistemas y Asistente Administrativa incluirá en su presupuesto los recursos requeridos para el mantenimiento y funcionalidad del sistema de seguridad de información, el cual contempla la criticidad de los activos de información involucrados, las herramientas tecnológicas que apoyen a la protección de los activos de información y el proceso de mejora continua.

- Recurso humano: Grancoop cuenta con personal competente necesario para responsabilizarse de la seguridad de la información y la gestión de los riesgos asociados, evaluar la eficacia de las acciones tomadas y garantizar la información documentada.

- Comunicación a través de correo electrónicos y en carpeta compartida a los responsables de entrega de productos y servicios y demás colaboradores para que consulten los requisitos exigidos en cualquier momento.

9. POLÍTICAS ESPECÍFICAS

9.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

A continuación, se definen los roles y responsabilidades para la administración, operación y gestión de la seguridad de la información.

9.1.1 ORGANIZACIÓN INTERNA.

La Administradora de Riesgos será responsable de revisar y proponer a las directivas para su aprobación, el texto de la Política de Seguridad de la Información, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejoras en pro de la seguridad de la información. Es responsabilidad de dicho cargo definir las estrategias de capacitación en materia de seguridad de la información al interior de Grancoop.

El jefe de Sistemas es responsable de implementar los controles tecnológicos (Seguridad Informática) en pro de la seguridad de la información.

La Asistente Administrativa proporcionará los mecanismos para propender por notificar a todo el personal que se vincula contractualmente con la Cooperativa, de las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan como recomendación del jefe de Sistemas y de la Administradora de Riesgos.

La Asistente Administrativa en apoyo con el Asesor Jurídico propenderá porque en todos los contratos que suscriba la Cooperativa quede consignada la cláusula de confidencialidad y la obligatoriedad tanto de trabajadores, directivos y terceros de dar cumplimiento a las políticas de seguridad de la información y tratamiento de datos personales.

Todos los usuarios de la información tienen la responsabilidad y obligación de cumplir con las políticas de seguridad de la información establecidas en el presente manual. Los jefes de cada Área deben asegurarse que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad, se realicen correctamente para lograr el cumplimiento de las políticas.

9.1.2 USO DE DISPOSITIVOS MÓVILES

La Cooperativa proveerá las condiciones necesarias para el manejo de dispositivos móviles Corporativos (Teléfonos Móviles, Teléfono inteligentes Smart phones, tablets, portátiles, etc.) que hagan uso de los servicios de la Cooperativa, como también velará porque se haga uso responsable de los equipos y servicios proporcionados tanto dentro como fuera de las oficinas de la Cooperativa.

Políticas dirigidas a: jefe de Sistemas.

- Investigar y probar las opciones de protección de los dispositivos móviles Corporativos que hagan uso de los servicios provistos por la Cooperativa.

Políticas dirigidas a: Todos los usuarios

- Los dispositivos móviles deberán contar con una clave de acceso, así como realizar los cambios periódicos que solicite el equipo.
- Evitar al máximo sostener conversaciones de información confidencial o privada de los Titulares por vía telefónica en lugares de alta concurrencia de público.
- El teléfono móvil siempre debe estar bajo la custodia del responsable y no se deben dejar desatendidos.
- Las acciones que se generen con los dispositivos móviles son únicamente responsabilidad del colaborador.
- Informar la pérdida o el robo del dispositivo tan rápido como sea posible al área de Sistemas, para proceder con el borrado del perfil Corporativo y evitar la pérdida de los datos y a la Asistente Administrativa para dar de baja el inventario y realizar el proceso legal pertinente.
- Está prohibido almacenar datos personales en dispositivos móviles de la Cooperativa.
- Abstenerse de prestar los equipos móviles para realizar llamadas o envío de cualquier información a través de estos a personas ajenas a la cooperativa.
- Se autoriza el uso de WhatsApp solo en dispositivos suministrados por la cooperativa, no se permite el envío de fotografías, audios y videos o cualquier otro archivo cuyo contenido no sea de carácter laboral y destinado para tal fin.
- No están autorizados a cambiar la configuración, desinstalar software, formatear o restaurar de fabrica los equipos móviles corporativos, cuando se encuentren a su cargo, únicamente deben aceptar y aplicar las actualizaciones.

9.1.3 POLÍTICAS DE INTERCAMBIO DE INFORMACION

- No estará permitido intercambiar información con entidades externas sin la debida autorización y acuerdos de confidencialidad que garantice los tratamientos de información pertinentes.
- Cuando se envié información sensible por correo electrónico, se debe colocar clave a los archivos adjuntos y está debe ser informada al destinatario por un medio diferente al correo electrónico.
- Los empleados de las organizaciones y de las empresas aliadas deben estar cubiertos con acuerdos de confidencialidad y, por lo tanto, serán responsables de la entrega de información no autorizada.
- En caso de ser necesario el envío y la recepción de información confidencial con los terceros contratados, se debe proteger con mecanismos de cifrado fuerte.
- La información sensible disponible al público a través de la página web, debe estar protegida por sitios seguros y, adicionalmente, con usuario y clave de acceso.
- La comunicación con entidades externas para el intercambio de información crítica se debe hará a través VPN o webservices y su configuración está a cargo del personal del área de sistemas.
- La información que viaja entre las oficinas, deberá estar cifrada usando hardware de propósito específico, o software, o una combinación de los anteriores, los cuales estarán totalmente separados e independientes de cualquier otro dispositivo o elemento de procesamiento de información, de seguridad informática, de transmisión y/o recepción de datos, de comunicaciones, de conmutación, de

enrutamiento, de gateways, servidores de acceso remoto (RAS) y/o de concentradores. En cualquiera de los casos anteriores se empleará cifrado fuerte.

- El jefe de sistemas deberá evaluar con regularidad la efectividad y vigencia de los mecanismos de cifrado adoptados.
- Es responsabilidad de los dueños de la información crítica no dejar copias impresas o documentos físicos en lugares de fácil acceso a personal no autorizado.

9.1.4 ACCIONES NO AUTORIZADAS

- Transmisión de contenido fraudulento, difamatorio, obsceno, ofensivo o de vandalismo, insultante o acosador, sea este material o mensajes.
- Interceptar, recopilar o almacenar datos sobre terceros sin su conocimiento o consentimiento.
- Escanear o probar la vulnerabilidad de equipos, sistemas o segmentos de red.
- Enviar mensajes no solicitados (spam), virus, o ataques internos o externos.
- Obtener acceso no autorizado a equipos, sistemas o programas, tanto al interior de la red como fuera de ella.
- No se podrá utilizar la red WIFI para obtener, manipular y compartir cualquier archivo de tipo musical o filmográfico, sin tener los derechos de propiedad intelectual.
- Dañar equipos, sistemas informáticos o redes y/o perturbar el normal funcionamiento de la red. Ser usada con fines de lucro, actividades comerciales o ilegales, por ejemplo, hacking. Ser utilizada para crear y/o la colocar un virus informático o malware en la red.
- Transmitir, copiar y/o descargar cualquier material que viole cualquier ley. Esto incluye entre otros: material con derecho de autor, pornografía infantil, material amenazante u obsceno o material protegido por secreto comercial o patentes.

9.2 SEGURIDAD DEL RECURSO HUMANO

Para Grancoop el factor humano es clave en la obtención de los objetivos organizacionales, por eso busca contar con personal capacitado cuyas competencias y cualidades cumplan con los requisitos exigidos por la Cooperativa para cada puesto de trabajo.

9.2.1 ANTES DE ASUMIR EL EMPLEO

<u>Selección</u>

Políticas dirigidas a: Asistente Administrativa

- Debe validar la veracidad de la información suministrada por el candidato antes de su vinculación.

