MANUAL

GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Código:	MAN.GIS.01
Versión:	13.00
Fecha de la versión:	12/02/2025
Clasificación de la Información:	Interna

Registro de firmas

Creado por / Modificado por	Revisado por	Aprobado por
Jersson Plaza Oficial Seguridad de la Información	Sandra Armijos Director de Desarrollo e Innovación	Consejo de Administración
Diego Quistanchala Analista de Seguridad y Protección de la Información	Santiago Rueda Jefe de Calidad y Procesos (E)	
Heidy Zurita Analista de Calidad y Procesos	María Belén Játiva Director de Riesgos Integrales	
	Andrés Hidalgo Director Jurídico	
	Comité de Seguridad de la Información	
	Fabian Cruz Gerente	
04/02/2025	**07/02/2025**	**12/02/2025**

Historial de Modificaciones

Fecha	Versión	Creado por / Modificado por	Descripción de la modificación
30/003/2016	1.00	Vinicio Cevallos Oficial de Seguridad de la Información	Creación del documento
20/10/2016	2.00	Vinicio Cevallos Oficial de Seguridad de la Información	Reforma integral
23/11/2017	3.00	Vinicio Cevallos Oficial de Seguridad de la Información	Se realizó reformas en las siguientes políticas: - Políticas relacionadas a la gestión de talento humano - Desvinculación de personal o cambios de puesto de trabajo. - Política de gestión de activos. - Política de Control de Accesos. - Política de seguridad en las telecomunicaciones
28/11/208	4.00	Vinicio Cevallos Oficial de Seguridad de la Información	Reforma Integral
30/06/2021	5.00	Álvaro Barrera Jefe de Seguridad de la Información	Reforma integral del documento de acuerdo con el cumplimiento de los requisitos del Sistema de Gestión de Calidad ISO 27001:2013.
24/02/2022	6.00	Sandra Armijos Jefe de Gestión de Calidad y Procesos Álvaro Barrera Jefe de Seguridad de la Información	Actualización de cargos conforme a la estructura. Actualización de la definición de clasificación de información pública con la finalidad de incluir la información que por normativa externa se requiere dar acceso al público en general.
17/06/2022	7.00	Santiago Rueda Analista de Procesos Álvaro Barrera Jefe de Seguridad de la Información	• Modificación de nombre de *Manual de Seguridad de la Información* a *Manual de Seguridad de la Información y* ***Ciberseguridad*** e inclusión de políticas orientadas a la implementación de controles de ciberseguridad considerando el marco normativo de la ISO 27032 de Ciberseguridad • Referencia a nueva base normativa emitida por entes de control: - Manual de Seguridad de la información y Ciberseguridad Ley Orgánica de Protección de Datos Personales • Referencia para aplicación de estándares externos - ISO 27001 - ISO 27002 - ISO 27032 - PCI DSS - PCI CP - PCI PTS • Cláusulas para contratos de servicios auxiliares • Se da de baja el *MAN-020 Manual de Control de Uso de Transferencias versión 01* y se procede a incluir en el presente Manual cláusulas para los

			contratos de servicios de cabales electrónicos en lo que respecta a transferencias, adicional se crea la Matriz de Seguimiento de Controles de Canales Electrónicos con el fin de validar anualmente el cumplimiento de la norma Resolución No. SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103.
09/11/2022	8.00	Santiago Rueda Analista de Procesos Álvaro Barrera Jefe de Seguridad de la Información	Se actualiza los siguientes anexos del Manual de Gestión de Seguridad de la Información y Ciberseguridad: - ANEXO A Titulares Propietarios de la información. - ANEXO B Titulares Propietarios de los servicios y sistemas de información. Se actualiza los cargos de los Anexos A y B acorde a la estructura vigente. Se incluye en el Anexo B el sistema de los HSMs definiendo: Titular, titular delegado, gestor de usuarios, encargado del tratamiento. Se actualiza el cargo Jefe de Gestión de Aplicaciones por Jefe de Desarrollo.
28/08/2023	9.00	Santiago Rueda Analista de Calidad y Procesos Álvaro Barrera Oficial de Seguridad de la Información	Se incluye políticas referente uso de comunicaciones en línea y redes sociales. Se actualiza políticas de Puesto de trabajo despejado y pantallas limpias. Las responsabilidades del Administrador de Contrato pasan al Manual de Adquisiciones y Contrataciones. Actualización de cláusulas en contratación en servicios en la nube acorde a la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211. Se actualizan las políticas de seguridad para bases y contratos de servicios de computación en la nube, considerando la Resolución No. SEPS-IGT-IGS-INR-INGINT-2022-0211, Norma Reformatoria a la Resolución No. SEPS-IGT-IR-IGJ-2018- 0279 de 26 de noviembre de 2018, que contiene la “Norma De Control Para la Administración del Riesgo Operativo y Riesgo Legal en las Entidades del Sector Financiero Popular y Solidario bajo el control de la Superintendencia De Economía Popular y Solidaria”
21/09/2023	10.00	Santiago Rueda Analista de Calidad y Procesos Álvaro Barrera Oficial de Seguridad de la Información	Se elimina el formato FR.MAN.GIS.01.01 Matriz de Seguimiento de Controles de Canales Electrónicos misma que está atada a la Resolucion-No.-SEPS-IGT-IR-ISF-ITIC-IGJ-2017-103 la cual ha sido derogada y el seguimiento de la normativa que la reemplaza, es responsabilidad del Director de Operaciones. Se crea el formato FR.MAN.GIS.01.01 Lista de Verificación de Requisitos de Seguridad para Desarrollo o Adquisición de Sistemas con el fin de proveer de una herramienta de validación para desarrollos internos y externos, alineado al marco normativo (Resolución Nro. SEPS-IGT-IGS-INSESF-

			INR-INGINT-INSEPS-2023-0270, Resolución Nro. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-009). Se actualiza la política *5.18.2 Formato de registros de auditoria* acorde a la norma ISO 27002.
28/02/2024	11.00	Santiago Rueda Analista de Calidad y Procesos Vinicio Cevallos Oficial Seguridad de la Información (E)	Se incluye en terminología la definición de aplicativo móvil, Desarrollo, Seguridad y Operaciones (DevSecOps), RBAC y Software. En el literal *5.4.1.2. Comité de seguridad de la información* se incluye que la actualización PSI se lo realizará de manera anual. En el literal *5.5.8. Políticas de puesto de Trabajo Despejado y Pantalla Limpia* en el acápite b para los colaboradores se define la política que *"Toda la información generada o que sea utilizada para el desempeño de sus actividades, deberán ser colocadas en el almacenamiento de la nube institucional. Bajo ningún motivo deberá mantener información almacenada de manera local".* En el literal *5.6.6 Desvinculación o Cambio del Puesto de Trabajo* se actualiza el acápite d que "*En caso de requerir una copia del respaldo de la información se deberá solicitar la autorización a la Gerencia de los respaldos que fueron almacenados en la nube institucional; debiendo para el efecto ingresar el requerimiento en el Sistema de Mesa de Servicios".* En el literal *5.7.2 Medidas de Seguridad* se actualiza el cuadro que las copias deben realizarse a los cargos que requieran respaldos, conforme se indica en el numeral *5.17 Respaldos.* En el literal *5.9.2 Depuración de Cuentas* en el acápite b se elimina la palabra eliminar y se incluye bloquear para que este acorde al sistema de directorio activo. En el literal *5.12.2 Generalidades* se crea el acápite c donde se define que para "*toda compra que involucre el acceso a información, sistemas o instalaciones, desarrollo de software, servicios en la nube, centros de procesamiento de datos principal y/o alternos contratados en la nube se lo realizará conforme lo establece el Manual de Adquisiciones y Contrataciones"*. En el literal *5.12.2 Generalidades* se incluye el acápite d. donde se define que para "toda compra de software debe cumplir con lo definido en el formato Anexo E Lista de Verificación de Requisitos de Seguridad para Desarrollo o Adquisición de Sistemas, el cual incluye un resumen de todos los requisitos de seguridad detallados en este manual". En el literal *5.17.1 Procesos de Ejecución de Respaldos* en el acápite h se incluye política para respaldos de información.

			En el literal *5.23.1.1. Jefe de Desarrollo* se incluye como política: *"Hacer cumplir el desarrollo de aplicativos con las leyes y regulaciones aplicables relacionadas con la privacidad de los datos, la protección de la información personal y otros requisitos legales y regulatorios".* En el literal *5.23.4 Cobertura de Vulnerabilidades* en el Proceso de Desarrollo en el acápite a se actualiza la política definiendo que *"los desarrolladores deben seguir las mejores prácticas de seguridad de la información durante el desarrollo y la codificación de aplicativos".* Se crea el literal 5.23.10 Seguridad en las Etapas del Desarrollo (DevSecOps). Se crea el literal *5.28.3 Métricas de Gestión de Seguridad de la Información.* El formato FR.MAN.GIS.01.01 Lista de Verificación de Requisitos de Seguridad para Desarrollo o Adquisición de Sistemas pasa a ser *ANEXO E Lista de Verificación de Requisitos de Seguridad para Desarrollo o Adquisición de Sistemas.*
04/12/2024	12.00	Jersson Plaza Oficial Seguridad de la Información Heidy Zurita Analista de Calidad y Procesos	Se actualiza terminología en función al Glosario Institucional. Se actualiza la sección de Comité de Seguridad de la Información conforme la resolución SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002 respecto los invitados del comité. Se actualiza los cargos conforme la estructura organizacional vigente y se mejora la redacción para aclarar la ejecución de actividades y responsabilidades.
12/02/2025	13.00	Diego Quistanchala Seguridad y Protección de la Información Jersson Plaza Oficial Seguridad de la Información Heidy Zurita Analista de Calidad y Procesos	Inclusión de nuevas definiciones en la terminología. Con la finalidad de fortalecer el control interno de la Cooperativa se incluye las siguientes políticas: - Dispositivo Electrónico ATM dentro de la sección de "Tipos de dispositivos". - Control de las medidas de seguridad y para fortalecer esta política se agrega la sección de "Responsables de las medidas". - Literal d) sobre la retención de identificadores personales deshabilitadas, en la sección "Depuración de cuentas". - Literal d) sobre implementar un control periódico para la emisión y revocación de los accesos físicos mediante una matriz. - En la sección "Seguridad en las etapas del desarrollo (DevSecOps)" se direcciona a la Metodología Desarrollo de Soluciones Tecnológicas para manifestar que en dicha metodología se describe la intervención del área de SI en las etapas de desarrollo. - Inclusión del literal e) sobre el control y verificación de licencias adquiridas por SI mediante un

			inventario, en la sección “Cumplimiento de Requisitos Legales” subsección “Conformidad Legal”. Modificación o inclusión de políticas requeridas por el Oficial de Seguridad de la Información: - En políticas que tengan relación con autorización o aprobación por parte del Gerente reemplazar por “*Autorización del Gerente en los casos de áreas con reporte directo o los subgerentes para las demás áreas*.” por funciones del nuevo cargo de “subgerentes”. - Inclusión del literal *e)* sobre el enviar y recibir correos de dominios gratuitos, en la sección de prohibiciones del “Uso de correo electrónico”. - Inclusión del literal *c,d,e,f,g,h, j* y *k* en la sección de “Uso, acceso y control de internet”. - Inclusión de los representantes y vocal en la sección de “Uso de comunicaciones en línea y redes sociales”. - En la sección “Medidas de seguridad”: • En la medida “Bloqueo de pantalla se aumenta el tiempo de inactividad de 3 a 5 minutos acorde buenas prácticas de SI. • Inclusión de la medida “Términos de uso aceptable” para que tenga concordancia con las medidas de seguridad mínimas por tipo de dispositivo. • Reforma integral de la medida: DLP, AIP, Control del software instalado y actualizaciones, para alinear su descripción y/o consideración acorde la medida. • Inclusión para que dispositivos móviles sean entregados a Mesa para su configuración a fin de que asegurar los dispositivos para su uso. • Inclusión para que dispositivos institucionales sean validados la hardenización por Mesa a fin controlar su ejecución por parte de SI. - Inclusión del literal b) en la sección “Período y mecanismo de cambio de contraseñas” para establecer la obligatoriedad de cambio de contraseñas para representantes de la Asamblea General, BIOS de ATM, sistema operativo de ATM, red Wi-Fi y cuando un colaborador se desvincula y tiene acceso al sistema de administración de contraseñas. - Inclusión literal b) en la sección “Relación con proveedores”, subsección de Generalidades para controlar que los procesos de adquisición o contratación que tenga relación con recopilación de información personal, creación de nuevos productos o implementación de nuevos servicios deben contar con la participación del área de SI.

			- En la sección “Protección Contra Software Malicioso” se ajusta conforme ejecución, en literal d) sobre las configuraciones en antivirus a cargo del área de TI, en literal e) las investigaciones de alertas del antivirus a cargo del área de SI y en literal f) de garantizar que las herramientas de seguridad verifiquen software malicioso a cargo del área de SI. - Inclusión de la responsabilidad del área de TI para asegurar que todos los dispositivos tengan la hora sincronizada en el literal b) de la sección “Sincronización de relojes”. - Inclusión de la sección “Control del software operacional” a fin de establecer lineamientos de instalación de software y responsabilidades. - Inclusión literal a) en la sección “Control de las vulnerabilidades técnicas” para que se ejecute de forma periódica el análisis de vulnerabilidades a todos los dispositivos tecnológicos. - Inclusión literal h) sobre la renovación de cuentas de usuarios VPN. Para mantener la relación y concordancia con otra normativa interna se fortalece o incluye políticas, tal como: - Inclusión de literal *g,h,i* y *j* en la sección “Gestor de Usuarios” para relacionar la normativa de Mesa de Atención Técnica. - Modificación del literal c) de la sección “Para ingreso de personal”; literal c) de la sección “Durante el empleo”; literal a) de la sección “Desvinculación o cambio del puesto de trabajo” para relacionar la normativa de TH. - Inclusión de “servidores” como dispositivo fijo dentro de la sección de “Tipos de dispositivos” a fin de alinear a estos equipos a las medidas de seguridad. Remplazo de los siguientes textos con la finalidad de estandarizar este documento: - “Sistemas informáticos” y “recursos informáticos” por “sistemas de información” conforme ISO 27002. - “Cuentas de usuario” por “identificadores o cuentas personales”. - “Equipo de usuario, computadoras” por “dispositivo institucional fijo o teletrabajo” - “Dar de baja o eliminar” por “deshabiltar” en los casos de referirse a identificadores o cuentas personales. - “Pre-producción” por “pruebas” conforme ISO 27002. - En función a las definiciones de “Dueños de la información” y “Titulares del activo”, se cambia en los casos necesarios esta terminología de “dueño”

			por "titular" o viceversa. Cuyo cambio también afecto a los anexos A y B. Se elimina las siguientes políticas: - No aplica actualmente: "*Se autoriza el servicio de correo electrónico para envío y recepción de correos desde y hacia dominios externos a la Cooperativa a: jefes, directores, subgerentes, Gerente, miembros de Consejos. La autorización a personal adicional deberá ser solicitado por los jefes de cada área*". - Por duplicidad con literal c) de la sección "Uso, acceso y control de internet": "*Si por algún motivo, un usuario requiera navegar en internet de forma que no estén estipulada en los lineamientos de este documento, debe presentar justificación y aprobación escrita de la Dirección a la que pertenece*." - Por duplicidad con la medida de "Bloqueo de pantalla" y "Cifrado de almacenamiento" de la sección "Medidas de seguridad": Si el dispositivo implementa la medida de cifrado de almacenamiento, debe también implementar la medida de bloqueo de pantalla. - Por ser parte del procedimiento de Incidentes de SI: a)Emitir un informe técnico de las causas que generaron el incidente y de las acciones de mitigación o cierre… b)Realizar el seguimiento de sistemas reinstalados para garantizar la estabilidad y seguridad y comunicar una vez alcanzado el período de seguimiento. - No aplica porque no se cuenta con la infraestructura: a) Los interruptores de emergencia deberán ubicarse cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento. Se realiza ajustes de forma, tales como: - Se traslada políticas a las secciones pertinentes a fin de relacionar el tema en una sola sección. - Modificación en los nombres de normativa interna relacionada con este documento acorde el portafolio de documentos vigente. - Actualización de cargos y nombres de áreas conforme la estructura organizacional vigente. - Se mejora la redacción para aclarar políticas y responsabilidades.

ÍNDICE

1. OBJETIVO 13

2. ALCANCE 13

3. USUARIOS 13

4. TERMINOLOGÍA 13

5. POLÍTICAS O LINEAMIENTOS 18

5.1 APLICACIÓN DE LOS CONTROLES DE SEGURIDAD 18
5.2 ANÁLISIS Y GESTIÓN DE RIESGOS 18
5.3 APLICACIÓN DE ESTÁNDARES EXTERNOS 18
5.4 ORGANIZACIÓN Y RESPONSABILIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) 18
5.4.1 Gobierno del SGSI 18
5.4.2 Supervisión del SGSI 21
5.5 OBLIGACIONES EN SEGURIDAD DE LA INFORMACIÓN 25
5.5.1 Generales 25
5.5.2 Acceso y permanencia en instalaciones 26
5.5.3 Uso de información y sistemas 26
5.5.4 Identificadores personales y claves de acceso 27
5.5.5 Uso de correo electrónico 28
5.5.6 Uso, acceso y control de internet 30
5.5.7 Uso de comunicaciones en línea y redes sociales 31
5.5.8 Políticas de puesto de trabajo despejado y pantalla limpia 35
5.6 SEGURIDAD EN RECURSOS HUMANOS 36
5.6.1 Para el ingreso de personal 36
5.6.2 Acuerdo de confidencialidad y no competencia 36
5.6.3 Durante el empleo 36
5.6.4 Segregación de funciones 37
5.6.5 Proceso disciplinario 37
5.6.6 Desvinculación o cambio del puesto de trabajo 37
5.7 SEGURIDAD EN DISPOSITIVOS TECNOLÓGICOS 38
5.7.1 Tipos de dispositivos 38
5.7.2 Medidas de seguridad 38
5.7.3 Medidas de seguridad mínimas por tipo de dispositivo 41
5.7.4 Responsables de las medidas de seguridad 42
5.7.5 Control de las medidas de seguridad 42
5.8 TELETRABAJO Y ACCESO REMOTO 42
5.8.1 Políticas generales 42
5.8.2 Responsabilidades específicas del teletrabajo y acceso remoto 42
5.9 CONTROL DE ACCESO 43
5.9.1 Políticas generales 43
5.9.2 Depuración de cuentas 44
5.9.3 Revisión de derechos de acceso 45
5.9.4 Control de acceso remoto de los usuarios 45
5.9.5 Control de acceso remoto de proveedores 45
5.9.6 Control de acceso de puertos de configuración 45
5.10 IDENTIFICACIÓN Y AUTENTICACIÓN 46
5.10.1 Identificadores o cuentas personales 46
5.10.2 Nomenclatura para identificadores personales 46
5.10.3 Identificadores o cuentas genéricas 48

5.10.4 Utilización de Cuentas Genéricas 50
5.10.5 Pantalla de autenticación en los sistemas de información 50
5.10.6 Aviso de acceso 51
5.10.7 Generación y reinicio de contraseñas 51
5.10.8 Distribución de contraseñas 51
5.10.9 Período y mecanismo de cambio de contraseñas 51
5.10.10 Longitud y Sintaxis de Contraseñas 52
5.11 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 52
5.11.1 Responsabilidades específicas 52
5.12 RELACIÓN CON PROVEEDORES 53
5.12.1 Responsabilidades específicas 53
5.12.2 Generalidades 53
5.12.3 Contrato con el proveedor 54
5.13 CONTROLES CRIPTOGRÁFICOS 61
5.13.1 Normas de Cifrado 61
5.13.2 Administración de Claves de Cifrado 61
5.14 SEGURIDAD FÍSICA Y DEL ENTORNO 62
5.14.1 Seguridad Física y Electrónica 62
5.14.2 Suministros de energía 62
5.14.3 Seguridad del Cableado 63
5.14.4 Mantenimiento de Equipos Tecnológicos (Hardware) 63
5.14.5 Movilización de dispositivos tecnológicos fuera de las instalaciones de la Cooperativa 63
5.14.6 Seguridad del equipamiento fuera del ámbito de la Cooperativa 63
5.14.7 Baja segura o reutilización de dispositivos tecnológicos 64
5.14.8 Inspección de cumplimiento de políticas de puesto de trabajo despejado y pantalla limpia 64
5.15 SEGURIDAD DE OPERACIONES TECNOLÓGICAS 64
5.15.1 Documentación de procedimientos de operación 64
5.15.2 Procedimientos de control de cambios 65
5.15.3 Planificación de la Capacidad 65
5.15.4 Separación entre ambientes de desarrollo, pruebas y producción 65
5.15.5 Acuerdos de Nivel de Servicios 66
5.16 PROTECCIÓN CONTRA SOFTWARE MALICIOSO 66
5.17 RESPALDOS 67
5.17.1 Procesos de ejecución de respaldos 67
5.17.2 Administración y seguridad de los medios de almacenamiento 68
5.18 MONITOREO DEL ACCESO Y USO DE LOS SISTEMAS 69
5.18.1 Registro de eventos 69
5.18.2 Formato de los registros de auditoría 70
5.18.3 Sincronización de relojes 70
5.18.4 Integridad y confidencialidad de los registros de auditoría 70
5.18.5 Disponibilidad y almacenamiento de los registros de auditoría 71
5.18.6 Monitoreo de los registros de auditoría 71
5.19 CONTROL DEL SOFTWARE OPERACIONAL 71
5.19.1 Instalación del software en los sistemas operativos 71
5.20 GESTIÓN DE LA VULNERABILIDAD TÉCNICA 71
5.20.1 Control de las vulnerabilidades técnicas 71
5.20.2 Restricciones de instalación de software 73
5.21 SEGURIDAD EN LAS COMUNICACIONES 74
5.21.1 Gestión de seguridad de la red 74
5.22 INTERCAMBIOS DE INFORMACIÓN Y SOFTWARE 78

5.22.1 Acuerdos de Intercambio de Información y Software 78
5.22.2 Seguridad del comercio electrónico 78
5.22.3 Sistemas de acceso público 78
5.23 APROBACIÓN DE SISTEMAS 79
5.23.1 Aprobación del sistema 79
5.23.2 Seguridad de la documentación del sistema 79
5.24 DESARROLLO SEGURO 79
5.24.1 Responsabilidades específicas de desarrollo seguro 79
5.24.2 Generalidades 80
5.24.3 Protección de los datos de prueba del sistema 80
5.24.4 Seguridad en las etapas del desarrollo (DevSecOps) 80
5.24.5 Seguridad en la documentación del software 83
5.24.6 Seguridad post implementación 83
5.25 GESTIÓN DE PROYECTOS 84
5.26 CLASIFICACIÓN Y TRATAMIENTO DE INFORMACIÓN 84
5.26.1 Niveles de clasificación 84
5.26.2 Clasificación y manejo 85
5.26.3 Reasignación o baja de equipos 86
5.26.4 Borrado, limpieza y destrucción física 87
5.26.5 Rotulado y etiquetado de información 89
5.26.6 Normas de inventario de información restringida y confidencial 89
5.27 CONTINUIDAD DEL NEGOCIO 90
5.28 CUMPLIMIENTO DE REQUISITOS LEGALES 90
5.28.1 Conformidad legal 90
5.28.2 Protección de datos y privacidad de la información personal 91
5.28.3 Legislación sobre monitoreo del abuso de sistemas y redes 91
5.28.4 Legislación sobre criptografía 91
5.29 REVISIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 91
5.29.1 Revisión independiente de la organización y estrategia de seguridad 91
5.29.2 Revisión independiente del cumplimiento normativo 91
5.29.3 Métricas de Gestión de Seguridad de la Información 92
5.30 ACCIONES 92
6 DOCUMENTOS DE REFERENCIA 92
7 NORMATIVA INTERNA 93
8 ANEXOS 93

1. Objetivo

Definir la organización y responsabilidades en la gestión de seguridad de la información y ciberseguridad, así como las líneas de actuación y los criterios que son de aplicación obligatoria en la Cooperativa, con el objetivo de reducir el riesgo residual al nivel aceptado en la institución.

2. Alcance

Este manual define las políticas generales y específicas para su aplicación en los procedimientos y gestión de Seguridad de la Información y Ciberseguridad.

3. Usuarios

Los usuarios de este documento son todos los colaboradores de la Cooperativa bajo dependencia laboral indefinida o temporal, representantes de la Asamblea General de la Cooperativa, vocales de los Consejos de Administración y Vigilancia, así como el personal externo con acceso a información de la Cooperativa o de sus socios/clientes.

4. Terminología

- **Activo:** componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos, recursos económicos y recursos humanos.
- **Activos de información:** se consideran a los servicios o herramientas creados o utilizados en medios digital, físico, electromagnético y otros; hardware o software, utilizados para el procesamiento, transferencia o almacenamiento de información; y, cualquier dato que tenga información valorada por la Cooperativa o que deba ser protegido como: infraestructura física como servidores, equipos de comunicación, equipos de usuario final, servicios, las personas y sus calificaciones, habilidades y experiencia e intangibles, como reputación e imagen.
- **Amenaza:** son acciones que pueden comprometer la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos.
- **Análisis de riesgos:** proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. El análisis de riesgos proporciona la base para la estimación de riesgos y las decisiones sobre el tratamiento de riesgos. El análisis de riesgos incluye la estimación de riesgos.
- **Aplicativo Móvil:** también conocido como app móvil, es un tipo de software diseñado para ejecutarse en un dispositivo móvil, como un teléfono inteligente o una tableta. Estas aplicaciones móviles suelen estar diseñadas para proporcionar a los usuarios una experiencia específica orientada a la realización de tareas.
- **Autenticación:** provisión de una garantía de que una característica afirmada por una entidad es correcta.

- **Cargos Similares:** cargos con nivel de Subgerencia, Dirección o Jefatura, pero que su denominación es diferente (Auditor Interno, Oficial de Cumplimiento, etc.)
- **Computación en la nube**: modelo de servicios de tecnología de la información que proporciona acceso a recursos informáticos, como almacenamiento, servidores y software, a través de internet.
- **Comunicación en línea externa:** es aquella que se lleva a cabo a través de los medios sociales y las diferentes plataformas que existen en Internet. Esta comunicación suele ser bidireccional, ya que permite que el emisor y el receptor puedan intercambiar opiniones sobre los mensajes que se ponen de manifiesto.
- **Confidencialidad:** característica de la información que se enfoca en mantener la información únicamente disponible para personal autorizado.
- **Control:** actividad para reducir el impacto o probabilidad de ocurrencia de un evento de riesgo.
- **Control de acceso:** significa garantizar que el acceso a los activos esté autorizado y restringido según los requisitos comerciales y de seguridad.
- **Control preventivo:** control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.
- **Ciberseguridad:** políticas, procedimientos y medidas de protección de la infraestructura tecnológica y de activos de información, a través del tratamiento de las amenazas que ponen en riesgo la información procesada, almacenada y transportada por los diferentes componentes tecnológicos interconectados.
- **Cifrado simétrico:** es un método de cifrado que utiliza una sola clave para cifrar y descifrar datos.
- **Cifrado asimétrico:** es una técnica que utiliza dos claves para cifrar y descifrar datos, una de las claves es pública y la otra es privada.
- **Clave privada:** es un código que se utiliza para cifrar y descifrar datos, y que solo conoce su propietario.
- **Clave publica**: es una clave que está disponible para que cualquiera pueda utilizarla, se utilizan en la criptografía para cifrar y descifrar datos.
- **Datos personales**: dato que identifica o hace identificable a una persona natural, directa o indirectamente.
- **Desarrollo, Seguridad y Operaciones (DevSecOps):** es un enfoque que aborda la cultura, la automatización y el diseño de plataformas, e integra la seguridad como una responsabilidad compartida durante todo el ciclo de vida de la TI.
- **Disponibilidad:** característica de la información que se enfoca en asegurar que los usuarios la podrán acceder cuando la necesiten.
- **Dueño de la información:** es quien tiene la autoridad sobre cómo se maneja, clasifica y utiliza la información. Es responsable de tomar decisiones relacionadas con la gestión de los datos, incluyendo su inventario, uso aceptable, clasificación y devolución.

