MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

SEPTIEMBRE DE 2019

GESTIÓN DE SEGURIDAD ELECTRÓNICA

Contenido

1. INTRODUCCIÓN

Gestión de Seguridad Electrónica, establece que la información es un activo fundamental para el desarrollo de las actividades de la organización, en razón a que es una herramienta de gran importancia para la toma de decisiones, motivo por el cual, Gestión de Seguridad Electrónica está comprometida a proteger los activos de información de la entidad (Empleados, información y entorno laboral), orientando sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad, a la continuidad de las operaciones de la organización, la administración y/o gestión de riesgos, la creación de cultura y conciencia de seguridad en los empleados, contratistas, proveedores y personas que hagan uso de los activos de información de Gestión de Seguridad Electrónica.

2. OBJETIVOS

Describir las pautas, directrices y reglas implementadas para generar una adecuada seguridad y protección de la información de los procesos de Gestión de Seguridad Electrónica.
Informar a empleados, contratistas, proveedores las normas y mecanismos que deben cumplir en las interacciones con los activos de información de Gestión de Seguridad Electrónica, y establecer el alcance de las responsabilidades que compromete en la gestión a cada uno de ellos.

3. ALCANCE

Las Políticas de seguridad de la Información están orientadas al cumplimiento de la confidencialidad, integridad y disponibilidad relacionadas con cualquier activo de información, que conllevan a implementar procedimientos y controles que deben ser cumplidos por los empleados, contratistas, proveedores, que laboren o tengan relación con Gestión de Seguridad Electrónica.
Gestión de Seguridad Electrónica socializa y exige cumplimiento de las políticas y procedimientos asociados al sistema de seguridad de la información a empleados, contratistas, proveedores.

4. REQUISITOS LEGALES Y/O REGLAMENTARIOS

Con el objeto de mitigar los riesgos relacionados con la confidencialidad, integridad y disponibilidad de la información, se tiene que cualquier incidente que viole el marco normativo legal vigente en Colombia, en materia de políticas de seguridad de la Información estará sujeto, entre otras, a lo establecido en las siguientes disposiciones legales:

Marco normativo de buenas prácticas para el tratamiento de la información: Ley 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales, Decreto Reglamentario 1377 de 2013, Ley 1098 de 2006 “Código de Infancia y Adolescencia”, 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, y se dictan otras disposiciones. Las recomendaciones y buenas prácticas de los estándares adoptadas por el ICONTEC NTC/ISO 27001 y NTC/ISO 27002.

Marco Normativo Sancionatorio: Ley 734 de 2002 por la cual se expide el Código Disciplinario único. Ley 1273 de enero 5 de 2009, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información.

5. TÉRMINOS Y DEFINICIONES

Se definen a continuación los siguientes términos técnicos:

Activo: Recurso del sistema de información o cualquier elemento que tenga valor para la organización.
Activo de Información: Todo aquel elemento lógico o físico que conforme cualquiera de los sistemas de información de la institución. Ej. Bases de datos, sistemas operacionales, redes, sistemas de información y comunicaciones, documentos impresos, fichas, formularios y recursos humanos
Administrador del Sistema: Persona responsable de administrar, controlar, supervisar y garantizar la operatividad y funcionalidad de los sistemas. Dicha administración está dirigida por la Gerencia de informática y se realizará por conducto de las Coordinaciones de la misma.

Administrador de Correo: Persona responsable de solucionar problemas en el correo electrónico, responder preguntas a los usuarios y otros asuntos en un servidor.
Análisis de riesgos: Proceso sistemático que permite identificar y determinar el impacto o grado de vulnerabilidad de los activos de la organización.
Ataque Cibernético: Intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado, por lo general con intenciones insanas y perjudiciales.
Brecha de Seguridad: deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal.
Buzón: También conocido como cuenta de correo, es un espacio exclusivo, asignado en el servicio de correo, para almacenar los mensajes y archivos adjuntos enviados por otros usuarios internos o externos a Gestión de Seguridad Electrónica.
Centro de Cómputo: También conocido como Centro de Procesamiento de Datos, o Data Center es una instalación que se encarga del procesamiento de datos e información de manera sistematizada. El procesamiento se lleva a cabo con la utilización de computadoras (Hardware) y programas (Software) necesarios para cumplir con dicha tarea.
Confidencialidad: Característica de la información por medio de la cual no se revela ni se encuentra a disposición de individuos, organizaciones o procesos no autorizados. La información debe ser vista o estar disponible solo a las personas autorizadas.
Control: Mecanismo para manejar el riesgo, incluyendo políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas, y que pueden ser de carácter administrativo, técnico o legal.
Correo Electrónico: También conocido como E-mail, es un servicio de red que permite a los usuarios enviar y recibir textos, imágenes, videos, audio, programas, a través de internet.
Cuentas de Correo: Son espacios de buzones para la recepción, envió y almacenamiento de mensajes de correo electrónico en internet.
Contraseña o Password: Es una forma de autenticación privada, compuesta por un conjunto de números, letras y caracteres, que permiten al usuario tener acceso a un computador, a un archivo y/o a un programa.
Disponibilidad: Es la garantía de poder acceder a los activos de la información cuando sea necesario, por personal autorizado.