- Debe elaborar con apoyo de la asesoría jurídica las cláusulas de confidencialidad, de protección de datos personales y seguridad de la información al inicio del vínculo laboral, garantizar que los colaboradores de la Cooperativa firmen estos compromisos y mantener en la carpeta de cada uno.

9.2.2 DURANTE LA EJECUCIÓN DEL EMPLEO

Políticas dirigidas a: Asistente Administrativa

- Exigirá a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y lineamientos establecidos por la Cooperativa.

Políticas dirigidas a: Gerentes, jefes y Asistente Administrativa

- Todos los colaboradores de Grancoop con periodicidad mínima anual y cuando sea necesario, los terceros que presten servicios en la Cooperativa, recibirán una inducción sobre las políticas y lineamientos de seguridad de la información, además de los procedimientos que apliquen para tal fin en sus labores o actividades desarrolladas en la Cooperativa.

9.2.3 TERMINACIÓN Y CAMBIO DE EMPLEO.

Políticas dirigidas a: Asistente Administrativa

- Deberá reportar al jefe de Sistemas y demás jefes de áreas, los cambios de cargo y/o área, para que se realice el proceso de remover los accesos anteriores.

- Cuando un trabajador termine su vinculación laboral, reportará al jefe de Sistemas y demás jefes de área esta novedad, en lo posible, el mismo día que se conozca el hecho.

Políticas dirigidas a: jefe de Sistemas y demás jefes de área.

- Bloqueará todos los accesos de un colaborador a los sistemas de información de la Cooperativa, en la fecha que indique la Asistente Administrativa de la terminación de su contrato de trabajo.

- Bloqueara todos los accesos de un colaborador a las plataformas externas que manejen información bajo la responsabilidad de la Cooperativa, en la fecha que indique la Asistente Administrativa de la terminación de su contrato de trabajo.

- Realizar cambios de claves de acceso en cada una de las plataformas externas que manejan información de la Cooperativa, al momento de rotación o desvinculación de personal.

9.3 GESTIÓN DE ACTIVOS QUE CONTIENEN INFORMACION

La Cooperativa, como propietaria de la información que maneja, tanto física como digital en sus sistemas de información, asigna responsabilidades a los Gerentes, jefes y directores de oficina, asegurando el cumplimiento sobre el uso adecuado de los activos de información.

9.3.1 INVENTARIO

Políticas dirigidas a: Asistente Administrativa

- La Cooperativa contará con un inventario actualizado de activos de información y otros activos asociados con la información, el cuál estará a cargo de la asistente administrativa. En este inventario se debe identificar los activos asociados con información e instalaciones de procesamiento de información y especificar los siguientes aspectos:

    - Datos digitales
    - Información impresa
    - Software
    - Infraestructura
    - Servicios de información y proveedores de servicios
    - Seguridad física
    - Relaciones comerciales
    - Responsables de los activos.

- Revisar el inventario con una periodicidad mínima de una vez al año.

- Procedimiento y condiciones generales para mantener el inventario en una condición razonablemente completa, precisa y actualizada a pesar de los cambios de equipo, personal, nuevos sistemas, etc.

    - La información debe ser clasificada por el dueño de la información y este a su vez debe informar a la Entidad sobre su clasificación de manera que la Entidad tome las medidas requeridas para preservar la confidencialidad e integridad de la misma.
    - Todos los aplicativos o sistemas de información necesariamente deben tener asignado un "propietario", el cual es el encargado de definir los niveles de privacidad de la información, así como los usuarios y permisos que cada uno deba tener sobre ella.
    - El dueño de la información es responsable por la actualización de la clasificación de la información de acuerdo a los cambios de la Cooperativa.
    - El dueño de la información es autónomo de reclasificarla cuando lo considere necesario y debe cambiar del rotulo o etiqueta y notificar a los usuarios y custodios.
    - Los responsables del proceso de gestión tecnológica son claramente custodios. Siempre que la información sea almacenada en un computador personal, el usuario inmediatamente será su custodio.
    - Los usuarios son responsables de familiarizarse y atender todos los aspectos de la política de seguridad. En caso de existir dudas por parte de los usuarios con respecto a la manipulación apropiada de la información estas deben ser consultadas con el custodio o dueño.

- Es deber de los responsables efectuar la clasificación de la información de acuerdo con los patrones definidos por este procedimiento.
- La información, datos y documentos deben ser claramente identificados, de manera que todos los usuarios estén enterados de su nivel de clasificación. Para ello deben de registrarlos en el Formato Inventario y Clasificación de Activos
- Se debe firmar un acuerdo de confidencialidad con terceras partes, en caso de requerir entregar información electrónica o escrita confidencial o interna, con las restricciones de su uso.
- Se deben utilizar los mecanismos apropiados de control de acceso a la información dependiendo de su nivel de clasificación.
- Los empleados, contratistas o terceros no pueden tomar información secreta, confidencial o interna cuando dejan de trabajar para la Entidad.
- Destrucción de Información secreta, confidencial o interna: Cuando ya no se requiera una información clasificada como confidencial/reserva o interna, debe ser destruida mediante un método aprobado por seguridad de la información.
- Se debe borrar la información secreta, confidencial o interna de los medios magnéticos por un método o programa aprobado por Seguridad de la Información, cuando se requiere deshacerse del medio o equipo, enviar a servicio técnico o devolver a su proveedor.
- En caso de enviar los equipos a mantenimiento o asignarle el equipo a una persona diferente que contenga información confidencial/reserva, la información debe ser borrada de manera que no sea posible su recuperación.
- Los equipos portátiles que contengan información secreta o confidencial, deben tener los mecanismos necesarios para evitar que ante la pérdida del equipo una persona no autorizada pueda acceder a la información almacenada.
- Información clasificada como confidencial/reserva o interna, al ser enviada a la impresora se tendrá acceso a través de un usuario y una clave, evitando que personal no autorizado tenga acceso a ésta.
- En el caso de envió por medio de correo electrónico fuera de la Cooperativa Grancoop de información secreta o confidencial requiere que el correo vaya firmado y utilice un esquema de cifrado.
- Los empleados de los terceros con los cuales la Cooperativa Grancoop tiene acuerdos comerciales no deben revelar información confidencial a terceras partes a menos que el originador de la información haya aprobado su revelación y la parte que la reciba haya firmado un acuerdo de confidencialidad.
- Con el fin de realizar el inventario, la clasificación y etiquetado de los activos de información los responsables deben utilizar el Formato de Inventario y Clasificación de Activos de Información
- La Asistente Administrativa y RRHH verificará que los activos de información se encuentren debidamente etiquetados de acuerdo a su clasificación, los líderes de procesos serán responsables de notificar cualquier cambio o adicción en sus activos de información de manera oportuna.
- Este procedimiento se debe realizar por lo menos una vez cada año o cuando se cree un nuevo activo de información no incluido en el inventario.

Propiedad de los Activos de Información

Políticas dirigidas a: jefe de Sistemas

- Es el responsable de los activos de información correspondientes a la plataforma tecnológica de la Cooperativa y, en consecuencia, debe asegurar su apropiada operación y administración.
- En conjunto con la Gerencia General, son quienes deben autorizar la instalación, cambio o eliminación de componentes de la plataforma tecnológica de la Cooperativa.
- Debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.
- Es responsable de preparar las estaciones de trabajo fijas y/o portátiles de los colaboradores y de hacer entrega de estas.

Uso aceptable de los activos

Políticas dirigidas a: Todos los usuarios

- Todos los colaboradores, directivos y terceros deberán ser responsables del uso que hacen de cualquier activo de información o de cualquier recurso de procesamiento de la información, el cual deberá ser conforme a los requisitos de seguridad de la información de la Cooperativa y con el único fin de llevar a cabo las labores de Grancoop, por consiguiente, no podrán ser utilizados para fines personales o ajenos a este.