- **Evento:** ocurrencia o cambio de un conjunto particular de circunstancias. Un evento puede ser una o más ocurrencias y puede tener varias causas. Un evento puede consistir en que algo no suceda. Un evento a veces puede ser referido como un "incidente" o "accidente".
- **Evento de seguridad de la información:** cualquier ocurrencia que puede afectar o que afectado la confidencialidad, integridad y disponibilidad de la información y los sistemas.
- **Gestión de incidentes de seguridad de la información:** procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
- **Gestión de riesgos:** desarrollo estructurado y aplicación de la cultura de gestión, a través de políticas, procedimientos y prácticas por medio de la definición de actividades para la identificación, análisis, evaluación y control de los riesgos.
- **Identificación de riesgos:** proceso de encontrar, reconocer y describir riesgos. La identificación de riesgos implica la identificación de las fuentes del riesgo, eventos, sus causas y sus posibles consecuencias. La identificación de riesgos puede involucrar datos históricos, análisis teóricos, opiniones informadas y de expertos, y las necesidades de las partes interesadas.
- **Incidente de seguridad de la información:** cualquier suceso que compromete o es capaz de comprometer la confidencialidad, disponibilidad o integridad de la información. Estos incidentes pueden incluir, pero no se limitan a, accesos no autorizados, robo de datos, interrupciones de servicios, infecciones de malware, y violaciones de políticas de seguridad.
- **Integridad:** característica de la información enfocada en mantener la información en las condiciones en que fueron creadas, sin modificaciones no autorizadas.
- **Inventario de activos:** lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.
- **ISO 27001:** norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002.
- **ISO 27002:** la norma 27002 de la Organización Internacional para la Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) es un reglamento reconocido a escala internacional que establece buenas prácticas para la seguridad de la información.
- **ISO 27017:** contiene directrices sobre los controles de seguridad de la información correspondientes al aprovisionamiento y uso de servicios en la nube.
- **ISO 27018:** protección de información personal en la nube.

- **ISO 27032:** la Organización Internacional de Normalización (ISO) creó el estándar 27032 enfocado en ciberseguridad, teniendo en cuenta que este es uno de los mayores riesgos a los que se enfrentan las empresas en la actualidad.
- **Monitoreo:** es el conjunto de técnicas visuales y auditivas para determinar el estado de un sistema, un proceso o una actividad. Para determinar el estado, puede ser necesario verificar, supervisar u observar críticamente.
- **PCI CP:** la normal internacional PSI CP (Payment Card Industry Car Production) por sus siglas en inglés, describe los requisitos de seguridad necesarios para el desarrollo, fabricación, personalización, transporte, y entrega de tarjetas de crédito; la seguridad física y lógica es su principal objetivo.
- **PCI DSS:** el estándar internacional de seguridad de datos de la industria de tarjetas de pago (en inglés Data Security Standard, DSS). Es la normativa que define el conjunto de requerimientos para gestionar la seguridad, definir las políticas y procedimientos, con el propósito de reducir el riesgo de fraude con tarjetas de crédito.

  Cualquier organización y sus proveedores críticos que, por su actividad participen en el procesamiento, transmisión o almacenamiento de información de tarjetas de crédito, están en la necesidad de cumplir con los requerimientos que establece PCI DSS.

  La norma PCI DSS especifica en su requerimiento 12 la necesidad de crear y mantener políticas de seguridad de la información.
- **PCI PTS:** el estándar internacional PCI PTS (Payment Card Industry PIN Transaction Security) por sus siglas en inglés, recoge los requisitos de seguridad para transacciones con PIN, está dirigido a los productores de los dispositivos de pago, para quienes definen los requisitos que deben seguir en el diseño, fabricación y transporte de estos dispositivos, así como, para las entidades que los utilicen; su principal objetivo es definir requerimientos de seguridad que reduzcan la probabilidad impactos de compromiso del PIN.
- **RBAC:** es un mecanismo de control de acceso que define los roles y los privilegios para determinar si a un usuario se le debe dar acceso a un recurso. Los roles se definen en función de características como la ubicación, el departamento o las funciones de un usuario. Los permisos se asignan según el acceso (lo que el usuario puede ver), las operaciones (lo que el usuario puede hacer) y las sesiones (cuánto tiempo puede hacerlo el usuario).
- **Riesgo:** es la posibilidad de que se produzca un evento que genere una afectación con un determinado nivel de impacto para la entidad. El riesgo se mide en términos de impacto y probabilidad.
- **Riesgo residual:** nivel de riesgo que resulta, una vez implementados los controles.
- **Segregación de funciones:** las funciones y áreas de responsabilidad deberán segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas, no intencionadas o usos indebidos de los activos de la Cooperativa, se deberá cuidar el hecho de que una persona por sí sola no pueda acceder, modificar o utilizar los activos sin autorización o sin que se detecte. En transacciones sensibles, se deberán implementar controles que garanticen que la persona que ingresa la solicitud o efectúa la transacción requiera la autorización de un superior.

- **Seguridad de la información:** son los mecanismos que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados.
- **Sistema de Gestión de la Seguridad de la Información (SGSI):** conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.
- **Sistema de Información:** conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes que manejan información.
- **Software:** software es un término informático que hace referencia a un programa o conjunto de programas de cómputo, así como a datos, procedimientos y pautas que permiten realizar distintas tareas en un sistema informático.
- **Soluciones MDM:** gestión de administración de dispositivos móviles, que se utilizan para acceder a información o recursos de la organización, asegurar los datos y mantener la productividad.
- **Titular del Activo:** se refiere a la persona física o jurídica que posee la propiedad o el derecho sobre un activo específico.
- **Técnicas de cifrado clave privada (cifrado simétrico):** cuando dos o más actores comparten la misma clave y esta se utiliza tanto para cifrar información como para descifrarla. Esta clave tiene que mantenerse en secreto dado que una persona que tenga acceso a la misma podrá descifrar toda la información cifrada con dicha clave, o introducir información no autorizada.
- **Técnicas de cifrado de clave pública (cifrado asimétrico):** cuando cada usuario tiene un par de claves: una clave pública (que puede ser revelada a cualquier persona) y una clave privada (que debe mantenerse en secreto). Las técnicas de clave pública pueden utilizarse para el cifrado y para generar firmas digitales.
- **Trazabilidad:** cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.
- **Vulnerabilidad:** se define como una debilidad o un fallo en un sistema de información que puede ser explotada por un atacante para comprometer la confidencialidad, integridad y disponibilidad de los datos.

5. Políticas o Lineamientos

5.1 Aplicación de los Controles de Seguridad

La Cooperativa define como activos estratégicos la información y los sistemas que la tratan, manifestando la determinación en alcanzar los niveles de seguridad necesarios que garanticen su protección.

Dicha seguridad será alcanzada mediante la implantación y gestión de los controles de seguridad adecuados (organizacionales, personas, físicos y controles tecnológicos), que son:

- Controles de seguridad que permitan la implementación de las políticas del presente documento, incluyendo los controles de seguridad que disponga la legislación y marco normativo.
- Controles de seguridad adicionales que se identifiquen como resultado de los análisis de riesgos.

5.2 Análisis y Gestión de Riesgos

La Cooperativa cuenta con la *Metodología de Evaluación de Riesgos de Seguridad de la Información* alineada a la *Metodología de Riesgo Operativo* de la Dirección de Riesgos Integrales.

Los controles y medidas de seguridad a ser implementados en función a los resultados de los análisis de riesgos considerarán la norma técnica ISO/IEC 27002 de Seguridad de la Información, así como la norma técnica ISO/IEC 27032:2012 de Ciberseguridad, o las que las sustituyan.

5.3 Aplicación de Estándares Externos

La Cooperativa tiene en consideración en materia de seguridad los siguientes estándares, guías y normativas de carácter internacional, de acuerdo con las limitaciones y ámbitos de aplicación que correspondan: ISO 27001, ISO 27002, ISO 27032, PCI DSS, PCI CP, PCI PTS, y las que disponga el ente de control.

5.4 Organización y Responsabilidades del Sistema de Gestión de Seguridad de la Información (SGSI)

5.4.1 Gobierno del SGSI

5.4.1.1 Consejo de Administración

a) Aprobar el *Plan Estratégico de Seguridad de la Información*, el mismo que debe estar alineado al Plan Estratégico de la Cooperativa;
b) Aprobar los recursos humanos, técnicos y financieros que sean necesarios;
c) Aprobar políticas, procesos, procedimientos, metodologías, roles y responsabilidades;
d) Aprobar el *Plan de Concientización y Formación*; y,
e) Aprobar el *Plan de Gestión de Riesgos de Seguridad de la Información*.

5.4.1.2 Comité de Seguridad de la Información (CSI)

Integración del CSI

El Comité de Seguridad de la Información está conformado por los siguientes miembros:

- **a)** El Presidente del Comité de Administración Integral de Riesgos, quien presidirá también el Comité de Seguridad de la Información y tendrá voto dirimente.
- **b)** El Gerente o su delegado debidamente justificado su ausencia, con voz y voto.
- **c)** El Oficial de Seguridad de la Información, quien actuará como secretario del Comité solo con voz.
- **d)** El Director de Tecnologías de la Información y Comunicación o su delegado debidamente justificado su ausencia, con voz y voto.
- **e)** Un delegado de Auditoría Interna con voz y voto.

El comité podrá invitar a las sesiones a los responsables de las áreas de negocio que juzgue del caso, quienes tendrán voz, pero no voto.

En el caso de delegaciones éstas deben ser con la debida justificación y deberán ser presentadas al presidente del comité con 24 horas de anticipación.

Funciones del CSI

- **a)** Deberá proponer al Consejo de Administración:
  1. La actualización anual del *Plan Estratégico de Seguridad de la Información*, en caso de que sea pertinente;
  2. Los recursos humanos técnicos y financieros necesarios para la gestión de seguridad de la información y verificar que su inversión sea eficiente y eficaz para el logro de los objetivos estratégicos;
  3. Las políticas, procedimientos, metodologías, roles y responsabilidades para la gestión de seguridad de la información y del SGSI;
  4. El *Plan de Concientización y Formación* de su personal en temas concernientes a seguridad de la información; y,
  5. El *Plan de Gestión de Riesgos de Seguridad de la Información* y verificar que esté alineado al Plan de Administración de Riesgos.

Además, el Comité de Seguridad de la Información es responsable de:

- **b)** Aprobar la implementación de controles de seguridad de la información, propuestos por el Oficial de Seguridad de la Información (OSI);
- **c)** Informar los riesgos de seguridad de la información al Comité de Administración Integral de Riesgos, para su consolidación en la matriz de riesgos y su seguimiento; y,
- **d)** Evaluar, dirigir, monitorear y supervisar la gestión de seguridad de la información y del SGSI.

Funcionamiento del CSI:

- **a)** Las sesiones del Comité de Seguridad de la Información se instalarán con la asistencia de al menos 3 de sus miembros, entre los cuales deberá estar su presidente.

b) El Comité sesionará de manera ordinaria al menos 2 veces al año. Podrá reunirse extraordinariamente cuando el presidente lo convoque por iniciativa propia, o a petición de uno de sus miembros y/o cuando por eventos de fuerza mayor o caso fortuito lo amerite. En las sesiones extraordinarias se tratará únicamente los puntos del orden del día.
c) Las decisiones serán tomadas por la mayoría de votos.
d) Las convocatorias tendrán el orden del día y deberán ser comunicados por el presidente, al menos 48 horas de anticipación excepto cuando se trate de sesiones extraordinarias que podrán ser convocadas en cualquier momento.
e) Las sesiones podrán realizarse de manera presencial o por cualquier medio tecnológico.
f) Las resoluciones constarán en las respectivas actas, las que deberá elaborar el secretario del Comité, quien además las fechará y numerará en forma secuencial, así como estarán suscritas por los asistentes. Será responsabilidad del secretario la custodia de las actas bajo principios de confidencialidad integridad y disponibilidad de la información.
g) Los lineamientos para el funcionamiento del Comité que no se encuentren establecidos en esta sección se regirán por lo dispuesto al *Reglamento de las Comisiones y Comités*.

5.4.1.3 Comité de Continuidad de Negocio

Las responsabilidades del Comité de Continuidad del Negocio se describen en el *Manual de Gestión de Continuidad del Negocio*.

5.4.1.4 Gerente

a) Liderar la gestión de seguridad de la información y el SGSI, de acuerdo con las disposiciones del Consejo de Administración y lo dispuesto en la resolución SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002 o la que la sustituya.
b) Designar al Oficial de Seguridad de la Información (OSI); y
c) Coordinar la participación activa de todas las partes interesadas que intervienen en SGSI y en la gestión de seguridad de la información.

5.4.1.5 Subgerentes, directores, jefes o cargos similares

a) Cumplir y hacer cumplir las políticas de seguridad de la información.
b) Gestionar oportunamente los recursos necesarios para que los controles existentes dentro de sus procesos y activos de información continúen operando, así como para la implementación de nuevos controles derivados de los análisis de riesgos o evaluaciones de seguridad.
c) Implementar los controles correspondientes en sus procesos y activos de información considerando las evaluaciones de riesgos.
d) Difundir las políticas de seguridad en sus equipos de trabajo y velar por el cumplimiento de estas.
e) Designar en sus áreas de responsabilidad a personas encargadas de velar por el cumplimiento de controles en términos de seguridad de la información, y su reemplazo ya sea de forma temporal o permanente.

f) Confirmar y validar de manera oportuna la devolución de los activos de información, así como la deshabilitación de los accesos físicos y digitales del personal propio o externo que tenga a su cargo, ante procesos de desvinculación o terminación del contrato.

g) Adoptar las medidas necesarias para garantizar la adecuada "Segregación de Funciones" en los procesos del negocio, operativos y tecnológicos bajo su responsabilidad.

h) Monitorear permanentemente el cumplimiento de la "**Política de puesto de trabajo despejado y pantalla limpia**" por parte del personal a su cargo, gestionando de manera oportuna el pedido y asignación de los elementos de seguridad necesarios para cumplir con la mencionada política (llaves de escritorios, arreglo de chapas, candados para laptops, llaves de archivadores, entre otros).

5.4.2 Supervisión del SGSI

5.4.2.1 Oficial de Seguridad de la Información

La misión, competencias y responsabilidades del Oficial de Seguridad de la Información están descritas en el *Manual Orgánico Funcional de la Cooperativa*.

5.4.2.2 Analista de Ciberseguridad

La misión, competencias y responsabilidades del Analista de Ciberseguridad están descritas en el *Manual Orgánico Funcional de la Cooperativa*.

5.4.2.3 Analista de Continuidad

La misión, competencias y responsabilidades del Analista de Continuidad están descritas en el *Manual Orgánico Funcional de la Cooperativa*.

5.4.2.4 Oficial de Seguridad Física

La misión, competencias y responsabilidades del Oficial de Seguridad Física están descritas en el *Manual Orgánico Funcional de la Cooperativa*.

5.4.2.5 Auditor interno

La misión, competencias y responsabilidades del Auditor Interno están descritas en el *Manual Orgánico Funcional de la Cooperativa*.

5.4.2.6 *Operación del SGSI*

Para la administración de los activos de información del Sistema de Gestión de Seguridad de la Información de la Cooperativa, se establecen los siguientes roles o funciones:

5.4.2.7 Dueño de la Información

Director, jefe o cargo similar, es responsable de cuidar la integridad, confidencialidad y disponibilidad del activo de información que le ha sido asignado; debe ejercer su autoridad para especificar y exigir las medidas de seguridad necesarias para la información y para los sistemas que la gestionan. Es el responsable de aceptar los riesgos inherentes y residuales identificados en los activos de información. En el *Anexo A Dueños de la Información*.

Sus responsabilidades son:

a) Velar por el cumplimiento de los controles de seguridad físicos y lógicos aplicables al activo de información.
b) Asignar a los activos de información bajo su titularidad el nivel de clasificación de la información correspondiente.
c) Levantar el inventario de sus tipos y activos de información en conjunto con el área de Seguridad de la Información cumpliendo el *Procedimiento Gestión de Activos de Información,* con el objetivo de confirmar su clasificación o proceder a reclasificarlos según corresponda.
d) Administrar los mecanismos y medidas de seguridad. Esta tarea puede ser delegada, en todo o en parte al "Encargado del Tratamiento del activo de información". Esta delegación no le exime de su responsabilidad, debiendo supervisar que las tareas delegadas son realizadas correctamente.
e) Facilitar los medios y recursos necesarios para el cumplimiento e implementación de los controles de seguridad.
f) Aprobar la estrategia de mitigación de los riesgos identificados en sus activos de información, acorde a la normativa de gestión de riesgos de Seguridad de la Información.
g) Autorizar el acceso y uso interno y externo de la información.
h) Asignar los niveles de acceso a los sistemas de información bajo su titularidad, mediante la aprobación de los perfiles y privilegios que los usuarios requieran según su cargo.
i) Solicitar bajo su criterio y necesidad al Oficial de Seguridad de la Información la realización de análisis de riesgos sobre los activos de información a su cargo.
j) Generar, promover y supervisar los requerimientos y/o realizar las gestiones necesarias para la implantación de controles derivados de los análisis de riesgos, marco normativo, informes de auditoría y demás requisitos de seguridad del activo bajo su titularidad.
k) Establecer los medios necesarios para que el personal que accede al activo de información a su cargo conozca y cumpla las normativas de seguridad requeridas para el uso de la información, así como las consecuencias en las que pudiera incurrir por su incumplimiento.
l) Definir requisitos de disponibilidad y criticidad del activo de información alineada a la estrategia de Continuidad de Negocio de la Cooperativa, facilitar los medios y recursos necesarios para el cumplimiento de estos requisitos y velar por su cumplimiento.
m) Autorizar las solicitudes de afectación o modificación directa en la base de datos de los sistemas bajo su titularidad.
n) Establecer el tiempo máximo de permanencia o custodio de información tanto en medio físico como electrónico, considerando los requerimientos legales y regulatorios.
o) Gestionar el cierre de vulnerabilidades de los activos bajo su titularidad, ya sea de manera directa o a través de los contratos de servicios pertinentes.
p) Autorizar los cambios funcionales a las aplicaciones bajo su titularidad.

La asignación de propiedad de los activos de información se podrá efectuar:

a) De forma individual para cada activo de información (por ejemplo: “el titular del sistema de Talento Humano es el Director de Talento Humano”).
b) Por proceso de negocio o naturaleza del activo de información (por ejemplo: el titular del proceso de Crédito, así como de la información sistemas informáticos relacionados con tal proceso es el Director Comercial”).
c) El Gerente delegará sus responsabilidades de seguridad a los subgerentes, directores, jefes o cargos similares mediante la designación de su titularidad en los activos de información, quienes además serán responsables de su seguridad de manera permanente. No obstante, el Gerente es en último término responsable de la seguridad del recurso y debe estar en capacidad de determinar si las responsabilidades delegadas fueron cumplidas correctamente.
d) La asignación de titularidad sobre los activos de información debe radicar en cargos de subgerentes, directores, jefes o cargos similares. No se podrá asignar la misma a cargos inferiores.
e) En última instancia el Gerente en los casos de áreas con reporte directo o los subgerentes para las demás áreas tienen la potestad de definir la titularidad de los dueños de la información de la Cooperativa.

5.4.2.8 Encargado del Tratamiento del Activo de Información

Gestiona el activo de información por cuenta del Titular. En el concepto de “tratamiento” se engloban los procesos de trabajo diario, procesos de almacenamiento, procesamiento y comunicación de la información, por lo que su definición incluye tanto a usuarios finales, como a los administradores de las plataformas informáticas.

Sus responsabilidades son:

a) Administrar los activos de información de acuerdo con las normas de seguridad correspondientes.
b) Implementar los controles de seguridad derivados de requisitos de fabricantes, normativa interna, normativa externa, vulnerabilidades identificadas y demás controles aplicables.
c) Cumplir estrictamente con los procedimientos de control de cambios establecidos en la Cooperativa.
d) Garantizar un ambiente de procesamiento y almacenamiento seguro, cuidando que se cumpla con las políticas y procedimientos de seguridad de la información en los activos de información que custodia.
e) Identificar y escalar riesgos que puedan afectar a la confidencialidad, disponibilidad e integridad de los activos o sistemas de información bajo su uso y/o administración, comunicando dicho particular a la jefatura del área, y al área de Seguridad de la Información.
f) Garantizar la disponibilidad del activo de información conforme a los acuerdos de nivel de servicios correspondientes (aplica a contratos de servicios con terceros).
g) En caso de identificar incidentes de seguridad de la información relacionados con el activo bajo su gestión o terceros que lo puedan afectar, deberá cumplir con el *Procedimiento de Incidentes y Peticiones de* Servicio; y, *Atención y Análisis de Incidentes de Seguridad de la Información* de la Cooperativa.

h) Garantizar la ejecución del proceso de respaldos, en función a las necesidades de los sistemas de información, alineado a los requisitos de continuidad y necesidades del negocio, incluyendo el tiempo de custodio y disponibilidad de estos.

5.4.2.9 Gestor de Usuarios

Son las áreas o cargos designados como responsables de gestionar las solicitudes de acceso de los usuarios (creación, deshabilitación de identificadores, gestión de perfiles, entre otros), a los sistemas de información, recursos, instalaciones, áreas de proceso de datos, servicios y redes de comunicaciones de la Cooperativa.

El detalle de los sistemas de información de la Cooperativa, sus titulares y gestores de usuarios, se especifica en el *Anexo B Titulares de Activos de Sistemas de Información*.

Sus responsabilidades son:

a) Desarrollar y mantener actualizado el instructivo para la gestión de accesos de la/s plataforma/s que administra.
b) Gestionar las solicitudes de acceso de los usuarios según el instructivo anterior, llevando un registro de las solicitudes atendidas.
c) Cumplir con los acuerdos de niveles de servicio comprometidos con el negocio.
d) Alinearse a los canales y normativa interna establecidos en la Cooperativa para la solicitud de accesos.
e) Validar el que los requerimientos cuenten con las autorizaciones necesarias. El Gestor de Usuarios no debería autorizar directamente las solicitudes de los usuarios, ni gestionar solicitudes que no dispongan de la autorización del titular del activo al que se solicita acceso.
f) En algunos casos, el titular del activo puede dejar establecidas autorizaciones predefinidas, como por ejemplo "autorizar la solicitud al sistema con el perfil de lectura a todos los colaboradores que lo soliciten", no siendo así necesaria la petición de autorización para todas las solicitudes que cumplan con el criterio predefinido. Estos criterios o autorizaciones predefinidas deben reflejarse en la Matriz de Cargo vs Perfil de Acceso debidamente firmadas por el titular del activo.
g) Bloquear los accesos de los usuarios ante la notificación de desvinculación de la Cooperativa en todos los sistemas de información.
h) Realizar la depuración mensual de las cuentas de todos los aplicativos bajo su responsabilidad, realizando la deshabilitación de identificadores correspondientes a colaboradores desvinculados y de identificadores de usuarios que no hayan realizado login en los últimos 60 días.
i) Realizar la depuración mensual de las cuentas personales del Active Directory, considerando a los colaboradores desvinculados, con permisos médicos extendidos y usuarios genéricos.
j) Realizar la depuración de los equipos de cómputo registrados en el Active Directory de forma mensual, eliminando aquellos correspondientes a colaboradores desvinculados y aquellos equipos que no hayan registrado un inicio de sesión en un periodo superior a 60 días.
k) Crear las cuentas personales, acorde a la nomenclatura de identificadores establecida en el presente documento, o justificar documentadamente la excepción correspondiente.

l) Distribuir las contraseñas, acorde a los lineamientos de entrega de contraseñas establecidos en el presente documento.

m) Deshabilitar todos los identificadores personales que no se hayan utilizado durante un periodo máximo de 60 días (periodo de inactividad).

5.4.2.10 Administrador de Contrato

Las responsabilidades del Administrador de Contrato respecto a la seguridad de la información se encuentran descritas en el *Manual de Adquisiciones y Contrataciones* y *Manual Gestión Jurídica.*

5.4.2.11 Colaboradores

Toda persona que directa o indirectamente, de forma total o parcial, accede a los datos en virtud de la "necesidad de conocer" inherente al desempeño de su actividad laboral en la Cooperativa. Sus responsabilidades en el ámbito de seguridad de la Información constan en el siguiente apartado "Obligaciones en Seguridad de la Información", del presente documento.

5.5 Obligaciones en Seguridad de la Información

5.5.1 Generales

a) Conocer y cumplir con los manuales, políticas, procedimientos, metodologías, planes, instructivos y demás documentos que publique la Cooperativa en materia de Seguridad de la Información. El desconocimiento de los documentos antes mencionados no exime de responsabilidad ante su incumplimiento.

b) Notificar apenas se conozcan incumplimientos normativos, posibles vulnerabilidades, riesgos, amenazas, incidentes o eventos sospechosos que afecten, pudieran afectar o hubieran afectado a la seguridad de la información (*Procedimiento Atención y Análisis de Incidentes de Seguridad de la Información).*

c) Participar obligatoriamente en cursos, capacitaciones, evaluación de conocimientos, conferencias o actividades, coordinadas por la Cooperativa en el ámbito de seguridad de la información.

d) Velar por la seguridad de los activos, sistemas y recursos de información que la Cooperativa pone a su disposición.

e) Utilizar adecuadamente los recursos de la Cooperativa; esto significa, pero no se limita, a que nunca se usarán activos de la Cooperativa para la publicación de material que pueda ser interpretado como ofensivo o difamatorio sobre los colaboradores, proveedores o socios/clientes en sitios de intercambio de contenido en la web, grupos de redes sociales, blogs o cualquier otra publicación digital.

f) Colaborar en las actividades relacionadas al Sistema de Gestión de Seguridad de la Información de la Cooperativa, como auditorías internas/externas, gestión de riesgos y seguimiento/implementación de acciones según corresponda.

g) Devolver todos los activos de la Cooperativa (información, dispositivos institucionales, llaves, candados de seguridad de laptops, tarjeta de identificación, tarjetas de acceso, teléfonos móviles, etc.) a la finalización de la relación laboral con la misma. En caso de proveedores y personal externo, el Administrador de Contrato será el encargado

de exigir la devolución de los activos por parte del personal de la empresa subcontratada.

5.5.2 Acceso y permanencia en instalaciones

Cumplir con las políticas establecidas en los manuales y procedimientos de Seguridad Física y Electrónica; y, Seguridad y Salud Ocupacional.

5.5.3 Uso de información y sistemas

a) Utilizar los activos, sistemas de información y redes de comunicaciones autorizados estrictamente para el cumplimiento de sus funciones dentro de la Cooperativa.
b) Acceder sólo a aquella información, sistemas, instalaciones y recursos a los que se encuentra explícitamente autorizado.
c) Cumplir con las restricciones de propiedad intelectual o industrial del software según su licencia correspondiente.
d) Intercambiar la información con empresas externas utilizando los canales, sistemas, criterios y controles establecidos en la Cooperativa, así como en los contratos de servicio correspondientes.
e) Cumplir con la Ley Orgánica de Protección de Datos Personales y su Reglamento vigente aplicable, velando por que los datos sean tratados de manera veraz, exacta y completa, respetando los principios de confidencialidad, integridad y disponibilidad según lo establecido en la normativa.
f) Finalizar las sesiones de los sistemas de información cuando no requiera su utilización.
g) Apagar de forma ordenada la estación de trabajo al finalizar la jornada laboral (salvo ciertas excepciones con la debida autorización).
h) Se autoriza la habilitación de puertos USB en la Cooperativa, para los siguientes cargos: Presidente y Secretaria del Consejo de la Administración; y, Gerente, debiendo implementarse controles de cifrado que garanticen la confidencialidad de la información de la Cooperativa almacenada en los dispositivos móviles. Toda excepción de habilitación de USB deberá ser autorizada por el Gerente en los casos de áreas con reporte directo o los subgerentes para las demás áreas.

