# MANUAL DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

## 1. INTRODUCCIÓN

SU MOTO DEL CAUCA S.A. reconoce la información como uno de los activos fundamentales para el logro de los objetivos definidos por la compañía y la eficiente prestación de sus servicios, es así como existe un compromiso con la gestión de riesgos en la protección de los activos de información y la reducción del impacto en caso tal ocurra un incidente de seguridad de la información, por tal razón SU MOTO DEL CAUCA S.A. ha decidido implementar un Sistema de Gestión de Seguridad de la Información que contribuya a mantener la integridad, confidencialidad y disponibilidad de la información.

Con el propósito de cumplir con los estándares de seguridad de los sistemas de información y garantizar la confidencialidad de la información, SU MOTO DEL CAUCA S.A. ha definido y documentado las políticas, alcance y metodología de gestión del riesgo del SGSI,

Las políticas incluidas en el presente manual serán un instrumento para crear conciencia en los empleados de la importancia y sensibilidad de la protección de información y se constituirá en la base para la implementación de controles, estándares y procedimientos los cuales serán de obligatorio cumplimiento para todos los empleados, por lo tanto será responsabilidad de todos, velar porque se lleven a cabo las actividades que propenden a salvaguardar la integridad, confidencialidad y disponibilidad de la información.

## 2. OBJETIVO

Presentar una visión general del Sistema de Seguridad de Información de SU MOTO DEL CAUCA S.A. , los elementos y políticas que lo conforman, garantizando su conocimiento en toda la organización.

## 3. ALCANCE

Los lineamientos de seguridad de la información de la presente política serán aplicables en todas las áreas de la organización y serán de obligatorio cumplimiento para todos los empleados de SU MOTO DEL CAUCA S.A. y personal que directa o indirectamente prestan sus servicios profesionales dentro de la empresa, utilicen y tengan acceso a los recursos de información.

## 4. REQUISITOS LEGALES APLICABLES AL SECTOR

- Ley 527 de 1999 - Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.
- Ley 1273 de 2009 - “De la Protección de la información y de los datos”

## 5. ELEMENTOS DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

MANUAL DE SEGURIDAD: Inspira y dirige todo el sistema, determina intenciones, alcance, objetivos, políticas y responsabilidades del SGSI

PROCEDIMIENTOS: Documentos en el nivel operativo, estos aseguran la planificación y operación de las actividades de seguridad de la información.

INSTRUCTIVOS: Documentos que describen como se realizan las actividades relacionadas con las seguridad de la información.

REGISTROS: Documentos que proporcionan evidencia objetiva del cumplimiento de los requisitos del SGSI.

6. DEFINICIONES

- Sistema de Gestión de Seguridad de la Información: Conjunto de elementos tales como políticas, procedimientos, documentación, estructura de organización, planificación de actividades, responsabilidades, procesos mediante el cual se establece, opera, monitorea, revisa, mantiene y mejora la seguridad de la información.
- Manual de Sistema de Gestión de Seguridad de la Información: Documento que expone y determina el alcance, objetivos, responsabilidades, políticas y directrices principales del SGSI.
- SEGURIDAD DE LA INFORMACIÓN: La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo de la operación normal de la compañía.
- ACTIVOS DE INFORMACIÓN: Todos aquellos recursos de valor para una empresa que generan, procesan, almacenan o transmiten información.
- PROPIETARIO DEL ACTIVO: Corresponde a una parte designada de la empresa, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad del activo, quiénes tienen acceso y pueden modificar, leer, procesar la información.
- CONFIDENCIALIDAD: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- INTEGRIDAD: Mantener la información libre de alteraciones, manipulaciones durante el proceso de difusión.
- DISPONIBILIDAD: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran
- INCIDENTE DE SEGURIDAD: Un incidente de seguridad es un evento adverso que haya vulnerado la seguridad de la información o que intente vulnerarla, y que puede comprometer o compromete la confidencialidad, integridad y/o disponibilidad de la información.
- COMITÉ DE SEGURIDAD DE LA INFORMACIÓN: Es un cuerpo integrado por representantes de diversas áreas de la compañía. El objetivo principal de este comité es el análisis de los temas concernientes a la seguridad de la información de la compañía y la toma decisiones en cuanto a seguridad se refiere. A su vez el comité, es el encargado de revisar y aprobar las políticas, normas y responsabilidades de seguridad como también regular cualquier cambio del Sistema de Seguridad siempre apuntando a la mejora continua.
- ACUERDO DE CONFIDENCIALIDAD: Es un documento en los que los empleados o terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la compañía, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso.
- CRIPTOGRAFÍA: Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles y asegurar su confidencialidad. El cifrado es una técnica útil para prevenir la fuga de información, el monitoreo no autorizado y el acceso no autorizado a información.
- SOFTWARE MALICIOSO: Software o programa de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.
- COPIA DE SEGURIDAD: Duplicado de la información contenida en la plataforma tecnológica, con el objeto de salvaguardarla en caso que ocurriese algún problema que impidiese acceder a los originales o su defecto perderlos.