Devolución de Activos de Información

Políticas dirigidas a: jefe de Sistemas

- Es responsable de recibir los equipos de trabajo fijo y/o portátil para su reasignación o disposición final.

- Es responsables de generar copias de seguridad de la información de los colaboradores que se retiran o cambian de labores, cuando les es formalmente solicitado a través de la Asistente administrativa.

Políticas dirigidas a: Todos los usuarios

- Todos los colaboradores, directivos de Grancoop y terceros deberán devolver todos los activos fijos que se encuentren a su cargo al terminar su empleo, contrato o acuerdo.

9.3.2 CLASIFICACIÓN DE LA INFORMACIÓN

La clasificación de la información constituye un elemento importante en la gestión de riesgos, ya que determina las necesidades, prioridades y el grado de protección necesario para cada tipo de información.

Toda Información utilizada en la Cooperativa, debe ser clasificada de la siguiente manera:

Pública: aquella que no cuenta con restricciones, por lo que su circulación puede darse a nivel interno y externo, sin que cause impacto negativo a la Cooperativa. Este tipo de información puede ser divulgada al público en general.
De uso Interno: Es aquella que es propia de la operación de los procesos de la Cooperativa. El acceso no autorizado a la información de uso interno podría ocasionar daños y/o inconvenientes menores a la Cooperativa.
Su uso es exclusivo del personal interno de la Cooperativa: No está permitida su divulgación a terceros, salvo que exista un requerimiento de orden legal, contractual o reglamentario que así lo establezca.

Privada: Es toda aquella que tiene un contenido que solo puede ser conocida por ciertas personas debido a sus funciones y cargos. Su uso es restringido y una divulgación no autorizada podría implicar un impacto negativo para la Cooperativa. Debe contar para su circulación con autorización del responsable de la información.

Confidencial: Es aquella información secreta, que pueda usarse en alguna actividad empresarial o comercial. Tiene un valor comercial por ser secreta y es objeto de medidas de seguridad razonables. Su divulgación no autorizada podría implicar un impacto muy negativo para la Cooperativa. Su uso es restringido. Este tipo de información puede ser divulgada a personas internas (Colaboradores y directivos) y/o externas a la Cooperativa con la debida autorización del responsable de la información.

Sensible: La Información Sensible es toda aquella que incorpore datos personales de categoría especial, según lo establecido por el artículo 5 de la Ley 1581 de 2012. Su circulación no autorizada constituye una causal de incumplimiento sancionable por la Superintendencia de Industria y Comercio. Su uso es reservado, estando autorizado sólo para determinadas personas según clasificación legal o reglamentaria. Requiere de los máximos controles de seguridad para su tratamiento.

<u>Clasificación de la Información</u>

Políticas dirigidas a: Asistente Administrativa.

- Clasifica los activos de información según los niveles de clasificación establecidos.

Políticas dirigidas a: jefe de Sistemas

- Debe efectuar la eliminación segura de la información en el equipo, ya sea por dada de baja o cambio de usuario.

Políticas dirigidas a: Todos los usuarios

- Los usuarios deben acatar las normas de la clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la Cooperativa.
- Informar a la Asistente administrativa la adquisición de nuevos activos de información para la actualización del inventario.
- La información física y digital de la Cooperativa debe tener un período de almacenamiento que puede ser dictaminado por requerimientos legales o por la Cooperativa.
- Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen y saquen copias: verificar las áreas adyacentes a impresoras, escáneres y fotocopiadoras para asegurarse que no quedaron documentos relacionados o adicionales; así mismo, recoger de las impresoras, escáneres y fotocopiadoras, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.
- Todos los usuarios deben asegurarse de que, en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desarrollo de sus labores.

Políticas dirigidas a: jefe de Sistemas y Asistente administrativa

- En el momento de dar de baja los activos de información, la Asistente Administrativa junto con el jefe de Sistemas se encargarán de gestionar la adecuada disposición de los equipos tecnológicos, así como su reutilización y borrado seguro de la información.

9.4 CONTROL DE ACCESO

El Área de Sistemas como responsable de las redes de datos y los recursos tecnológicos debe propender por implementar medidas de seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización, con el fin de impedir accesos no autorizados a los sistemas de información, bases de datos y servicios de red, controlar la conexión entre la red de la Cooperativa y otras redes públicas, revisar las actividades que llevan a cabo los usuarios en los sistemas y asignar responsabilidades frente al uso de contraseñas y equipos.

9.4.1 REQUISITOS DE LA COOPERATIVA PARA CONTROL DE ACCESO

Política de control de acceso

Políticas dirigidas a: jefe de Sistemas

- Restringir el acceso de todo el personal (incluyendo contratistas y visitantes) a los Datacenter y Centros de Cableado y sólo pueden acceder a través de su autorización.
- Para preservar la seguridad de los equipos de los servidores y equipos de comunicaciones y, en general, todos los dispositivos de los Datacenters, centros de cableado y los armarios (Racks), deben permanecer cerrados y al final del día dejar asegurado con llave, de la cual se contarán con dos copias, una para el jefe de sistema y otra para la asistente administrativa.
- Para el uso de cámaras de video adquiridos para supervisar el acceso físico de personas a la Cooperativa, áreas críticas o que resguardan información confidencial, se establece el siguiente procedimiento de tratamiento de copias:
  - **Frecuencia de operaciones del sistema de seguridad y vigilancia:** El sistema de seguridad y vigilancia operará las veinticuatro (24) horas del día, los 365 días del año, estando sujeto a cualquier desperfecto mecánico imprevisto ya sea por fallas técnicas o por inclemencias del tiempo (fuertes lluvias o tormentas eléctricas)
  - **Instalación de los equipos de vigilancia:** El jefe de Sistemas es el encargado de la instalación de las cámaras y los equipos necesarios para el funcionamiento del sistema de seguridad y vigilancia, además se encargará de proveer el mantenimiento necesario para que puedan funcionar de manera efectiva y se puedan mantener en condiciones óptimas.
  - **De la ubicación de las cámaras**: Las cámaras de seguridad estarán ubicadas en lugares estratégicos específicamente para la seguridad y vigilancia de las instalaciones de la Cooperativa Grancoop.
  - **Monitoreo de Cámaras:** La Asistente Administrativa y el jefe de Sistemas podrán monitorear las cámaras en cualquier momento del día para verificar que todo se encuentre en orden, en caso de que la Asistente Administrativa observe algún fallo en las grabaciones deberá reportarlo al Jefe de Sistemas. Se dará acceso a las cámaras externas dispuestas para vigilar el perímetro, y de las cámaras de la entrada de la Oficina principal de Cali a la empresa de seguridad, quienes realizaran un monitoreo aleatorio de las mismas. Así mismo las rondas que realizan los agentes de la empresa de seguridad, deberán de informar al jefe de Sistemas si es que alguna cámara de seguridad y vigilancia está en mala posición o si tiene algún percance o desperfecto para su normal funcionamiento.
  - **Revisión de las grabaciones:** En caso de algún evento en el que se deba recurrir a revisar las grabaciones de las cámaras de seguridad se cuenta con un periodo máximo de dos meses para la oficina de Cali, y de un mes para la Oficina de Palmira. Solo se encuentran autorizados para esta revisión el jefe de Sistemas y la Asistente Administrativa a través de un aplicativo al cual se acceder con usuario, contraseña y sistema de reconocimiento facial.
  - **Tiempo de Custodia de las grabaciones**: Se establece dos meses para que este en custodia el archivo histórico del sistema informático para la oficina de Cali y un mes para la oficina de Palmira. Las grabaciones que resulten del sistema de seguridad y vigilancia se guardaran y mantendrán en

la memoria del servidor (DVR) una vez utilizado todo el espacio en el disco de memoria del DVR, el sistema automáticamente remplazara las grabaciones anteriores por unas nuevas.