Las siguientes actividades se encuentran explícitamente prohibidas:

a) Acceder, enviar o almacenar la información de la Cooperativa mediante canales, aplicaciones o repositorios web externos de almacenamiento que no sean de propiedad de la Cooperativa, esto incluye pero no se limita a: Google Drive, Drop Box, Whatsapp Web y demás redes sociales personales entre otros, por lo que, el intercambio de información institucional entre colaboradores, representantes de la Asamblea General, miembros de los Consejos de Administración y Vigilancia de la Cooperativa, debe ser utilizando específicamente los recursos del sistema Office 365 de la Cooperativa (Sharepoint, One Drive, Outlook).
b) Acceder o intentar acceder a información, instalaciones, equipos o sistemas informáticos a los que no se tenga explícitamente autorización, así como utilizar cuentas o credenciales de un tercero.
c) Intentar o aumentar el nivel de privilegios de su usuario o de terceros en los sistemas sin autorización.

d) Instalar software cuya licencia de uso no sea de propiedad o se encuentre bajo acuerdo de suscripción para uso de la Cooperativa, incluyendo esquemas de renta de software o servicio en la nube.

e) Instalar, configurar o desinstalar el software en los dispositivos institucionales fijos, teletrabajo y móviles. Esta actividad le corresponde única y exclusivamente al área de Mesa de Atención Técnica, por tanto, se prohíbe que los usuarios realicen este tipo de actividades.

f) Modificar, borrar o reemplazar cualquier programa, configuración o archivo que impida o dificulte el normal funcionamiento de los sistemas y equipos.

g) Desactivar o desconfigurar sin autorización los mecanismos de protección instalados en los sistemas (cortafuegos, antivirus, DLP, entre otros.)

h) Aprovechar indebidamente de las vulnerabilidades o debilidades que puedan tener los sistemas de información o redes de comunicación.

i) Conectar a la red de comunicaciones de la Cooperativa, equipos de cómputo o dispositivos de comunicación de propiedad de los colaboradores o personal externo, esto incluye, pero no se limita a: tabletas, equipos móviles, switches, hubs, excepto a redes aisladas definidas para propósitos específicos que permitan únicamente acceso a internet, o mediante el empleo de los protocolos de teletrabajo con la debida autorización.

j) Sacar respaldos de información institucional en medios extraíbles. La información que requiera ser respaldada deberá ser almacenada en nube de la Cooperativa. Todo requerimiento de copia de información hacia medios extraíbles deberá contar con la autorización del Gerente en los casos de áreas con reporte directo o los subgerentes para las demás áreas.

k) Mantener dispositivos institucionales fuera del dominio de la Cooperativa.

l) Mantener dispositivos institucionales sin los controles de seguridad mínimos establecidos en el presente manual.

5.5.4 Identificadores personales y claves de acceso

a) Cada colaborador es responsable de las acciones relacionadas al uso de los identificadores, contraseñas y cuentas institucionales que le han sido asignados.

b) Las contraseñas son personales, secretas e intransferibles, debiéndose mantener su confidencialidad sin excepción.

c) No se escribirán o mantendrán contraseñas en papel, a menos que esta cumpla con los principios de debido resguardo y pueda ser almacenada en forma segura (caja fuerte).

d) No se permite la escritura, copia o reproducción de contraseñas en ficheros electrónicos sin cifrado.

e) Para almacenamiento de contraseñas en medios digitales, se lo realizará utilizando el sistema de gestión de contraseñas “Password Safe”.

f) Los usuarios deberán efectuar el cambio de sus contraseñas de manera mensual de acuerdo con la política “Período y mecanismo de cambio de contraseñas” del presente manual.

g) Siempre que exista una sospecha de perdida de confidencialidad de contraseñas el usuario debe gestionar el cambio inmediato de las mismas, debiendo reportar el incidente al área de Seguridad de la Información cumpliendo el *Procedimiento de Atención* y *Análisis de Incidentes de Seguridad de la Información y Ciberseguridad*.

h) No se deberán utilizar palabras del diccionario, números de cedulas, fechas de nacimiento o partes del nombre o apellido del usuario para generar contraseñas.
i) Se prohíbe el uso de contraseñas de la Cooperativa en servicios externos o personales (por ejemplo, en cuentas de correo gratuitas de Internet, blogs, entre otros.) u otros propósitos ajenos a la Cooperativa.
j) Se prohíbe intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de la Cooperativa.
k) En caso de evidenciarse compartición de contraseñas o uso de cuentas de terceras personas, se aplicará el régimen disciplinario tanto al dueño de las credenciales como a la persona que utilizó las mismas.

5.5.5 Uso de correo electrónico

a) La Cooperativa establece como herramienta oficial de comunicación electrónica el servicio de correo institucional bajo el dominio: "@29deoctubre.fin.ec", por tanto, el intercambio de información institucional deberá ser a través de la cuenta de correo institucional entre personal, representantes de la Asamblea General, miembros de los Consejos de Administración y Vigilancia de la Cooperativa.
b) Los mensajes de correo electrónico pueden ser tratados como comunicaciones públicas, por lo que debe seleccionarse cuidadosamente la información enviada por esta vía.
c) Cada colaborador es responsable de las acciones relacionadas al uso de correo electrónico institucional que le ha sido asignado.
d) Los correos electrónicos que se creen en el día a día constituyen documentos oficiales de la Cooperativa, por lo que podrán ser solicitados por la Gerencia como evidencia de políticas, acciones, decisiones, transacciones oficiales y de la gestión efectuada por el colaborador.
e) Se autoriza el servicio de correo electrónico para envío de correos internos a todo el personal que por sus funciones requiera de dicho servicio.
f) El servicio de correo electrónico institucional y la información gestionada es propiedad de la Cooperativa.
g) Se considera correo electrónico institucional tanto el interno, entre terminales de la red de la Cooperativa, como el externo, dirigido o proveniente de otras redes públicas o privadas y especialmente, de Internet.
h) Cualquier archivo introducido en la red institucional o en el dispositivo institucional a través de mensajes de correo electrónico que provengan de redes externas, deberá cumplir los requisitos establecidos en la presente norma y en las referidas a propiedad intelectual e industrial y a control de virus.

Las siguientes actividades están expresamente prohibidas:

a) Enviar mensajes de correo electrónico de forma masiva o con fines personales, comerciales o publicitarios ajenos a las tareas laborales (Spam).
b) Enviar o reenviar indebidamente mensajes en cadena o de tipo piramidal.
c) Enviar mensajes con anexos de gran tamaño (capacidad), que genere afectación de los servicios de red.
d) Enviar o reenviar correos con información institucional, hacia cuentas de dominio personales o de terceros, sin la debida autorización.

e) Enviar y recibir mensajes de correo electrónico de dominios gratuitos, salvo se cuente con la autorización del Gerente en los casos de áreas con reporte directo o de los Subgerentes para las demás áreas, registrado en el formulario que corresponda.
f) Falsificar mensajes de correo electrónico.
g) Abrir archivos de fuentes con dudosa procedencia sin consulta previa al área de Mesa de Atención Técnica para su escalamiento al área de Seguridad de la información.
h) Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios sin su consentimiento.
i) Enviar mensajes o imágenes con material ilegal, ofensivo, difamatorio, inapropiado o con contenidos discriminatorios por razones de género, edad, sexo, discapacidad, etc., o de aquellos que promuevan el acoso sexual.
j) Acceder a servicios de correo electrónico externos, desde la infraestructura de comunicaciones de la Cooperativa, ya sean públicos, privados o de otras instituciones o empresas, esto incluye, pero no se limita a: Gmail, Hotmail, Yahoo Mail, entre otros.
k) Efectuar respaldos de buzones y correos electrónicos institucionales, en medios extraíbles (discos externos, memorias flash, cds) o en sitios de almacenamiento en la nube que no sean de propiedad y estén bajo autorización explícita de la Cooperativa (Dropbox, Google Drive, entre otros).
l) Enviar correos con copias ocultas, a excepción de comunicaciones enviadas de manera masiva por personal autorizado por el Gerente en los casos de áreas con reporte directo o los subgerentes para las demás áreas.
m) Acceder a los sistemas de información y a la red institucional desde fuera de la infraestructura de la Cooperativa sin conectarse previamente mediante VPN.
n) Acceder a los sistemas de la Cooperativa desde equipos personales que no estén autorizados y registrados por parte de la Cooperativa y a los cuales no se les haya aplicado las medidas de seguridad que garanticen el manejo y control adecuado de la información institucional dispuestas en la presente normativa o por el área de Seguridad de la Información derivadas del análisis de riesgos.
o) Conectarse a la red institucional y a los sistemas institucionales desde fuera de la infraestructura de la Cooperativa sin el uso de doble factor de autenticación.
p) Salvo pedidos explícitos de entes de control, o casos excepcionales autorizados por escrito por el Gerente en los casos de áreas con reporte directo o los subgerentes para las demás áreas se deberá evitar la grabación de información institucional en dispositivos extraíbles, promoviendo la compartición de dicha información mediante medios electrónicos y canales autorizados por la Cooperativa con los debidos controles de seguridad.
q) Salvo pedidos explícitos de entes de control, o casos excepcionales autorizados por escrito por el Gerente en los casos de áreas con reporte directo o los subgerentes para las demás áreas se deberá evitar la impresión de documentos con clasificación Restringida y Confidencial, promoviendo la compartición de dicha información mediante medios electrónicos con los debidos controles de seguridad.

La Cooperativa se reserva el derecho de revisar, sin previo aviso, los mensajes de correo electrónico enviados, recibidos o creados con la cuenta de correo institucional y los archivos LOG del servidor (registros de auditoría), con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a Cooperativa o hacerla incurrir en responsabilidad.

5.5.6 Uso, acceso y control de internet

a) El presente manual no abarca todos los aspectos negativos en los que se pueda incurrir en la utilización de Internet. Por lo tanto, toda actividad que: viole la ley, las regulaciones, el *Reglamento Interno de Trabajo* o que perjudique el desempeño de la red, de los servicios, de la imagen de la Cooperativa o afecte las relaciones con los socios/clientes y demás colaboradores, así no se mencione o incluyan dentro de este documento, se entenderán comprendidas en éste.

b) Cada colaborador es responsable de las actividades relacionadas al uso de internet en su máquina o con el identificador personal que le ha sido asignado.

c) Los accesos a internet serán dados en función a los perfiles de navegación establecidos para cada cargo de acuerdo con lo definido por el área de Seguridad de la Información, las excepciones deberán solicitarse mediante la herramienta Soluciones 29 únicamente por los directores y en los casos de jefaturas con reporte directo al Gerente serán autorizadas por el Oficial de Seguridad de la Información.

d) El acceso a Internet mediante la red Wi-Fi a las redes autorizadas para los colaboradores está permitido únicamente para los dispositivos institucionales, siempre y cuando se valide que estos cuenten con todas las configuraciones de seguridad y hardening adecuadas.

e) Las redes Wi-Fi deberán aplicar el perfilamiento de navegación de acuerdo con la "Matriz de Perfiles de Navegación" autorizada por el Oficial de Seguridad de la Información.

f) Para los visitantes o proveedores que requieran acceso a Internet, el colaborador responsable deberá solicitar motivadamente la autorización al Oficial de Seguridad de la Información e ingresar el requerimiento a través de la herramienta Soluciones 29.

g) Se debe usar redes segmentadas para los colaboradores y visitantes o proveedores.

h) Para permitir la conexión Wi-Fi, deberá implementar un método de autenticación o filtrado adicional.

i) Los usuarios autorizados a usar el internet deben hacerlo únicamente en actividades relacionadas con su trabajo.

j) El Oficial de Seguridad de la Información, deberá autorizar la descarga de información, archivos de programas con o sin licencia, licencia de pruebas o licencia universal, ya sea por motivos de prueba o uso temporal debidamente justificado y aceptado formalmente por parte del director y en los casos de jefaturas con reporte directo al Gerente serán autorizadas por el Oficial de Seguridad de la Información.

k) El área de Seguridad de la Información deberá controlar la navegación de Internet de los colaboradores conectados a la red LAN y Wi-Fi, en función de los perfiles autorizados.

Las siguientes actividades están expresamente prohibidas:

a) Visitar sitios cuyo contenido sea ofensivo (racismo, intolerancia, agresividad, etc.)

b) El acceso a debates en tiempo real (chat / redes sociales), salvo en aquellos supuestos en que esté relacionado con los cometidos del puesto de trabajo del colaborador y autorizados por la Cooperativa.

c) Buscar información que contenga o pueda afectar en cualquier sentido seguridad y reputación de la Cooperativa o sus actividades.

d) Acceder o publicar cualquier información referente a, o que contengan pornografía moderada o explícita (incluye imágenes de desnudos parciales o totales que pueden o no incluir acto sexual).
e) Publicar información de la Cooperativa en medios electrónicos, sin que ésta haya sido revisada y aprobada.
f) Usar el dispositivo institucional o su acceso a internet para perpetrar cualquier tipo de fraude o piratería tanto de software como de vídeo o música.
g) Realizar cualquier actividad comercial (legal o ilegal) no relacionada a la Cooperativa.
h) Usar el sistema para enviar material ofensivo o acosador a otros usuarios dentro o fuera de la Cooperativa.
i) Realizar cualquier actividad deliberada que consuman los recursos de la red (ancho de banda, acceso a otros servidores, etc.), como la descarga de archivos de gran tamaño. Ejemplo: vídeos audio, software legal de gran tamaño. La descarga de archivos o programas incluye, pero no se limita a:
- Software gratuito, con o sin licencia.
- Software de prueba.
- Archivos de vídeo o audio como, pero sin limitarse a: mp3, mpg4, avi, ogg, etc.
- Archivos de imágenes, fondos de pantallas o similares
- Utilitarios.
- Software o aplicaciones licenciadas (cuya licencia de uso no sea de propiedad o no haya sido adquirida por la Cooperativa, o que su uso no haya sido explícitamente aprobado por la Cooperativa)

j) Intentar acceder sin autorización a los sitios restringidos mediante la utilización de herramientas o sitios web que permitan evadir los controles o cualquier otro medio no permitido legítimo.
k) Entrar o visitar sitios de procedencia desconocida o dudosa.
l) Hacer clic en anuncios comerciales de cualquier tipo o ventanas emergente (aun cuando la misma reporte de daños o problemas en su estación de trabajo).
m) Usar los dispositivos institucionales para navegación recreativa.
n) Descargar y ejecutar aplicaciones de internet.
o) Instalar plugins de terceros en el explorador de internet sin aprobación explícita (ver secciones "**Excepciones**" de este manual).
p) Entregar o escribir información confidencial como contraseñas, números de tarjetas de débito, números de tarjetas de crédito, nombres de socios/clientes, teléfonos, u otros similares en formularios, foros de discusión, blogs, etc.

La Cooperativa se reserva el derecho de monitorizar y comprobar, de forma aleatoria y sin previo aviso, cualquier sesión de acceso a Internet iniciada por un usuario de la red institucional.

5.5.7 Uso de comunicaciones en línea y redes sociales

5.5.7.1 Transparencia

a) Solamente aquel representante, vocal, colaborador o proveedor autorizado explícitamente para hablar en el nombre de la Cooperativa podrá hacerlo y deberá indicar de forma inequívoca si lo hace en su propio nombre o en el de Cooperativa.

b) Nadie podrá afirmar o hablar en el nombre de la Cooperativa o expresar una posición oficial de la Cooperativa en redes sociales o comunicaciones en línea externas sin estar expresamente autorizado para ello, debiendo indicar cuál es su puesto en la Cooperativa. El representante, vocal, colaborador o proveedor también deberá informar cuál es su relación con la Cooperativa cuando le sea solicitado.

c) En cualquier caso, el representante, vocal, colaborador o proveedor, a menos que esté autorizado a hablar en el nombre de Cooperativa, debe dejar claro que son opiniones exclusivamente suyas y que no reflejan necesariamente las opiniones o posiciones de Cooperativa.

5.5.7.2 Precisión en la información

a) Ningún representante, vocal, colaborador o proveedor divulgará deliberadamente una información falsa, engañosa o que induzca a errores en relación con la Cooperativa.

b) Las comunicaciones se basarán en datos actuales, exactos, completos, no restringidos y no confidenciales. La Cooperativa tomará todas las medidas razonables para asegurarse de la validez de la información comunicada a través de cualquier canal, pero es el representante, vocal, colaborador o proveedor en primer lugar, el que tiene la responsabilidad de asegurar su precisión. Las anécdotas y las opiniones serán identificadas como tales.

5.5.7.3 Protección de la información restringida y/o confidencial

a) Todo representante, vocal, colaborador o proveedor debe proteger la información de la Cooperativa.

b) En ningún caso se divulgará o comentará en redes sociales o comunicaciones en línea externas a la Cooperativa información restringida y/o confidencial que no se haya hecho pública previamente por el dueño de la información.

c) Ante la duda, representante, vocal, los colaboradores o proveedores deben abstenerse de publicar la información hasta que se haya obtenido la autorización interna pertinente para su publicación.

d) Los representante, vocal, colaboradores o proveedores deben respetar las normas de divulgación de información relevante y financiera. Se deberá tener especial atención a su carácter sensible y no se deberá publicar, ni comentar, de ningún modo y en ningún lugar, información que esté clasificada, o pueda ser restringida y confidencial, aplicando los requisitos de seguridad establecidos en el presente documento.

e) Igualmente, deben tener especial atención con la información relativa a productos, servicios, actividades o estrategias de la Cooperativa y se abstendrán de publicar material (texto, vídeo, audio o imágenes) que pueda dañar a la marca de la Cooperativa y/o alguna de sus marcas registradas (nombres de productos y servicios. En cualquier caso, se deben tener en cuenta las directrices internas. En ningún caso harán comentario sobre los productos, servicios, actividades o estrategias que no hayan sido anunciados oficialmente.

5.5.7.4 Respeto de los derechos de propiedad intelectual

a) Todos los representante, vocal, colaboradores o proveedores deben respetar los derechos de terceros en las redes sociales y comunicaciones en línea, en particular los derechos de autor, marcas registradas y derechos de publicidad. Si se publica algo

que está protegido por los derechos de autor (por ejemplo, una fotografía) se debe obtener un permiso por escrito tanto del autor como de las personas que aparezcan.

5.5.7.5 Responsabilidad

a) El representante, vocal, colaborador o proveedor será considerado responsable directo de la información que comparta en sus actividades online y redes sociales, debiendo tener cuidado con lo que publica, expone o divulga de cualquier forma.
b) El representante, vocal, colaborador o proveedor debe tratar de garantizar que sus comunicaciones reflejen la identidad y valores de la Cooperativa.

5.5.7.6 Privacidad

a) El representante, vocal, colaborador o proveedor debe proteger su propia privacidad para evitar ser víctima de robo de identidad o fraude. Es altamente recomendable no compartir datos personales, como cumpleaños, dirección postal, dirección de correo electrónico o número de teléfono en ningún perfil. Naturalmente esto no aplica en redes sociales de ámbito "institucional", dirigidas a facilitar la colaboración en el entorno laboral, en las cuales es conveniente incluir en el perfil aquellos datos profesionales que muestren al resto de la organización el puesto de trabajo, responsabilidades, intereses, áreas y datos de contacto profesionales. También es importante mantener la información protegida y utilizar sitios que tengan las configuraciones de seguridad y privacidad activas.
b) El representante, vocal, colaborador o proveedor debe respetar la privacidad de otros usuarios, debiéndose cuidar especialmente la publicación de cualquier información de carácter personal de otras personas, observando lo indicado al respecto en los apartados anteriores. Se prohíbe almacenar información de carácter personal de socios o clientes en equipos personales, así como su envío o publicación mediante redes sociales.
c) Se debe acatar el estricto cumplimiento de la Ley Orgánica de Protección de Datos Personales y su reglamento.

5.5.7.7 Titularidad

a) El representante, vocal, colaborador o proveedor que, para el ejercicio de sus funciones para con la Cooperativa, participe en la gestión de redes sociales, tanto si las ejercitan en nombre y representación de la Cooperativa, como en calidad de colaborador o proveedor de la misma, bien a través de una cuenta registrada a nombre de la Cooperativa, o bien, en su propio nombre, debe cesar en el uso de los contactos, grupos e información que haya adquirido durante el transcurso de la relación contractual que le vincula a la Cooperativa y por razón de ella, en el momento en que se extinga dicho vínculo o cuando así lo determine la Cooperativa.
b) En consecuencia, debe devolver los mismos a su titular, la Cooperativa, para que ésta última pueda hacer uso de ellos con el carácter pleno y exclusivo.

5.5.7.8 Directrices

Cuando el representante, vocal, colaborador o proveedor entre en una Red Social pondrá especial atención en el cumplimiento de las siguientes directrices:

a) Revisar su cuenta y su configuración de privacidad, asegurándose de saber quién puede acceder a las publicaciones antes de publicarlas. También debe comprobar que no está revelando más información personal que la estrictamente necesaria.
b) No divulgar o utilizar su cuenta institucional de la Cooperativa en las redes sociales.
c) No usar la misma contraseña de sus cuentas institucionales en las redes sociales.
d) Revisar sus mensajes antes de publicarlos, asegurándose de que no revelen nada que no debieran revelar.
e) En redes externas, considerar detenidamente las solicitudes de conexión, sobre todo si son de personas que no conoce. No revelar más información personal y/o profesional de la necesaria. Escribir en primera persona.
f) No hablar en nombre de la Cooperativa, a no ser que se esté expresamente autorizado para ello.
g) Asegurarse de que se está autorizado a hacer declaraciones en el nombre de la Cooperativa. Si tiene alguna duda sobre este punto, deberá consultar a su jefe directo.
h) Respetar el presente manual, la legislación aplicable, incluyendo las leyes sobre difamación, discriminación, acoso, regulación y los derechos de autor y uso legítimo.
i) No utilizar el logotipo de la Cooperativa ni las marcas comerciales de la Cooperativa a menos que se esté específicamente autorizado para ello.
j) No divulgar informaciones internas, restringidas y confidenciales, ni ninguna información propiedad de la Cooperativa que no sea de dominio público, información estratégica o financiera, los productos actuales o los previstos, el software, la investigación, los inventos, los procesos, las técnicas, los diseños u otros datos técnicos.
k) Obtener el permiso del propietario de una obra intelectual antes de compartir o publicar su obra.
l) No hacer referencia a los colaboradores de la Cooperativa, socios, clientes o proveedores sin su aprobación.
m) En el caso de publicar contenido en algún sitio que no pertenezca a la Cooperativa y que tenga algo que ver con lo que hace o esté relacionado con temas de la Cooperativa, utilizar un aviso legal como éste: "Lo que se publica en este sitio es opinión exclusivamente personal".
n) Asegurarse de que sus actividades online no interfieran con el desempeño de su trabajo.
o) No acceder a contenidos inapropiados o ilegales.
p) No comparar productos ni servicios de otras empresas con los de la Cooperativa.
q) No crear perfiles de Redes Sociales en nombre de la Cooperativa sin la autorización correspondiente por parte del Subgerente de Negocios.
r) Finalizar en el uso de los contactos, grupos e información que hayan adquirido como consecuencia de la gestión de Redes Sociales en su ámbito de trabajo, durante el transcurso de la relación laboral que les vincula con la Cooperativa y por razón de esta, en el momento en que se extinga dicho vínculo o cuando así lo determine de la Cooperativa.
s) Queda expresamente prohibido utilizar el nombre y logotipo de la Cooperativa en redes sociales y comunicaciones en línea personales, para proselitismos políticos internos o externos a la Cooperativa.

t) Queda expresamente prohibido el envío de fotos de socios/clientes y familiares, fotos de sus sitios de trabajo, fotos de sus domicilios, ubicación por medio de WhatsApp o cualquier otra red social no autorizada por la Cooperativa.

5.5.7.9 Uso de redes sociales institucionales

a) Antes de crear un sitio de Red Social Institucional debe obtener la aprobación del Subgerente de Negocios. Esta creación necesariamente debe seguir e incluir los siguientes aspectos:
- Involucrar a las áreas de Seguridad de la Información y Dirección de TIC en la definición del proyecto.
- Tener en cuenta la información intercambiada, clasificándola como confidencial, restringida, de uso interno o pública, implementando los niveles de protección y las medidas de seguridad en función de dicha clasificación, acorde al presente manual.
- Configurar los controles en los canales en línea y redes sociales para impedir que la información publicada sea modificada, alterada o borrada de forma ilícita.

b) Si ya hay alguna Red Social Institucional creada antes de la fecha de publicación de este manual ésta debe ser revisada por el Subgerente de Negocios para su aprobación y adhesión a todos los procedimientos establecidos en el presente manual.

c) Si un colaborador y/o proveedor desea hacer uso oficial de las redes sociales y convertirse en un portavoz oficial, debe obtener la autorización del Subgerente de Negocios.

d) Una vez que le sea concedida la autorización oficial, el colaborador y/o proveedor podrá participar en una red desempeñando su papel, haciéndolo en conformidad con este manual y la legislación aplicable.

e) Si el colaborador tiene alguna duda o preocupación sobre la utilización de las redes sociales y el presente manual, dirigirá sus preguntas al Subgerente de Negocios u Oficial de Seguridad de la Información.

5.5.8 Políticas de puesto de trabajo despejado y pantalla limpia

Al levantarse de su puesto de trabajo, durante la hora de almuerzo y al finalizar la jornada laboral el colaborador deberá:

a) Despejar su escritorio de documentos físicos y/o medios extraíbles que contengan información propiedad de la Cooperativa o de sus socios/clientes, éstos deben guardarse en un lugar seguro y bajo llave.

b) Los gabinetes, cajones y archivadores de contengan documentos y/o medios extraíbles con información cuya clasificación no sea Pública deben quedar cerrados.

c) No se deberán dejar expuestas llaves de archivadores, oficinas o escritorios.

d) Bloquear el o los equipos en los que se encuentre trabajando.

e) Las laptops deberán estar ancladas a los escritorios con los candados de seguridad debidamente instalados.

De manera permanente el colaborador deberá:

a) Evitar almacenar en el escritorio (pantalla) del equipo asignado ningún tipo de archivo, salvo los accesos directos a las aplicaciones necesarias para el cumplimiento de sus funciones.

b) Toda la información generada o que sea utilizada para el desempeño de sus actividades, deberán ser colocadas en el almacenamiento de la nube institucional. Bajo ningún motivo deberá mantener información almacenada de manera local (dispositivo institucional).
c) Cuando se imprima o digitalice documentos con información cuya clasificación no sea Pública, deberá ser retirada del equipo inmediatamente.
d) Los dispositivos de impresión y digitalización deben permanecer limpios de documentos.
e) No está permitido mantener cajas con documentación Restringida o Confidencial dentro de las oficinas o pasillos, sin que se cuente con controles de acceso físico que limiten el acceso a esta documentación.
f) Evitar escribir las contraseñas de acceso a los sistemas de información en cuadernos, pizarras, o cualquier mecanismo impreso de acceso visual, entre otros.
g) Los puestos de trabajo deben permanecer limpios y ordenados.

5.6 Seguridad en Recursos Humanos

5.6.1 Para el ingreso de personal

a) La Dirección de Talento Humano deberá cumplir con los controles determinados en el *Procedimiento de Reclutamiento y Selección* de la Cooperativa.
b) Una vez seleccionado y contratado un nuevo colaborador, durante el *Procedimiento de Inducción del Personal* se deberá realizar la comunicación de las políticas, procedimientos y responsabilidades generales de seguridad de información.
c) Se deberá considerar, la comunicación a las áreas pertinentes para que asignen los recursos y accesos tanto físicos como lógicos que correspondan para el nuevo colaborador.

5.6.2 Acuerdo de confidencialidad y no competencia

El Director de Talento Humano deberá gestionar la firma del Acuerdo de Confidencialidad y no Competencia, con los colaboradores, previa la revisión del contenido con la Dirección Jurídica, o quien haga sus veces, documento que deberá ser firmado previo a que se le dé al colaborador acceso a los recursos de tratamiento de información de la Cooperativa.