Evento de Seguridad de La información: Ocurrencia identificada de una situación de sistema, servicio o red que indica una posible violación de la política de seguridad de la información o falla de salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad de un activo de información.

Firma Digital: La firma digital hace referencia, en la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos, a un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento.

Incidente de Seguridad de la información: Es la identificación de la ocurrencia de un hecho que está relacionado con los activos de información, que indica una posible brecha en las Políticas de Seguridad o falla en los controles y/o protecciones establecidas.

Infraestructura de Procesamiento de Información: Es cualquier sistema de procesamiento de información, servicio, plataforma tecnológica, o instalación física que los contenga.

Firewall: Dispositivo que permite bloquear o filtrar el acceso en redes de comunicación.

Hacker: Persona dedicada a realizar entradas no autorizadas a los sistemas, por medio de redes de comunicación como Internet, con el objeto de encontrar vulnerabilidades en los sistemas.

Host: Termino usado en informática para referirse a los computadores conectados a la red, que proveen y/o utilizan servicios de ella. Los usuarios deben utilizar hosts para tener acceso a la red

Integridad: La propiedad de salvaguardar la exactitud y completitud de los activos de información.

Internet: Conjunto de redes conectadas entre sí, que utilizan el protocolo TCP/IP para comunicarse entre sí.

Intranet: Red privada dentro de una empresa, que utiliza el mismo software y protocolos empleados en la Internet global, pero que es de uso interno.

LAN: (Local Area Network). (Red de Área Local). Red de computadoras ubicadas en el mismo ambiente, piso o edificio.

Malware: Código malicioso o cualquier tipo de programa desarrollado para causar daños o introducirse de forma no autorizada en algún sistema informático.

Política: Son instrucciones mandatarias que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños.

Red: Se tiene una red, cada vez que se conectan dos o más computadoras de

manera que pueden compartir recursos.

Riesgo residual: Es el riesgo remanente, después de la implantación de las medidas de seguridad determinadas en el plan de seguridad de la información.

Sistema de Gestión de Seguridad de la información: SGSI La parte del sistema total de gestión, basada en un enfoque de riesgo de negocios, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

Seguridad: Mecanismos de control que evita el uso no autorizado de recursos.

Seguridad de la Información: Son medidas preventivas que incluyen factores de confidencialidad, integridad, disponibilidad, autenticidad, responsabilidad, aceptabilidad y confiabilidad de la información.

Servidor: Computadora que comparte recursos con otras computadoras, conectadas con ella a través de una red.

Sistema Operativo: Programa o conjunto de programas que permiten administrar los recursos de hardware y software de una computadora, servidor o dispositivo móvil.

Terceros: Se entiende por tercero a toda persona, jurídica o natural ajena a Gestión de Seguridad Electrónica, como proveedores, contratistas o consultores, que provean servicios o productos a la Entidad.

Troyano: Es un programa con una determinada función o utilidad, pero que contiene código oculto para ejecutar acciones no esperadas por el usuario.

Virus: Software malicioso que tiene por objeto alterar el normal funcionamiento de una computadora, reemplazando así programas ejecutables, sin la autorización ni el conocimiento del usuario.

6. ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN

6.1 POLÍTICA DE ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN

Gestión de Seguridad Electrónica crea un esquema de seguridad de la información definiendo y estableciendo roles y responsabilidades que involucren las actividades de operación, gestión y administración de la seguridad de la información, así como la creación del Comité y el Oficial de Seguridad de la Información.

6.1.1 Funciones del Comité SIG

- Proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como las bases de datos e información en general.
- Revisar el estado general de la seguridad de la información.
- Aprobar las modificaciones o nuevas políticas de seguridad de la información.
- Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
- Identificar necesidades de evaluación de los procesos soportados por los recursos informáticos y su plataforma tecnológica.
- Realizar otras actividades inherentes a la naturaleza del comité relacionadas con la seguridad de la información.
- Asegurar que exista una dirección y apoyo gerencial sobre los principios y las metas para soportar la administración y desarrollo de iniciativas sobre la gestión de la seguridad de los activos de la información, a través de compromisos apropiados y de recursos adecuados, como la formulación y mantenimiento de las políticas de seguridad de la información a través de todos los empleados de la organización.
- Validar las políticas de seguridad de la información y procedimientos para el uso adecuado y administración de los recursos informáticos asignados a los empleados de la organización, asegurando que la información se encuentre protegida. Política para uso de dispositivos móviles.