- DESAFECTACIÓN DE LOS EQUIPOS: Es el proceso de destrucción y sobrescritura de la información, producto de afecciones en los medios de almacenamientos.

## 7. DIRECCIONAMIENTO DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN.

### 7.1 Política General

SU MOTO DEL CAUCA S.A. dispondrá de un Sistema de Seguridad de la Información orientado a identificar, analizar y minimizar los riesgos a los cuales se encuentran expuestos los activos de información, asegurando la protección y correcto manejo de los datos e información de la compañía dentro de los sistemas de cómputo, archivos y documentación, así como el cumplimiento de los requerimientos legales y normativa vigente. Será compromiso de todos los empleados adoptar las directrices del presente manual con el fin de preservar la confidencialidad, disponibilidad e integridad de la información.

### 7.2 objetivos de seguridad de la información

- Mantener procesos, procedimientos y controles que conduzcan a la gestión adecuada de los activos de información y sistemas informáticos de SU MOTO DEL CAUCA S.A.
- Garantizar la protección de los activos de información contra eventos internos o externos que representen riesgo.
- Cumplir con la legislación y normatividad vigente que aplica en SU MOTO DEL CAUCA S.A. para la prevención y gestión adecuada de Seguridad de la Información.
- Promover una cultura de seguridad de la información en SU MOTO DEL CAUCA S.A. donde se garantice una eficiente gestión, para la minimización de los riesgos a los cuales se expone la confidencialidad, integridad y disponibilidad de los activos de información

## 8. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

### 8.1 Compromiso de la Gerencia

- Definir y establecer los roles y responsabilidades relacionados con la seguridad de la información.
- Revisar y aprobar las Políticas de Seguridad de la Información contenidas en el presente manual.
- Facilitar la divulgación de las Políticas de Seguridad de la Información a todos los funcionarios de la entidad y al personal provisto por terceras partes.
- Asignar los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad de la información de la organización.
- Coordinar la creación del Comité de Seguridad de la Información.

### 8.2 Comité de Seguridad de la Información

- Revisar periódicamente el estado general de la seguridad de la información.

- Proponer modificaciones o nuevas políticas de seguridad de la información.
- Apoyo, revisión y regulación de los temas referentes a la seguridad de la información.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información en la organización.
- Monitorear los incidentes de seguridad de la información.
- Velar por el cumplimiento de las Políticas de la Seguridad de la Información expuestas en el presente manual.

### 8.3 Propietarios de Activos de Información

- Definir la clasificación de la información.
- Determinar los niveles de acceso a la información.
- Autorizar la asignación de permisos de acceso.
- Apoyar en la generación de los controles necesarios para el almacenamiento, procesamiento, distribución y uso de la información.
-

### 8.4 Coordinador de Seguridad de la Información

La Dirección designa como Coordinador de Seguridad de la Información al SU MOTO DEL CAUCA S.A. quien se encargará de:

- Determinar los niveles de acceso a la información.
- Coordinar las acciones del Comité de Seguridad e impulsar la implementación y cumplimiento de la presente Política.
- Brindar Seguridad de los sistemas de información.
- Documentar y mantener actualizada la información, y definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones, perfiles y competencias.
- Regular cambios y mejoras al sistema en cuanto a: objetivos, adecuación del alcance y política.