5.6.3 Durante el empleo

a) La Dirección de Talento Humano deberá realizar evaluaciones periódicas de los colaboradores en lo referente a las competencias para el desempeño del cargo.
b) La Dirección de Talento Humano deberá coordinar con Seguridad de la información un plan de capacitación y concientización de todo el personal en lo concerniente a seguridad de la Información.
c) Ante ausencias temporales de colaboradores por permisos médicos, calamidad doméstica y vacaciones por más de 72 horas, la Dirección de Talento Humano deberá en máximo 12 horas comunicar, al área de Mesa de Atención Técnica; y, Seguridad Física y Electrónica para bloquear los accesos tanto físicos como lógicos, salvo exista una autorización formal del Gerente en los casos de áreas con reporte directo o los subgerentes para las demás áreas, con el fin de habilitar el usuario para cumplimiento de temas laborales.

5.6.4 Segregación de funciones

El jefe inmediato debe validar el perfil del cargo, en el cual las funciones y áreas de responsabilidad deberán segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas; o, usos indebidos de los activos de la Cooperativa, se deberá cuidar el hecho de que una persona por sí sola no pueda acceder, modificar o utilizar los activos sin autorización o sin que se detecte.

5.6.5 Proceso disciplinario

La Dirección de Talento Humano debe aplicar la normativa establecida en el *Reglamento Interno de Trabajo* para las sanciones ante el incumplimiento de las normas de seguridad de la información, que hayan sido comunicadas por el Oficial de Seguridad de la Información.

5.6.6 Desvinculación o cambio del puesto de trabajo

a) La Dirección de Talento Humano deberá comunicar a las áreas pertinentes dentro de un máximo de 12 horas desde que se hacen efectivos los procesos de desvinculación de personal y cambio de funciones, con el objetivo de que retiren, asignen, bloqueen o eliminen recursos y accesos según corresponda.

b) El bloqueo de accesos para los colaboradores que se ausenten de la Cooperativa por un lapso mayor a 72 horas deberá ser de carácter mandatorio, toda excepción deberá contar con la autorización formal del Gerente en los casos de áreas con reporte directo o los subgerentes para las demás áreas.

c) Todo proceso de desvinculación de personal deberá ser liderado por la Dirección de Talento Humano, quien coordinará con el jefe directo, el área Administrativa y de ser necesario con las áreas de Seguridad Física y Seguridad de la Información, las medidas pertinentes, en función a salvaguardar los activos e información de la Cooperativa, entre las que se pueden citar:

- Apagado del equipo y bloqueo de los accesos físicos y lógicos en el mismo momento en que se comunica al colaborador su separación de la institución.
- Recepción del equipo del colaborador inmediatamente después de haber comunicado la terminación de la relación laboral.

d) En cualquier escenario de terminación de la relación laboral, es responsabilidad del jefe inmediato o su delegado, validar y garantizar la recepción de la información del colaborador, tanto en medios digitales como físicos. En caso de requerir una copia del respaldo de la información se deberá solicitar la autorización del Gerente en los casos de áreas con reporte directo o los subgerentes para las demás áreas, de los respaldos que fueron almacenados en la nube institucional; debiendo para el efecto ingresar el requerimiento en la herramienta Soluciones 29 y adjuntar la autorización formal correspondiente.

e) La Dirección de Talento Humano generará la solicitud de respaldo de la información del colaborador que ha dejado de prestar servicios para la Cooperativa mediante la herramienta Soluciones 29 hacia el área de Infraestructura y Producción; y, Mesa de Atención Técnica, con el fin de realizar los respaldos de nube y equipo, esta información se deberá guardar en un contenedor en nube.

f) La Dirección de TIC deberá implementar soluciones técnicas que garanticen el respaldo y disponibilidad de la información de los cargos detallados en el literal h de la sección "**Procesos de ejecución de respaldos**" de este manual.

5.7 Seguridad en dispositivos tecnológicos

5.7.1 Tipos de dispositivos

La Cooperativa define los siguientes tipos de dispositivos:

- **Dispositivo Institucional Fijo**: Computadoras tipo desktop y servidores de propiedad de la Cooperativa.
- **Dispositivo Institucional Teletrabajo**: Computadoras portátiles de propiedad de la Cooperativa (laptops).
- **Dispositivo Institucional Móvil**: Teléfonos celulares, tablet's, con sistema operativo (Android, iOS Windows) propiedad de la Cooperativa.
- **Dispositivo Personal**: Computadoras tipo desktop, computadoras portátiles y teléfonos móviles que un colaborador o usuario externo utiliza para acceder a las aplicaciones y a la información de la Cooperativa.
- **Dispositivo Electrónico ATM**: cajeros automáticos dispensadores o recicladores que permiten a los usuarios realizar transacciones bancarias.

En la siguiente tabla se definen los requisitos que deben aplicarse a cada uno de los dispositivos citados anteriormente:

	TIPOS DE DISPOSITIVOS				
REQUISITO	**INSTITUCIONAL FIJO**	**INSTITUCIONAL TELETRABAJO**	**INSTITUCIONAL MÓVIL**	**DISPOSITIVO PERSONAL**	**ATM**
El dispositivo es propiedad de la Cooperativa	X	X	X	-	X
El dispositivo puede salir de las instalaciones de la Cooperativa	–	X	X	X	X
El dispositivo puede conectarse directamente a la red interna LAN de la Cooperativa	X	X	-	-	X
El dispositivo puede conectarse directamente a la red interna Wi-Fi para colaboradores de la Cooperativa	-	X	X	-	-
El dispositivo puede conectarse directamente a una red Wi-Fi gestionada por la Cooperativa para invitados (*)	-	-	-	X	-
El dispositivo puede conectarse a la red interna a través de un gateway VPN	-	X	X	X	-
El dispositivo puede conectar directamente a otras redes no controladas por la Cooperativa (por LAN, Wi-Fi, 3G, 4G, etc.)	-	X	X	X	-

(*) la salida a Internet desde la red de invitados debe estar monitorizada y los usuarios de los dispositivos deben aceptar normas de uso aceptable.

5.7.2 Medidas de seguridad

En la siguiente tabla se describen las medidas de seguridad aplicables a los dispositivos:

MEDIDA	DESCRIPCIÓN	CONSIDERACIONES ADICIONALES
Control usuario privilegiado	Control de la cuenta de administración del dispositivo, de forma que el usuario no tenga permisos privilegiados en el mismo	- El usuario no debe tener acceso a las cuentas con permisos privilegiados para instalar software, administrar controladores, acceder a los archivos del sistema operativo, etc.

MEDIDA	DESCRIPCIÓN	CONSIDERACIONES ADICIONALES
Bloqueo de pantalla	Bloqueo con clave de la pantalla del dispositivo pasado un tiempo de inactividad	- En dispositivos móviles, el desbloqueo debe ser amigable para el usuario. - El tiempo de inactividad no podrá ser superior a 5 minutos ni inferior a un tiempo que haga incómodo el uso del dispositivo fijo y teletrabajo. - En el caso concreto de dispositivos móviles el tiempo de inactividad no será superior a 5 minutos y el mecanismo de bloqueo será mediante pin, patrón de desbloqueo o métodos de desbloqueo biométricos. - En el caso de dispositivos ATM no debe bloquearse la pantalla ya que brinda un servicio 24/7.
Términos de uso aceptable	Reglas y directrices que definen cómo los usuarios pueden interactuar con los sistemas y recursos tecnológicos de la Cooperativa.	- Los usuarios deben conocer y aplicar términos de uso aceptable, para poder utilizar los recursos tecnológicos de la Cooperativa.
Cifrado del almacenamiento	Almacenamiento cifrado de la información de la Cooperativa en el dispositivo	- En dispositivos fijos, teletrabajo y ATM se deben utilizar soluciones de cifrado completo de disco y memory flash (que permitan la gestión de claves y recuperación de la información). - En dispositivos móviles se utiliza soluciones MDM para la implementación de políticas de seguridad.
Data Loss Prevetion (DLP)	Controla la pérdida, filtración o acceso no autorizado a datos sensibles dentro de la Cooperativa.	- En función de las acciones no permitidas de los usuarios, se monitorea, detecta y bloquea la transferencia o uso indebido de datos, protegiendo así la información crítica y cumpliendo con normativas de seguridad y privacidad.
Azure Information Protection (AIP)	Servicio en la nube de Microsoft que permite clasificar, etiquetar y proteger documentos y correos electrónicos	En dispositivos fijos y teletrabajo se instala esta solución de Microsoft para proteger, detectar, clasificar y controlar la información confidencial de la Cooperativa.
Limpieza metadatos	Limpieza de los metadatos de los documentos del dispositivo con información de la Cooperativa	- La limpieza de los metadatos debe realizarse de forma automática sin intervención expresa del usuario.
Backup / almacenamiento remoto	Copia de seguridad de la información de los usuarios que manejan información sensible o clasificada como restringida y confidencial de la Cooperativa	- Las copias de backup deben almacenarse en un sistema remoto de forma cifrada. - Las copias deben realizarse a los cargos que requieran respaldos, conforme se indica en la sección “**Respaldos**” de este manual.
Borrado seguro remoto	Posibilidad de borrado seguro de la información de la Cooperativa almacenada localmente en el dispositivo desde una consola central	- Aplica para dispositivos móviles mediante la utilización de soluciones MDM para borrado seguro remoto. - La consola central debe autenticarse de forma fehaciente al dispositivo antes de realizar un borrado remoto. - El borrado debe realizarse con un algoritmo de seguridad y efectividad reconocida.
Logs	Generación y almacenamiento de los eventos de seguridad que se producen en el dispositivo	- El almacenamiento de los eventos debe ser remoto y deben posibilitar un análisis forense de un incidente de seguridad. - Los eventos de los que hay que guardar registro son los relacionados con la configuración de seguridad y los accesos realizados en el dispositivo.
Control del software instalado y actualizaciones	Inventario y actualización del software instalado en el dispositivo (nuevas versiones, configuraciones y parches)	- Se debe llevar un inventario de software autorizado licenciado y no licenciado por la Cooperativa. - Es recomendable comprobar y actualizar el software autorizado.

MEDIDA	DESCRIPCIÓN	CONSIDERACIONES ADICIONALES
Análisis de vulnerabilidades	Análisis de configuraciones débiles y errores del software (por falta de parches) en los dispositivos	- Se deben identificar las vulnerabilidades graves de seguridad por falta de parches y las relacionadas con "0 days".
Antimalware	Control de virus, troyanos, gusanos, APTs y malware en general que pudiera existir en el dispositivo (de forma latente o en ejecución)	- Las firmas se deben actualizar periódicamente (al menos diariamente) de forma automática. - La actualización debe poderse realizar a través de la red interna y a través de Internet. - Se debe analizar cualquier punto de entrada de archivos al dispositivo (adjuntos de correo, USB, descargas de Internet, etc.).
Cortafuegos	Control del tráfico permitido hacia y desde el dispositivo	- Debe inspeccionar y permitir el bloqueo de tráfico de entrada y salida. - Debe bloquear y permitir las aplicaciones que pueden recibir y enviar tráfico. - Debe poder enviar logs y alarmas a una consola central.
IPS (Intrusion Prevention System)	Análisis del tráfico sospechoso hacia y desde el dispositivo	- Las firmas de tráfico sospechoso se deben actualizar periódicamente (al menos diariamente) de forma automática. - La actualización debe poderse realizar a través de la red interna y a través de Internet.
VPN (Virtual Private Network)	Software de acceso remoto del dispositivo a la red interna de la Cooperativa	- El componente instalado de la solución VPN en el dispositivo permite establecer un túnel cifrado con el gateway de acceso a la red interna (sólo los colaboradores y proveedores autorizados por la Cooperativa pueden hacer uso).
Filtros de privacidad	Uso de filtros de privacidad físicos en las pantallas de los dispositivos ATM	- Los filtros de privacidad pueden ser plásticos removibles o autoadhesivos.
Candado	Uso de candados de seguridad para dispositivos teletrabajo	- Los candados pueden utilizar llaves o combinaciones de códigos numéricos.
Seguridad fuera de las instalaciones	Medidas de seguridad fuera de las instalaciones de la Cooperativa	- No se deberán dejar desatendidos los dispositivos móviles y de teletrabajo en zonas públicas, centros de conferencia, lugares de reunión, habitaciones de hoteles y otras áreas desprotegidas fuera de las instalaciones de la Cooperativa. - Se deberán tomar las precauciones de seguridad necesarias en automóviles, aviones u otros medios de transporte. - No se permite el uso de computadores de uso público de hoteles o café internet para acceso remoto a la red de la Cooperativa.
Seguro	Seguro ante pérdida o robo	- La Cooperativa deberá disponer de un seguro que cubra la pérdida o daño de todos los dispositivos a excepción de los dispositivos personales.
Autorización	Justificación de uso	- Todo dispositivo móvil deberá ser asignado con la autorización del Gerente en los casos de áreas con reporte directo o subgerentes para las demás áreas, confirmando la necesidad de su entrega en función a las responsabilidades del cargo del colaborador en la Cooperativa. - Los dispositivos móviles autorizados deben ser entregados al área de Mesa de Atención técnica para su configuración con la finalidad de que cuente con las seguridades necesarias para su buen uso.

MEDIDA	DESCRIPCIÓN	CONSIDERACIONES ADICIONALES
Hardening	Configuración de seguridad previo a la entrega o puesta en producción	- Los dispositivos deberán contar con todas las configuraciones y parches de seguridad, previo a su entrega al usuario final o puesta en producción. - Los dispositivos fijos, teletrabajo, móvil y ATM deberán contar con una lista de verificación debidamente firmada por el responsable (Mesa de Atención Técnica) de validar la hardenización en el dispositivo y deberá ser entregada al área de Seguridad de la Información.
Gestión de parches	Instalación permanente de parches de seguridad	- En los dispositivos se deberá instalar de manera permanente los parches de seguridad establecidos por el fabricante. - Es recomendable que los dispositivos personales cuenten con los parches de seguridad establecidos por el fabricante.

5.7.3 Medidas de seguridad mínimas por tipo de dispositivo

En la siguiente tabla se definen las medidas de seguridad mínimas aplicables que deben implementarse en los diferentes tipos de dispositivos (O=Obligatorio, R=Recomendado).

	TIPO DE DISPOSITIVO				
MEDIDA	INSTITUCIONAL FIJO	INSTITUCIONAL TELETRABAJO	INSTITUCIONAL MÓVIL	PERSONAL	ATM
Control usuario privilegiado	O	O	O	-	O
Bloqueo de pantalla	O	O	O	R	-
Términos de uso aceptable	O	O	O	O	O
Cifrado del almacenamiento	O	O	R	R	O
DLP (Data Loss Prevention)	O	O	R	-	-
Azure Information Protection	O	O	O	R	-
Limpieza metadatos	R	R	-	-	-
Backup/almacenamiento remoto	R	R	R	-	-
Borrado seguro remoto	-	R	O	R	-
Logs	O	O	O	-	O
Control del software instalado y actualizaciones	O	O	O	R	R
Análisis de vulnerabilidades	R	O	R	R	O
Antimalware	O	O	O	R	O
Cortafuegos	-	O	-	R	R
IPS (Intrusion Prevention System)	-	O	-	-	-
VPN (Virtual Private Network)	-	O	O	O	-
Filtros de privacidad	-	O	R	-	-
Candado	-	O	-	-	O
Consideraciones de seguridad fuera de las instalaciones	-	O	O	-	O
Autorización	O	O	O	-	O
Hardening	O	O	R	-	O
Gestión de parches	O	O	R	R	-
Seguro contra robo	O	O	O	-	O

5.7.4 Responsables de las medidas de seguridad

La Dirección de TIC, Dirección Administrativa y el área de Seguridad de la Información son responsables de asegurar que las medidas de seguridad antes detalladas sean aplicadas en cada activo o proceso a su cargo dentro de su ámbito.

5.7.5 Control de las medidas de seguridad

El área de Seguridad de la Información deberá aplicar controles periódicos, de forma anual, para verificar la efectividad de las medidas de seguridad implementadas en los diferentes tipos de dispositivos. Se dará prioridad a aquellos dispositivos expuestos físicamente, utilizando mecanismos o herramientas previamente autorizadas por la Cooperativa.

5.8 Teletrabajo y acceso remoto

5.8.1 Políticas generales

a) Toda conexión remota a los sistemas de información de la Cooperativa mediante internet deberá ser realizada mediante VPN, esto incluye colaboradores y proveedores. Toda excepción deberá estar justificada técnicamente y contar con la aprobación del Director de Tecnologías de la Información y Comunicación (TIC) y Oficial de Seguridad de la Información.

b) Los requerimientos de acceso remoto deben utilizar protocolos de comunicación segura (ssh). No se autorizarán accesos remotos al servicio de telnet, salvo que los componentes tecnológicos a los que se requiere el acceso no permitan el uso de protocolos seguros.

c) El sistema deberá implementar mecanismos de seguridad que garanticen la imposibilidad de reutilizar una sesión una vez cerrada.

d) Toda actividad efectuada por parte de los usuarios remotos deberá generar registros de auditoría.

e) Toda conexión remota deberá disponer de controles de doble factor de autenticación.

5.8.2 Responsabilidades específicas del teletrabajo y acceso remoto

5.8.2.1 Subgerentes, directores, jefes o cargos similares

Autorizar el acceso remoto a los servicios de la Cooperativa, confirmando la justificación de su uso en función a las necesidades de trabajo del colaborador, debiendo además gestionar solicitud de baja del servicio cuando ya no sea requerido.

5.8.2.2 Dirección de Tecnologías de la Información y Comunicación (TIC)

a) Implementar controles que garanticen lo establecido en “**Políticas Generales**” de la presente sección.

b) Configurar los permisos de acceso remoto, acorde a las solicitudes que le hayan sido escaladas, verificando que disponen de la respectiva autorización.

c) Mantener registros exactos y actualizados de todos los canales de comunicación de datos abiertos, así como de todas las personas a quienes se ha entregado el acceso.

d) Registrar y atender los tickets relacionados con el servicio de acceso remoto que hayan sido ingresados por los usuarios, verificando que disponen de la respectiva autorización.

5.8.2.3 Colaborador

a) Establecer conexiones remotas únicamente desde dispositivos proporcionados por la Cooperativa o dispositivos personales, cumpliendo con las políticas de seguridad establecidos en este manual, en ninguna circunstancia se podrán emplear computadores públicos de hoteles, centros comerciales, cafés internet, entre otros.

b) Cuando la conexión desde el exterior se realice con dispositivos institucionales teletrabajo o móvil, el usuario debe tomar en cuenta:

- Que dichos equipos son para uso exclusivo del colaborador y sólo serán utilizados para fines laborales.
- Los dispositivos institucionales no deben prestarse a terceros salvo autorización expresa que incluirá, en todo caso, la definición de las condiciones de uso.

5.9 Control de acceso

5.9.1 Políticas generales

a) Todos los accesos sobre los sistemas de información o entornos de la Cooperativa deberán cumplir con el principio de "Negación por Omisión". Es decir, todo acceso esta implícitamente prohibido a menos que haya sido autorizado de manera explícita a través de la solicitud pertinente o de la matriz de perfilamiento de cargos debidamente aprobada.

b) El acceso a redes y servicios de red de la Cooperativa debe estar sustentado en una necesidad real y únicamente se otorgará acceso a aquellos componentes para cuyo uso se disponga de una autorización especifica.

c) Se establecerá, documentará y revisará los lineamientos de control de accesos en base a las necesidades de seguridad y de servicio de la Cooperativa.

d) Los controles de acceso son tanto lógicos como físicos y deberán considerarse conjuntamente para aislar la información, las aplicaciones o los sistemas.

e) Los perfiles orientados a administración, operación, soporte técnico y gestión de accesos de las plataformas no deberán tener habilitados privilegios de funciones del negocio, así también, los perfiles definidos para áreas del negocio no podrán tener habilitadas opciones de operación, soporte o administración técnica de la plataforma, incluyendo funciones para gestión de accesos.

f) En general, y salvo justificación documentada, se evitará la propagación de privilegios entre objetos. En estos supuestos, los usuarios deberán estar autorizados por el propietario del objeto receptor del acceso y contar con un análisis de segregación funcional que asegure la no acumulación de privilegios que lo lleven a omitir controles.

g) El procedimiento para iniciar la sesión en un sistema de información deberá diseñarse para minimizar la oportunidad de acceso no autorizado.

h) Los sistemas para la gestión de contraseñas deberán ser interactivos y establecer contraseñas seguras y robustas. Todas las contraseñas deberán estar en cumplimiento de los lineamientos para la sintaxis de contraseñas establecidos en la sección "**Longitud y sintaxis de contraseñas**" del presente manual.

i) Se deberán implementar mecanismos de autenticación y control de acceso, que garanticen que ningún usuario o sistema pueda conectarse y hacer uso de las redes y servicios de la Cooperativa sin previa autorización.

j) Los perfiles de acceso deberán ser definidos y aprobados por los titulares de activo (sistemas, redes o recursos), quienes considerarán los siguientes criterios para el efecto:
- Los principios de: “Necesidad de Conocer”, “Necesidad de Usar”, “Mínimos Privilegios”.
- Los procesos de negocio, de manera que se permita una adecuada “Segregación de Funciones”.
- La clasificación de información del sistema.
- Los requisitos individuales de seguridad del sistema.
- La legislación aplicable y obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
- Se deberán considerar reglas de acceso en función de la red y medio por el que se conectan (dentro de las instalaciones, línea telefónica, desde Internet, entre otros.)
- Otros sistemas de información que necesiten interactuar con este.

k) Las reglas de acceso deben ser definidas a grupos de usuarios, no se permitirán reglas de acceso individuales (para un único usuario o equipo), con las debidas excepciones justificadas.

l) Los puertos destino en una regla de acceso deben estar claramente identificados, en base al servicio o aplicativo que se requiere acceder. No se autorizarán requerimientos de acceso a todos los puertos (ANY) o a un rango de puertos no justificado, con las debidas excepciones justificadas.

m) Las direcciones de red internas (direcciones IP) descritas como dirección origen o dirección destino deben estar claramente identificadas y validadas. No se autorizarán requerimientos que especifiquen rangos de direcciones IP no justificados.

n) Todo objeto de usuario en el firewall debe estar asociado de acuerdo con la siguiente nomenclatura: <usuariodominio>_descripción de servicio(pc/wi-fi,etc).

o) Todo objeto servidor en el firewall debe seguir la siguiente nomenclatura:
Ambiente, Servicio/Aplicativo, Nombre del equipo

p) Toda nueva regla de acceso en los Firewalls debe tener como mínimo la siguiente información:
- Tipo de regla (Emergente)
- Fecha de creación
- Fecha de expiración
- Número de ticket de herramienta Soluciones 29
- Siglas del responsable de quien configura la regla

q) Las reglas de acceso en los Firewalls deben ser configuradas de acuerdo con el tiempo establecido en el requerimiento autorizado.

r) Las reglas de acceso entre servidores – servidores y para grupo de administradores deben estar configuradas como permanentes.

5.9.2 Depuración de cuentas

El Gestor de Usuarios de cada sistema deberá cumplir los siguientes lineamientos de manera obligatoria:

a) Efectuará al menos semestralmente la depuración de las cuentas de los sistemas que administra. Para este efecto, emitirán el listado total de cuentas del sistema, incluyendo como mínimo los siguientes datos:

- Identificador de la cuenta
- Nombre del usuario de la cuenta
- Estado de la cuenta
- Perfil asignado
- Opciones/transacciones por cada perfil

b) Efectuará una comparación entre el listado emitido y el listado de personal interno de la Cooperativa, procediendo a deshabilitar aquellas cuentas del personal que ya no presten servicios para la misma.

c) El Gestor de Usuario deberá notificar mediante oficio las acciones y resultados de la depuración de cuentas realizada al área de Seguridad de la Información.

d) Las cuentas personales del Active Directory, de los colaboradores desvinculados, deberán permanecer deshabilitadas por el lapso de dos años, posterior a este tiempo el Gestor de Usuarios procederá con la eliminación definitiva.

5.9.3 Revisión de derechos de acceso

El área de Seguridad de la Información efectuará al menos anualmente la revisión de derechos de acceso en los sistemas críticos de la Cooperativa, validando las matrices de perfiles con las áreas de negocio para actualizarlas y garantizar el acceso a las transacciones y módulos, en base a las necesidades de trabajo y considerando los criterios de segregación de funciones.

5.9.4 Control de acceso remoto de los usuarios

La Dirección de TIC deberá considerar lo siguiente:

a) Desarrollar un procedimiento que defina el proceso de otorgamiento de acceso remoto.

b) No estará permitida la autenticación basada exclusivamente en la dirección origen del equipo del usuario (dirección IP, dirección MAC y demás).

c) La robustez y fiabilidad del mecanismo de autenticación que se utilice en cada caso estará de acuerdo con la criticidad de la red y los sistemas e información a la que se pueda acceder.

d) Filtrar las conexiones permitidas por acceso remoto, de forma que los colaboradores y personal externo sólo tengan acceso a los sistemas y servicios que necesiten.

5.9.5 Control de acceso remoto de proveedores

a) La Dirección de TIC deberá definir e implantar un procedimiento de control de acceso remoto de proveedores.

b) El acceso remoto de un proveedor para desarrollo, mantenimiento, diagnóstico o soporte para puesta en producción de un sistema interno deberá ser solicitado por el titular del activo mediante formulario.

c) Se limitará al tiempo estrictamente necesario para realizar la prestación de servicio establecida.

d) Previamente a la autorización se analizará el riesgo que implica el acceso remoto del proveedor y será condicionante para la toma de decisión, todo pedido será autorizado por el Oficial de Seguridad de la Información.

5.9.6 Control de acceso de puertos de configuración

a) La Dirección de TIC implementará medidas que garanticen que los puertos de configuración y/o administración se encuentren controlados, su acceso remoto o físico

debe estar restringido sólo al personal autorizado (administradores de red y personal de soporte).

5.10 Identificación y autenticación

5.10.1 Identificadores o cuentas personales

b) Cada usuario tendrá su propio y único identificador, el cual será generado de forma que pueda ser asociado de manera única e inequívoca con su propietario.

c) Todo identificador tendrá un propietario que será responsable de las acciones que se realicen con dicho identificador. En aquellos casos en los que la aplicación de este control no sea posible, el Gestor de Usuarios deberá considerar los criterios de gestión de cuentas genéricas definidos en el presente manual.

d) Los usuarios se identificarán y autenticarán para acceder a los sistemas de información, aplicativos móviles, recursos, áreas de procesamiento de datos y redes de comunicaciones de la Cooperativa, de modo que se pueda reconocer (identificación) y comprobar (autenticación) la identidad del usuario que accede de forma inequívoca, personalizada y autorizada, para el efecto se emplearán mecanismos de identificación y autenticación acordes al nivel de seguridad requerido.

e) No se permitirá el acceso anónimo a los sistemas de información, recursos, áreas de proceso de datos y redes de comunicaciones de la Cooperativa a no ser que expresamente hayan sido catalogados como públicos.

5.10.2 Nomenclatura para identificadores personales

5.10.2.1 Nomenclatura personal interno

a) Todos los identificadores o cuentas personales de los colaboradores creados en los entornos tecnológicos de la Cooperativa incluyendo aplicaciones, bases de datos, sistemas operativos y equipos de red deberán cumplir con el siguiente estándar de nomenclatura:

Estructura: **NA**

N	Primera letra del nombre del colaborador
A	Primer apellido del colaborador

b) Manejo de colisiones:

En caso de que coincidan dos identificadores, se empleará la siguiente estructura:

Estructura: **NSA**

N	Primera letra del nombre del colaborador
S	Primera letra del segundo nombre del colaborador
A	Primer apellido del colaborador

En un tercer caso de coincidencia, se empleará la siguiente estructura:

Estructura: **NSAP**

N	Primera letra del primer nombre del colaborador
S	Primera letra del segundo nombre del colaborador
A	Primer apellido del colaborador
P	Primera letra del segundo apellido del colaborador

5.10.2.2 Nomenclatura personal externo

Los identificadores de usuarios externos creados en los entornos tecnológicos de la Cooperativa incluyendo aplicaciones, bases de datos, sistemas operativos y equipos de red deberán cumplir con el siguiente estándar de nomenclatura:

a) Cuentas personales: Se procurará asignar cuentas personales para la ejecución de servicios por parte de terceras partes, para esto se deberán cumplir con la siguiente nomenclatura:

Estructura del identificador: **NA.EMPRESA**

Empresa	Nombre de la empresa externa
N	Primera letra del nombre del usuario
A	Primer apellido del usuario

Manejo de colisiones:

Estructura: **NSA.EMPRESA**

Empresa	Nombre de la empresa externa
N	Primera letra del nombre del usuario
A	Primer apellido del usuario
S	Primera letra del segundo nombre del usuario

b) Cuentas genéricas: Dependiendo de las cláusulas del contrato de servicios, del tipo de servicio contratado, del nivel de riesgo de la actividad, de los perfiles asignados, así como de las necesidades de rastreabilidad de las acciones efectuadas por el proveedor, se analizará la posibilidad de asignar cuentas genéricas para la ejecución del servicio.