7. SEGURIDAD PARA LOS RECURSOS HUMANOS

Gestión de Seguridad Electrónica implementa acciones para asegurar que los empleados, contratistas, proveedores, entiendan sus responsabilidades del cumplimiento de las políticas como usuarios y la responsabilidad de los roles asignados.
La información almacenada en los equipos de cómputo de la Entidad es propiedad de Gestión de Seguridad Electrónica y cada usuario es responsable por proteger su integridad, confidencialidad y disponibilidad.

Se capacita y sensibiliza a los empleados sobre las políticas de seguridad de la información.

Se asegura que los empleados, contratistas y demás colaboradores de Gestión de Seguridad Electrónica, adopten sus responsabilidades en relación con las políticas de seguridad de la información y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de la información.

En situaciones de incumplimiento y/o violaciones a las políticas de seguridad de la información se deberá tramitar el cumplimiento de la ley 734 de 2013, ley 200 de 1995 y demás normas que reglamenten los procesos disciplinarios para los empleados del estado.

7.1 Proceso Disciplinario

Dentro de la estrategia de seguridad de la información de Gestión de Seguridad Electrónica, está establecido un proceso disciplinario formal para los empleados que hayan cometido alguna violación de las Políticas de Seguridad de la Información.
El proceso disciplinario también se debería utilizar como disuasión para evitar que los empleados, contratistas y los otros colaboradores de Gestión de Seguridad Electrónica violen las políticas y los procedimientos de seguridad de la información, así como para cualquier otra violación de la seguridad. Las investigaciones disciplinarias corresponden a actividades pertenecientes al proceso de gestión del Área de Talento Humano.
Actuaciones que conllevan a la violación de la seguridad de la información establecidas por Gestión de Seguridad Electrónica son entre otras:

- No firmar los acuerdos de confidencialidad o de entrega de información o de activos de información.
- No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
- No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral, “documentos impresos que contengan información pública reservada, información pública clasificada (privada o semiprivada)”.

- No guardar la información digital, producto del procesamiento de la información perteneciente a Gestión de Seguridad Electrónica.
- Dejar información confidencial, en carpetas compartidas o en lugares distintos al servidor de archivos, obviando las medidas de seguridad.
- Dejar las gavetas abiertas o con las llaves puestas en los escritorios, dejar los computadores encendidos en horas no laborables.
- Permitir que personas ajenas a Gestión de Seguridad Electrónica, deambulen sin acompañamiento, al interior de las instalaciones, en áreas no destinadas al público.
- Almacenar en los discos duros de los computadores personales de los usuarios, la información de la Entidad. Solicitar cambio de contraseña de otro usuario, sin la debida autorización del titular o su jefe inmediato.
- Hacer uso de la red de datos de la institución, para obtener, mantener o difundir en los equipos de sistemas, material pornográfico (penalizado por la ley) u ofensivo, cadenas de correos y correos masivos no autorizados.
- Utilización de software no relacionado con la actividad laboral.
- Recibir o enviar información institucional a través de correos electrónicos personales, diferentes a los asignados por la institución.
- Enviar información confidencial por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.
- Utilizar equipos electrónicos o tecnológicos desatendidos o a través de sistemas de interconexión inalámbrica, sirvan para transmitir, recibir y almacenar datos.
- Usar dispositivos de almacenamiento externo en los computadores, cuya autorización no haya sido otorgada por el Área de TI de Gestión de Seguridad Electrónica.
- Permitir el acceso de empleados a la red corporativa, sin la autorización de Área de TI de Gestión de Seguridad Electrónica.
- Utilización de servicios disponibles a través de internet, como FTP y Telnet, no permitidos por Gestión de Seguridad Electrónica o de protocolos y servicios que no se requieran y que puedan generar riesgo para la seguridad.
- Negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de Gestión de Seguridad Electrónica.
- No cumplir con las actividades designadas para la protección de los activos de información de Gestión de Seguridad Electrónica.

- Destruir o desechar de forma incorrecta la documentación corporativa.
- Registrar información confidencial, en pos-it, apuntes, agendas, libretas, etc sin el debido cuidado.
- Almacenar información confidencial, en cualquier dispositivo de almacenamiento que no pertenece a Gestión de Seguridad Electrónica o conectar computadores portátiles u otros sistemas eléctricos o electrónicos personales a la red de datos de Gestión de Seguridad Electrónica, sin la debida autorización.
- Promoción o mantenimiento de negocios personales, o utilización de los recursos tecnológicos de Gestión de Seguridad Electrónica para beneficio personal.
- El que impida u obstaculice el funcionamiento o el acceso normal al sistema informático, los datos informáticos o las redes de telecomunicaciones de Gestión de Seguridad Electrónica, sin estar autorizado.
- El que destruya, dañe, borre, deteriore o suprima datos informáticos o un sistema de tratamiento de información de Gestión de Seguridad Electrónica.
- El que distribuya, envíe, introduzca software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica de Gestión de Seguridad Electrónica.
- El que viole datos personales de las bases de datos de Gestión de Seguridad Electrónica.
- El que superando las medidas de seguridad informática suplante un usuario ante los sistemas de autenticación y autorización establecidos por Gestión de Seguridad Electrónica.
- No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de Gestión de Seguridad Electrónica o permitir que otras personas accedan con el usuario y clave del titular a éstos.
- Permitir el acceso u otorgar privilegios de acceso a las redes de datos de Gestión de Seguridad Electrónica a personas no autorizadas.
- Llevar a cabo actividades fraudulentas o ilegales, o intentar acceso no autorizado a cualquier computador de Gestión de Seguridad Electrónica.
- Ejecutar acciones tendientes a eludir o variar los controles establecidos por Gestión de Seguridad Electrónica.
- Retirar de las instalaciones, estaciones de trabajo o computadores portátiles que contengan información corporativa sin la autorización pertinente.
- Sustraer de las instalaciones de Gestión de Seguridad Electrónica, documentos con información calificada como confidencial, o abandonarlos en

