OSYA
ORGANIZACIÓN
SERVICIOS Y ASESORÍAS
"Administradora de
Recursos Humanos"

MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN
ORGANIZACIÓN SERVICIOS Y ASESORIAS

Contenido

1. INTRODUCCIÓN

LA ORGANIZACIÓN SERVICIOS Y ASESORÍAS, con sus empresas ORGANIZACIÓN SERVICIOS Y ASESORIAS SAS, ORGANIZACIÓN NACIONAL DE SERVICIOS SAS, Y ASEO SERVICIOS SAS, considera la información como un elemento importante e indispensable en el cumplimiento de los objetivos organizacionales, razón por la cual es necesario establecer un procedimiento que asegure la protección de la información de manera adecuada sin importar la forma como es manejada, almacenada, procesada o transportada.
El presente documento describe las políticas y Medidas de seguridad de la información definidas por la organización. Para la elaboración del mismo, se tuvo presente el siguiente las leyes aplicables demás regulaciones, el capítulo décimo segundo del título primero de la Circular Básica Jurídica de la Superintendencia Financiera de Colombia, la norma ISO 27001:2013 y las recomendaciones del estándar ISO 27002:2013. Las políticas incluidas en este manual se constituyen como parte fundamental del sistema de gestión de seguridad de la información de la organización y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.

La seguridad de la información es una prioridad para la ORGANIZACIÓN y por tanto es responsabilidad de todos sus empleados, clientes y proveedores velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas.

2. ASPECTOS GENERALES

2.1. COMPROMISO DE LA DIRECCION

La Gerencia General de la Organización Servicios y Asesorías, aprueba esta Política de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la entidad.

La gerencia manifiesta su compromiso a través de:

La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en este documento.

La promoción activa de una cultura de seguridad.

Facilitar la divulgación de este manual a todos los empleados de la organización.

El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.

La verificación del cumplimiento de las políticas aquí mencionadas.

2.2. OBJETIVO

El presente documento tiene como objetivo establecer políticas que aseguren la información de la ORGANIZACIÓN SERVICIOS Y ASESORIAS.

2.3. ALCANCE

Las políticas de seguridad de la información cubren todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, empleados, clientes, proveedores y cualquier otro tercero que laboren o tengan relación con la ORGANIZACIÓN, para conseguir un adecuado nivel de seguridad y calidad de la información relacionada.

2.4. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

La Organización Servicios y Asesorías consiente de la importancia de garantizar la seguridad de la información a implementado un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

Los empleados, clientes, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información de la organización, deben adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

La Política General de Seguridad de la Información de la organización se construye en base a políticas, Medidas y procedimientos específicos los cuales guiarán el manejo adecuado de la información de la Organización. Adicionalmente, se establecerán políticas específicas de seguridad de la información las cuales se fundamentan en los dominios y objetivos de control del Anexo A de la norma internacional ISO 27001:2013.

El Comité de Seguridad tendrá la potestad de modificar la Política General o las Políticas Específicas de Seguridad de la Información de acuerdo con las necesidades de revisión establecidas periódicamente o a la aplicabilidad de las mismas.

2.5. SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los empleados, clientes, personal externo y proveedores de la ORGANIZACIÓN SERVICIOS Y ASESORIAS. Por tal razón, las violaciones a las Políticas Seguridad de la Información serán clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

2.6. DEFINICIONES

Activo de información: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de la organización y, en consecuencia, debe ser protegido.

Acuerdo de Confidencialidad: es un documento en los que los empleados, clientes o proveedores de la organización o los provistos por proveedores manifiestan su voluntad de mantener la confidencialidad de la información de la organización, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

Análisis de riesgos de seguridad de la información: proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Autenticación: es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Capacity Planning: es el proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita la entidad para satisfacer las necesidades de procesamiento de dichos recursos de forma eficiente y con un rendimiento adecuado.

Centros de cableado: son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Cifrado: es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

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

Criptografía: es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

Custodio del activo de información: es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

Datos de la Empresa: Información del Negocio de la Empresa como Información de clientes, tarifas, acuerdos y cualquier negociación a terceros considerada clasificada

Derechos de Autor: es un conjunto de Medidas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Disponibilidad: es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

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

Guías de clasificación de la información: directrices para catalogar la información de la organización y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información.

Hacking ético: es el conjunto de actividades para ingresar a las redes de datos y voz de la institución con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

Incidente de Seguridad: es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencia, el número de veces ocurrido o el origen (interno o externo).

Integridad: es la protección de la exactitud y estado completo de los activos.
Inventario de activos de información: es una lista ordenada y documentada de los activos de información pertenecientes a la organización.