- **Para el almacenamiento de las grabaciones. -** El jefe de Sistemas es el encargado directo del almacenamiento y el custodio de las grabaciones que resulten del sistema de seguridad y vigilancia.

- Para impedir el acceso a conexiones o puntos de red de acceso público, dispositivos de telecomunicaciones, manuales, hardware de redes o comunicaciones y líneas de telecomunicaciones se implementa como control físico la inhabilitación desde el centro de cableado de aquellos puntos que no están en servicio los siguientes.
- Revisar los accesos a la red y sistemas de información solicitados por los jefes y Gerencias de Área para la asignación de privilegios de usuarios.
- Realizar la revisión anual de los derechos de acceso y uso de la información, de conformidad con los cambios informados por la Asistente Administrativa referentes a ingresos, ascensos y retiros.
- Capacitar y concientizar a los usuarios sobre el uso apropiado de los sistemas de información, redes, contraseñas y estaciones de trabajo.

- Implementar mecanismos para la activación y desactivación de derechos de acceso a las redes y sistemas de información.

Políticas dirigidas a: Asistente Administrativa

- Reportar inmediatamente a todo el personal de la Cooperativa, el ingreso, retiro y ascensos de colaboradores para habilitar y deshabilitar los accesos concedidos tanto en el área de sistemas, como en otras aplicaciones administradas por otras áreas según sea el caso.

Políticas dirigidas a: Gerentes o jefes de Área

- Dar autorización de creación de perfiles, suministro de accesos y privilegios para los colaboradores que usan los servicios de red.

Políticas dirigidas a: Todos los usuarios

- Todos los usuarios de los servicios de información son responsables del manejo de sus datos de autenticación para el uso y acceso a los recursos informáticos de la Cooperativa.

- Los usuarios deben mantener en secreto su información de autenticación a los sistemas y plataformas externas.

- Los usuarios son responsables de todas las actividades realizadas con su identificador ID en la red.

- Los usuarios deben hacer un uso correcto de la información a la cual tienen acceso.

- Los usuarios deben hacer uso de los datos e información contenidos en los recursos informáticos de la empresa, única y exclusivamente para fines administrativos u operativos y en razón a las funciones asignadas.

9.4.2 GESTIÓN DE ACCESO DE USUARIOS

Suministro de Acceso de Usuarios

Políticas dirigidas a: jefe de Sistemas

- El jefe de Sistemas debe establecer ambientes separados para desarrollo, pruebas y producción, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad en producción.

- El jefe de Sistemas debe controlar que los desarrolladores no tengan acceso a los ambientes de producción, excepto que cuente con autorización del jefe de Sistemas.

Políticas dirigidas a: Gerentes y jefes de Área

- Deben autorizar los accesos a sus aplicativos o sistemas de información, de acuerdo con los perfiles establecidos.

Gestión de información secreta para la autenticación de usuarios.

Políticas dirigidas a: Asistente Administración.

- La Cooperativa incluirá en los contratos de trabajo de los colaboradores una cláusula de confidencialidad de identificación de acceso con el fin de proteger la integridad y confidencialidad de la información.

9.4.3 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES

Procedimiento de ingreso (Log-On) seguro

Políticas dirigidas a: jefe de Sistemas

- Al momento de la asignación de usuarios, verificar que el cargo, rol, área de trabajo y dependencia correspondan a la solicitud.

- Todas las contraseñas de servicios, servidores o elementos de comunicación deben ser cambiadas inmediatamente se ponga en ambiente productivo y por ninguna razón deben de quedar con las contraseñas por defecto o asignadas por terceros.

Políticas dirigidas a: Todos los usuarios

- El usuario, en el primer inicio de sesión, debe cambiar la contraseña inicial asignada por el Área de Sistemas, según se lo indiquen, en cada uno de los sistemas.

- El usuario no debe mostrar la contraseña al momento de ser digitada para la autenticación.

- Debe guardar secreto de las credenciales y no apuntarlas en documentos o dispositivos que sean de fácil acceso a terceros.

- Verificar que el puesto de trabajo no tenga indicios de manipulación por parte de otro personal.

- Verificar que las conexiones del cableado eléctrico, de comunicaciones y periféricos, estén bien conectados y no se les haya cambiado de enchufe o puerto y que adicionalmente no tengan ningún dispositivo entre ellos y el computador o equipo del sistema de información.

- Ubicarse en su estación de trabajo de manera cómoda, pero observando que nadie pueda espiar sus credenciales de acceso a su espalda o de lado.

- Abstenerse de compartir las credenciales con otros usuarios bajo cualquier circunstancia, excepto en los casos que se necesite replicar un determinado caso con el personal de Sistemas.

- Notificar inmediatamente al Gerente o jefe responsable de área cualquier indicio de que sus credenciales hayan sido comprometidas o usadas por otros usuarios.

Sistema de Gestión de Contraseñas

Políticas dirigidas a: jefe de Sistemas

- Todos los sistemas de información de Grancoop, propenderá por tener las siguientes características mínimas en su autenticación.

  - Imponer el uso de contraseñas individuales para determinar responsabilidades.
  - Permitir que los trabajadores puedan cambiar sus propias contraseñas.
  - En lo posible se recomienda al momento de crear contraseñas de calidad con las siguientes características:

- Una longitud mínima de 8 caracteres alfanuméricos, al menos una letra mayúscula y un número.
- Cambiar la contraseña como mínimo cada 60 días.
- Informar a los trabajadores cambiar las contraseñas en el primer ingreso al sistema cualquiera que este sea.

Uso de Programas Utilitarios Privilegiados

Políticas dirigidas a: Todos los usuarios

- No se permite el uso de herramientas, programas o técnicas que vulneren los controles que se han establecido.
- Los sistemas de seguridad como antivirus, prevención de perdida de datos instalados en los equipos de cómputo de Grancoop, no deben de ser deshabilitados, interferidos o burlados de ninguna manera.

Control de acceso a Códigos Fuente de programas

Políticas dirigidas a: jefe de Sistemas

- Debe establecer las medidas de seguridad para que solo el personal autorizado tenga acceso a los códigos fuentes y que no sean modificados sin autorización.

9.5 SEGURIDAD FÍSICA Y DEL ENTORNO.

La Cooperativa velará por la implantación de mecanismos de seguridad física que garanticen el perímetro de las instalaciones en todas sus sedes, también propenderá por controlar las amenazas físicas externas e internas y las condiciones medioambientales.

9.5.1 ÁREAS SEGURAS

Controles de acceso físico.

Políticas dirigidas a: jefe de Sistemas y Asistente Administrativa

- Se debe tener acceso controlado y restringido al cuarto del servidor principal y centro de cableado, para ello deberá mantenerse cerrado con llave cuyo control será del jefe de sistemas o quien éste autorice en su ausencia.

- Grancoop cuenta con sensor y alarma para la detección de intrusos de la organización.

- Adicional se cuentan con botones de pánico alertan a la central de seguridad de la empresa contratada sobre situaciones irregulares que estén presentando en las instalaciones.

- Con periodicidad anual se realizarán pruebas al sistema de sensor, alarmas y botones de pánico.

- Todas las instalaciones de Grancoop tanto oficina principal, como las agencias de palmira y Tuluá contarán con sistema de cámara de video, las cuales serán de monitoreo por parte de la Asistente Contable y el jefe de sistemas.

- Cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información o de procesamiento de datos críticas para Grancoop, contará con una barrera como una pared, una puerta con control de acceso o un escritorio o recepción atendido por un funcionario de Grancoop.