lugares públicos o de fácil acceso.

- No realizar el borrado seguro de la información en equipos o dispositivos de almacenamiento de Gestión de Seguridad Electrónica, para traslado, reasignación o para disposición final.
- Ejecución de cualquier acción que pretenda difamar, abusar, afectar la reputación o presentar una mala imagen de Gestión de Seguridad Electrónica o de alguno de sus empleados.
- Realizar cambios no autorizados en la plataforma tecnológica de Gestión de Seguridad Electrónica.
- Copiar sin autorización los programas de Gestión de Seguridad Electrónica, o violar los derechos de autor o acuerdos de licenciamiento.

8. GESTIÓN DE ACTIVOS DE INFORMACIÓN

Gestión de Seguridad Electrónica es el dueño de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los empleados y los contratistas, derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato.
Gestión de Seguridad Electrónica es propietario de los activos de información y los administradores de estos activos son los empleados, contratistas o demás colaboradores de Gestión de Seguridad Electrónica que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de Tecnología y Sistemas de Información (TIC).

Gestión de Seguridad Electrónica mantiene un inventario actualizado de sus activos de información, quedando bajo la responsabilidad de cada propietario de información y centralizado por el área de calidad.

8.1 Política de uso de los activos

Gestión de Seguridad Electrónica implementa las directrices para lograr y mantener la protección adecuada y uso de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.
Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de vídeo, música, y fotos y

cualquier tipo de archivo que no sean de carácter institucional.

8.2 Política de uso de equipos

Los usuarios no podrán realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo.

8.3 Política de navegación.

Gestión de Seguridad Electrónica permite el acceso al servicio de internet, estableciendo lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.
El Área de TI implementa herramientas para evitar la descarga de software no autorizado y/o código malicioso en los equipos corporativos.

Los usuarios de los activos de información de Gestión de Seguridad Electrónica tienen restringido el acceso a redes sociales, webs que contenga contenido (difamatorio, ofensivo, obsceno, vulgar, racista, pornográfico, subversivo, violento, Juegos de azar, loterías, pornográfico, alcohol tabaco, drogas) así como servicios: criptomonedas, servicios anonimizadores, proxy de internet, plataformas de hacking que puedan perpetuar delitos informáticos.

Se prohíbe la descarga, uso, intercambio y/o instalación de programas, juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución.

8.4 Clasificación de la información

Gestión de Seguridad Electrónica consiente de la necesidad de asegurar que la información reciba el nivel de protección apropiado de acuerdo al tipo de clasificación establecido por la ley, Gestión de Seguridad Electrónica define reglas de como clasificar la información.
Se considera información toda forma de comunicación o representación de

conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que genere Gestión de Seguridad Electrónica por ejemplo:

- Formularios / comprobantes propios o de terceros.
- Información en los sistemas, equipos informáticos, medios magnéticos/electrónicos o medios físicos como papel.
- Otros soportes magnéticos/electrónicos removibles, móviles o fijos.
- Información o conocimiento transmitido de manera verbal o por cualquier otro medio de comunicación.

Los usuarios responsables de la información de Gestión de Seguridad Electrónica, deben identificar los riesgos a los que está expuesta la información de sus áreas, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.

9 CONTROL DE ACCESOS

Gestión de Seguridad Electrónica define las reglas para asegurar un acceso controlado, físico o lógico, a la información y plataforma informática.
La conexión remota a la red de área local de Gestión de Seguridad Electrónica debe realizarse a través de una conexión VPN segura suministrad, la cual debe ser aprobada, registrada y auditada, por el Área de TI.

El acceso a los activos de información de Gestión de Seguridad Electrónica estará permitido únicamente a los usuarios autorizados, el cual deberá utilizar durante el proceso de autenticación.

El funcionario que disponga de usuario(s) de acceso a los activos de información, será responsable de su uso, el cual es personal e intransferible.

9.1 Establecimiento, uso y protección de claves de acceso

Ningún usuario deberá acceder a la red o a los servicios TIC de Gestión de Seguridad Electrónica, utilizando una cuenta de usuario o clave de otro usuario.