### 8.5 Empleados, contratistas, proveedores

Todos los empleados de SU MOTO DEL CAUCA S.A. y personal que directa o indirectamente prestan sus servicios profesionales dentro de la empresa son responsables de la información que manejan y deberán cumplir los lineamientos establecidos para proteger y preservar la información a la cual accedan y procesen; evitando el uso indebido, accesos no autorizados, exposiciones, modificaciones y entrega a externos.
Todo funcionario que utilice la infraestructura tecnológica de SU MOTO DEL CAUCA S.A. tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está clasificada como confidencial y/o crítica; así mismo reportar los incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.

## 9. GESTIÓN DE ACTIVOS.

9.1 Clasificación de Activos

Los propietarios de la información y el Coordinador de Seguridad de la Información serán los encargados de clasificar los activos de información de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.

9.2 Inventario de Activos.

SU MOTO DEL CAUCA S.A. contará con un inventario de activos identificados y clasificados, donde define su nivel de sensibilidad, criticidad y medidas de tratamiento de acuerdo a su clasificación con el objeto de garantizar que reciban el nivel apropiado de protección.

10. SEGURIDAD DE LOS RECURSOS HUMANOS

10.1 Términos y condiciones de contratación

El jefe de gestión humana incluirá las funciones referentes a la seguridad de la información en las descripciones de las funciones de cada uno de los empelados e informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información.

10.2 Compromisos de Confidencialidad

Todos los empleados de SU MOTO DEL CAUCA S.A. , contratista y proveedores, que realicen labores en la organización y que involucre el manejo de información, deben conocer, entender, firmar y aceptar el correspondiente acuerdo de confidencialidad, donde se comprometan a no divulgar, usar o explotar la información confidencial de SU MOTO DEL CAUCA S.A. y proteger y hacer buen uso de la misma, respetando los niveles de clasificación en cuanto a criticidad y protección, por consecuente cualquier violación de lo establecido será considerado un incidente de seguridad y tendrá su sanción dependiendo la magnitud de los hechos: Llamado de atención con suspensión sin remuneración o acta de descargos.

10.3 Capacitación en seguridad de la información

Todos los empleados recibirán una adecuada capacitación y actualización periódica en materia de las políticas y procedimientos relativas a la seguridad de la información. Esto comprende los requerimientos de seguridad, las responsabilidades legales y el uso correcto de las instalaciones y de la información a su cargo.

10.4 Comunicación de incidentes

Se establecerá un procedimiento para el reporte de incidentes relativos a la seguridad de la información; el procedimiento deberá establecer que todo el personal de SU MOTO DEL CAUCA S.A. empleados y/o proveedores o contratistas, deben reportar cualquier incidente al Coordinador de Seguridad de la Información inmediatamente este se detecte o se posea algún tipo de sospecha.

10.5 Desvinculación de personal

Se establecerá un procedimiento de desvinculación de personal o cambio de labores de empleados, donde se estipulen las actividades que se deberán ejecutar previo al retiro de alguno de los empleados.

El jefe de Gestión Humana deberá reportar al Coordinador de Seguridad de la Información la desvinculación o modificación del cargo con el fin de realizar las actividades de: Devolución de activos, deshabilitación de equipos de la red, deshabilitación de usuario de correo y usuario de SU

MOTO DEL CAUCA S.A. . La vigencia de los derechos de acceso y su revocatoria, debe estar estrechamente relacionados con la terminación de la relación laboral.

## 11. SEGURIDAD FÍSICA Y AMBIENTAL

### 11.1 Perímetro de seguridad física.

SU MOTO DEL CAUCA S.A. velará por la efectividad de los mecanismos de protección física que aseguren el perímetro y control de acceso a todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas áreas en donde se encuentren los equipos e infraestructura de los sistemas de información de la organización, considerándose áreas de acceso restringido.

### 11.2 Control de acceso físico

SU MOTO DEL CAUCA S.A. contará con los mecanismos de control de acceso adecuados para garantizar que se le permita el acceso únicamente a personal autorizado, tales como vigilancia privada, identificación de visitantes, sistema de alarmas, etc. en los sitios donde existan sistemas de información, equipos de cómputo y comunicaciones considerados críticos por la entidad deben contar mínimo con seguridad de acceso con guardia 7x24x365, sistemas de detección y extinción de incendio, circuito cerrado de televisión con cámaras, redundancia de recursos y alta disponibilidad N+1.