Las mencionadas cuentas deberán tener un nombre asociado al servicio prestado o ejecutado.

5.10.2.3 Excepciones

a) La presente política aplica a todos los sistemas de información de la Cooperativa con excepción de los sistemas que tecnológicamente no permitan aplicarlo.

b) Para aquellos sistemas de información que al momento de aprobación del presente manual no cumplieran con la nomenclatura especificada en este artículo, el Gestor de Usuarios del sistema deberá presentar un plan de alineamiento a la norma. Toda

excepción al presente manual deberá ser autorizada por el Director de TIC y Oficial de Seguridad de la Información, la misma que deberá considerar el impacto y los riesgos que implica la adopción de esta.

c) Para aquellos casos en donde por limitaciones de las aplicaciones, exista la necesidad de crear más de una cuenta para una misma persona, para generar el identificador se adicionará un numero secuencial iniciado en 1, sumado al identificador de la cuenta ya creada, ejemplo: “acastillo”, “acastillo1”, “acastillo2”, restringiéndose la existencia de múltiples cuentas atadas a un mismo custodio a un máximo de 3 en un mismo sistema, contando cada cuenta con la justificación técnica respectiva.

5.10.2.4 Deshabilitación o bloqueo de identificadores o cuentas personales

a) Se deshabilitarán los identificadores personales de colaboradores que se hayan desvinculado de la Cooperativa, así como de usuarios externos que no sigan prestando sus servicios en la Cooperativa, se bloquearán los derechos de acceso asociados al identificador en todos los sistemas de información, recursos, áreas de proceso de datos y redes de comunicaciones de la Cooperativa en los que tuviera acceso dentro de las 12 horas posteriores a su desvinculación.

b) Los responsables de solicitar la deshabilitación o bloqueo de un identificador personal son:

- La Dirección de Talento Humano (o su delegado), para el caso de usuarios internos o colaboradores.
- Los Administradores de Contrato para el caso de usuarios externos o proveedores.
- Excepcionalmente el Oficial de Seguridad de la Información o Analista de Ciberseguridad pueden solicitar la deshabilitación o bloqueo de un identificador personal si se considera que puede ser origen de un incidente de seguridad o para salvaguardar los intereses de la Cooperativa.

5.10.3 Identificadores o cuentas genéricas

a) Son todas aquellas cuentas que no corresponden a identificadores personales, que no se apegan al estándar de nombramiento establecido en este documento, cuentas por defecto de las plataformas tecnológicas y aplicaciones o cuentas que requieren ser utilizadas por dos o más colaboradores.

b) Todo requerimiento de creación de cuentas genéricas deberá ser aprobado por el Oficial de Seguridad de la Información y por el titular del activo. Las solicitudes deberán estar justificadas por motivos de negocio y tener definidos los periodos de vigencia de la cuenta; la aprobación deberá considerar los niveles de riesgo relacionadas al uso de estas cuentas y brindar una autorización expresa de la aceptación del riesgo o de los controles mitigantes implementados para su cobertura.

c) La Cooperativa establece los siguientes tipos de cuentas genéricas:

5.10.3.1 Cuentas genéricas funcionales

Son cuentas que vienen creadas por defecto en los sistemas para su administración, las políticas de su uso son las siguientes:

a) La contraseña de toda cuenta genérica funcional deberá ser cambiada previo a la puesta en producción del sistema.
b) Cuando técnicamente sea posible, se deberá renombrar toda cuenta genérica funcional, con un nombre aprobado por el área de Seguridad de la Información.
c) Cuando técnicamente sea posible, se deberá deshabilitar toda cuenta genérica funcional.
d) Para administrar los sistemas de información no se deberán usar cuentas genéricas funcionales, por lo que se deberán crear nuevas cuentas para cada uno de los administradores, las cuales serán denominadas Cuentas Genéricas Administrativas.
e) Las cuentas genéricas funcionales serán de uso restringido y únicamente para tareas que requieran dicho nivel de accesos. Su uso deberá ser justificado, documentado y aprobado tanto por el Director de TIC y el Oficial de Seguridad de la Información. La solicitud de creación será realizará a través del formulario pertinente debidamente aprobado previo a su uso.
f) Los formularios de creación deberán ser archivados en repositorio en nube y custodiados por la Dirección de TIC, dicho repositorio deberá ser compartido con permisos de solo lectura al área de Seguridad de la Información.

5.10.3.2 Cuentas genéricas administrativas

Son cuentas de administración personalizadas y definidas por la Cooperativa para el personal de administración de cada sistema de información, mismas que están sujetas a los siguientes lineamientos:

a) La creación de este tipo de cuentas debe ser evaluada por los responsables de la Dirección de TIC y área de Seguridad de la Información, considerando que deben cumplir la política de nombramiento definida en este documento.
b) El tiempo de caducidad de claves para este tipo de cuentas deberá ser al menos cada 90 días, o cuando exista un cambio de personal en sus custodios.
c) Durante el uso de la cuenta, se registrarán las acciones (registros de auditoría) que se realicen con la misma, así como las personas que tenían acceso a la misma en el momento de la acción.
d) La solicitud de uso será realizará a través del formulario pertinente y deberá contar con todas las aprobaciones previo a su utilización.

5.10.3.3 Cuentas genéricas dinámicas

Son cuentas requeridas para comunicación entre sistemas de información. Ejemplo: cuentas empleadas para la comunicación con la base de datos (ODBC), mismas que están sujetas a los siguientes lineamientos:

a) Deben cumplir la política de manejo, sintaxis y longitud de contraseñas, pero sin aplicar la política de caducidad de clave. Todo cambio de contraseña se lo deberá coordinar mediante un control de cambios conforme lo establecido en el respectivo procedimiento.
b) La clave asignada a estas cuentas deberá estar dividida en dos partes: una parte debe ser definida por el administrador del sistema y la otra por parte del Analista de Ciberseguridad, en ningún caso la clave entera debe estar bajo conocimiento de una sola persona.

c) Cada parte de la clave deberá ser entregada de forma independiente y en sobre sellado al Oficial de Seguridad de la Información y se dejará constancia de lo actuado mediante el acta pertinente.
d) Los sobres serán almacenados en una locación externa e independiente de la Dirección de TIC y Seguridad de la Información en una bóveda o caja fuerte destinada exclusivamente para este fin.
e) El Oficial de Seguridad de la Información será el custodio de las llaves o mecanismos de acceso a la bóveda o caja fuerte donde se almacenen los sobres de contraseñas.
f) Al ingresar la clave esta no debe estar en texto claro, de tal manera que ninguna de las partes pueda ver la clave completa.
g) La solicitud de uso será realizará a través del formulario pertinente y deberá contar con todas las aprobaciones previo a su utilización.

5.10.4 Utilización de *Cuentas Genéricas*

a) La cuenta no deberá tener en ningún caso privilegios avanzados que supongan un riesgo alto (excepto si se tratan de cuentas genéricas administrativas o funcionales, refiérase a dichas cuentas en el presente documento).
b) Para toda cuenta genérica se asignará formalmente una persona responsable de la cuenta quien será la propietaria la misma y se responsabilizará por su uso (aplica también a cuentas genéricas de accesos privilegiados).
c) El propietario de la cuenta genérica deberá mantener una lista actualizada con el grupo de personas que la utilizan y deberá notificar formalmente al área de Seguridad de la Información cualquier cambio en dicha lista.
d) La Dirección de TIC deberá mantener un listado actualizado de cuentas genéricas con sus respectivos propietarios y deberá notificar formalmente al área de Seguridad de la Información cualquier cambio.
e) Cuando un usuario o sistema de información ya no deba tener acceso a la cuenta genérica (aplica también a cuentas genéricas de accesos privilegiados), el propietario de la cuenta deberá tomar las acciones necesarias para el bloqueo o cambio inmediato de contraseña.

5.10.5 Pantalla de autenticación en los sistemas de información

a) Las pantallas de autenticación presentarán únicamente información pública necesaria.
b) Las contraseñas deberán ser enmascaradas en pantalla durante la introducción de estas mientras se realice la autenticación.
c) La autenticación de un usuario se realizará mediante la validación de los datos proporcionados. Si la autenticación es errónea, el sistema sólo facilitará información del proceso fallido.
d) En el acceso a servidores web, telnet, SSH, entre otros. no debe presentarse información sobre el sistema operativo (nombre, versión, entre otros.) ni de los servidores.
e) Las aplicaciones web mediante canales electrónicos para uso de los socios/clientes de la Cooperativa), las cuentas de usuario se bloquearán automáticamente si tienen 3 intentos fallidos de autenticación seguidos. Para sistemas de información diseñados para el uso de los colaboradores de la Cooperativa, dicho parámetro podrá ser configurado hasta 5 intentos fallidos.

5.10.6 Aviso de acceso

a) Los sistemas de información donde técnicamente sea factible, se recomienda presentar una pantalla de aviso que exprese la propiedad del sistema por parte de la Cooperativa, la necesidad de contar con autorización para el ingreso al sistema y las restricciones para su uso. Cuando técnicamente sea posible dicho mensaje aparecerá previo, durante o inmediatamente después del proceso de autenticación satisfactorio.

b) Una vez completado el proceso de autenticación, se recomienda presentar al usuario la fecha y hora del último acceso satisfactorio, así como el número de autenticaciones fallidas realizadas desde la fecha.

5.10.7 Generación y reinicio de contraseñas

a) Las contraseñas iniciales o reiniciadas de los usuarios serán siempre diferentes y aleatorias, no se utilizará la misma contraseña por defecto ni en el alta, ni en el reinicio de estas.

b) Los sistemas de información contarán con funcionalidades que permitan forzar a los usuarios a cambiar las contraseñas iniciales o reiniciadas, en el primer acceso o uso de estas.

c) En el reinicio de una contraseña, el Gestor de Usuarios identificará inequívoca y fehacientemente al usuario que solicita el cambio. Esta nueva contraseña se comunicará al usuario por un medio que garantice la identidad de este.

d) Las generación y reinicio de contraseñas de las cuentas genéricas se encuentran establecidas en la sección de "**Identificadores o cuentas genéricas**" de este manual.

5.10.8 Distribución de contraseñas

a) La distribución de las contraseñas deberá ser realizada de manera separada a la comunicación del identificador asociado, garantizándose en todo el proceso la confidencialidad e integridad de las contraseñas.

b) No se permitirá la distribución de contraseñas en texto legible a través de redes públicas o externas a la red de la Cooperativa.

5.10.9 Período y mecanismo de cambio de contraseñas

a) Los sistemas de información contarán con características que obliguen al cambio de las contraseñas en un período máximo de 30 días para colaboradores.

b) Los sistemas de información contarán con características que obliguen al cambio de las contraseñas en un período máximo de un año para representantes de la Asamblea General, previa coordinación del Gestor de Usuario y Secretaria de Presidencia.

c) Existirán mecanismos que permitan a un usuario el cambio de contraseña a petición de este en cualquier momento.

d) Los mecanismos de cambio de contraseña (a petición del usuario o porque el sistema le obligue al cambio) cumplirán las siguientes funcionalidades:

- Las contraseñas no se visualizarán en pantalla durante la introducción de estas.

- Se pedirá la contraseña antigua antes de continuar con el mecanismo de cambio de contraseña.
- Se pedirá confirmación de la nueva contraseña antes de proceder al cambio (para evitar posibles errores de escritura).
- No se permitirá la reutilización de al menos las 5 últimas contraseñas que el usuario haya utilizado.
- Se verificará la correcta longitud y sintaxis de la nueva contraseña antes de proceder al cambio.

e) La periodicidad de cambio de contraseñas de BIOS de los dispositivos ATM deberá ser de forma anual previa coordinación de Mesa de Atención Técnica y Canales Electrónicos, cuyo respaldo debidamente firmado deberá ser entregado al área de Seguridad de la Información. El custodio de estas contraseñas será el área de Canales Electrónicos y el programa para administrar las contraseñas deberá estar protegido con una clave de acceso.

f) La periodicidad de cambio de contraseñas de: usuario de acceso al sistema operativo y acceso remoto de los dispositivos ATM deberá ser de forma anual por el área de Canales Electrónicos, cuyo respaldo debidamente firmado deberá ser entregado al área de Seguridad de la Información. El custodio de estas contraseñas será el área de Canales Electrónicos y el programa para administrar las contraseñas deberá estar protegido con una clave de acceso.

g) En caso de desvinculación de un colaborador con acceso al sistema de administración de contraseñas, el colaborador responsable a cargo deberá cambiar inmediatamente la clave de acceso al sistema de administración de contraseñas.

h) La contraseña de acceso a la red Wi-Fi establecida para el personal externo deberá ser cambiada de forma anual.

5.10.10 Longitud y Sintaxis de Contraseñas

Las contraseñas deben cumplir con la siguiente longitud y condiciones:

a) Longitud mínima de doce caracteres.

b) Y deberá incluir una combinación de:

- Letras mayúsculas
- Letras minúsculas
- Números
- Caracteres especiales (por ejemplo: !, $, &, *)

5.11 Gestión de Incidentes de Seguridad de la Información

5.11.1 Responsabilidades específicas

5.11.1.1 Colaboradores, proveedores o personal externo

Todos los colaboradores, proveedores, o cualquier tercero involucrado en la utilización de la información y los sistemas de información de la Cooperativa, son responsables de:

a) Notificar inmediatamente cualquier anomalía o incidente que afecte o pudiera afectar a la seguridad de la información o los sistemas de información.

b) Colaborar en todo lo necesario y facilitar todos los datos que le solicite el área de Seguridad de la Información.

5.11.1.2 Titular del activo

a) Valorar junto con el Oficial / Analista de Seguridad y Protección de la Información, el impacto del incidente e identificar las acciones de carácter inmediato que sean necesarias.
b) En caso de ser requerido activar los procedimientos de contingencia para mantener la operación.
c) Realizar o delegar el seguimiento de los sistemas corregidos para garantizar que se ha alcanzado la estabilidad y seguridad de estos durante el período de seguimiento.

5.11.1.3 Oficial de Seguridad de la Información

Asegurar el cumplimiento del *Procedimiento Atención y Análisis de Incidentes de Seguridad de la Información*.

5.11.1.4 Encargado del tratamiento del activo

a) Notificar de manera inmediata los incidentes de seguridad que afecten o pudieran afectar a la seguridad de su sistema cumpliendo lo establecido en el *Procedimiento Atención y Análisis de Incidentes de Seguridad de la Información*.
b) Proporcionar todos los datos que le solicite el área de Seguridad de la Información en un plazo máximo de 48 horas laborables.
c) Colaborar con el titular del activo en lo necesario para restablecer la operatividad normal previa a la ocurrencia del incidente.
d) Identificar e implementar las acciones de carácter inmediato que sean necesarias para aislar el activo de información y evitar que el incidente se propague conforme lo establece el *Procedimiento Atención y Análisis de Incidentes de Seguridad de la Información*.
e) Reinstalar todos los sistemas afectados y cambiar las contraseñas de estos siguiendo los procedimientos y estándares de seguridad de la Cooperativa, con el objetivo de que el incidente no vuelva a producirse (si el *Equipo de Respuesta a Incidentes* lo considera necesario).

5.12 Relación con proveedores

5.12.1 Responsabilidades específicas

Las responsabilidades específicas del Administrador de Contrato se encuentran descritas en el *Manual de Adquisiciones y Contrataciones*.

5.12.2 Generalidades

a) No se deberán otorgar a terceros el acceso a la información ni a las instalaciones de procesamiento de esta, mientras no se haya garantizado la implementación de los controles apropiados y se haya firmado un contrato que defina las condiciones para la conexión o el acceso.
b) Todo proceso de adquisición o contratación de bienes o servicios que recopilen información personal, creación de nuevos productos o implementación de nuevos servicios deberá contar con la participación del área de Seguridad de la Información. A fin de ser informados de manera oportuna para evaluar los posibles riesgos y

asegurar que se cumplan las normativas de seguridad establecidas, garantizando la protección de la información y la continuidad operativa de la Cooperativa.

c) Toda compra de software deberá contar con la autorización explicita de los responsables de la Dirección de TIC, Dirección de Riesgos Integrales y Seguridad de la Información, en función de garantizar el cumplimiento de estándares y el alineamiento a las normas correspondientes.

d) Toda compra que involucre el acceso a información, sistemas de información, desarrollo de software, servicios en la nube, centros de procesamiento de datos principal y/o alternos en la nube deberá sujetarse a lo establecido el *Manual de Adquisiciones y Contrataciones.*

e) Toda compra de software debe cumplir con lo definido en el *Anexo E Lista de Verificación de Requisitos de Seguridad para Desarrollo o Adquisición de Sistemas*, el cual incluye un resumen de todos los requisitos de seguridad detallados en este manual.

f) Dependiendo de la naturaleza del proceso de compra y de sus riesgos implícitos, se deberá considerar al menos la inclusión de las siguientes cláusulas en el documento de requisitos técnicos (términos de referencia), los cuales deberán ser parte de las bases de concurso y de los diferentes tipos del contrato.

5.12.3 Contrato con el proveedor

5.12.3.1 *Cláusulas por acceso a información, sistemas de información o instalaciones*

Si el servicio a ser contratado implica el acceso por parte del proveedor a los activos de información, instalaciones o sistemas de información de la Cooperativa, se deberán incluir las siguientes clausulas, según sea aplicable:

- El PROVEEDOR confirma que dispone de políticas, procedimientos, y manuales de seguridad de la Información, comprometiéndose a brindar el servicio alineado a las mejores prácticas y políticas de seguridad de la Información (ejemplo: Norma ISO 27001, norma PCI), según corresponda.
- El PROVEEDOR se compromete a devolver a LA COOPERATIVA toda la información de propiedad de la Cooperativa que se haya empleado o generado en el servicio contratado, comprometiéndose a destruir de su infraestructura tecnológica, de manera segura (mediante métodos que garanticen que no podrá ser recuperada tanto digital como físicamente), toda la información Confidencial y/o Restringida, calificada como tal por la Cooperativa.
- El PROVEEDOR garantiza que el personal asignado a la ejecución del proyecto o prestación del servicio contratado con LA COOPERATIVA ha sido capacitado debidamente en materia de Seguridad de la Información y que mantiene un proceso continuo de capacitación en dicho ámbito.
- El PROVEEDOR confirma que dispone de un proceso de selección del personal asignado a la prestación del servicio contratado por LA COOPERATIVA, el cual incluye un proceso de validación de antecedentes laborales y personales, garantizando la idoneidad del personal contratado.
- EL PROVEEDOR confirma que cuenta con un Proceso de Control de Cambios, en los procesos tecnológicos que dan soporte al servicio contratado por LA

COOPERATIVA y que dicho proceso deberá estar coordinado con el proceso de Control de Cambios de la Cooperativa.

- EL PROVEEDOR declara contar con todos los permisos, autorizaciones o concesiones para la prestación de los servicios contratados por LA COOPERATIVA.
- EL PROVEEDOR declara contar con personal técnico, sistemas e infraestructura necesaria, acorde al servicio contratado, con el fin de garantizar un óptimo servicio a LA COOPERATIVA.
- EL PROVEEDOR deberá garantizar la disponibilidad de recurso humano y tecnológico para poder brindar el servicio contratado en escenarios de confinamiento o emergencia sanitaria.
- EL PROVEEDOR debe asegurar la prestación del servicio para el que fue contratado en línea con los requerimientos de continuidad de operación establecidos por LA COOPERATIVA.
- EL PROVEEDOR deberá colaborar y permitir a LA COOPERATIVA realizar auditorías sobre la calidad del servicio, cumplimiento de políticas o infraestructura tecnológica y física que soporta la prestación de los servicios incluidos en la relación contractual, auditorías que serán notificadas a EL PROVEEDOR con mínimo tres (3) días calendario de antelación, indicando los nombres y documentos de identidad de las personas que las realizarán, pudiendo ser estos trabajadores o personal externo autorizado por LA COOPERATIVA o sus entes reguladores.
- Todo proceso de auditoria estará sujeto a los conceptos de confidencialidad de información definido en las políticas de seguridad de LA COOPERATIVA.
- El proveedor deberá presentar anualmente la evidencia de cumplimiento de Ley Orgánica de Protección de Datos Personales.

5.12.3.2 *Cláusulas para Contratación de Desarrollo de Software*

Para contratos de servicios de desarrollo o adquisición de software, se deberá considerar la inclusión de al menos las siguientes cláusulas:

- EL PROVEEDOR garantiza que el software que es motivo del contrato de servicios en la versión vendida a LA COOPERATIVA ha sido sometido a un análisis de vulnerabilidades y que las mismas han sido mitigadas (aplica a adquisición de software).
- EL PROVEEDOR garantiza que el código ha sido (o va a ser) desarrollado empleando mejores prácticas de desarrollo de software, tanto en lo relacionado a la calidad del código (eficiencia, uso, funcionalidad, fiabilidad, portabilidad y mantenimiento), así como en seguridad. Respecto a los criterios de seguridad, deberá garantizar el alineamiento de mejores prácticas en desarrollo de software (ejemplo: OWASP).
- EL PROVEEDOR se compromete a efectuar un análisis de vulnerabilidades del código desarrollado, debiendo realizar el cierre de estas previo la entrega a LA COOPERATIVA y a su puesta en producción.
- En caso de que LA COOPERATIVA identifique vulnerabilidades en el código entregado por EL PROVEEDOR, ya sea antes de la salida a producción, o dentro de la vigencia del contrato de soporte, EL PROVEEDOR deberá efectuar el cierre de estas, sin que dicho trabajo implique costo para la Cooperativa.

- En caso de que LA COOPERATIVA identifique problemas de funcionalidad en el código entregado por EL PROVEEDOR, ya sea antes de la salida a producción, o dentro de la vigencia del contrato de soporte, EL PROVEEDOR deberá efectuar el cierre de estas, sin que dicho trabajo implique costo para la Cooperativa.

5.12.3.3 *Cláusulas de Confidencialidad de la Información*

- EL PROVEEDOR reconoce y acepta que, en el transcurso de su contratación por parte de LA COOPERATIVA, EL PROVEEDOR puede recibir o tener acceso a información relacionada a LA COOPERATIVA. EL PROVEEDOR se compromete a considerar como Confidencial, Restringida, toda la información relacionada con el objeto del contrato, y aquella que obtenga durante la prestación de sus servicios.
- EL PROVEEDOR se compromete a manejar la información de LA COOPERATIVA de acuerdo con la obligación de reserva y sigilo, y en aplicación de la normativa vigente respecto de LA COOPERATIVA sobre el manejo, recolección, recepción, transmisión, almacenamiento, disposición y administración de datos, de conformidad con las normas establecidas, de manera especial por el Código Orgánico Monetario y Financiero.
- EL PROVEEDOR se compromete a custodiar y mantener la confidencialidad de toda credencial de autenticación que sea entregada por parte de LA COOPERATIVA, cuyo control les sea temporalmente confiado debido a la prestación de servicios establecidos por el presente contrato. Dichas credenciales deberán ser utilizadas únicamente por empleados autorizados para tal uso, y en estricta ejecución del objeto del presente contrato. Información de terceros obtenida durante el manejo de las cuentas de propiedad de LA COOPERATIVA deberá ser tratada en aplicación de los estándares de confidencialidad previamente establecidos.
- EL PROVEEDOR se compromete a trasladar sus obligaciones al personal que dedique al cumplimiento del presente contrato, y a advertir a tal personal de todas las obligaciones que adquiere por este instrumento. EL PROVEEDOR implementará además toda normas y políticas administrativas, encaminadas a garantizar el correcto uso de la información proporcionada y garantizará la debida protección de datos de titularidad de LA COOPERATIVA. El acceso a dicha información deberá limitarse tan sólo a personal directamente involucrado en la prestación de los servicios, y no podrá ser revelada o cedida a terceros en ningún caso, ni aún en el supuesto de terminación de este contrato.
- Los documentos, procesos, manuales y demás material que sea entregado por LA COOPERATIVA a EL PROVEEDOR para uso de ésta, quedará bajo su custodia y responsabilidad, desde el momento de su recepción hasta su total entrega o elaboración, obligándose EL PROVEEDOR a guardar confidencialidad sobre la información a la que, con ocasión del presente contrato, tenga acceso o genere.
- EL PROVEEDOR se obliga a informar a LA COOPERATIVA, por escrito e inmediatamente, de cualquier posible ruptura de confidencialidad que fuese descubierta en sus operaciones. Si una ruptura tal es descubierta por LA COOPERATIVA, el Administrador del contrato es responsable de la notificación formal de los posibles incumplimientos, para lo cual debe enviar comunicación

escrita a EL PROVEEDOR sobre la investigación de la incidencia. De confirmarse el incumplimiento y bajo previa notificación a EL PROVEEDOR, LA COOPERATIVA se reserva el derecho de ejecutar las acciones legales pertinentes, así como la terminación unilateral del presente contrato.

- Ninguna de las PARTES incurrirá en responsabilidad alguna cuando la información confidencial que se le haya proporcionado llegue a ser de conocimiento de un tercero por una de las siguientes causas:
    - Que la información confidencial sea o llegue a ser de dominio público durante la vigencia del contrato, excepto si dicha circunstancia es causada por la negligencia o el incumplimiento de una de las partes.
    - Cuando el dueño de la información confidencial autorice por escrito, a través de su representante legal, que la otra parte difunda la información confidencial sin restricciones a terceros, según lo establezca; o
    - En caso de que cualquiera de las partes se vea obligada, por disposición administrativa o por orden judicial a entregar, total o parcialmente, la información confidencial, debiendo comunicarlo por escrito a las otras partes en el momento en que tenga conocimiento del requerimiento correspondiente, siempre y cuando se hayan agotado todos los medios legales para evitarlo.
- Por todo lo anteriormente citado, ninguna de las PARTES podrá retener o conservar indebidamente información Confidencial que haya sido proporcionada conforme al contrato y no podrá divulgarla incluso después de la terminación o resolución del contrato.

5.12.3.4 *Cláusulas de Propiedad Intelectual*

- El lema comercial, nombre, logo y todo signo distintivo y marcas de LA COOPERATIVA son de exclusiva propiedad de ésta última. EL PROVEEDOR se halla autorizado a utilizar dichos signos distintivos y marcas única y exclusivamente dentro de los parámetros establecidos por el presente contrato y relacionados con su ejecución. Todo otro uso, comercial o no, de signos distintivos y marcas de LA COOPERATIVA queda expresamente prohibido, tanto respecto de EL PROVEEDOR como de sus proveedores directos, indirectos, contratistas, funcionarios, empleados o directivos, y de terceros que mantengan relación comercial o profesional con EL PROVEEDOR.
- Todos los contenidos creativos, productos, estudios y datos elaborados, ejecutados u obtenidos por EL PROVEEDOR para LA COOPERATIVA son de expresa y exclusiva propiedad de esta última. EL PROVEEDOR cede expresamente y de modo exclusivo todo derecho sobre dicho material, en favor de LA COOPERATIVA, EL PROVEEDOR no podrá reutilizar tal material en servicios prestados para otro cliente o en beneficio propio. La misma prohibición opera respecto de los proveedores directos e indirectos de EL PROVEEDOR, así como de sus contratistas, funcionarios, empleados o directivos, y de terceros con relación comercial o profesional a su respecto.
- EL PROVEEDOR se compromete a respetar, en el curso de la prestación de los servicios brindados a LA COOPERATIVA, los derechos de propiedad intelectual de titularidad de terceros. Si un elemento o material preexistente, protegido por

derechos de propiedad intelectual, es incorporado a los contenidos, productos, y servicios brindados por EL PROVEEDOR a LA COOPERATIVA, EL PROVEEDOR deberá informar por escrito, expresa y previamente, a LA COOPERATIVA sobre dicha inclusión, complementando tal información con la evidencia de haber obtenido los derechos intelectuales o la autorización necesaria de la legitimidad absoluta a tal incorporación a fin de no causar daños a la Cooperativa. En ausencia de dicha información previa y de los documentos justificativos necesarios al efecto, cualquier uso indebido de propiedad intelectual de titularidad de terceros será de única y exclusiva responsabilidad de EL PROVEEDOR, reservándose LA COOPERATIVA el derecho de ejecutar las acciones legales pertinentes al respecto.