Gestión de Seguridad Electrónica, suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.

El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta, en donde se llevará a cabo la validación de los datos personales; en caso de ser solicitado el cambio de contraseña para otra persona, debe ser realizada por su jefe inmediato (previa autorización por parte del Jefe de Área de TI).
Las claves o contraseñas deben:

Tener mínimo ocho (8) caracteres alfanuméricos.

Cada vez que se cambien estas deben ser distintas por lo menos de las últimas veinte anteriores.

La contraseña debe cumplir con tres requisitos:

- Caracteres en mayúsculas
- Caracteres en minúsculas
- Caracteres no alfabéticos (Ejemplo: ¡,$,%,&)

Las cuentas de los usuarios que hagan más de 3 intentos fallidos de acceso quedarán deshabilitadas y los usuarios deberán solicitar su desbloqueo al área de TI.

9.2 Manejo de contraseñas para administradores de tecnología

Se garantiza en las plataformas de tecnología que el ingreso a la administración en lo posible, se realice con la vinculación directamente de las credenciales de los usuarios de directorio activo.
Los usuarios súper-administradores y sus correspondientes contraseñas a las consolas administrables se dejan en custodia en buzón encriptado en la unidad de almacenamiento central NAS de Gestión de seguridad electrónica, las credenciales allí contenidas deben ser modificadas de manera mensual o cuando amerite.
El personal del Área de TI no debe dar a conocer su clave de usuario a terceros de los sistemas de información, sin previa autorización del Director del Área de TI.
Los usuarios y claves de los administradores de sistemas y/o del personal del Área de TI son de uso personal e intransferible.
El personal del Área de TI debe emplear obligatoriamente las claves o

contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee de acuerdo al rol asignado.
Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar procedimiento de salvaguarda o custodia de las claves o contraseñas en un sitio seguro. A este lugar solo debe tener acceso el Director del Área de TI o al Director General.

9.3 Política de uso de puntos de red de datos (red de área local – LAN)

Asegurar la operación correcta y segura de los puntos de red.

Las direcciones internas, configuraciones e información relacionada con la topología y diseño de los sistemas de comunicación y redes de la entidad serán restringidas, de tal forma que no sean conocidas por usuarios internos, clientes o personas ajenas a Gestión de Seguridad Electrónica sin la previa autorización del Área de TI.

Todas las conexiones a redes externas que accedan a la red interna de la Entidad pasarán a través de un punto adicional de control como: firewall, gateway, o servidor de acceso.

9.3.1 Segregación en redes

La infraestructura tecnológica de Gestión de Seguridad Electrónica que soporta aplicaciones debe estar separada en segmentos de red físicos y Lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a Internet. La separación de estos segmentos debe ser realizada por medio de elementos de conectividad perimetrales e internos de enrutamiento y de seguridad.

9.3.2 Control de Acceso Remoto

La administración remota de equipos o de la infraestructura de cómputo debe dejar evidencia escrita de la justificación por las que se asigna, al igual que de la responsabilidad que tiene el funcionario a quien se otorga este permiso, la solicitud debe ser realizada por el Jefe del Área correspondiente y debe ser avalada por el Área de TI.

9.4 Políticas específicas para usuarios de Gestión de Seguridad Electrónica

Definir las pautas generales para asegurar una adecuada protección de la información de Gestión de Seguridad Electrónica por parte de los usuarios de la Entidad.
Es responsabilidad de los administradores de los sistemas de información garantizar que los puertos físicos y lógicos de configuración y acceso privilegiado de las plataformas de infraestructura que soportan los sistemas de información deben estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.

10 CIFRADO

10.1 Política de controles criptográficos

Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de cómputo de Gestión de Seguridad Electrónica, sea por cualquier medio tecnológico existente, siempre deberá estar autenticado y sus conexiones deberán estar cifradas.

Toda información confidencial que se extraiga deberá estar cifrada para evitar que la misma pierda su confidencialidad.

11 SEGURIDAD FÍSICA Y AMBIENTAL

El Área de TI, debe mantener actualizado el programa de seguridad física de las instalaciones, así como el programa de mantenimiento de las barreras de seguridad (Perimetrales e internas) de las instalaciones pertenecientes a Gestión de Seguridad Electrónica.
Todas las áreas destinadas al procesamiento, almacenamiento de documentos o información, así como aquellas en las que se encuentren los equipos de cómputo y demás infraestructura de los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. Por tanto, contarán con medidas de control de acceso físico en el perímetro de tal forma que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información.

11.1 Políticas de seguridad del centro de datos y centros de cableado

En las instalaciones del centro de datos o de los centros de cableado, No está permitido:

- Fumar dentro del Data Center.
- Introducir alimentos o bebidas al Data Center
- El porte de armas de fuego, corto punzantes o similares.
- Mover, desconectar y/o conectar equipo de cómputo sin autorización.
- Modificar la configuración del equipo o intentarlo sin autorización.
- Alterar software instalado en los equipos sin autorización.
- Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas.
- Extraer información de los equipos en dispositivos externos.
- Abuso y/o mal uso de los sistemas de información.
- Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.