### 11.3 Seguridad de oficinas e instalaciones

Los visitantes de las oficinas de SU MOTO DEL CAUCA S.A. deben ser escoltados durante todo el tiempo por un funcionario autorizado. Esto significa que se requiere de un escolta tan pronto como un visitante entra a un área y hasta que este mismo visitante sale del área controlada. Todos los visitantes requieren una escolta incluyendo clientes, antiguos empleados, miembros de la familia del funcionario.

Los centros de cómputo o áreas de la organización consideradas críticas, deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá registrar el motivo del ingreso y estar acompañada permanentemente de un funcionario de SU MOTO DEL CAUCA S.A. . En los centros de cómputo o áreas que SU MOTO DEL CAUCA S.A. considere críticas deberán existir elementos de control de incendio, inundación, alarmas y estar demarcados como zona restringida. Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso.

### 11.4 Seguridad de los equipos

#### 11.4.1 Ubicación de los equipos

Los equipos de cómputo (computadores, servidores, impresoras, equipos de comunicación, entre otros) no deben moverse o reubicarse sin la aprobación previa del Coordinador de Seguridad de la Información.

Los equipos de cómputo deberán estar situados y protegidos con el fin de reducir los riesgos de las amenazas ambientales y los riesgos y las oportunidades de acceso no autorizado.

Los servidores de SU MOTO DEL CAUCA S.A. se encontraran salvaguardados en otro país bajo estrictos controles de acceso tanto en el lugar, como al espacio donde se encuentran estos.

#### 11.4.2 Suministros de energía

Las protecciones de los equipos frente a las insuficiencias de la energía eléctrica se hacen a través de ups, para computadores y teléfonos.
Los empleados se comprometen a NO utilizar la red regulada de energía (tomacorrientes naranja o UPS) para conectar equipos eléctricos diferentes a su computador, como impresoras, cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras y en general cualquier equipo que implique una mayor carga sobre esa red.

### 11.4.3 Mantenimiento de equipos

Cualquier cambio que se requiera realizar en los equipos de cómputo de la empresa (cambios de procesador, monitor, teclado, mouse, adición de memoria o tarjetas) debe tener previamente una evaluación técnica del área de sistemas, el Auxiliar de Mantenimientos y la autorización del Coordinador del Sistema de Seguridad de la Información o el responsable de los inventarios para la actualización de seriales, responsables y hojas de vida de los equipos.
La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal autorizado, previa autorización del área de sistemas, Auxiliar de Mantenimientos o Coordinador de Seguridad de la Información. Periódicamente se ejecutarán mantenimientos preventivos a los equipos de cómputo para asegurar su continua disponibilidad e integridad y óptimo funcionamiento.

### 11.5 Escritorios y pantallas limpias

Sobre los escritorios u oficinas abiertas y durante la ausencia de los empleados de SU MOTO DEL CAUCA S.A. no deben permanecer a la vista documentos en papel, dispositivos de almacenamiento como cd, memorias USB, con el fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

## 12. CONTROL DE ACCESOS

### 12.1 Control de acceso a redes

SU MOTO DEL CAUCA S.A. contará con dos redes una para el personal administrativo y otra para el personal comercial. El Coordinador de Seguridad de la Información definirá controles para garantizar la seguridad de los datos y los servicios conectados a la redes de la compañía, contra el acceso no autorizad y evitar la afectación de los equipos a través de redes.