  <u>Protección contra amenazas externas y ambientales</u>

  Políticas dirigidas a: jefe de Sistemas

- Los servidores de Grancoop deben ser mantenidos en un ambiente seguro y protegido, para ello se deberá contar además del control de acceso:
  - ✓ Detector de temperatura.
  - ✓ Detector de humo
  - ✓ Bajo riesgo de inundación.
  - ✓ Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).
  - ✓ Realizar mantenimiento y pruebas de funcionamiento con periodicidad mínima anual a la UPS.
  - ✓ Cámara para monitoreo al centro de cómputo principal.
  - ✓ Cuenta con un sistema de aire acondicionado para control y soporte de calor
  - ✓ Garantizar el suministro de energía cuando para no afectar los sistemas y servicios cuando se presenten fallas de energía, para ello Grancoop deberá contar con una planta eléctrica como sistema de suministro eléctrico redundante.
  - ✓ Deberá realizar pruebas a la planta una vez por semana y con periodicidad anual se deberá realizar mantenimiento a la planta eléctricas

9.5.2 EQUIPOS

Seguridad del Cableado

- La instalación y mantenimiento del cableado eléctrico y de comunicaciones de la Cooperativa, debe ser realizado por personal calificado con el fin de garantizar su integridad y correcto funcionamiento.
- Verificar que se cumplen con los requerimientos especificados en los reglamentos técnicos para instalaciones nuevas o remodelaciones (cableado certificado).

Mantenimiento de Equipos

- Propender por que los equipos críticos de la infraestructura de servicios de Computo estén cubiertos por mantenimiento y soporte adecuados de hardware y/o software.
- Se debe realizar las tareas de mantenimiento preventivo a todos los equipos de cómputo, servidores y elementos de comunicaciones con una periodicidad mínima anual.
- Sólo el personal autorizado podrá realizar mantenimiento y llevar a cabo reparaciones en los equipos de la infraestructura de Grancoop.

Ubicación y protección de los equipos

Políticas dirigidas a: Todos los usuarios

- Todos los equipos de cómputo deben estar conectados a tomas de energía regulada.
- Está prohibido almacenar bases de datos que manejen datos personales en equipos portátiles o computadores de escritorio, a menos que esté autorizado por el área de Sistemas y Asistente administrativa.

Retiro de Activos de Información

Políticas dirigidas a: Asistente Administrativa.

- Será la encargada de autorizar el retiro de activos de información de las instalaciones de la Cooperativa.

Seguridad de equipos y activos fuera de las instalaciones

Políticas dirigidas a: Líderes de Área

- Todo equipo de cómputo o elemento que contenga información sensible de Grancoop, que sea destinado para labores fuera del ámbito de la Cooperativa, deberá ser autorizado por el jefe del área responsable de dicho equipo.

Políticas de reutilización o eliminación segura de equipos

Para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso, se establece lo siguiente:

Políticas dirigidas a: jefe de Sistemas

- Realizar eliminación segura de datos a los equipos que contengan información sensible de Grancoop.

Políticas dirigidas a: Asistente Administrativa

- Se encargará de la eliminación segura de todos los elementos que hayan sido dado de baja, que intervengan en el procesamiento de datos y que contengan información sensible de la Cooperativa y evitar que se revele información.
- Llevar un control y registro de cada uno de los medios que se eliminan.

Equipos de usuarios desatendidos

Políticas dirigidas a: Todos los usuarios

- Cierre de las aplicaciones (Log-Off) cuando ya no los necesiten.

- Al terminar la Jornada laboral se deben asegurar que los equipos queden apagados en su totalidad.

Política de "Escritorio Limpio y Pantalla Limpia"

Políticas dirigidas a: Todos los usuarios

- Todos los escritorios de los trabajadores deben de permanecer limpios de documentos en papel y dispositivos de almacenamiento removibles y pantallas limpias, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información.

- Evitar el consumo de alimentos cerca al equipo de cómputo.

9.6 SEGURIDAD DE LAS OPERACIONES.

El jefe de Sistemas es el encargado de la operación y administración de los recursos tecnológicos de la Cooperativa, manteniendo la documentación actualizada de los procesos para la ejecución de actividades, asegurando que los cambios efectuados sobre los recursos tecnológicos sean adecuadamente controlados y autorizados. Así mismo velará por la eficiencia de los controles implantados en los procesos operativos asociados a los recursos tecnológicos con el objeto de proteger la integridad, confidencialidad y disponibilidad de la información.

9.6.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES

Gestión de cambios

Políticas dirigidas a: jefe de Sistemas

- Debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas por el Gerente o jefe de Área que solicitó el cambio.

- Para solicitar estos cambios o requerimiento, se deberá programar reunión con todos los colaboradores involucrados en dicho proceso, y realizar un acta firmada por los asistentes en la que se describa los puntos tratados.

- Debe asegurarse que los sistemas de información suministrados por terceros cuenten con un acuerdo de licenciamiento sobre su uso y derechos de propiedad intelectual.

Separación de los ambientes de desarrollo, pruebas y producción

Políticas dirigidas a: jefe de Sistemas

- Los sistemas de información sensibles para la Cooperativa deberán propender por estar en un ambiente dedicado y aislado siempre que sea posible.

- Los ambientes de desarrollo, pruebas y producción deben existir en lo posible para todos los componentes de los aplicativos de Grancoop.

9.6.2 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

Controles contra códigos maliciosos

Políticas dirigidas a: jefe de Sistemas

- Todos los equipos de cómputo de Grancoop deben de contar con el software antivirus establecido y constantemente actualizado.

- Se restringe el uso de CD´s, memorias tipo USB y otros medios removibles de origen desconocido o, los únicos equipos autorizados son los pertenecientes a la Gerencia General y Gerencia Financiera, de igual manera, en estos equipos los dispositivos móviles deberán ser sometidos a la revisión del antivirus instalado en el disco antes de su utilización.
- Se restringe el uso de los equipos por parte de personas ajenas a las actividades propias de la Cooperativa. El jefe de sistema dispondrá un equipo para que los asociados puedan realizar la actualización de datos a través de la oficina virtual, este equipo no tendrá acceso a sistemas o aplicaciones que permitan el acceso a información.

- Los archivos comprimidos bajo el formato ZIP o cualquier otro tipo de archivo que se descarguen por Internet o por correo electrónico, deberán ser revisados por el antivirus inmediatamente después de haber sido desempaquetados y antes de ser ejecutados.

9.6.3 COPIAS DE RESPALDO

Respaldo de la información

Toda la información que se encuentra alojada en los servidores y equipos de cómputo, debe contar con un respaldo periódico, con el fin de garantizar la disponibilidad de la información en caso de ser requerida por alguna eventualidad, para ello se establece lo siguiente:

Políticas dirigidas a: jefe de Sistemas

Diariamente, se debe realizar una copia de seguridad de la información de producción, dejando respaldo en el disco del servidor local, en un servidor de archivos externo (almacenamiento en la nube) y con periodicidad semanal en un dispositivo de almacenamiento USB. Verificar que la copia esté correcta, una queda a cargo del jefe de sistemas y otra para la Gerente General, ambas para su custodia por fuera de la Cooperativa.

Adicional a la información de producción, se debe hacer una copia los viernes en la mañana del back up del día anterior, de programas fuentes de producción, Se coloca bajo custodia.

Se debe hacer copia de seguridad antes del cierre, cuando todos los usuarios del sistema están listos para iniciar este proceso (Incluyendo las oficinas sucursales).

Se debe hacer una copia de seguridad mensual de las copias diarias.

Mensualmente se debe hacer una copia de seguridad de fuentes de desarrollo y se deja en custodia.