Los centros de cómputo deben mantener las condiciones físicas y ambientales óptimas recomendadas, así como controles automáticos para incendio, temperatura y cuando sea posible, monitoreo por Circuito Cerrado de Televisión.

11.2 Políticas de seguridad de los Equipos

Gestión de Seguridad Electrónica, debe poseer la infraestructura necesaria, con el fin de actuar contra eventos que pongan en riesgo la integridad y confidencialidad de la información, y es así, que los equipos de cómputo están conectados a las instalaciones eléctricas apropiadas de corriente regulada, fase, neutro y polo a tierra, para evitar pérdidas o daños de la información como activo fundamental.

11.2.1 Política de escritorio y pantalla limpia

Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los usuarios.
Los empleados, contratistas, personas en comisión, pasantes y terceros que tienen algún vínculo con Gestión de Seguridad Electrónica, deben conservar su

escritorio libre de información, propia de la Entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
Los usuarios de los sistemas de información y comunicaciones de Gestión de Seguridad Electrónica, deben bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.
Los usuarios de los sistemas de información y comunicaciones de Gestión de Seguridad Electrónica deben cerrar las aplicaciones y servicios de red cuando ya no los necesiten.
Al imprimir documentos con información confidencial, deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.
No se debe utilizar fotocopiadoras, escáneres, equipos de fax, cámaras digitales y en general equipos tecnológicos que se encuentren desatendidos.

11.3 Política de manejo disposición de información, medios y equipos

La Entidad establece actividades para evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios proporcionados por Gestión de Seguridad Electrónica, velando por la disponibilidad y confidencialidad de la información.

Los medios y equipos donde se almacena, procesa o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.

El servicio de acceso a Internet, Intranet, Sistemas de información, medio de almacenamiento, aplicaciones (Software), cuentas de red, navegadores y equipos de cómputo son propiedad de Gestión de Seguridad Electrónica y deben ser usados únicamente para el cumplimiento de su misión.

Se debe realizar la aplicación del procedimiento de borrado seguro en los equipos de cómputo y demás dispositivos, una vez el funcionario haya sido retirado de la Entidad, de acuerdo a lo definido por Gestión de Seguridad Electrónica.

Está restringida la copia de archivos en medios removibles de almacenamiento,

USB, unidades ópticas de grabación en todos los equipos de cómputo; la autorización de uso de los medios removibles debe ser tramitada a través del Área de TI y será objeto de auditorías de seguridad mediante el módulo de prevención de pérdidas de datos.

12 SEGURIDAD DE LAS OPERACIONES DE TIC

Se definieron procedimientos, registros e instructivos de trabajo debidamente documentados, los cuales serán progresivamente implementados, con el fin de asegurar el mantenimiento y operación adecuada de la infraestructura tecnológica.
Cada procedimiento tendrá un responsable para su definición, mantenimiento e implementación.
Para la gestión de las operaciones de la infraestructura de procesamiento de información en Gestión de Seguridad Electrónica El Área de TI, con el apoyo de las áreas, establecerá mecanismos que permitan segregar las funciones de administración (sistemas operativos, bases de datos y aplicaciones), monitoreo y operación, separando entre estos los diferentes ambientes de desarrollo, pruebas y producción.
No deberán realizarse pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción, con el fin de evitar problemas de disponibilidad o confidencialidad de la información. Así mismo, en los ambientes de desarrollo si se llegaran a utilizar datos reales del ambiente de producción, se debe definir el protocolo de seguridad que permita salvaguardar la integridad de la información.

12.1 Política de respaldo y restauración de información

La restauración de copias de respaldo en ambientes de producción debe estar aprobada por el propietario de la información y solicitadas a través de correo electrónico al área de TI.

Semanalmente los administradores de la plataforma de backup de Gestión de Seguridad Electrónica, verificarán la correcta ejecución de los procesos de backup.
Los medios que vayan a ser eliminados o que cumplan el periodo de retención deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.

El administrador de la plataforma de backup, deben generar tareas de restauración aleatorias de la información y deben ser documentadas.
La información previamente definida y contenida en los servidores de Gestión de Seguridad Electrónica, se respaldará de forma periódica, determinada según el procedimiento " Copia de respaldo de Información". Adicionalmente, se realizarán pruebas periódicas de recuperación y verificación de la información almacenada en los medios con el fin de verificar su integridad y disponibilidad.

12.2 Copias en estaciones de trabajo de usuario final

Gestión de Seguridad Electrónica Asegura la realización de copias de información en estaciones de trabajo de usuario final, en el medio de almacenamiento central NAS.
Ningún usuario final debe realizar copias de la información contenida en la estación de trabajo a medios extraíbles de información.
Los medios que vayan a ser eliminados o que cumplan el periodo de retención deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.