### 12.2 Gestión de acceso de usuario

Se realizará un procedimiento de registro y anulación de usuario para permitir la asignación de derechos de acceso. La creación y eliminación de un identificador de usuario debe ser realizada inmediatamente el empleado haya ingresado o finalizado su relación con la compañía. Los sistemas operacionales, bases de datos y aplicativos deberán contar con roles predefinidos o con un módulo que permita definir roles o administrar usuarios, delimitando las acciones permitidas por cada uno de estos de acuerdo con la función y cargo de los usuarios que acceden a él. El Coordinador de Seguridad de la Información o Jefe Inmediato autorizará el acceso a los empleados

y contratistas que laboran para pero solo a la información necesaria para el desarrollo de sus actividades.
Las claves de acceso compartidas asignadas a los funcionarios de los sistemas información de SU MOTO DEL CAUCA S.A. tendrán únicamente carácter de consulta, estas no deben permitir modificación de la información, no deben divulgarse hacia el exterior de la entidad, se cambiarán anualmente o cuando se requiera y exclusivamente se utilizarán para la gestión de la compañía, por ejemplo la clave de acceso de Intranet de SU MOTO DEL CAUCA S.A.

### 12.3 Control de acceso a sistemas y aplicaciones

El personal comercial de SU MOTO DEL CAUCA S.A. contará con restricciones para el acceso al software al utilizar equipos móviles (portátiles, tabletas) en áreas externas a la compañía, para esto es necesario un certificado de validación externa. El certificado tendrá validez de 30 días y se deberá pedir autorización de certificar el equipo nuevamente a través de la plataforma de soporte del sistema.

### 12.4 Administración de Contraseñas.

El control de acceso a todos los sistemas de información de SU MOTO DEL CAUCA S.A. se hace por medio de códigos de identificación y palabras claves o contraseñas únicas para cada usuario, y frecuencia de cambio de 60 días.
Las contraseñas o claves de acceso a los recursos informáticos asignados a los funcionarios son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.

## 13. GESTIÓN DE COMUNICACIONES Y OPERACIONES.

### 13.1 Documentación de procedimientos.

Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta política y sus cambios serán autorizados por el Coordinador de Seguridad de la Información.

### 13.2 Gestión de Cambios

Las modificaciones o adiciones en las funcionalidades del sistema deberán seguir el procedimiento establecido para ello; el Coordinador de Seguridad de la Información, establecerá, coordinará y controlará los cambios realizados a la plataforma tecnológica, asegurándose de su debida autorización por el área correspondiente, este debe garantizar que todo cambio realizado que conlleve a una modificación de acceso, parámetros o del software, están soportadas por solicitudes realizadas por los usuarios y se mantendrán los niveles de seguridad y protección necesarios.

### 13.3 Manejo de incidentes.

Se asignaran funciones y se establecerán procedimientos para el manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad.
Cualquier brecha en la seguridad o sospecha en la mala utilización en el Internet, la red corporativa o Intranet, o los recursos informáticos de cualquier nivel (local o institucional) debe ser comunicada por el empleado que la detecta en forma inmediata y confidencial al Coordinador de Seguridad de la Información.

Los empleados y contratistas que realicen las labores de administración de la plataforma tecnológica son responsables de la implementación y permanencia de los controles sobre los recursos tecnológicos.
Las violaciones a las políticas y controles de seguridad de la información serán reportadas, registradas y monitoreadas por el Coordinador de Seguridad de la Información.

### 13.4 Protección contra software malicioso

SU MOTO DEL CAUCA S.A. proveerá los mecanismos necesarios para garantizar la protección de la información contenida en la plataforma tecnológica, a través de controles para evitar la divulgación, modificación o daño ocasionados por un software malicioso. Tales controles se realizaran a través de un antivirus en los equipos y firewall IP en las redes, que reduzca el riesgo de contagio de software malicioso y garantice la seguridad de la información de la plataforma tecnológica de elementos de entrada y de salida en la misma.
SU MOTO DEL CAUCA S.A. deberá asegurar que el software de antivirus, cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica; el Auxiliar de Mantenimientos será el sujeto responsable de realizar tareas de escaneo de virus. Ningún empleado podrá modificar la configuración establecida para el software antivirus.

### 13.5 Desafectación de los equipos.

La información puede verse comprometida por la utilización inadecuada de los equipos. Los medios de almacenamiento afectados y que contienen material sensible, serán destruidos o sobrescritos de forma segura.

### 13.6 Copia de seguridad.

Toda la información contenida en los equipos de cómputo, estarán adheridos al Drive de Google, permitiendo automatizar la protección de la información en la nube de la compañía y a su vez serán sincronizados automáticamente. El Propietario de la Información, será el responsable del almacenamiento la información que cada uno maneja en sus equipos en el archivo de Google Drive.