Se debe hacer una copia de seguridad diaria de la carpeta "Mis documentos", a los siguientes equipos de: Gerente general, Gerente financiera, Contador y Auxiliar contable y semanal a todos los equipos (Incluyendo los anteriores).

Las copias del numeral anterior se deben almacenar por ocho días (Copias diarias) y por tres semanas (Las copias semanales).

Se debe llevar un registro diario en Excel de las copias diarias de producción, para el control de identificación.

Diariamente se debe realizar la carga de la copia de seguridad de la base de datos principal en un servidor de contingencia.

Se debe realizar copia de las imágenes de las máquinas virtuales del sistema NEXTCLOUD y Servidor de desarrollo.

- Debe realizar pruebas de recuperación periódicas, con el fin de comprobar su integridad y uso en caso de ser necesario, para ello se establece el siguiente procedimiento:

- Procedimiento para probar, de forma regular, las copias generadas y así garantizar su integridad y funcionalidad al momento de una restauración.

  Jefe de sistemas diariamente deberá cargar en el servidor contingencial, el backup o copia de seguridad del día anterior y validar su correcta restauración.
  En caso de generarse una falla o alera de error en la carga de la base de datos informix se deberá revisar inmediatamente el incidente ocurrido y sus causas, resolverlo y cargar nuevamente el backup en el servidor contingencial hasta asegurarse de que el proceso ha corrido exitosamente.

  <u>Sincronización de Relojes</u>

  Políticas dirigidas a: jefe de Sistemas

- Todos los equipos tanto, servidores, switches, equipos de cómputo, circuito cerrado de cámaras de vigilancia - CCTV, y todos aquellos dispositivos tecnológicos que se tienen en la Cooperativa se deben sincronizar a la hora legal colombiana, sin excepción alguna.

- Para garantizar el cumplimiento de la política, el área de sistemas verificará cada dos meses que cada equipo cuente con la correcta sincronización de relojes. Para la correcta sincronización de la

hora según lo expuesto en el numeral 14, del artículo 6, del Decreto 4175 de 2011, deberá apoyarse del Instituto Nacional de Metrología de Colombia (www.inm.gov.co, opción hora legal).

9.6.5 CONTROL DE SOFTWARE OPERACIONAL

Instalación de software en sistemas operativos

Políticas dirigidas a: jefe de Sistemas

- Solo el personal autorizado de Sistemas realizará la actualización del software operacional, aplicaciones y librerías.

9.6.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA

Gestión de las vulnerabilidades técnicas

Políticas dirigidas a: Todos Los Usuarios

- Notificar cualquier incidencia en los sistemas de información que pueda indicar un fallo producido por la explotación de alguna vulnerabilidad, notificar la necesidad de cualquier cambio que considere necesario para que el área de Sistemas valide si los cambios propuestos pueden incluir nuevas vulnerabilidades en los sistemas de información y sus estructuras de soporte.

Restricciones sobre la instalación de software

Políticas dirigidas a: jefe de Sistemas

- Solo el personal de sistemas o tercero autorizado por el jefe de sistemas podrá instalar software en los equipos de cómputo de la Cooperativa. Este software debe ser el avalado por el jefe de Sistemas.

- Ningún colaborador diferente al autorizado por el jefe de sistemas deberá tener permisos de administrador para la instalación de software en los computadores asignados para su desempeño.

9.7 ADQUISICIÓN DESARROLLO Y MANTENIMIENTO DE SISTEMAS

La Cooperativa propenderá por garantizar que el software adquirido y desarrollado al interior como por terceras partes, cumpla con los requisitos de seguridad y calidad establecidos.

9.7.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Políticas dirigidas a: jefe de Sistemas

- Establecer las actualizaciones de los sistemas operativos, según su criticidad y verificar el control de versiones, con el fin de determinar si la actualización puede interferir con el funcionamiento de los sistemas de información.

- Realizar las actualizaciones o coordinar su instalación.

- Informar cualquier fallo y hacer las pruebas iniciales de las aplicaciones.
- Garantizar el licenciamiento, calidad del software desarrollado y la inclusión de cláusulas de seguridad de la información en los contratos con terceros que fabriquen software.

- Ejecutar y coordinar los cambios que han sido planeados para las aplicaciones.

- Instalar los nuevos Sistemas de Información o las actualizaciones en los ya existentes.
- Realizar el análisis de los requerimientos de cambios solicitados en primera instancia, en caso de ser viable se notifica a los desarrolladores, aprobando las pruebas después de los cambios y ejecutando los cambios en el respectivo servidor.

- Coordinar y supervisar los cambios realizados en la infraestructura de comunicaciones y los sistemas de información.

- Atender las solicitudes y requerimientos de los usuarios ante incidentes y cambios inadecuados en los sistemas de información.

- Crear y monitorear un entorno de red en el que se realicen las pruebas y se analice el funcionamiento de los sistemas de información antes de pasarlo a producción.

- Definir e implementar políticas de desarrollo seguro para proteger los datos personales en el ambiente de desarrollo de software.

- Al realizar pruebas con datos personales mantener el mismo nivel de seguridad de las bases de datos objeto de pruebas, de conformidad con lo previsto en la ley de protección de datos personales.

- Supervisar las acciones de pruebas en los sistemas que realizan los desarrolladores.

- Implementar los cambios técnicos para la instalación, prueba y puesta en marcha del nuevo sistema de información.

Políticas dirigidas a: Asistente Administrativa, jefe de sistemas y Administrador de Riesgos.

- Realizar las capacitaciones informadas por el jefe de Sistemas y Asistente Administrativa y verificar que el personal que usa o tiene acceso al nuevo sistema de información, acate y cumpla las normas y recomendaciones operativas y de seguridad de la información, especificadas.

- Debe notificar las fallas e incidencias de seguridad.

Políticas dirigidas a: Desarrolladores (internos o externos)

- Los desarrolladores deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.

- Los desarrolladores deben verificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas y reconocidas en el mercado.
- Los desarrolladores deben asegurarse que en las áreas que se requiera no se permitan conexiones recurrentes a los sistemas de Información construidos con el mismo usuario.

- Los desarrolladores deben asegurar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros.

Políticas dirigidas a: Todos los usuarios

- Deben realizar reportes de cualquier falla, inconsistencia o cambio no documentado en el funcionamiento de las aplicaciones después de la actualización.

9.7.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE

Política de desarrollo seguro

Políticas dirigidas a: Gerente o jefe de área que solicitó el requerimiento

- Deben aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.

Políticas dirigidas a: jefe de Sistemas

- Debe implementar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas.

- A través de sus colaboradores, debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches o cambios generados.

Políticas dirigidas a: Desarrolladores (internos o externos)

- Los desarrolladores de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro, pasando desde el diseño hasta la puesta en producción.

- Los desarrolladores deben construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.

- Los desarrolladores deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos, entre otros.

- Los desarrolladores deben suministrar mecanismos de desconexión o cierre de sesión de los aplicativos que permitan finalizar completamente la sesión iniciada.

- Los desarrolladores deben garantizar que no se divulgue información sensible en mensajes de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios y propender por implementar mensajes de error genéricos.

- Los desarrolladores no podrán acceder a los ambientes de producción con fines de modificación de programas o datos propios de las aplicaciones previo un mecanismo de autorización de acceso.

9.7.3 DATOS DE PRUEBA

Protección de datos de prueba

Políticas dirigidas a: jefe de Sistemas

- En los casos que se tenga que usar datos reales se debe tener en cuenta los siguientes requisitos:

  - Al definir las características de una aplicación, se deben implementar medidas de seguridad para garantizar la integridad, confidencialidad y disponibilidad de los datos personales que contendrán las bases de datos asociadas.