12.3 Registro y seguimiento de eventos de sistemas de información y comunicaciones

Preservar la integridad, confidencialidad y disponibilidad de los registros de eventos (logs) generados por los sistemas de información y comunicaciones de Gestión de Seguridad Electrónica.

Los empleados y contratistas de Gestión de Seguridad Electrónica, deben informar inmediatamente al área de calidad cualquier situación sospechosa, o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información.

El área de calidad será la encargada de realizar el escalamiento, seguimiento a la investigación y seguimiento a los eventos e incidentes de seguridad reportados.

12.4 Control de software operacional de Gestión de Seguridad Electrónica

Generar acciones que permitan preservar la integridad de los sistemas operativos pertenecientes de Gestión de Seguridad Electrónica.
Los responsables de la administración de las plataformas de producción estarán obligados a controlar el acceso y uso de los programas fuente, el acceso a los archivos de los sistemas y/o a las aplicaciones que operan en ellas, así como a la programación de las actualizaciones necesarias a realizar.
No se permitirá la instalación de herramientas de desarrollo ni programas fuente en los sistemas de producción.
No se permitirá el uso de versiones de software en los sistemas de producción que no sean soportadas por los fabricantes, ni versiones de prueba que no hayan sido liberadas al mercado (Beta), a menos que sea autorizado por el Director de TI.

12.5 Gestión de vulnerabilidades

Una vez identificadas las vulnerabilidades técnicas potenciales, Gestión de Seguridad Electrónica, identificará los riesgos asociados y los controles de seguridad a ser tenidos en cuenta (esta acción puede implicar la actualización de sistemas vulnerables y/o aplicación de las medidas de acción necesarias).

El Oficial de Seguridad de la información realizará el seguimiento y verificación de que se hayan corregido las vulnerabilidades identificadas.

13 SEGURIDAD DE LAS TELECOMUNICACIONES

Gestión de Seguridad Electrónica, identificará los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión sobre los servicios de red, incluyendo los mismos en los contratos establecidos con sus contratistas.

13.1 Política para la transferencia de información.

Gestión de Seguridad Electrónica protege la información transferida al interior y exterior.

El Área de TI, realiza el control del uso de sistemas de transferencia de archivos confidenciales asegurando el encriptado de la información antes de su envío por cualquier tipo de medio.

13.2 Política de uso de correo electrónico

El personal del Área de TI no debe dar a conocer su clave de usuario a terceros de los sistemas de información, sin previa autorización del Director del Área de TI.

Los usuarios y claves de los administradores de sistemas y del personal del Área de TI son de uso personal e intransferible.

El personal del Área de TI debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee Gestión de Seguridad Electrónica de acuerdo al rol asignado.
Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar procedimientos de salvaguarda o custodia de las claves o contraseñas en un sitio seguro. A este lugar solo debe tener acceso el Director de TI o el Director General.
Se prohíbe enviar o reenviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral, las buenas costumbres y/o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos.

La cuenta de correo electrónico deberá ser usada para el desempeño de las funciones asignadas dentro de Gestión de Seguridad Electrónica.
Los mensajes y la información contenida en los buzones de correo son de propiedad de Gestión de Seguridad Electrónica. El usuario podrá crear un histórico de su correo siempre y cuando sea almacenado en el disco duro en el PC del usuario.

13.3 Uso de mensajería instantánea y redes sociales

Gestión de Seguridad Electrónica define las pautas generales para asegurar una adecuada protección de la información, en el uso del servicio de mensajería instantánea y de las redes sociales, por parte de los usuarios autorizados.

La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador de Gestión de Seguridad Electrónica, que sea creado a nombre personal en redes sociales como: twitter®, facebook®, youtube® likedink®, blogs, instagram, etc, se considera fuera del alcance de las políticas establecidas y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.
Toda información distribuida en las redes sociales que sea originada por Gestión de Seguridad Electrónica, debe ser autorizada por los jefes de área para ser socializadas y con un vocabulario corporativo.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Garantizar que la seguridad es parte integral de los sistemas de información.

El Desarrollo de tecnologías informáticas se debe orientar sobre herramientas basadas en tecnologías de última generación, que permitan la portabilidad y escalabilidad de las aplicaciones.
La supervisión y seguimiento a proyectos de infraestructura informática, deben incorporar como un elemento básico de la supervisión, el cumplimiento de la aplicación de políticas de seguridad tanto en el desarrollo de la solución como en el producto final que será entregado Gestión de Seguridad Electrónica.

Todos los desarrollos de software deben surtir una fase de pruebas de funcionalidad en la cual se evidencien los controles establecidos en relación con la integridad de la información que será ingresada una vez se lleve a cabo su implementación.

Los desarrollos de software deben involucrar la correspondiente documentación interna y externa que permitan identificar su seguimiento.