### 13.7 Intercambios de información

El intercambio electrónico de información, grupos de charla y utilidades será utilizado únicamente para el ejercicio de las funciones de competencia de cada funcionario y de las actividades de. SU MOTO DEL CAUCA S.A. .
Se implementarán controles para reducir los riesgos de incidentes de seguridad en el correo electrónico, contemplando que:

- Los funcionarios de SU MOTO DEL CAUCA S.A. . no deberán utilizar versiones escaneadas de firmas personales para dar la impresión de que un mensaje de correo electrónico o cualquier otro tipo de comunicación electrónica hayan sido firmados por la persona que la envía.

- La propiedad intelectual desarrollada o concebida mientras el funcionario se encuentre en el sitio de trabajo, es propiedad exclusiva de SU MOTO DEL CAUCA S.A. . Esta política incluye patentes, derechos de reproducción, marca registrada y otros derechos de propiedad intelectual según lo manifestado en memorandos, planes, estrategias, productos, software, códigos fuentes, documentación y otros materiales.

### 13.8 Seguridad en comunicaciones

Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de, SU MOTO DEL CAUCA S.A. . deberán ser consideradas y tratadas como información confidencial.
Todas las conexiones a redes externas tiempo real que accedan a la red interna de la compañía, debe pasar a través de un cortafuegos, denominado sistema de defensa electrónica que incluyen servicios de cifrado y verificación de datos, detección de ataques cibernéticos, detección de intentos de intrusión, administración de permisos de circulación y autenticación de usuarios.
Todo intercambio electrónico de información o interacción entre sistemas de información con entidades externas deberá estar soportado con un documento de formalización.

### 13.9 Auditorias de sistemas de información.

SU MOTO DEL CAUCA S.A. contará con un software transaccional en donde todos los sistemas automáticos que operen y administren información sensitiva, valiosa o crítica para la compañía como son los aplicativos en producción, sistemas operativos, sistemas de bases de datos y telecomunicaciones generan un libro con la bitácora de auditoría de la tareas principales (adición, modificación, borrado).

- El libro de bitácora de auditoría proporcionará suficiente información de las actividades de los usuarios para facilitar el monitoreo y control.
- Los archivos de auditoría serán custodiados en forma segura para que no puedan ser modificados y para que puedan ser leídos únicamente por personas autorizadas; los usuarios que no estén autorizados deben solicitarlos al área encargada de su administración y custodia, que será el Coordinador de Seguridad de la Información.
- Todos los computadores de Finsocial estarán sincronizados con la fecha y hora exacta para que el registro en la auditoría sea correcto.

## 14. DESARROLLO Y MANTENIMIENTO DEL SISTEMA DE INFORMACIÓN

### 14.1 Desarrollo de Software

El Coordinador de Seguridad de la Información, junto con su equipo de trabajo serán los responsables de recepcionar, coordinar y controlar las solicitudes de mejora o cambios requeridos para la plataforma tecnológica, tanto en el software operativo, como los sistemas de información de SU MOTO DEL CAUCA S.A.
Los requerimientos de mejora o modificaciones al software operativo los realizaran los usuarios del sistema, a través del aplicativo de soporte del mismo software y deberán estar autorizados por el área correspondiente.
Los ambientes de desarrollo de sistemas, pruebas y producción deberán permanecer separados para su adecuada administración, operación, control y seguridad; y en cada uno de ellos se instalarán las herramientas necesarias para su administración y operación.

### 14.2 Controles criptográficos

SU MOTO DEL CAUCA S.A. posee técnicas criptográficas para la protección de la información con el fin de asegurar una adecuada protección de su confidencialidad e integridad.
Las técnicas de controles criptográficos para los casos de:
1. Protección de claves de acceso a sistemas, datos y servicios.
2. Generación de certificados de validación externa para acceso al software.

### 14.3 Instalación de Software

Todo software que utilice SU MOTO DEL CAUCA S.A. Será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la organización.
Debe existir una cultura informática al interior de la organización que garantice el conocimiento por parte de los empleados y contratistas de las implicaciones que tiene el instalar software ilegal en los computadores de SU MOTO DEL CAUCA S.A.