5.12.3.5 *Cláusulas en Contratación de Servicios en la Nube*

En el caso de contratar servicios de infraestructura, plataforma y/o software conocido como computación en la nube, se deberán incluir al menos las siguientes cláusulas:

- EL PROVEEDOR dispone de Centros de procesamiento de datos principal y/o alterno, contratados en la nube, implementados siguiendo el estándar ANSI/TIA-942 o superior y contar como mínimo con la certificación TIER III o su equivalente para diseño, implementación y operación.
- EL PROVEEDOR dispone de Certificación ISO 27001 en seguridad de la información para los servicios ofertados, así como, la implementación de los controles establecidos en los estándares ISO 27017 (controles de seguridad para servicios en la nube), ISO 27018 (protección de información personal en la nube) y/o aquella que aplique conforme el servicio ofertado;".
- EL PROVEEDOR se compromete a contar con informes de auditorías de seguridad relacionadas con el servicio contratado por LA COOPERATIA, con base en el perfil de riesgo del proveedor de servicios en la nube, por lo menos una (1) vez al año, con el fin de identificar amenazas y vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que brindan. Los procedimientos de auditoría deben ser ejecutados por personas o empresas especializadas en seguridad de la información en la nube e independientes al proveedor, aplicando estándares vigentes y reconocidos a nivel internacional. El proveedor de servicios en la nube debe definir y ejecutar planes de acción para gestionar las vulnerabilidades detectadas.
- EL PROVEEDOR se compromete a efectuar la entrega periódica a LA COOPERATIVA de informes y certificaciones que demuestren la calidad, desempeño y efectividad en la gestión de los servicios contratados, así como la vigencia de las certificaciones solicitadas.
- EL PROVEEDOR se compromete a contratar anualmente con una empresa auditora de prestigio un examen de auditoría independiente, de los servicios que son objeto de la contratación.
- EL PROVEEDOR dispone de representación comercial en el país, con capacidad para brindar soporte integral con personal y representar legalmente al proveedor internacional en el país (aplica a proveedores internacionales)
- EL PROVEEDOR confirma que dispone de capacidad para transferir sólidamente los conocimientos.

- La información almacenada por EL PROVEEDOR estará a disposición permanente de LA COOPERATIVA y a través de ésta, del organismo de control, por medio de los canales o mecanismos que disponga para el efecto. La información es de estricta confidencialidad y no podrá ser comercializada o utilizada para otros fines distintos a los manejados por la entidad dueña de la información.
- La información proporcionada por LA COOPERATIVA no podrá ser utilizada para ningún propósito diferente al establecido en los contratos, inclusive bajo el modelo de subcontrataciones.
- La notificación de término del contrato deberá ser informada por EL PROVEEDOR con la debida anticipación, con el propósito de garantizar la continuidad de las operaciones de LA COOPERATIVA.
- En caso de terminación del contrato de servicios de infraestructura, plataforma y/o software, la información será devuelta por EL PROVEEDOR a LA COOEPRATIVA de forma inmediata, conservando un respaldo de seguridad por un período de al menos tres meses debiendo observar estricta confidencialidad y el impedimento para utilizarla y comercializarla.

5.12.3.6 *Cláusulas ante la Entrega de Credenciales de Acceso*

- La Cooperativa hará la entrega a EL PROVEEDOR de las credenciales de acceso para ejecución del servicio. EL PROVEEDOR se compromete a gestionar dichas credenciales y accesos acorde a las Políticas de seguridad de LA COOPERATIVA, por lo que deberá garantizar la confidencialidad y el buen uso de estas. cualquier uso indebido derivado del mal manejo de las credenciales entregadas, será de única y exclusiva responsabilidad de EL PROVEEDOR, reservándose LA COOPERATIVA el derecho de ejecutar las acciones legales pertinentes al respecto. Al finalizar el contrato de servicios EL PROVEEDOR deberá efectuar la devolución de las credenciales a la Cooperativa.

5.12.3.7 *Cláusulas para Servicios que Implican Información de Tarjetas de Débito y/o Crédito*

Opción A: Proveedor certificado PCI

Se incluirá las siguientes clausulas en el contrato para los proveedores que deben contar con la certificación.

PROTECCIÓN DE DATOS DE TARJETA DE DEBITO Y/O CRÉDITO DE LOS SOCIOS/CLIENTES

- EL PROVEEDOR será responsable por la seguridad del almacenamiento y/o tratamiento de los datos de tarjetas de débito y/o crédito de los socios/clientes de la Cooperativa que recibiera con motivo de la prestación de sus servicios bajo este Contrato;
- A tal fin, EL PROVEEDOR declara y garantiza a la Cooperativa que: (i) cumple y cumplirá durante toda la vigencia del Contrato con el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (“PCI DSS”); y (ii) cuenta y contará durante toda la vigencia del Contrato con un certificado AoC [Attestation of Compliance] que acredite fecha de cumplimiento y versión de la norma PCI DSS, el cual será remitido a la Cooperativa a solo requerimiento; y

- Las obligaciones previstas en esta Cláusula son aplicables a todos los datos de tarjeta de crédito por operaciones que EL PROVEEDOR gestione, procese, almacene o transmita, en función de los servicios prestados a la Cooperativa.

Opción B: Proveedor no certificado PCI

Se incluirá las siguientes clausulas en el contrato:

PROTECCIÓN DE DATOS DE TARJETA DE DEBITO Y/O CRÉDITO DE LOS SOCIOS/CLIENTES

- EL PROVEEDOR será responsable por la seguridad del almacenamiento y/o tratamiento de los datos de tarjetas de débito y/o crédito de los socios/clientes de la Cooperativa que recibiera con motivo de la prestación de sus servicios bajo este Contrato;
- A tal fin, EL PROVEEDOR declara y garantiza a la Cooperativa que cumple y cumplirá durante toda la vigencia del Contrato con el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago ("PCI DSS");
- EL PROVEEDOR acepta que la Cooperativa realice pruebas de penetración, monitoreos o auditorías de seguridad informática en los sistemas o instalaciones de EL PROVEEDOR, a fin de verificar el cumplimiento con las normas PCI DSS; y,
- Las obligaciones previstas en esta Cláusula son aplicables a todos los datos de tarjeta de crédito por operaciones que EL PROVEEDOR gestione, procese, almacene o transmita, en función de los servicios prestados a la Cooperativa.

5.12.3.8 *Cláusulas para contratos de servicios auxiliares*

- EL PROVEEDOR deberá presentar con periodicidad anual, evidencia de validez de la certificación ISO 27001 de seguridad de la Información en el servicio contratado por la Cooperativa, o a su vez, deberá presentar un Reporte SOC Tipo II emitido por un tercero (La auditoría de los Controles de Servicio y Organización 2 conocida como SOC II, es un estándar internacional que permite evaluar los controles de seguridad de un proveedor y las amenazas de ciberseguridad).
- EL PROVEEDOR deberá presentar con periodicidad anual un informe de conformidad del cumplimiento de la resolución No. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-009 "Norma de control de seguridades en el uso de canales electrónicos" o la que le sustituya, el cual incluya toda la evidencia de su cumplimiento, el mismo que deberá ser emitido por una firma auditora externa al proveedor.

5.12.3.9 *Cláusulas para contratos de* *Servicios de Canales Electrónicos*

- EL PROVEEDOR deberá presentar con periodicidad anual, evidencia de validez de la certificación ISO 27001 de seguridad de la Información en el servicio contratado por la Cooperativa, o a su vez, deberá presentar un Reporte SOC Tipo II emitido por un tercero (La auditoría de los Controles de Servicio y Organización 2 conocida como SOC II, es un estándar internacional que permite evaluar los controles de seguridad de un proveedor y las amenazas de ciberseguridad).
- EL PROVEEDOR deberá presentar con periodicidad anual un informe de conformidad del cumplimiento de la resolución No. SEPS-IGT-IGS-INSESF-INR-

INGINT-INSEPS-009 “Norma de control de seguridades en el uso de canales electrónicos” o la que le sustituya, el cual incluya toda la evidencia de su cumplimiento, el mismo que deberá ser emitido por una firma auditora externa al proveedor.

5.13 Controles Criptográficos

5.13.1 Normas de Cifrado

a) Todos los dispositivos fijos, móviles, teletrabajo, ATM propiedad de la Cooperativa deberán estar cifradas. Se excepcionarán las maquinas que técnicamente no cumplan las características técnicas (memoria, disco procesador) que permitan aplicar el control.

b) El cifrado de los dispositivos mencionados en el literal anterior deberá ser realizado en la preparación y configuración del equipo previo a la entrega a los usuarios finales (cuando el dispositivo es nuevo o es reasignado).

c) El área de Seguridad de la Información verificará periódicamente los controles de cifrado implementados.

d) La transmisión de información del negocio a través de redes de comunicaciones no controladas por la Cooperativa deberá estar cifrada.

e) Se cifrarán todas las comunicaciones en el acceso remoto de los usuarios a la red interna de la Cooperativa.

f) Se cifrarán todas las comunicaciones inalámbricas.

g) Considerando los análisis de riesgos se podrá no sólo cifrar la información transmitida sino la transmisión en sí, mediante el uso de técnicas adecuadas como redes privadas virtuales basadas en estándares (por ejemplo: IPSec, SSL, entre otros.) mediante dispositivos de cifrado de red.

5.13.1.1 Algoritmos de Cifrado

Se deberá identificar el nivel requerido de protección con base en el análisis de riesgos tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado, así como la longitud de las claves criptográficas a utilizar. Se deberán emplear únicamente algoritmos de cifrado acorde con los estándares internacionales vigentes.

5.13.2 Administración de *Claves de Cifrado*

La Dirección de TIC deberá cumplir los siguientes lineamientos:

a) Deberá desarrollar un procedimiento considerando:
- Que las claves no estén expuestas a revelación, modificación, pérdida o destrucción.
- Independencia de funciones para el proceso de recuperación de información cifrada, que incluya aprobaciones por parte del titular.

b) Se deberán considerar además las siguientes normas:
- Cuando se utilicen técnicas de cifrado simétrico o de clave privada, se garantizará la confidencialidad en el intercambio de las claves (por un canal seguro o cifradas mediante mecanismos de cifrado asimétrico).

- Cuando se utilicen técnicas de cifrado asimétrico, en el intercambio, la autenticidad e integridad quedará avalada por una autoridad de certificación de confianza, bien interna (PKI interna) o externa (Verisign, entre otros). En el caso de uso de servicios criptográficos de terceros, los acuerdos de prestación de servicios deberán cubrir aspectos de responsabilidad civil, fiabilidad y seguridad del servicio y tiempos de provisión.

5.14 Seguridad Física y del Entorno

5.14.1 Seguridad Física y Electrónica

a) Se deberá cumplir con las políticas establecidas en la normativa interna del área de Seguridad Física y Electrónica.
b) Los lineamientos para los accesos físicos a las áreas restringidas de la Cooperativa deberán ser definidos por el área de Seguridad de la Información en conjunto con Seguridad Física y Electrónica.
c) Los lineamientos para el acceso físico a las instalaciones de la Cooperativa deberán ser establecidas por el área de Seguridad Física y Electrónica, y documentados para cumplimiento de la normativa interna.
d) El área de Seguridad de la Información deberá revisar de forma anual la matriz de accesos físicos del área de Seguridad Física y Electrónica, con la finalidad de controlar la emisión y revocación de este tipo de accesos.

5.14.2 Suministros de energía

La Dirección Administrativa deberá considerar los siguientes lineamientos:

a) Implementar controles para garantizar que los equipos estén protegidos frente a fallos eléctricos y otras anomalías en el suministro necesario para la Cooperativa (agua, ventilación, aire acondicionado, entre otros). Los controles estarán acordes a la criticidad de los equipos, requisitos regulatorios y del negocio.
b) Contar con un generador de respaldo para garantizar la continuidad operativa en caso de cortes o fallas prolongados de energía.
c) Los generadores deberán ser probados periódicamente de acuerdo con las instrucciones del fabricante o proveedor.
d) Disponer de un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado.
e) Proveer de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía.
f) Implementar protección contra rayos en todas las instalaciones de la Cooperativa a nivel nacional y deberán adaptar filtros de protección contra rayos en todas las líneas de comunicaciones externas.

La Dirección de TIC deberá considerar los siguientes lineamientos:

a) Se recomienda usar UPS para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de la Cooperativa. Los planes de contingencia deben contemplar las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS deberán inspeccionarse

periódicamente para asegurar que tienen la capacidad requerida y se deberán probar de conformidad con las recomendaciones del fabricante o proveedor.

5.14.3 Seguridad del Cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información deberá ser protegido contra interceptación o daño. La Dirección Administrativa y Dirección de TIC deberán tener en cuenta los siguientes controles:

a) Las líneas de energía eléctrica y telecomunicaciones que se conectan con las instalaciones de procesamiento de información deberán ser subterráneas, siempre que sea posible, o sujetas a una adecuada protección alternativa.
b) El cableado de red deberá estar protegido contra interceptación no autorizada o daño, por ejemplo, mediante el uso de conductos o evitando trayectos que atraviesen áreas públicas.
c) Los cables de energía deberán estar separados de los cables de comunicaciones para evitar interferencias.
d) Entre los controles adicionales a considerar para los sistemas sensibles o críticos se encuentran los siguientes:
- Instalación de conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección.
- Uso de rutas o medios de transmisión alternativos.
- Uso de cableado de fibra óptica.
- Iniciar barridos para eliminar dispositivos no autorizados conectados a los cables.

5.14.4 Mantenimiento de Equipos Tecnológicos (Hardware)

La Dirección de TIC deberá definir procesos que garanticen el mantenimiento adecuado de los equipos tecnológicos (hardware), para asegurar que su disponibilidad e integridad sean permanentes. Se deberán considerar los siguientes lineamientos:

a) El equipamiento deberá mantenerse de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor.
b) Solo el personal autorizado por la Dirección de TIC podrá brindar mantenimiento preventivo y/o correctivo en el equipamiento.
c) Se deberán mantener registros de todas las fallas supuestas o reales y de todo el mantenimiento preventivo y correctivo.
d) Deberán implementarse controles cuando se retiran equipos de Cooperativa para su mantenimiento, de manera que no se exponga la confidencialidad de la información que contengan.

5.14.5 Movilización de dispositivos tecnológicos fuera de las instalaciones de la Cooperativa

El área de Seguridad Física y Electrónica deberá controlar que los dispositivos tecnológicos de la Cooperativa no puedan ser movilizado fuera de las instalaciones de la Cooperativa sin autorización del jefe inmediato o del titular del activo.

5.14.6 Seguridad del equipamiento fuera del ámbito de la Cooperativa

El área de Seguridad Física y Electrónica deberá establecer y difundir de manera periódica recomendaciones de protección física dirigidas hacia el personal de la Cooperativa, con el objetivo de proteger aquellos equipos que por temas de trabajo son trasladados fuera de las instalaciones de la Cooperativa, considerando los siguientes lineamientos:

a) El equipamiento y dispositivos no deben permanecer desatendidos en lugares públicos.
b) Los dispositivos fijos y teletrabajo deben ser transportadas como equipaje de mano y de ser posible camufladas, durante el viaje.
c) Se deberán respetar permanentemente las instrucciones del fabricante, por ejemplo, protección por exposición a campos electromagnéticos fuertes.
d) Se recomienda la contratación de un seguro para proteger el equipo fuera del ámbito de la Cooperativa.

5.14.7 Baja segura o reutilización de dispositivos tecnológicos

a) La Dirección de TIC deberá implementar procedimientos que garanticen que todos los medios de almacenamiento incluyendo los diferentes tipos de dispositivos, excepto los dispositivos personales, sean borrados de manera segura, previo a su baja o reasignación, para el efecto deberá considerar los lineamentos especificados en el presente manual.

5.14.8 Inspección de *cumplimiento de políticas de puesto de trabajo despejado y pantalla limpia*

a) Los jefes departamentales y Jefes de Agencias serán los encargados de velar por el cumplimiento de las "**Políticas de puesto de Trabajo Despejado y Pantalla Limpia**" por parte de los colaboradores a su cargo.
b) El área de Seguridad de la Información deberá efectuar inspecciones presenciales en el edificio Administración Central de manera trimestral para evaluar la efectividad del control, el cual será documentado y entregado mediante informe al Oficial de Seguridad de la Información para su respectiva gestión.
c) Para el caso de agencias, el área de Seguridad de la Información podrá solicitar a los Jefes de Agencia la evidencia del cumplimiento del control citado, debiendo el Jefe de Agencia emitir un informe dentro de los 7 días laborables posterior a la solicitud.
d) El área de Seguridad Física y Electrónica apoyará con el cumplimiento de evaluación del control citado, mediante el monitoreo a través de cámaras de seguridad de manera aleatoria, reportando en caso de detectar los incidentes al área de Seguridad de Información.

5.15 Seguridad de Operaciones Tecnológicas

5.15.1 Documentación de procedimientos de operación

La Dirección de TIC deberá desarrollar y aplicar los procesos de operación tecnológicos bajo su gestión, los mismos que deberán ser formalizados y ponerse a disposición de todos los usuarios que los necesiten acorde lo establecido en el *Procedimiento Administración Documental*.

5.15.2 Procedimientos de control de cambios

La Dirección de TIC debe establecer un procedimiento formal de control de cambios, considerando los siguientes lineamientos:

- Mantener un registro de los niveles de autorización aprobados.
- Garantizar que los cambios solicitados sean efectuados por usuarios formalmente autorizados.
- Aplicar controles y procedimientos de integridad para garantizar que el ambiente de producción no sea comprometido por los cambios realizados.
- Detallar los componentes tecnológicos como: software, hardware y bases de datos que se vean afectados por los cambios realizados.
- Obtener aprobación formal para los cambios solicitados antes de que sean efectuados.
- Garantizar que la implantación se lleve a cabo minimizando la no disponibilidad de los aplicativos de la Cooperativa.
- Garantizar que la documentación del sistema será actualizada cada vez que se completa un cambio y la documentación vieja sea archivada o eliminada.
- Mantener un control de versiones para todas las actualizaciones de software, hardware y sus configuraciones.
- Mantener toda la documentación que permita evidenciar todas las solicitudes de cambios.
- Garantizar que la documentación técnica y de usuario se actualicen según los cambios efectuados.
- Definir un procedimiento para el control de cambios emergentes.

5.15.3 Planificación de la *Capacidad*

La Dirección de TIC deberá monitorear las demandas de capacidad y realizar proyecciones de los futuros requerimientos, a fin de garantizar la disponibilidad del poder de procesamiento y almacenamiento adecuados. Estas proyecciones deben tomar en cuenta la planificación estratégica de la Cooperativa, requisitos regulatorios, requerimientos de negocios, sistemas de información, tendencias actuales y proyectadas en el procesamiento de la información de la Cooperativa. Se deberán identificar e implementar acciones para evitar potenciales cuellos de botella o fallas en rendimiento de los sistemas, que podrían plantear una amenaza a la seguridad o a los servicios de la Cooperativa.

5.15.4 Separación entre ambientes de desarrollo, pruebas y producción

Los ambientes de desarrollo, pruebas y producción deberán estar separados al menos de manera lógica, a fin de reducir el riesgo de cambios accidentales o accesos no autorizados al software o a los datos. Se deben tener en cuenta los siguientes controles:

a) El software en desarrollo, pruebas y producción debe ejecutarse en diferentes procesadores o equipos virtuales.
b) Las actividades de desarrollo, pruebas y producción deben estar separadas.
c) Cuando no es requerido, los compiladores, editores y otros utilitarios del sistema no deben ser accesibles desde los sistemas que están en ambiente de producción.
d) Se deben utilizar diferentes procedimientos de conexión para sistemas en ambiente de pruebas y producción, a fin de reducir el riesgo de error. Se debe comunicar a los

usuarios la obligatoriedad de utilizar diferentes contraseñas para estos sistemas, y los menús deben desplegar adecuados mensajes de identificación.

5.15.5 Acuerdos de Nivel de Servicios

La Dirección de TIC deberá establecer formalmente acuerdos de nivel operativo(OLA) con las áreas de la Cooperativa, en donde se definan los niveles de criticidad de los incidentes de disponibilidad de sus aplicaciones, basándose los siguientes parámetros definidos por el negocio:

- Porcentaje/número de usuarios internos afectados.
- Porcentaje/número de socios afectados.
- Tiempo de indisponibilidad de la aplicación.
- Sanciones de entes reguladores.
- Pérdidas financieras.
- Afectación a la imagen institucional.

5.16 Protección Contra Software Malicioso

Se deberá implementar medidas para controlar y prevenir la entrada de virus y otros programas maliciosos en la Cooperativa.

Para esto deberá cumplir los siguientes lineamientos:

a) El área de Seguridad de la Información deberá controlar en todos los puntos de comunicación con el exterior, tanto en los accesos compartidos (como correo electrónico, navegación web, redes sociales, etc.), como en los accesos locales (por ejemplo, dispositivos USB, discos duros externos, etc.).

b) El sistema antivirus deberá tener características que permitan su actualización automática, con el objetivo de contar con las últimas definiciones de virus emitidas por el fabricante.

c) El sistema antivirus estará configurado para realizar revisiones periódicas del contenido de software y datos de todos los sistemas de información de la Cooperativa.

d) La Dirección de TIC deberá garantizar que las configuraciones preestablecidas en los diferentes tipos de dispositivos no podrán ser modificadas por el usuario final.

e) Las alertas emitidas por el sistema antivirus deberán ser investigadas por el área de Seguridad de la Información, debiendo reportar conforme al *Procedimiento Atención y Análisis de Incidentes de Seguridad de la Información*.

f) El área de Seguridad de la Información deberá garantizar que las herramientas de seguridad verifiquen la presencia de software malicioso en archivos adjuntos a mensajes de correo electrónico, archivos descargados por Internet, archivos de medios electrónicos de origen incierto o no autorizado, antes de su uso.

g) Se deberán documentar normativa interna para formalizar la administración de los sistemas antivirus en la Cooperativa, en donde se establezca el cargo del responsable de su administración, la configuración de los sistemas, los procesos de monitoreo, escalamiento, comunicación y remediación ante incidentes.

h) El área de Seguridad de la Información deberá garantizar la disponibilidad de soluciones antivirus para todos tipos de dispositivos de usuario final que se defina emplear en la Cooperativa.

5.17 Respaldos

5.17.1 Procesos de ejecución de respaldos

La Dirección de TIC deberá cumplir con:

a) Lo especificado en el artículo 225 del Código Orgánico, Monetario y Financiero, que especifica: "*Las entidades del sistema financiero nacional mantendrán sus archivos contables físicos, incluyendo los respaldos respectivos, por el plazo de diez años contados a partir de la conclusión de la operación correspondiente y por quince años en el formato digital autorizado por las superintendencias*".

b) Desarrollar la normativa interna que corresponda para formalizar y controlar la obtención de copias de respaldo de la información y software, que contengan como mínimo los siguientes parámetros:

- Los responsables de realizar las copias de respaldo y posterior custodia.
- Periodicidad de las copias de respaldo.
- Número de copias.
- Tipo de respaldo (completa o diferencial/incremental).
- Tiempos máximos de almacenamiento (fecha de expiración) y si es necesario eliminar la información una vez alcanzada la fecha de expiración (así como el procedimiento de destrucción exigido).
- Tiempos mínimos aceptables para recuperar la información.
- Necesidad de guardar las copias de respaldo y los procedimientos asociados en un lugar geográficamente distinto, que no se encuentre bajo la misma zona de riesgo natural.
- Necesidad de cifrar la información respaldada.
- Períodos de retención.
- Periodicidad de pruebas de respaldo y recuperación.

c) Los parámetros antes indicados serán establecidos para cada sistema de información o información respaldada, en función de los siguientes aspectos:

- La naturaleza de la información (financiera, contratos con clientes, registros de accesos, sistemas operativos, entre otros.).
- Los requisitos de disponibilidad determinados por el titular del activo de información de acuerdo con las necesidades del negocio.
- Los requisitos legales aplicables.
- Los niveles de servicio acordados.
- Definiciones internas de retención de información y datos definidas por el dueño de información.
- Riesgo tecnológico implícito.
- Nivel de clasificación de la información.
- Los planes de continuidad de negocio.

d) Los procedimientos de respaldo para los sistemas individuales deberán ser probados regularmente para asegurar que cumplan con los requerimientos de los planes de continuidad del negocio. Para sistemas críticos, los procedimientos de respaldo deberán abarcar toda la información, aplicaciones y data de todos los sistemas, necesarios para recuperar el sistema completo en caso de un desastre.

e) Deberá además implementar controles que impidan que la información respaldada sea restaurada o accedida sin contar con la autorización del dueño de la información.

f) Se requiere que todos los sistemas de respaldo cuenten con registros de auditoría que permitan efectuar controles de respaldos y restauraciones.

g) Deberá definir un proceso de respaldos para garantizar la confidencialidad, integridad y disponibilidad de la información de la nube institucional de los colaboradores, para lo cual deberá garantizar el provisionamiento del espacio necesario para resguardar el respaldo de la información de la nube institucional de un usuario activo, inactivo o desvinculado.

h) Los respaldos de la información de la nube institucional de un usuario se lo deben realizar bajos los siguientes parámetros:

1) Respaldar permanentemente la información de usuarios activos quienes manejan información sensible o clasificada como restringida y confidencial que se encuentran desempeñando sus funciones en los siguientes cargos:
   - Presidente de la Asamblea General de Representantes,
   - Presidente de los consejos,
   - Presidente de los diferentes comités y comisiones que ameriten,
   - Gerente,
   - Subgerentes,
   - Directores,
   - Jefes de Administración Central,
   - Oficiales,
   - Secretarias de Presidencia y Gerencia,
   - Secretarios de los diferentes comités y comisiones; y,
   - Área de Auditoría interna

2) El tiempo de retención de los respaldos de usuarios inactivos es de 6 meses contando desde la fecha de su desvinculación de la Cooperativa.

5.17.2 Administración y seguridad de los medios de almacenamiento

5.17.2.1 Administración de medios informáticos de almacenamiento

Se deberá definir procedimientos para la administración de medios informáticos de almacenamiento, por ejemplo: asignación, reasignación de dispositivos institucionales, cambio de discos duros de servidores, ya sean de dispositivos fijos o teletrabajo, CDs, DVDs, cintas, considerando los siguientes lineamientos:

a) Si ya no son requeridos por el titular, deberá efectuarse la eliminación segura de la información de cualquier medio informático de almacenamiento que requiera ser reasignado a otro colaborador, donado o dado de baja.

b) Se debe requerir autorización del titular, para retirar cualquier medio informático de almacenamiento de la Cooperativa.

c) Todos los medios deben almacenarse en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.

5.17.2.2 Transporte de medios informáticos de almacenamiento

La Dirección de TIC deberá asegurar que el transporte de medios informáticos de almacenamiento incluya controles de protección contra el acceso no autorizado, mal uso o daño durante el transporte, considerando su nivel de clasificación.

Se deberán considerar los siguientes lineamientos:

a) Utilización de empresas de servicios de transporte especializadas.
b) Los dispositivos empleados para embalaje y envío de medios físicos, deben ser adecuados para proteger el contenido de posibles daños físicos o lógicos probables que surjan durante el tránsito; y, deberá estar de acuerdo con las especificaciones de los fabricantes.
c) Se deberán adoptar controles especiales, cuando resulte necesario, a fin de orden fortuito sensible contra exposición o modificación no autorizadas.