15 RELACIONES CON PROVEEDORES Y TERCEROS

15.1 Política de Proveedores

Se deben establecer criterios de selección proveedores, establecidas en el procedimiento de compras y política de seguridad de la información para la relación con proveedores.
Se establece mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad de la información de Gestión de Seguridad Electrónica, las cuales deben se divulgadas por los empleados responsables de la realización y/o firma de contratos o convenios.
En los contratos o acuerdos con los proveedores y/o contratistas se debe incluir una causal de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las políticas de seguridad de la información.
Los contratistas, oferentes y/o proveedores deben aceptar y firmar el acuerdo de confidencialidad establecido por Gestión de Seguridad Electrónica.
Se deben identificar los riesgos para la información y los servicios de procesamiento de información que involucren partes externas a Gestión de Seguridad Electrónica. El resultado del análisis de riesgos será la base para el establecimiento de los controles y debe ser presentado al área de calidad.
Los empleados de Gestión de Seguridad Electrónica que fungen como supervisores de contratos relacionados con sistemas de información deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas.

16 GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

Gestión de Seguridad Electrónica asegura que los eventos e incidentes de seguridad que se presenten con los activos de información, sean comunicados y atendidos oportunamente, empleando el procedimiento definido “Gestión de incidentes”, con el fin de ejecutar oportunamente las acciones correctivas.
Los empleados y contratistas de Gestión de Seguridad Electrónica, deberán informar inmediatamente al área de Calidad cualquier situación sospechosa, o

incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información.

El área de calidad será el encargado de realizar el escalamiento y seguimiento a la investigación y seguimiento a los eventos e incidentes de seguridad reportados.

Todos los incidentes de seguridad reportados serán investigados y se les hará seguimiento por parte del área de calidad. Los resultados de las investigaciones serán informados a la dirección, especificando las causas, consecuencias, responsabilidades, solución y acciones para evitar que se presenten nuevamente.

17 GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Con el fin de prevenir interrupciones en las actividades de la plataforma informática, Gestión de Seguridad Electrónica desarrollo e implemento un Plan de Continuidad para asegurar que los procesos misionales de Gestión de Seguridad Electrónica podrán ser restaurados dentro de escalas de tiempo razonables.
Gestión de Seguridad Electrónica tiene definido un plan de acción que permite mantener la continuidad del negocio teniendo en cuenta los siguientes aspectos:

- Identificación y asignación de prioridades a los procesos críticos de Gestión de Seguridad Electrónica de acuerdo con su impacto en el cumplimiento de la misión de la Entidad.

- Documentación de la estrategia de continuidad del negocio.

- Documentación del plan de recuperación del negocio de acuerdo con la estrategia definida anteriormente.

- Plan de pruebas de la estrategia de continuidad del negocio.

La alta dirección de Gestión de Seguridad Electrónica, se encargará de la definición y actualización de las normas, políticas, procedimientos y estándares relacionados con la continuidad del negocio, igualmente velará por la implantación y cumplimiento de las mismas.

18 CUMPLIMIENTO

Los diferentes aspectos contemplados en el presente documento son de obligatorio cumplimiento para todos los empleados, contratistas y otros colaboradores de Gestión de Seguridad Electrónica. En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, Gestión de Seguridad Electrónica tomará las acciones disciplinarias y legales correspondientes.

18.1 Política de tratamiento de datos personales

Gestión de Seguridad Electrónica implementó una política de datos personales que contempla:
Datos de menores de edad: El suministro de los datos personales de menores de edad es facultativo y debe realizarse con autorización de los padres de familia o representantes legales del menor, en concordancia con lo establecido por la Ley 1098 de 2006 “Código de Infancia y Adolescencia”.
Las áreas de Gestión de Seguridad Electrónica que tratan con datos personales de empleados, proveedores, contratistas, u otras personas deben obtener la autorización para el tratamiento de datos personales que permita recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de Gestión de Seguridad Electrónica , así mismo los Jefes de área deben asegurar que tendrán acceso a los datos personales únicamente los empleados autorizados.

18.2 Cumplimiento de requisitos legales y contractuales

Gestión de Seguridad Electrónica respeta y acata las normas legales existentes relacionadas con seguridad de la información, para lo cual realizará una continua revisión, identificación, documentación y cumplimiento de la legislación y requisitos contractuales aplicables, relacionada con la seguridad de la información.
Gestión de Seguridad Electrónica, establece la política para protección de derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.
El Área de TI deberá garantizar que todo el software que se ejecute los activos de información de Gestión de Seguridad Electrónica esté protegido por derechos de autor y requiera licencia de uso o sea software de libre distribución y uso.

18.3 Revisiones de Seguridad de la Información

Garantizar la aplicabilidad de las políticas y procedimientos implementados en Gestión de Seguridad Electrónica.
Los Directores y Jefes de Área, deben verificar y supervisar el cumplimiento de las políticas de seguridad de la información en su área de responsabilidad.

El área T.I en acompañamiento del Área Calidad establecen el procedimiento para revisar periódicamente los sistemas de información con el herramientas automáticas y especialistas técnicos.