## 15. GESTIÓN DE INCIDENTES

Se establecerán funciones y procedimientos para el manejo de incidentes con el objeto de garantizar una respuesta rápida, eficaz y sistemática a los incidentes relativos a la seguridad de la información; este procedimiento determinará las acciones de comunicación, tratamiento y respuesta a los incidentes.
Los incidentes relativos a la seguridad de la información serán comunicados al Coordinador de Seguridad de la Información inmediatamente sean detectados y este mismo será responsable de dar respuesta e indicar los recursos necesarios para la investigación y resolución del incidente; además se encargará del monitoreo.

## 16. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

Con el fin de contrarrestar las interrupciones para el normal desarrollo de las actividades del negocio y proteger sus procesos críticos de fallas en los sistemas de información o desastres asegurando la pronta y oportuna recuperación, Finsocial establecerá, documentará, implementará y mantendrá un Plan de Contingencia del Negocio, donde:

- Determinará las actividades para la identificación de riesgos y siniestros a los cuales se halla sujeta la seguridad de la información y puedan ocasionar interrupciones en el desarrollo de las actividades.
- Considerará el análisis de riesgo, de prevención de emergencia, de respaldo y recuperación ante la ocurrencia de un desastre o evento; la metodología para evaluación de los riesgos y el impacto; además de la magnitud de daño como del período de recuperación.

El área de Sistemas de con apoyo del Coordinador de Seguridad de la Información serán los responsables de actualizar periódicamente y probar anualmente el plan de contingencia que permita a las aplicaciones críticas y sistemas de cómputo y comunicación estar disponibles en el evento de un desastre de grandes proporciones como terremoto, explosión, terrorismo, inundación etc.
Las crisis suelen provocar "reacciones de pánico" que pueden ser contraproducentes y a veces incluso más dañinas que las provocadas por el incidente que las causo; por ello en el presente documento se establece claramente las responsabilidades y funciones del personal, así como los protocolos de acción correspondientes.

## 17. BUENAS PRÁCTICAS PARA USO DE INTERNET

Los virus informáticos son una de los principales riesgos de seguridad para los sistemas, por tal razón se deben tomar las siguientes precauciones de seguridad sobre la utilización de Internet:

1. No utilizar canales de chat o grupos sociales como Facebook, Messenger, etc., en horario laboral con fines personales sin previa autorización de SU MOTO DEL CAUCA S.A. __

2. No descargar de Internet, ni alojar en los discos duros de los equipos de cómputo, música, videos, ni cualquier tipo de software sin licenciamiento.

3. No abrir ningún mensaje, sitio web, ni archivo de fuente desconocida o muy poco conocidas. En caso de personas conocidas, se deben tomar precauciones, asegurándose de que esa persona es la responsable del envío y ante cualquier duda, borrar el mensaje, para evitar la contaminación de un virus.

4. Todos los funcionarios SU MOTO DEL CAUCA S.A. , tienen la obligación a dar cumplimiento a la Ley 679 de 2001, acatando las prohibiciones que le han sido impuestas. Por consiguiente se obligan a no utilizar los servicios, redes y sistemas de Finsocial que impliquen directa o indirectamente, bajar o consultar información de actividades sexuales y/o material pornográfico.

5. Los spam o correos basura son los mensajes no deseados que hacen referencia a publicidad pudiendo además contener virus; estos mensajes deben eliminarse sin ser leídos para evitar el aumento de la cantidad del correo basura en el buzón, así como la posibilidad de intrusión de virus en el sistema.

6. Usar regularmente un programa antivirus y verificar periódicamente su actualización, el área de sistemas presta el soporte que se requiera para tal fin.

7. No bajar nada de sitios web de los que no se tenga referencias de seriedad, o que no sean medianamente conocidos. Si se bajan archivos, copiarlos a una carpeta y revisarlos con un antivirus actualizado antes de abrirlos.

8. No utilizar la cuenta de correo electrónico suministrada por SU MOTO DEL CAUCA S.A. , para asuntos personales.

9. Activar las actualizaciones automáticas (Windows y Office), las cuales pueden proteger los equipos de ataques de virus proveniente de Internet.