5.18 Monitoreo del acceso y uso de los sistemas

5.18.1 Registro de eventos

a) Los sistemas, así como el detalle y cantidad de eventos a registrar en un sistema de información o red de comunicaciones estará determinado:
- Por el análisis de riesgos del sistema o de la red.
- Por la legislación aplicable del Ecuador.
- Por la conveniencia en el monitoreo del cumplimiento eficaz y eficiente de los controles de seguridad establecidos.

b) Se registrarán todos los eventos de seguridad, es decir, todos los sucesos, ocurrencias o fallos observables en un sistema de información o red de comunicaciones que puedan estar relacionados con la confidencialidad, integridad o disponibilidad de la información.
c) Especialmente se registrarán la actividad de los administradores y operadores de los sistemas de información.
d) Con carácter general, los eventos de seguridad de los que será necesario generar y almacenar un registro de auditoría son:
- Los eventos requeridos por la legislación aplicable del Ecuador.
- Los intentos de autenticación fallidos.
- Los accesos de los usuarios a los sistemas, tanto autorizados como los intentos no autorizados.
- Los eventos de operación y administración de los sistemas: el uso de cuentas privilegiadas de administración (root, admin, entre otros), el uso de programas y utilidades. de administración, la parada y arranque de los sistemas, la instalación o desinstalación de dispositivos de almacenamiento o de entrada/salida.
- Los cambios en los parámetros de configuración de los sistemas.
- Los errores de funcionamiento de los sistemas y las redes.
- Los accesos a redes de comunicaciones, tanto autorizados como los intentos no autorizados: acceso remoto a la red interna (por RAS, ADSL, red privada virtual, entre otros.), accesos a Internet, entre otros.
- El tráfico no permitido o rechazado por los cortafuegos y los dispositivos de encaminamiento (al menos de los protocolos más comunes y/o peligrosos).
- Las alertas generadas por los dispositivos de detección/prevención de intrusos (IDS/IPS).
- Los cambios en los privilegios de acceso: alta, baja y modificación de usuarios, cambios en los perfiles, entre otros.

- Los cambios en los sistemas de seguridad, como la activación/desactivación o cambios en la configuración de los antivirus, de los sistemas de control de acceso, entre otros.
- El acceso al código fuente de los sistemas desarrollados internamente.
- La activación/desactivación o cambios en la configuración de los mecanismos que generan los registros de auditoría.
- Las modificaciones o borrado de los ficheros con registros de auditoría.

5.18.2 Formato de los registros de auditoría

a) Los registros de auditoría deberán contener cuando sea relevante y aplicable al menos:

- Identificadores personales (ID)
- Nombre del usuario
- Actividades del sistema
- Fechas, tiempos y detalles de eventos clave, por ejemplo, conexión (log-on) y desconexión (log-on)
- Identidad o localización del dispositivo, si es posible e identidad del sistema
- Registro de intentos de acceso a los sistemas exitosos y fallidos
- Registro de intentos de acceso a los recursos y a los datos exitosos y fallidos
- Cambios de configuración del sistema
- Uso de privilegios
- Uso de utilidades y aplicaciones del sistema
- Archivos a los que se ha accedido y el tipo de acceso
- Direcciones y protocolos de red
- Alarmas generadas por el sistema de control de acceso
- Activación y desactivación de los sistemas de protección, tales como sistemas de antivirus y de protección de intrusos
- Registro de transacciones ejecutadas por usuarios en las aplicaciones

b) Podría requerirse que ciertos registros de auditoria sean archivados como parte de la norma de retención de registros o debido a los requerimientos de recolección de evidencia.

5.18.3 Sincronización de relojes

a) Los relojes de todos los sistemas de información y dispositivos que generen registros de auditoría deberán sincronizarse con la misma fuente de tiempo.

b) Cuando una computadora o dispositivo de comunicaciones tenga la capacidad de operar un reloj en tiempo real, este se debe configurar según un estándar acordado, por ejemplo: Tiempo Coordinado Universal (UCT) o tiempo estándar local. Como se sabe que algunos relojes se desajustan con el tiempo. La Dirección de TIC deberá asegurar que todos los dispositivos tecnológicos tengan la hora sincronizada.

5.18.4 Integridad y confidencialidad de los registros de auditoría

La Dirección de TIC es la responsable de cumplir con los siguientes lineamientos:

a) Establecer controles que garanticen la integridad y confidencialidad de los registros de auditoría, así como para evitar el borrado de estos o desactivación no autorizada de los mecanismos que los generan.

b) Sólo permitirá el acceso a los registros de auditoría y el control de los mecanismos que los generan a las personas debidamente autorizadas por el Oficial de Seguridad de la Información. En todo caso, los mecanismos y los registros de auditoría no estarán bajo control directo de los usuarios y administradores cuyas actividades sean origen de los registros, sin que se deba permitir, en ningún caso, la desactivación o modificación de estos.

5.18.5 Disponibilidad y almacenamiento de los registros de auditoría

La Dirección de TIC es la responsable de cumplir con los siguientes lineamientos:

a) Los registros de auditoría serán guardados por un periodo de tiempo que tenga en cuenta la legislación aplicable y requisitos del negocio.
b) Establecer mecanismos que detecten si la capacidad de los medios que almacenan los registros de auditoría es superada o llega a un porcentaje de ocupación determinado. Estos mecanismos se implantarán igualmente en aquellas configuraciones que permitan la sobre escritura de "registros" si se llega a un tamaño máximo de archivo.
c) En base a un análisis de riesgos y al volumen de registros de auditoría que gestione la Cooperativa, podrá establecer la necesidad del uso de un sistema centralizado para el almacenamiento y gestión de los registros de auditoría.

5.18.6 Monitoreo de los registros de auditoría

a) En base al análisis BIA se establecerán los servicios y procesos sobre los cuales el área de Seguridad de la Información efectuará el monitoreo de registros de auditoría.
b) La Dirección de TIC será responsable de implementar soluciones que permitan centralizar y emitir alarmas para ejecutar el monitoreo antes citado.

5.19 Control del software operacional

5.19.1 Instalación del software en los sistemas operativos

a) Se deberá instalar y usar el software autorizado en los dispositivos tecnológicos de la Cooperativa con el fin de garantizar que solo se utilicen aplicaciones que sean seguras y confiables para proteger la información.
b) El inventario del software instalado en los dispositivos de la Cooperativa deberá ser actualizado y revisado anualmente por el Oficial de Seguridad de la Información asegurando el cumplimiento con regulaciones externas e internas.
c) La Dirección de TIC deberá instalar y preparar los diferentes tipos de dispositivos (fijos, teletrabajo, móviles y ATM) en función a la matriz de software autorizada por Seguridad de la Información.

5.20 Gestión de la vulnerabilidad técnica

5.20.1 Control de las vulnerabilidades técnicas

a) El análisis de vulnerabilidades de todos los dispositivos tecnológicos deberá ser ejecutados de forma periódica por el área de Seguridad de la Información, para identificar y mitigar las debilidades que podrían ser explotadas por atacantes.

b) El titular de activo será el responsable de gestionar la remediación de las vulnerabilidades que afecten a los servicios, sistemas operativos, software y aplicaciones de la Cooperativa ya sea que se encuentren bajo administración directa por parte de la Cooperativa, como a través de contratos de servicios gestionados con terceras partes. Gestión que deberá se efectuada en función de minimizar el tiempo de exposición de los sistemas de información y el riesgo de que las vulnerabilidades puedan ser explotadas.

c) La Dirección de TIC deberá gestionar:

- La definición y aprobación formal por parte del Comité de Tecnologías de la Información y Comunicación de estándares de software base para dispositivos institucionales fijos y teletrabajo (incluye: sistema operativo, bases de datos, utilitarios, navegadores).
- La definición y aprobación formal por parte del Comité de Tecnologías de la Información y Comunicación de estándares de aplicaciones y software ofimático para dispositivos institucionales fijos.
- La definición y aprobación formal de estándares de hardware para dispositivos institucionales fijos, equipos de comunicación.
- Toda adquisición de hardware y software comercial o nuevos desarrollos internos deben estar alineada a los estándares definidos en los puntos anteriores, los mismos que deben ser aprobados por el Comité de Tecnologías de la Información y Comunicación.
- La designación de roles y responsabilidades dentro de la Dirección de TIC, asociadas con la gestión de las vulnerabilidades técnicas; su identificación, análisis, aplicación y verificación del parche, entre otros.
- La disponibilidad de un inventario del software instalado en la Cooperativa, el cual incluya: nombre, fabricante, versión, versión de parches, entre otros.
- La formalización de las fuentes de información de vulnerabilidades.
- Los parches deberán ser obtenidos de los propios fabricantes de las plataformas.
- Para el tratamiento de vulnerabilidades se deberá considerar los siguientes lineamientos:
  - Todo software y sistema operativo estará actualizado con los últimos parches de seguridad recomendados por el fabricante.
  - Se deberá priorizar la instalación de los parches que solucionen las vulnerabilidades más graves en los sistemas con más exposición y riesgo, atendiendo a su criticidad.

Criticidad	Tiempo máximo de resolución
Crítica	30 días
Alta	45 días
Media	60 días
Baja	90 días

  - Cualquier excepción a los tiempos establecidos deberá ser debidamente justificada por parte del titular del activo. En caso de que el tiempo de remediación propuesto por el titular duplique el tiempo establecido, se

requerirá de la autorización del Gerente en los casos de áreas con reporte directo o los subgerentes para las demás áreas para proceder con la extensión del plazo citado.

- Los parches serán probados y evaluados en ambiente de pruebas, certificando la no afectación del servicio antes de su instalación en ambiente de producción, debiendo estar alineado al proceso de control de cambios institucional. Se deberá analizar si la instalación de un parche introduce más riesgo que el riesgo de exposición a la vulnerabilidad.
- En los casos en los que un parche no esté disponible o no pueda ser instalado, se estudiarán las medias compensatorias orientadas a reducir el riesgo de exposición (introducir nuevas reglas en los cortafuegos, quitar el servicio afectado en el sistema, configurar el IDS/IDP, entre otros).
- Todo parche deberá, en lo posible, incluir en su documentación la información referente a su procedimiento de vuelta atrás o desinstalación. Si el parche no permite lo anterior, deberá documentarse esta situación.

5.20.2 Restricciones de instalación de software

a) La actualización o instalación del software operacional, aplicaciones y bibliotecas de programas en servidores sólo deberá ser realizada por los administradores previamente autorizados por la Dirección de TIC.

b) La actualización o instalación del software operacional, aplicaciones y bibliotecas de programas en dispositivos institucionales fijos, sólo deberá ser realizada por personal de Mesa de Atención Técnica, conforme a la matriz de software base autorizado.

c) La actualización o instalación del software operacional, aplicaciones y bibliotecas de programas en dispositivos móviles de usuario final, sólo deberá ser realizada por herramientas MDM (Mobile Device Management).

d) La actualización o instalación del software operacional, aplicaciones y bibliotecas de programas en dispositivos ATM, sólo deberá ser realizada por personal de Mesa de Atención Técnica, en coordinación con el área de Canales Electrónicos.

e) La Cooperativa, autoriza la instalación de aplicaciones de software comercial, mediante el esquema de adquisición, arrendamiento de licencias y/o suscripciones.

f) El despliegue de las aplicaciones de software comercial en los dispositivos institucionales deberá considerar de manera permanente la disponibilidad de las licencias de software adquiridas o bajo esquema de arrendamiento. No se podrán instalar paquetes de software comercial sobre los que no se disponga de las licencias respectivas.

g) Los contratos de adquisición de licencias de software deben considerar la inclusión del servicio de “Mantenimiento o Soporte” por parte del proveedor, para garantizar la disponibilidad de parches de seguridad y actualizaciones del sistema, gestionando la renovación continua de dicho servicio. La Dirección de TIC deberá evaluar los riesgos de trabajar con software que encontrándose en ambiente de producción deje de tener soporte del fabricante y considerar la actualización hacia versiones nuevas o migración hacia otros sistemas.

h) Cualquier decisión para actualizar a una versión nueva deberá tomar en cuenta los requerimientos comerciales para el cambio, y la seguridad de la versión; es decir, la

introducción de la nueva funcionalidad de seguridad o el número y severidad de los problemas de seguridad que afectan esta versión.

i) Para adquisición o instalación de nuevo software, la Dirección de TIC formalizará la ejecución de un análisis mediante un informe que avale compatibilidad técnica de la aplicación, el mismo que deberá ser revisado por el área de Seguridad de la Información.

j) Los contratos de adquisición de licencias de software deben considerar la inclusión del servicio de "Soporte" por parte del proveedor, para garantizar ayuda y soporte en la aplicación ante problemas que pueda presentar el sistema.

k) Se prohíbe la descarga, instalación y uso de "Software Libre", definiendo como software libre a aquel software que permite a los usuarios ejecutar, copiar, distribuir y estudiar el software, e incluso modificarlo y distribuirlo modificado (también llamado de "Código Abierto").

l) Se prohíbe la descarga, instalación y uso de "Software Gratuito", independientemente de que éste sea libre o no.

m) Se prohíbe la descarga e instalación de "Software de Dominio Público", éste último es aquel que no requiere de licencia, pudiendo cualquiera hacer uso de él.

n) Toda excepción a las disposiciones señaladas en los numerales k), l) y m) del presente artículo deberá estar respaldada de un análisis técnico por parte de la Dirección de TIC el mismo que deberá ser autorizado por el Oficial de Seguridad de la Información.

o) Los aplicativos instalados en los dispositivos institucionales fijos sólo deberán mantener códigos ejecutables aprobados; y no códigos de desarrollo o compiladores.

p) Se autoriza el uso de compiladores o herramientas de desarrollo a las áreas o cargos autorizados por la Dirección de TIC.

q) Tanto para nuevas aplicaciones como para cambios, se debe garantizar la ejecución de las pruebas correspondientes previas a su paso a producción. Las pruebas para realizar sobre un aplicativo dependerán del alcance y criticidad del cambio se deberán considerar según corresponda: pruebas funcionales y técnicas. Se deberá definir esquemas que permitan mantener control de versiones de todo el software implementado, así como la documentación del sistema.

r) Se deberá establecer una estrategia de "regreso a la situación original" antes de implementar los cambios, que incluya mantener las versiones previas del software de aplicación como una medida de contingencia, junto con toda la información requerida y los parámetros, procedimientos, detalles de configuración y software que corresponda.

s) Todo equipo de cómputo que disponga de características o ejecute funciones de servidor (web, de archivos, base de datos, procesamiento de información, entre otros) deberá ser instalado y residir en los centros de cómputo definidos por la Dirección de TIC, no está permitido que estos equipos permanezcan o funcionen fuera de las instalaciones antes indicadas.

5.21 Seguridad en las comunicaciones

5.21.1 Gestión de seguridad de la red

5.21.1.1 Procedimientos de seguridad en las redes de comunicaciones

a) La Dirección de TIC deberá definir, implantar y mantener procedimientos de gestión de las redes, dispositivos de comunicación y sistemas de seguridad perimetral que forman la red de la Cooperativa, esto incluye la instalación, configuración y gestión segura de cada tipo de dispositivo. Estos procedimientos estarán documentados, publicados y disponibles para los administradores que lo necesiten.

b) No se permitirá la puesta en producción de ningún elemento de red que no haya sido configurado con los lineamientos de seguridad vigentes para la plataforma, sistema de información o equipo de conectividad.

c) Los procedimientos de instalación y configuración de seguridad deberán ser respaldados con documentación vigente emitida oficialmente por el fabricante.

5.21.1.2 Planificación de redes de comunicaciones

a) La Dirección de TIC deberá implementar procesos de monitoreo de las redes de comunicaciones con el objetivo de evaluar, ajustar y planificar la capacidad de los enlaces de comunicaciones y los elementos de red (routers, cortafuegos, switches, entre otros) de acuerdo con el rendimiento esperado y reducir así el riesgo de posibles fallos.

b) La planificación de la capacidad deberá tener en cuenta los acuerdos de nivel de servicios establecidos con el negocio, referentes al tiempo de respuesta en el acceso a la información y los sistemas que la tratan, así como la tendencia actual y proyectada del acceso a los recursos.

c) Basándose en un análisis de impacto al negocio y en ejercicios de análisis de riesgos, se planificará la disponibilidad de la red para que responda automáticamente a los cortes en los enlaces de comunicaciones o fallos de los dispositivos esenciales de encaminamiento y equipamiento de electrónica de red (enlaces de backup, redundancia, entre otros).

5.21.1.3 Subdivisión de Redes

a) En base a análisis de riesgo, se deberán implementar controles dentro de la red, a fin de segregar grupos de servicios de información, usuarios y sistemas de información.

b) El nivel de riesgo de cada segmento de red identificado estará influenciado por los siguientes factores:

- Si el segmento está dedicado a sistemas de usuarios o a albergar servidores centrales.
- La criticidad de los sistemas conectados al segmento (y de la información que tratan).
- La criticidad de la información que se transmite.
- La criticidad de los servicios existentes.
- La exposición potencial a amenazas externas (conexión con Internet, entre otros).
- El número y naturaleza de los usuarios conectados en el segmento lógico de red (colaboradores, subcontratados, administradores, entre otros).
- Los mecanismos de seguridad implantados (cortafuegos, sistemas de detección de intrusos, cifrado, entre otros).

- La condición cableada o inalámbrica de las redes que forman el segmento lógico de red, considerando las redes inalámbricas como redes de mayor riesgo.
- Las necesidades de acceso de los usuarios de acuerdo con las normas de control de acceso y uso de servicios que se defina.
- El coste o tiempo de recuperación del segmento de red en caso de caída.

5.21.1.4 Control de conexión a la red interna

a) La Dirección de TIC deberá definir procedimientos para conexión a la red interna de la Cooperativa, el mismo que debe considerar los siguientes lineamientos:

- Toda conexión de la red interna de la Cooperativa con una red externa deberá ser autorizada previamente.
- Cualquier conexión de la red interna con otras redes externas estará protegida con un cortafuego.
- No se permitirá el uso de módems ni otros mecanismos similares (ADSL, entre otros) de conexión a redes externas en sistemas que estén conectados a la red interna, a menos que se garantice una conexión segura a dicha red acordada formalmente entre las partes.
- En el acceso de los usuarios a la red interna se implantarán mecanismos que comprueben que la seguridad del computador personal que se conecta es suficiente y no pone en peligro la seguridad de la red interna.
- En base a un análisis de riesgos se implementarán sistemas de control y análisis de configuración de la red.
- Implementar controles que garanticen que el entorno del acceso remoto sea seguro.

5.21.1.5 Conexión de redes externas

a) Esquemas de conectividad permitidos

De manera obligatoria, toda conexión a la red institucional de la Cooperativa mediante redes externas deberá efectuarse mediante esquemas de conectividad que aseguren la confidencialidad de la información transmitida, permitiéndose el uso de cualquiera de los siguientes esquemas:

- Uso de VPN.
- Enlace de datos cifrado con hardware y/o software.

b) Proceso de aprobación

Las solicitudes de conectividad serán gestionadas por el área de Infraestructura y Producción mediante el formulario de aprobación definido para tal efecto, debiendo la mencionada área mantener el custodio de las solicitudes de aprobación.

c) Justificación

El acceso mediante VPN deberá estar justificado en función a necesidades por motivos de trabajo que requiera manejo de turnos, tareas de soporte tecnológico o de negocio, así como en escenarios de contingencia o continuidad, dicha justificación deberá ser incluida en los formularios de solicitud debiendo especificarse el tiempo de caducidad del permiso, el mismo que no deberá superar el año calendario.

d) Configuración de la VPN

Se deberá considerar lo siguiente:

- Crear cuentas de usuario con permisos de acceso personalizados;
- Determinar el software permitido para realizar conexiones VPN;
- Establecer un tiempo para la desconexión automática de la VPN tras un periodo de inactividad.

e) Control de ruteo de red

Se controlará la configuración de encaminamiento y las rutas implementadas en las redes de comunicaciones, de manera que se garantice la correcta implementación de los criterios y normas que regulan el tráfico permitido entre los segmentos lógicos de red.

- Los controles de ruteo deben basarse en la verificación positiva de direcciones de origen y destino.
- Los cortafuegos y dispositivos de encaminamiento de red deberán establecer mecanismos para evitar el "spoofing".
- No se permitirá el encaminamiento basado en técnicas de "source routing".
- Se protegerá la integridad del servicio de traducción de direcciones (DNS) en las redes de comunicaciones.
- Se protegerá la integridad del servicio de asignación dinámica de direcciones (DHCP), en caso de que se utilice.

f) Monitoreo de la seguridad de red

- El área de Seguridad de la Información deberá, gestionar la realización de las auditorías de seguridad de la infraestructura tecnológica con base en el perfil de riesgo de la Cooperativa, por lo menos una vez al año, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que se brindan. Los procedimientos de auditoría deben ser ejecutados por personal independiente a la Cooperativa, capacitado y con experiencia, aplicando estándares vigentes y reconocidos a nivel internacional; estas auditorías deben incluir al menos pruebas de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación. La Dirección de TIC deberá definir y ejecutar planes de acción sobre las vulnerabilidades detectadas, derivadas de los informes entregados por el área de Seguridad de la Información.
- Se establecerán sistemas de detección/protección de intrusos de red (IDS/IPS de red) para registrar y monitorear los eventos de seguridad de la red. Estos sistemas deberán tener actualizadas las firmas de definición de ataques facilitadas por el fabricante.
- Los registros que producen estos eventos se analizarán periódicamente por parte de la Dirección de TIC, escalando los incidentes de seguridad al Área de Seguridad de la Información mediante los canales establecidos.

g) Redes inalámbricas

- La Dirección de TIC deberá implementar en las redes inalámbricas mecanismos de seguridad que garanticen un nivel de protección similar a las redes cableadas.
- Para alcanzar los mismos niveles de protección se deberán establecer al menos los siguientes mecanismos (considerando el análisis de riesgos pertinente):
  - Autenticación y control de acceso a la red (por ejemplo, 802.1x, filtrado de direcciones MAC, entre otros.).

- Sistema de detección de intrusos en redes inalámbricas para la detección de puntos de acceso no autorizados ("Rogue Access Point"), robos de sesión, falsificación de parámetros de red ("MAC spoofing"), robo de credenciales de autenticación, intentos de rotura de claves de sesión, barrido de frecuencias, denegación de servicio, alteración o retransmisión de paquetes, entre otros.).
- Cifrado de las comunicaciones (AES en WPA2, entre otros.).
- Reducción de la cobertura de la red, de forma que el alcance de esta quede limitado a la zona en la que se quiere dar acceso.
- Seguridad física del punto de acceso inalámbrico.

h) Renovación de cuentas de usuarios de VPN

- Las cuentas de usuario de VPN se deberán renovar su autorización mediante el formulario de creación hasta el 20 del mes de enero de cada año, de lo contrario las cuentas serán deshabilitadas.

5.22 Intercambios de información y software

5.22.1 Acuerdos de Intercambio de Información y Software

a) Se deberán establecer acuerdos formales, incluyendo los acuerdos de custodia de software cuando corresponda, para el intercambio de información y software (tanto electrónico como manual) con entidades externas. Las especificaciones de seguridad de los acuerdos de esta índole deberán reflejar el grado de sensibilidad de la información de negocio involucrada. La Dirección Jurídica emitirá el criterio jurídico sobre las condiciones de los acuerdos.

5.22.2 Seguridad del comercio electrónico

La Dirección de TIC deberá implementar controles que garanticen los siguientes lineamientos:

a) La información relativa a comercio electrónico será protegida según los controles definidos por los correspondientes análisis de riesgos, y de acuerdo con la legislación vigente.

b) Las transacciones on-line de comercio electrónico serán protegidas frente a las amenazas de transmisión incompleta, duplicación, pérdida, alteración o revelación no autorizada.

5.22.3 Sistemas de acceso público

a) Se deberán implementar los controles necesarios para garantizar la protección de la integridad de la información publicada electrónicamente por la Cooperativa de manera pública. Así mismo, se deberá garantizar que toda la información publicada cumpla con leyes y normativas correspondientes.

b) Todas las páginas web puestas en producción que permitan recolectar información clasificada como Restringida o Confidencial, así como el ingreso o despliegue de información personal de clientes y ejecución de transacciones que impliquen flujo de dinero deberán tener certificados digitales (https).

c) Previo a la publicación de nuevas funcionalidades en las páginas web de la Cooperativa o a la publicación de nuevas páginas, se deberá garantizar que el código no contenga vulnerabilidades.

d) Deberá existir un proceso de autorización formal por parte del negocio, antes de que la información se ponga a disposición del público.

5.23 Aprobación de sistemas

5.23.1 Aprobación del sistema

a) Para que un sistema sea puesto en producción deberá cumplir con los siguientes lineamientos:

- El cumplimiento de los requisitos de capacidad definidos durante la fase de diseño o por el proveedor del sistema.
- El cumplimiento de los requisitos de seguridad definidos en el requerimiento funcional.
- La entrega de documentación técnica y de usuario de los sistemas.
- La aceptación formal del área requirente del sistema.

5.23.2 Seguridad de la documentación del sistema

Se deben considerar controles para proteger la documentación del sistema de accesos no autorizados acorde a su nivel de clasificación, considerando también los criterios de disponibilidad e integridad de estos.

5.24 Desarrollo Seguro

5.24.1 Responsabilidades específicas de desarrollo seguro

5.24.1.1 Jefe de Desarrollo de Software

a) Planificar, desarrollar y ejecutar las actividades relacionadas con el desarrollo y actualización software. Además, debe planificar la ejecución de pruebas técnicas previo a su escalamiento al responsable de Control de Calidad.

b) Hacer cumplir el desarrollo de aplicativos con las leyes y regulaciones aplicables relacionadas con la privacidad de la información, la protección de datos personales y otros requisitos legales y regulatorios.

5.24.1.2 Responsable de Control de Calidad

a) Planificar y ejecutar las actividades relacionadas con las pruebas funcionales y de seguridad de los sistemas críticos nuevos o modificados antes de ejecutar la instalación en los servidores de producción.

5.24.1.3 Responsable de Control de Cambios

a) Instalar en entornos productivos los desarrollos y modificaciones realizadas por el área de Desarrollo de Software, cumpliendo con la normativa definida.

b) Estandarizar el ciclo de vida de desarrollo de software, criterios de seguridad y de calidad en el desarrollo de software.

c) Analizar y velar por el cumplimiento de las políticas y lineamientos de este manual durante todo el ciclo de vida de desarrollo de software.

d) Establecer una gestión de vulnerabilidades técnicas orientada a analizar los problemas de seguridad que surgen en los productos de software, que sean publicadas por los proveedores de tecnología y las agencias especializadas (CVE, OWASP) o detectados por cualquier usuario y proponer las medidas de mitigación al riesgo definido.

5.24.2 Generalidades

a) Toda modificación de software ya sea por actualizaciones, parametrizaciones o inclusión de nuevas funcionalidades, debe ser analizada previamente en ambientes independientes de desarrollo y prueba, con el objetivo de identificar y analizar los riesgos de seguridad que acarrea dicha modificación.

b) Se debe planificar detalladamente las etapas de paso a producción, incluyendo respaldos, recursos, conjunto de pruebas pre y pos - producción y los criterios de aceptación de estas.

c) Los desarrolladores ya sean internos o externos, no deben tener acceso a entornos productivos o información de producción que contenga datos sensibles.

d) Se debe establecer un acuerdo previo con los terceros, que resguarde la propiedad intelectual y asegure los niveles de confidencialidad de la información manejada en el ciclo de vida de desarrollo de software.

e) Los desarrollos ya sea internos y externos deben cumplir con lo definido en el *Anexo E Lista de Verificación de Requisitos de Seguridad para Desarrollo o Adquisición de Sistemas*, el cual incluye un resumen de todos los requisitos de seguridad detallados en este manual.

5.24.3 Protección de los datos de prueba del sistema

La Dirección de TIC deberá implementar las siguientes medidas para garantizar que los datos de prueba estén protegidos y controlados:

a) Deberá evitar el uso de bases de datos de producción que contengan información Confidencial en ambientes de pruebas o desarrollo. Si se utiliza información de esta índole, esta debe ser despersonalizada antes del uso. En el caso de información de ambiente de producción clasificada como Restringida o Confidencial contenida en ambientes de desarrollo y pruebas, ésta deberá ser enmascarada o codificada.

b) Los procedimientos de control de accesos, que se aplican a los sistemas en ambientes de producción, también deberán aplicarse a los sistemas en ambientes de pruebas.

c) Para ambientes de desarrollo no podrán utilizarse datos de producción o pruebas, sin la autorización expresa del dueño de la información y el conocimiento del área de Seguridad de la Información.

d) Se debe llevar a cabo una autorización por separado cada vez que se copie información de producción a un ambiente de pruebas o desarrollo.