  - Crear entornos separados de prueba con datos reales.

  - Restringir el acceso a los desarrolladores al entorno de producción desde los entornos de desarrollo. Si el personal de desarrollo necesita acceder al entorno de producción a realizar tareas de mantenimiento o de otro tipo, debe estar autorizado por el jefe de Sistemas.

  - Solo se pueden usar datos reales en las pruebas cuando se disponga de la autorización expresa del jefe de Sistemas.

  - Prohibir la realización de pruebas con datos reales en entornos que no cumplan con los requisitos de seguridad de la Cooperativa.

  - El jefe de Sistemas es el encargado de otorgar privilegios a los desarrolladores para ejecutar tareas en el ambiente de producción.

  - Identificación y autenticación de usuarios. Control de accesos.

  - Bases de datos que estén en soportes enviados fuera de las instalaciones de la Cooperativa o sean transmitidas deben estar cifradas (en caso de datos privados o sensibles).

  - El jefe de Sistemas debe eliminar la información de los ambientes de pruebas, una vez estas han concluido.

9.8 RELACIONES CON LOS PROVEEDORES

La Cooperativa establecerá mecanismos de control en sus relaciones con terceros, asegurando que la información a la que tengan acceso, así como servicios que sean suministrados por los mismos, cumplan las políticas de seguridad de la información.

Los colaboradores encargados de la interventoría con terceros se asegurarán de la divulgación de las políticas de seguridad de la información a terceros.

9.8.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES U OTROS TERCEROS

Política de seguridad de la información para las relaciones con los proveedores

Políticas dirigidas a: Asistente Administrativa

- Deben elaborar modelos de Acuerdos de Confidencialidad y Acuerdos de Intercambio de Información con proveedores y terceros. Se debe tener cuenta la responsabilidad civil como penal para los proveedores y terceros contratados. Deberá contar con apoyo del asesor jurídico y jefe de sistemas. Estos acuerdos deben ser entregados a todo el personal de la Cooperativa.

Políticas dirigidas a: jefe de Sistemas

- Debe establecer las condiciones de conexión adecuadas para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la Cooperativa.
- Debe establecer las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los proveedores de servicios.
- Debe verificar en el momento de la conexión y, cuando se considere pertinente, el cumplimiento de las condiciones de conexión de los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la Cooperativa.
- Debe verificar las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los proveedores de servicios.

Políticas dirigidas a: Todos los usuarios

- No se permite intercambiar información con entidades externas ni iniciar con ellas la prestación de un servicio, sin la debida autorización y acuerdos de confidencialidad que garantice los tratamientos de información pertinentes.

- Al intervenir contratos con proveedores y terceros deben divulgar las políticas, normas y procedimientos de seguridad de la información de la Cooperativa a dichos terceros, así como velar porque el acceso a la información y a los recursos de almacenamiento o procesamiento de la misma, por parte de los terceros se realice de manera segura, de acuerdo con las políticas y lineamientos de seguridad de la información.

- Cuando se celebren contratos de servicios, el colaborador a cargo será responsable de que dichos contratos estén cubiertos con acuerdos de confidencialidad y que en ellos se especifiquen claramente las condiciones, así como la entrega de información no autorizada.

- Cuando existan cambios en los servicios que prestan las terceras partes, estos deben ser documentados e incluidos en los acuerdos de servicios o contratos.

- En caso de ser necesario el envío y la recepción de información confidencial con los terceros contratados, se debe proteger con mecanismos de cifrado fuerte.

- Cuando se envié información sensible por correo electrónico, se debe colocar clave a los archivos adjuntos y está debe ser informada al destinatario por un medio diferente al correo electrónico.

- La información sensible disponible al público a través de sitios web, debe estar protegida por sitios seguros y, adicionalmente, con usuario y clave de acceso, como es el caso de la oficina virtual.

- En los contratos o acuerdos de servicios se incluyen los requisitos y condiciones requeridas para el intercambio de información.

- La Cooperativa podrá realizar auditorías a las terceras partes para evaluar la seguridad de la información y, como mínimo, se evaluarán integridad, disponibilidad, confidencialidad y calidad del servicio.

Políticas dirigidas a: Gerentes, jefes de Área y Asistente Administrativa

- En la intervención de contratos con proveedores y terceros deben monitorear periódicamente, el cumplimiento de los Acuerdos de Confidencialidad, Acuerdos de Intercambio de información y los requisitos de Seguridad de la Información de parte de los proveedores y de servicios.

9.9 CONTROLES CRIPTOGRÁFICOS

- Los sitios web creados para el procesamiento de la información de la Cooperativa como la oficina virtual y página Web, deben ser sitios seguros y utilizar certificados digitales emitidos por un ente certificador legalmente constituido en el país.

- Las comunicaciones con terceras partes para la prestación de servicios, deben utilizar mecanismos de encriptación fuertes.

- En el almacenamiento de la información sensible o crítica en archivos, así como las claves de usuarios a los sistemas de información, se deben utilizar herramientas que cuenten con algoritmos de encriptación.

9.10 POLÍTICAS DE TELETRABAJO

Tele-trabajo significa que los equipos de información y comunicación se utilizan para permitir que los empleados realicen su trabajo fuera de la Cooperativa. Esto incluye el uso de teléfonos móviles, tabletas, portátiles y similares fuera de las instalaciones de la Cooperativa, por lo cual:

- El acceso remoto a los servidores que se encuentran fuera de las instalaciones de la Cooperativa, debe estar autorizado por el jefe de área solicitante, o quien delegue la gerencia general.

- Las áreas de trabajo remoto fuera de su sede principal, deben cumplir con todas las políticas y controles del sistema de seguridad definido para proteger la información que viaje en ellos.

- El jefe de sistemas y demás personal del área son responsables de proporcionar el servicio de acceso

9.11 POLÍTICAS DE ACCESO A LAS REDES WIFI

- El acceso a las redes inalámbricas por parte de los empleados, a través de WiFi, se debe realizar con autenticación usuario y contraseña, independientemente de la herramienta que se quiera utilizar para controlar el acceso. El usuario y contraseña solo será de conocimiento del jefe de sistemas y quien él autorice.

- Las redes WiFi para asociados o visitantes se debe realizar mediante accesos independientes y por redes lógicas independientes a las redes corporativas.

- Solo se permite el uso de WIFI a los equipos corporativos, de uso exclusivo para la Cooperativa.

9.12 POLÍTICAS DE ANÁLISIS DE VULNERABILIDADES

El jefe de sistemas deberá implementar un sistema de análisis de vulnerabilidades informáticas que cumpla al menos con los siguientes aspectos:

- Estar basado en un hardware de propósito específico (appliance) totalmente separado e independiente de cualquier dispositivo de procesamiento de información, de comunicaciones y/o de seguridad informática.

- Generar, de manera automática, por lo menos dos (2) veces al año, un informe consolidado de las vulnerabilidades encontradas. Los informes de los últimos dos (2) años deben contener sus planes de acción y sus remediaciones.
- Realizar un análisis diferencial de vulnerabilidades, comparando el informe actual con respecto al inmediatamente anterior.
- Las herramientas usadas en el análisis de vulnerabilidades deberán estar homologadas por el CVE (Common Vulnerabilitis and Exposures) y actualizadas a la fecha de su utilización.

Los informes generados deberán tomar como referencia la lista de nombres de vulnerabilidades CVE publicada por la corporación Mitre (www.mitre.org).

10. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Según la norma ISO 27035, un Incidente de Seguridad de la Información está indicado por un único o una serie de eventos seguridad de la información indeseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información.

Con el objeto de detectar, reportar, controlar, monitorear y responder de forma oportuna y apropiada ante la ocurrencia de un evento y/o incidente de seguridad de la información, se ha establecido el siguiente procedimiento.

Los incidentes se clasifican en las siguientes categorías:

a) Acceso no autorizado: Comprende todo tipo de ingreso y operación no autorizado a los sistemas, tanto exitosos como no exitosos. Son parte de esta categoría:

- Accesos no autorizados exitosos, sin perjuicios visibles a componentes tecnológicos.
- Robo de información
- Borrado de información
- Alteración de la información
- Intentos recurrentes y no recurrentes de acceso no autorizado
- Abuso y/o Mal uso de los servicios informáticos internos o externos que requieren autenticación

b) Código malicioso: Esta categoría comprende la introducción de códigos maliciosos en la infraestructura tecnológica de la organización. Son parte de esta categoría:

- Virus informáticos
- Troyanos
- Gusanos informáticos

c) Denegación del servicio: Esta categoría incluye los eventos que ocasionan pérdida de un servicio en particular. Los síntomas para detectar un incidente de esta categoría son:

- Tiempos de respuesta muy bajos sin razones aparentes.
- Servicio(s) interno(s) inaccesibles sin razones aparentes
- Servicio(s) Externo(s) inaccesibles sin razones aparentes

d) Escaneos, pruebas o intentos de obtención de información de la red o de un servidor en particular. Esta categoría agrupa los eventos que buscan obtener información de la infraestructura tecnológica de la organización y comprende:

- Sniffers (software utilizado para capturar información que viaja por la red)
- Detección de Vulnerabilidades

e) Mal uso de los recursos tecnológicos: Esta categoría agrupa los eventos que atentan contra los recursos tecnológicos por el mal uso y comprende:

- Mal uso y/o Abuso de servicios informáticos internos o externos
- Violación de las normas de acceso a Internet
- Mal uso y/o Abuso del correo electrónico de la organización
- Violación de las Políticas, Normas y Procedimientos de Seguridad Informática establecidas para proteger la información

Descripción del procedimiento

El colaborador que detecta el incidente debe reportar inmediatamente al jefe inmediato o líder del proceso o en su defecto al jefe de sistemas o Asistente administrativa según sea el caso, de forma escrita a través del correo electrónico y de forma verbal.

El líder del proceso informa inmediatamente al jefe de sistemas o Asistente administrativa, de forma escrita a través de correo electrónico y de forma verbal.
El líder de sistema debe reportar el evento presentado al Gerente General, asistente administrativa y administrador de riesgos, e iniciar la gestión junto a su equipo de trabajo, para darle la atención adecuada según su severidad, para ello se han establecido unos niveles de prioridad y posibles tiempos de respuesta:

Nivel de criticidad	Definición	Tiempo de respuesta
Catastrófico	Pérdida total de la información – Sistemas críticos	5minutos
Mayor	Pérdida de información de asociados – Sistemas pertenecientes al área de sistemas y puestos de trabajo con funciones críticas	15 minutos
Moderado	Divulgación de información de asociados-Sistemas que apoyan más de un proceso.	30 minutos
Menor	Divulgación de información no oficial-Sistemas que apoyan un solo proceso	1 hora
Insignificante	Uso inadecuado de información pública-Sistemas no críticos o puestos de trabajo con funciones no críticas	3 horas

Para la atención y gestión del incidente se debe incurrir a estrategias que permitan tomar decisiones oportunas para evitar la propagación del incidente y así disminuir los daños, la pérdida de la confidencialidad, integridad y disponibilidad de la información, un ejemplo de ello es el bloqueo de cuentas ante la detección de intentos de accesos no autorizados o desconectar de la red un equipo que ha sido infectado con virus, y de ser necesario activar el plan de continuidad del negocio.

Una vez se haya impedido la propagación del incidente, se debe identificar el daño ocasionado, solucionarlo y eliminar cualquier huella que pueda seguir generando afectaciones, restablecimiento de la información, sistemas o servicios afectados.

Si el incidente se desencadena en fraudes para la Cooperativa, el Gerente General se deberá poner en contacto con las entidades encargadas para la investigación y sanción de estos hechos denominados delitos informáticos, así como informar tal situación a la Superintendencia de la Economía Solidaria.

El jefe de sistemas y Asistente administrativa debe analizar junto con las personas del área donde ocurrió el incidente, el gerente general y el administrador de riesgos las causas que llevaron a materialización del incidente, establecer nuevos controles que permitan prevenir incidentes similares en el futuro. De esta reunión debe quedar un acta firmada por los asistentes, y en ella describir el incidente presentado, la gestión realizada y nuevos controles implementados como acción de mejora.

El Gerente General tomará las medidas disciplinarias según sea el caso.

Estos incidentes deben quedar registrados en la planilla de reporte de eventos de riesgo operativo a cargo del administrador de riesgos.

9.9.1 POLÍTICAS DE GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN

Tratamiento y reporte de incidentes de seguridad

Políticas dirigidas a: Gerentes, jefes de Área y Asistente Administrativa

- Serán responsables de realizar el reporte de los incidentes de seguridad de la información en los casos que sean necesarios.
- Son los encargados del seguimiento, documentación y análisis de los incidentes de seguridad de la información encontrados.
- La Asistente Administrativa es responsables de poner en conocimiento los procedimientos de gestión de incidentes a los colaboradores contratados al inicio de la relación laboral.
- Velar por el correcto funcionamiento y operación de la Gestión de Incidentes de Seguridad de la Información.

Políticas dirigidas a: Todos los usuarios

Todo el personal de la Cooperativa es responsable de reportar de manera escrita debilidades e incidentes de seguridad oportunamente para atender el incidente.

En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, los colaboradores deben notificarlo a la Asistente Administrativa para que se le dé el trámite necesario.

10. CUMPLIMIENTO

La Cooperativa velara por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información.

10.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

Identificación de la legislación aplicable y de los requisitos contractuales

Políticas dirigidas a: jefe de sistemas, Asistente Administrativa y Administradora de Riesgos

- Deben identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la Cooperativa y relacionados con seguridad de la información.

Políticas dirigidas a: jefe de Sistemas

- Debe garantizar que todo software que se ejecuta en la Cooperativa está protegido por derechos de autor y requiere licencia de uso, o, en su lugar, sea software de libre distribución y uso.

Políticas dirigidas a: Todos los usuarios

- Los usuarios no deben instalar ningún tipo de software en los equipos de trabajo que se le asignaron para el desarrollo de sus actividades laborales.

- Los usuarios deben cumplir con las leyes de derecho de autor y acuerdos de licenciamiento de software.

Privacidad y Protección de Datos Personales

Políticas dirigidas a: Asistente Administrativa

- Establecer las políticas y los lineamientos necesarios para el adecuado tratamiento (recolección, almacenamiento, uso, circulación y supresión) de los datos personales de los asociados de la Cooperativa.

Políticas dirigidas a: Demás áreas que realizan tratamiento de datos personales.

- Acoger e implementar todas las políticas, lineamientos, protocolos y procedimientos dados para el adecuado tratamiento de la información en general y de los datos personales en particular.

11. DIVULGACIÓN DE INFORMACIÓN

En el presente Manual se encuentra documentada la política de Seguridad de información, sus principios y objetivos. Este documento será divulgado a todos los colaboradores de la Cooperativa y directivos a través de correos electrónicos. A las demás partes interesadas a través de la página web.

Con periodicidad anual el administrador de riesgos realizará una capacitación o socialización de las políticas del sistema de seguridad de la información.

El presente acuerdo rige a partir de su aprobación

COMUNÍQUESE Y CÚMPLASE

Dado en Santiago de Cali a los 24 días del mes de junio de 2022.

JEFFERSON OREJUELA	**JAIRO ANTONIO LARA LOZANO**
PRESIDENTE	**SECRETARIO**