5.24.4 Seguridad en las etapas del desarrollo (DevSecOps)

Para integrar la seguridad al desarrollo de las aplicaciones durante todo el proceso, la Dirección de TIC deberá considerar en la *Metodología de Desarrollo de Soluciones Tecnológicas* los lineamientos básicos que se detallan a continuación:

a) Implementar herramientas de análisis estático de código y análisis dinámico de seguridad para realizar pruebas de seguridad continuas en todo el proceso de desarrollo.
b) Implementar un control de versiones para garantizar la integridad y trazabilidad de código fuente.
c) Implementar controles de acceso basados en roles (RBAC) y autenticación multifactor (MFA) en todos los sistemas y servicios utilizados en el proceso de desarrollo.
d) Implementar procedimiento de escaneo periódico en todos los entornos de desarrollo con la finalidad de responder rápidamente a posibles incidentes de seguridad.
e) Realizar formación y concienciación en seguridad para todo el personal del equipo del área de Desarrollo de Software.

Adicional a los lineamientos detallados anteriormente el área de Desarrollo de Software deberá considerar en las diferentes etapas de desarrollo de software los siguientes lineamientos:

5.24.4.1 Levantamiento y definición de requerimientos

a) Como parte de la fase de levantamiento de requerimientos se debe contemplar la definición de requerimientos de seguridad activa y pasiva que permitan cumplir con lineamientos establecidos en este manual.
b) En el análisis de factibilidad de los requerimientos, se debe considerar el nivel de criticidad del sistema y el nivel de protección de seguridad que requieren los datos que en este se originen, almacenen o consulten.
c) Todos los requerimientos deben ser documentados y serán aceptados por el titular del activo, incluyendo su paso a producción.

5.24.4.2 Seguridad durante el diseño de los sistemas o funcionalidades

a) El nivel de confidencialidad de todos los elementos que componga el software debe ser definido teniendo en cuenta la criticidad de los datos manejados en el mismo.
b) Si se requiere el uso de cifrado de datos, este debe ceñirse a los lineamientos descritos en la sección de "**Controles Criptográficos**" del presente manual.
c) Si se utiliza un sistema gestor de bases de datos, se debe emplear las herramientas y mecanismos de seguridad necesarios para garantizar el nivel de protección adecuado.
d) Todos los programas deberán incluir la generación de registros de auditoría, considerando como mínimo la identidad del usuario que lee, borra, escribe, o actualiza, el tipo de evento y la fecha y hora del evento. Estos registros deben ser protegidos contra la manipulación no autorizada.
e) En la etapa de diseño se debe proyectar el rendimiento esperado, con el objetivo de no sobre dimensionar los recursos necesarios para el funcionamiento del sistema (ancho de banda, RAM, recursos del servidor, etc.).

5.24.4.3 Seguridad para el desarrollo y ejecución de pruebas

a) Todo cambio debe ceñirse a los lineamientos descritos en los procedimientos de control de cambios de acuerdo con el tipo de cambio.

b) Todo cambio debe ser expresamente aprobado por el titular del activo y debe contar con la documentación de soporte requerida en este manual.

c) Durante el desarrollo se debe contemplar el manejo de transacciones sensibles a fin de poder implementar parámetros adicionales de aprobación, verificación o tokens.

d) Las pruebas deben ser realizadas en forma automática, almacenando criterios y datos de pruebas en archivos de tal forma que se deje evidencia de su ejecución.

e) Los datos de entrada y salida de los sistemas de información estarán sujetos a las siguientes consideraciones:

- Se deben realizar las validaciones de datos de entrada y salida en un sistema confiable en entornos no productivos
- Construir los aplicativos para que validen los datos de entrada y generen los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas
- Los datos de entrada suministrados por los usuarios deben ser validaos y sanitizados antes de ser procesados, se considerarán aspectos como tipos de datos, rangos válidos y longitud, entre otros.
- Validar el intento de ingreso de bytes nulos, caracteres de nueva línea o caracteres de alteración de rutas.
- Se debe garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores personales de sesión o información de los usuarios. Los mensajes de error deben ser genéricos.
- No incluir las cadenas de conexión a las bases de datos en el código de los aplicativos.
- Se debe cerrar la conexión a las bases de datos desde los aplicativos, tan pronto como estas no sean requeridas.
- Remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.
- Prevenir la revelación de la estructura de directorios de los sistemas construidos.
- Se debe garantizar la protección del código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.
- No se debe permitir que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.
- Se debe utilizar funciones de control de integridad (hash) para verificar la integridad del código interpretado, bibliotecas, ejecutables y archivos de configuración previo a su utilización.

f) Se deberá considerar los siguientes lineamientos durante el desarrollo para la identificación y mitigación de vulnerabilidad, garantizando la seguridad de las aplicaciones:

- Los desarrolladores deben seguir las mejores prácticas de seguridad de la información durante el desarrollo y la codificación de aplicativos.
- Se deberá realizar la revisión de vulnerabilidades del código de software crítico, desde la etapa de desarrollo, para garantizar que las vulnerabilidades sean mitigadas previo a la puesta en producción.

- Se debe establecer un plan de actualización para el software que es desarrollado o utilizado en la Cooperativa, asegurando que las últimas versiones y parches sean instalados lo antes posible, con el fin de evitar que alguna vulnerabilidad sea explotada.

5.24.4.4 Seguridad para la implementación de sistemas

a) Se debe velar por la implementación de los controles de seguridad al mismo tiempo que la implementación de los componentes, funciones o módulos a los cuales controla.
b) Se debe efectuar el ajuste o alineamiento de los controles establecidos en la fase de diseño.
c) Las aplicaciones deben contar con un sistema de autenticación de usuario, que mínimo exija nombre de usuario y contraseña. Además, en los casos que la aplicación esté expuesta a internet, debe implementarse la validación de captcha.
d) Las aplicaciones deben contar con manejo de diferentes roles con permisos de acceso y operaciones asociados a estos.
e) Toda implementación debe tener procesos de roll back probados y definidos antes de la salida a producción.
f) Como parte de la implementación se generará un control de versiones el cual debe estar documentado y formar parte de los ítems de configuración asociados al cambio.

5.24.5 Seguridad en la documentación del software

a) El diccionario de datos o repositorio de metadatos debe mantener una descripción actualizada de las definiciones de datos.
b) Si el desarrollador incluye comentarios en el programa fuente, estos no deben divulgar información de configuración, lógica del aplicativo o cualquier otro dato que pueda llevar a vulnerar los controles o seguridades del sistema.
c) Todo sistema desarrollado por la Cooperativa debe cumplir con los lineamientos de controles de acceso establecidos en este manual.
d) La documentación de los desarrollos debe generarse a lo largo de cada una de las fases del ciclo de desarrollo de software y no dejarse hasta el final.
e) La documentación debe ser desarrollada por el personal del área de Desarrollo de Software y revisada por el titular del activo para su aceptación.
f) Se debe actualizar la documentación pertinente cada vez que exista un cambio en sus funcionalidades.
g) El almacenamiento y resguardo de la documentación de los cambios y desarrollos de software debe ser almacenada y protegida de acuerdo con los niveles de clasificación de cada documento y cumpliendo con los lineamientos establecidos en este manual.

5.24.6 Seguridad post implementación

a) Se debe revisar y auditar la existencia de los controles de seguridad definidos en la etapa de diseño.
b) Al menos una vez cada año, se debe realizar un escaneo de las aplicaciones críticas puestas en producción, en busca de vulnerabilidades, manteniendo un registro de los resultados y las acciones correctivas tomadas.

5.25 Gestión de proyectos

a) El análisis de los requisitos de seguridad de la información deberá alinearse a la *Metodología de Proyectos*, para garantizar que los riesgos sean identificados y tratados como parte del proyecto. Esto se aplica en general a cualquier proyecto independientemente de su carácter, por ejemplo, proyectos de procesos del negocio, proyectos de tecnología, de gestión de instalaciones, entre otros. La Gestión de Proyectos deben garantizar que:

- Se lleve a cabo una evaluación de los riesgos de seguridad de la información en una etapa temprana del proyecto, para identificar controles necesarios.
- La seguridad de la información forme parte de las fases de la metodología del proyecto.
- Las responsabilidades de seguridad de la información estén asignadas en roles específicos definidos en la *Metodología de Proyectos*.

5.26 Clasificación y tratamiento de información

5.26.1 Niveles de clasificación

La Cooperativa clasifica la información en los siguientes niveles:

5.26.1.1 Confidencial

a) Información de alta sensibilidad que debe ser protegida por su relevancia sobre decisiones estratégicas, impacto financiero, oportunidades de negocio, potencial de fraude o requisitos legales. Su divulgación deberá estar autorizada explícitamente por su titular.
b) Esta información es, pero no se limita a: claves de acceso a sistemas (socios/clientes y colaboradores internos), información de decisión del negocio, PAN (número principal de tarjeta), fecha de caducidad de la tarjeta, CVV2, información de productos nuevos, información de negocios nuevos.

5.26.1.2 Restringida

a) Información sensible, interna a áreas o proyectos a los que debe tener acceso controlado un grupo reducido de personas y no todo el personal de la institución, que debe ser protegida por su impacto en los intereses de la Cooperativa, de sus clientes y empleados.
b) En lo relativo a clientes, la divulgación o visualización no autorizada de esta información dentro de la Cooperativa podrá violar la privacidad de personas, violar las normas de sigilo y reserva de información bancaria.
a. Su divulgación deberá estar autorizada explícitamente por su titular.
b. Esta información es, pero no se limita a: depósitos y demás captaciones de cualquier naturaleza que reciba la Cooperativa por parte de sus socios/clientes, los datos de carácter personal de los socios/clientes de la Cooperativa, etc.

5.26.1.3 Interna

a) Información que, sin ser Confidencial ni Restringida, debe mantenerse en el ámbito interno de la Cooperativa y no debe estar disponible externamente, excepto a terceras partes involucradas previo compromiso de confidencialidad y conocimiento del titular de esta.
b) Esta información es, pero no se limita a: memos, avisos, comunicaciones, oficios, políticas, procedimientos, reglamentos.
c) Cualquier información no clasificada se tratará como de INTERNA, por lo que su divulgación deberá estar autorizada por su propietario.

5.26.1.4 Pública

a) Es la información que, por su naturaleza o por normativa externa, puede ser visible o divulgada por el personal general de la Cooperativa, socios/clientes o público en general, sin riesgo de que su contenido pueda afectar en ningún sentido la integridad, economía o reputación de la Cooperativa. Esta información es, pero no se limita a: publicaciones, anuncios de prensa o medios de comunicación, página web de la Cooperativa, etc.
b) Únicamente el Gerente puede decidir clasificar una información como PÚBLICA. En caso de requerirse su publicación en la página web, se debe solicitar la autorización a la Gerente, para posteriormente solicitarlo a la Jefatura de Marketing.

5.26.2 Clasificación y manejo

	CONFIDENCIAL	RESTRINGIDA	INTERNA	PUBLICA
Decisión clasificación / cambio / desclasificación y propietario de la información	Vocales del Consejo de Administración, Consejo de Vigilancia, Gerente, Subgerente, Director y Propietarios delegados explícitamente	Vocales del Consejo de Administración, Consejo de Vigilancia, Gerente, Subgerentes Directores, Jefes, homólogos y Propietarios delegados explícitamente	Colaboradores internos	Vocales del Consejo de Administración, Consejo de Vigilancia, Gerente, Subgerente, Directores, Jefes, homólogos y Propietarios delegados explícitamente
Permisos de acceso	Propietario y aquellos usuarios o grupos permitidos por éste.	Propietario y aquellos usuarios o grupos permitidos por éste.	Colaboradores	No aplica
Rotulado y manejo	En cualquier copia impresa de información confidencial se debe incluir la etiqueta: CONFIDENCIAL en cada hoja del documento. Cuando se extrae información, no dejar la información desatendida en ningún momento ni	En cualquier copia impresa de información restringida se debe incluir la etiqueta: RESTRINGIDO en cada hoja del documento. Cuando se extrae información, no dejar la	En cualquier copia impresa de información clasificada como Interna debe incluir la etiqueta: INTERNA en cada hoja del documento. No debe ser propagada a través de ningún	No aplica

	transportarla en el equipaje de mano, y asegurarse de que los compañeros de viaje no pueden acceder a ella. Se debe evitar dejar información confidencial o de carácter personal en los equipos multifunción de la Cooperativa (papeles en las fotocopiadoras e impresoras y documentos en formato electrónico en el escáner).	información desatendida en ningún momento ni transportarla en el equipaje de mano, y asegurarse de que los compañeros de viaje no pueden acceder a ella. Se debe evitar dejar información confidencial o de carácter personal en los equipos multifunción de la empresa (papeles en las fotocopiadoras e impresoras y documentos en formato electrónico en el escáner).	medio ni salir de la Cooperativa salvo necesidad justificada o autorización expresa de la misma.	
Normas de almacenamiento	Digital: cifrada. Impreso: bajo llave o cualquier otro mecanismo que garantice confidencialidad. Numerar copias y registrar al destinatario.	Digital: cifrada. Impreso: bajo llave o cualquier otro mecanismo que garantice confidencialidad.		
Distribución	A las personas autorizadas. Digital: cifrado. Impreso: mecanismo similar (sobre cerrado), entrega en mano y acuse de recibo.	A las personas autorizadas. Digital: cifrado. Impreso: mecanismo similar (sobre cerrado), entrega en mano y acuse de recibo.	Personal externo no lo puede reproducir o copiar sin justificación (debe estar sujeto a acuerdo de confidencialidad).	Directa a quien lo solicita o que la Cooperativa entregue mediante medios o canales oficiales
Destrucción	Según Políticas de borrado, limpieza y destrucción física			

5.26.3 Reasignación o baja de equipos

Tipo de información almacenada en el medio	¿Medio reutilizable?	¿Quedará fuera del control de la organización?	Proceso a ejecutar
Interna	No	Independientemente	Destrucción Física
Interna	Si	No	Borrado
Interna	Si	Si	Limpieza (formateo o borrado de registros)
Confidencial, Restringida	No	Independientemente	Destrucción Física
Confidencial, Restringida	Si	no	Limpieza
Confidencial, Restringida	Si	Si	Destrucción Física

5.26.4 Borrado, limpieza y destrucción física

Documentación impresa			
Tipo de medio	**Borrado**	**Limpieza**	**Destrucción Física**
Papel	Ver destrucción física	Ver destrucción física	Destruir el papel usando trituradores de corte transversal que producen partículas que son de superficie pedazo de material ≤ 320 mm2 (por ejemplo, pedazos 4 x 80 mm) o anchura de tira ≤ 2 mm. Longitud tira sin determinar. Referencia norma seguridad de nivel P-4 Norma DIN.

Dispositivos móviles			
Tipo de medio	**Borrado**	**Limpieza**	**Destrucción Física**
Celular	Elimine manualmente toda la Información, como las llamadas realizadas, mensajes de texto, números de teléfono, etc. A continuación, realizar un reseteo total del fabricante para reiniciar el teléfono celular a su configuración predeterminada de fabrica	Lo mismo que el borrado	Se podrá aplicar cualquiera de los siguientes procedimientos: - Triturar - Desintegrar - Pulverizar - Incinerar

Dispositivos de Red			
Tipo de medio	**Borrado**	**Limpieza**	**Destrucción Física**
Switch	Realice un reseteo total del equipo para devolverlo a la configuración predeterminada de fabrica	Lo mismo que el borrado	Se podrá aplicar cualquiera de los siguientes procedimientos: - Triturar - Desintegrar - Pulverizar - Incinerar

Equipamiento			
Tipo de medio	**Borrado**	**Limpieza**	**Destrucción Física**
Máquina de fax	Realice un reseteo total del equipo para devolverlo a la configuración predeterminada de fabrica	Lo mismo que el borrado	Se podrá aplicar cualquiera de los siguientes procedimientos: - Triturar - Desintegrar - Pulverizar - Incinerar
Notebook	Realice un reseteo total del equipo para devolverlo a la configuración	Lo mismo que el borrado	- Triturar - Desintegrar - Pulverizar - Incinerar

	predeterminada de fabrica Efectuar un formateo de bajo nivel de todas las particiones del disco duro del equipo.		- Desmagnetizar el disco (daño permanente del mismo) - Se permite el uso de herramientas de software aprobadas por norma PCI que garanticen la eliminación total de la información del disco duro del equipo
Pc escritorio	Realice un reseteo total del equipo para devolverlo a la configuración predeterminada de fabrica Efectuar un formateo de bajo nivel de todas las particiones del disco duro del equipo.	Lo mismo que el borrado	- Triturar - Desintegrar - Pulverizar - Incinerar - Desmagnetizar el disco duro (daño permanente del mismo) - Se permite el uso de herramientas de software aprobadas por norma PCI que garanticen la eliminación total de la información del disco duro del equipo
Tablet	Realice un reseteo total del equipo para devolverlo a la configuración predeterminada de fábrica. En caso de ser aplicable por el tipo de equipo, se tendrá que eliminar manualmente toda la Información, como las llamadas realizadas, mensajes de texto, números de teléfono, etc	Lo mismo que el borrado	- Triturar - Desintegrar - Pulverizar - Incinerar - Desmagnetizar el disco (daño permanente del mismo) - Se permite el uso de herramientas de software aprobadas por norma PCI que garanticen la eliminación total de la información del disco duro del equipo

Memorias			
Tipo de medio	**Borrado**	**Limpieza**	**Destrucción Física**
SD/ Flash Disk	Borrar la información contenida utilizando métodos validados de sobre escritura, por ejemplo mediante formateo a bajo nivel	Ver destrucción física	- Triturar - Desintegrar - Pulverizar - Incinerar - Desmagnetizar el disco (daño permanente del mismo)

Discos Ópticos			
Tipo de medio	**Borrado**	**Limpieza**	**Destrucción Física**
CD	Ver destrucción física	Ver destrucción física	- Seguir el siguiente orden de actividades: - Eliminar la información contenida en las etiquetas

			- Destruir usando equipos con nivel de seguridad O-3 Norma DIN
DVD	Ver destrucción física	Ver destrucción física	- Seguir el siguiente orden de actividades: - Eliminar la información contenida en las etiquetas - Destruir usando equipos con nivel de seguridad O-3 Norma DIN

5.26.5 Rotulado y etiquetado de información

Las siguientes normas deberán ser acatadas por todos los colaboradores que generen documentos en la Cooperativa:

a) Los documentos en formato digital y físico que se generen en la Cooperativa deben incluir en todas sus hojas una etiqueta en el encabezado o pie de página de acuerdo con el nivel de clasificación establecido.

b) En caso de clasificar documentos ya impresos, se deberán utilizar sellos con el rotulado equivalente, el mismo que debe constar en un lugar visible, en la parte superior o en la parte inferior derecha de cada hoja del documento.

c) La clasificación debe aparecer con el siguiente etiquetado, dependiendo del nivel de clasificación:

Clasificación	Rotulado (Utilizar Mayúsculas y Negrilla)
Información Confidencial	CONFIDENCIAL
Información Restringida	RESTRINGIDA
Información Interna	INTERNA
Información Pública	PÚBLICA (etiquetado opcional)

5.26.6 Normas de inventario de información restringida y confidencial

a) La Cooperativa deberá disponer de un inventario de la información Confidencial y Restringida de cada una de sus subgerencias, direcciones, con la designación de sus Titulares. El inventario deberá tener como mínimo los siguientes campos:

- Dirección: Nombre de la subgerencia y/o dirección
- Proceso: Nombre del proceso dentro de la dirección.
- Producto: Nombre del producto al cual soporta el proceso
- Activo de información: Nombre del activo de información
- Descripción: Descripción del activo de Información
- Clasificación en base a su confidencialidad, puede ser Confidencial o Restringido
- Disponibilidad: Requisito de disponibilidad del activo de Información, puede ser: Alta, Media o Baja
- Integridad: Requisito de integridad del activo de Información, puede ser: Alta, Media o Baja
- Titular: Nombre del titular del activo
- Cargo: Nombre del Cargo del titular del activo

- Formato: Formato en el que se encuentra el activo de información, puede ser Impreso o Digital
- Ubicación: Ubicación física o electrónica donde se encuentra almacenada la información.

b) Personal autorizado para su uso: En el caso de información Restringida, el registro o inventario de información clasificada deberá incluir los cargos, roles o funciones concretos que tienen acceso a la información. En el caso de información Confidencial, el registro puede incluir los nombres, cargos o grupos de trabajo o áreas que tienen autorización para acceder a la información

c) El responsable de mantener actualizado anualmente el inventario de activos de cada área será el director del área, quien podrá delegar esta función según considere pertinente.

d) En las auditorías anuales realizadas por el departamento de Seguridad de Información, se comprobará el cumplimiento de estas normas por parte de los responsables del cumplimiento del presente artículo.

5.27 Continuidad del negocio

Los procedimientos de Continuidad del Negocio deberán considerar todas las normativas citadas en el presente documento.

5.28 Cumplimiento de requisitos legales

5.28.1 Conformidad legal

a) La Cooperativa mediante la Dirección de TIC, implementará controles para garantizar el cumplimiento de las restricciones definidas en los acuerdos de licencias de uso, en lo referente a la utilización de software, productos y material protegido por derechos de propiedad intelectual.

b) De igual modo, el software o material producido por la Cooperativa susceptible de protección intelectual será registrado y protegido jurídicamente, la gestión de este proceso se la llevará a cabo en coordinación con la Dirección Jurídica.

c) Las áreas de negocio, a excepción del área de Seguridad de la Información, posterior a la adquisición y recepción de sistemas de información, tienen la obligación de hacer la entrega formal a la Dirección de TIC de:

- Manuales de instalación, configuración y de usuario.
- Software de Instalación.
- Códigos de activación de licencia.
- Acuerdos de licencias.

d) La Dirección de TIC para cumplimiento de este control, tendrán en cuenta los siguientes puntos:

- Se responsabilizará en mantener un inventario actualizado con el software que se utiliza dentro de la Cooperativa, en el que se indiquen el número de licencias totales, el número de licencias utilizadas, versión, soporte del fabricante, entre otros.
- Estará a cargo del control y custodia de las licencias compradas y entregadas por las diferentes áreas, así como de los manuales, los mismos

que deberán ser resguardados en sitios específicos que garanticen su disponibilidad e integridad, con acceso restringido solamente a personal autorizado.

- Administración de herramientas para gestión centralizada de software y licencias en los ordenadores de los usuarios.
- Implementación de controles que eviten que los usuarios puedan emplear e instalar software que no esté dentro del estándar o no se encuentre autorizado en la institución.
- Comprobaciones periódicas para verificar que sólo se instalan productos con licencia y software autorizado.

e) El área de Seguridad de la Información deberá mantener un inventario actualizado de licencias de las herramientas y servicios de seguridad, que permita verificar y controlar las licencias adquiridas de forma periódica.

5.28.2 Protección de datos y privacidad de la información personal

a) El tratamiento de información con datos de carácter personal cumplirá con los requisitos de la legislación y contratos aplicables, siendo necesaria la implementación de las medidas que correspondan.

5.28.3 Legislación sobre monitoreo del abuso de sistemas y redes

a) El monitoreo del uso que los usuarios hagan de los sistemas de información y redes de comunicaciones de la Cooperativa cumplirá con los requisitos de la legislación aplicable. En esta línea, se informará a los usuarios de la potestad de la institución para monitorear el uso de estos.

5.28.4 Legislación sobre criptografía

a) El uso de controles criptográficos cumplirá con los requisitos de la legislación aplicable.

5.29 Revisión de la Seguridad de la Información

5.29.1 Revisión independiente de la organización y estrategia de seguridad

a) El área de Auditoría Interna incluirá dentro de su plan anual de auditoría, la revisión de la organización y estrategia en seguridad de la información de la Cooperativa.

5.29.2 Revisión independiente del cumplimiento normativo

a) La Cooperativa se someterá y colaborará con las auditorías externas que las entidades de control dispongan.

b) El área de Auditoría Interna incluirá dentro de su plan anual de auditoría la revisión periódica de las áreas de la organización, con el objetivo de garantizar el cumplimiento de las normas y estándares de seguridad de la información, así como para evaluar los controles de seguridad implementados.

c) El alcance podrá considerar:

- Áreas.
- Procesos.

- Sistemas de información.

d) La revisión estará a cargo de personal competente en el ámbito de seguridad de la información ya sea interno o externo a la Cooperativa.

e) Los subgerentes, directores y/o jefes de las áreas y titulares de activos (sistemas de información) deberán apoyar y generar iniciativas para la revisión periódica de la conformidad de sus procesos y sistemas, respecto a los estándares y requisitos de seguridad de la información aplicables.

5.29.3 Métricas de Gestión de Seguridad de la Información

a) Las políticas de gobernanza de seguridad de la información deben ir acompañadas de métricas que permitan evaluar tanto la eficacia como el desempeño de los diferentes procesos y controles de seguridad implementados en la Cooperativa. Es importante revisar y ajustar estas métricas anualmente para garantizar que sigan siendo relevantes y útiles para la gestión de la seguridad de la información.

Estas métricas se encontrarán definidas en la *Matriz de Control de Indicadores* publicada en la intranet.

5.30 Acciones

a) El incumplimiento de estas políticas determinará la utilización por parte de la Cooperativa de las restricciones que considere oportuno en la utilización de los medios contemplados en este documento y la aplicación del régimen disciplinario, en su caso.

b) Cuando existan indicios de uso ilícito o abusivo por parte de un colaborador, la Cooperativa realizará las comprobaciones oportunas y, si fuera preciso, realizará una auditoría en la computadora del colaborador o en los sistemas que ofrecen el servicio, que se efectuará en horario laboral y en presencia de un representante del área de Talento Humano, con respeto a la dignidad e intimidad del colaborador.

6 Documentos de Referencia

- Ley Orgánica de Protección de Datos Personales
- ISO/IEC 27000, 27001, 27002 Seguridad de la Información
- ISO/IEC 27032:2012 Gestión de la Ciberseguridad
- PCI DSS
- PCI CP
- PCI PTS
- Resolución No. SEPS-IGT-IR-IGJ-2018-021
- Resolución No. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-IGJ-0116
- Resolución No. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-2023-270
- Resolución No. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-009
- Resolución No. SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002
- MAN.GJU.01 Manual de Gestión Jurídica
- MAN.GDE.02 Manual de Adquisiciones y Contrataciones

7 Normativa Interna

- PR.GIS.SI.01 Gestión de Activos de información
- PR.GIS.SI.02 Revisión de derechos de accesos
- PR.GIS.SI.03 Atención y Análisis de Incidentes de Seguridad de la Información
- PR.GIS.SI.04 Cifrado de datos críticos
- PR.GIS.SI.06 Control y monitoreo de seguridad de la información

8 Anexos

- Anexo A Dueños de la información – SharePoint documental
- Anexo B Titulares de Activos de sistemas de información – SharePoint documental
- Anexo C Metodología Evaluación y Valoración de Tipos y Activos de Información – SharePoint documental
- Anexo D Metodología de Evaluación de Riesgos Seguridad de la Información y Ciberseguridad –SharePoint documental
- Anexo E Lista de Verificación de Requisitos de Seguridad para Desarrollo o Adquisición de Sistemas –SharePoint documental

El **Manual de Gestión de Seguridad de la Información y Ciberseguridad,** reformado, ha sido conocido y aprobado por unanimidad por el Consejo de Administración de la Cooperativa de Ahorro y Crédito “29 de Octubre” Ltda., en sesión ordinaria celebrada el 12 de febrero de 2025, según el acta No. 004-2025, para constancia de lo cual suscribe:

PRESIDENTE	SECRETARIA
GRAL. HEGEL PEÑAHERRERA	**SRA. KARINA NAVAS**