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

Medio removible: es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

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

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

Propietario de la información: es la unidad organizacional o proceso donde se crean los activos de información.

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

Registros de Auditoría: son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos de la Organización. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

Responsable por el activo de información: es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.
SGSI: Sistema de Gestión de Seguridad de la Información.

Sistema de información: es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por la organización o de origen externo ya sea adquirido por la organización como un producto estándar de mercado o desarrollado para las necesidades de ésta.

Sistemas de control ambiental: son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características del mismo, fundamentalmente humedad y temperatura y, de manera adicional, también permite controlar su pureza y su movimiento.

Software malicioso: es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

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

Vulnerabilidades: son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la Organización (amenazas), las cuales se constituyen en fuentes de riesgo.

3. POLÍTICAS DE LA ORGANIZACIÓN RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN

3.1. POLÍTICA DE ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACION

LA ORGANIZACIÓN SERVICIOS Y ASESORIAS, establecerá un esquema de seguridad de la información en donde existan responsabilidades y roles definidos que consideren actividades de administración, operación y gestión de la seguridad de la información.

3.1.1. Medidas que rigen para la estructura organizacional de seguridad de la información

ALTA DIRECCION

- La Alta Dirección revisará y aprobará las Políticas de Seguridad de la Información contenidas en este documento.
- La Alta Dirección debe promover activamente una cultura de seguridad de la información dentro de la organización
- La Alta Dirección de la organización definirá y establecerá los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo.
- La Alta Dirección definirá y establecerá el procedimiento de contacto con las autoridades en caso de ser requerido, así como los responsables para establecer dicho contacto.
- La Alta Dirección facilitará la divulgación de las Políticas de Seguridad de la Información a todos Los empleados de la entidad y a los proveedores.
- La Alta Dirección asignará los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad de la información de la Organización.

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN:

- **A**ctualizará y presentará ante la Gerencia general las Políticas de Seguridad de la Información, la metodología para el análisis de riesgos de seguridad y la metodología para la clasificación de la información, según lo considere pertinente.
- Analizará los incidentes de seguridad que le son escalados y activará el procedimiento de contacto con las autoridades, cuando lo estime necesario.
- Verificará el cumplimiento de las políticas de seguridad de la información aquí mencionadas.

GERENCIA DE GESTION

- La GERENCIA DE GESTIÓN planeará y ejecutará las auditorías internas al Sistema de Gestión de Seguridad de la Información de la ORGANIZACIÓN SERVICIOS Y ASESORIAS a fin de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad y regulaciones aplicables.
- La GERENCIA DE GESTIÓN ejecutará revisiones totales o parciales de los procesos o áreas que hacen parte del alcance del Sistema de Gestión de Seguridad de la Información, con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas no conformidades.
- La GERENCIA DE GESTION informará a las áreas responsables los hallazgos de las auditorías.

DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología asignará las funciones, roles y responsabilidades, a sus empleados para la operación y administración de la plataforma tecnológica de la organización. Dichas funciones, roles y responsabilidades estarán documentadas y apropiadamente segregadas.

TODOS LOS USUARIOS

- Los empleados, clientes, proveedores y personal externo que realicen actividades en o para la Organización, tienen la responsabilidad de cumplir con las políticas, Medidas, procedimientos y estándares referentes a la seguridad de la información.

3.2. POLITICA PARA USO DE DISPOSITIVOS MOVILES

- La Organización establecerá las condiciones para el manejo de los dispositivos móviles (teléfonos, inteligentes y tabletas, entre otros) institucionales y/o personales. Así mismo, velará porque los empleados hagan un uso responsable de los servicios y equipos proporcionados por la entidad.

3.2.1. Medidas para uso de dispositivos móviles

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología deberá garantizar la protección de los dispositivos móviles institucionales y personales relacionados con la Organización a través de los diferentes actores vinculados a ella.
- La Dirección de Tecnología establecerá las configuraciones aceptables para los dispositivos móviles institucionales o personales que estén relacionados con actividades de la ORGANIZACIÓN SERVICIOS Y ASESORIAS.
- La Dirección de Tecnología establecerá un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles institucionales que serán entregados a los usuarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.
- La Dirección de Tecnología activará la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles institucionales haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.
- La Dirección de Tecnología configurará la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.
- La Dirección de Tecnología contará con una solución de copias de seguridad para la información contenida en los dispositivos móviles; dichas copias deben acogerse a la Política de Copias de Respaldo de la Información.
- La Dirección de Tecnología instalará un software de antivirus tanto en los dispositivos móviles institucionales. Como en los personales que hagan uso de los servicios provistos por la Organización.
- La Dirección de Tecnología activará los códigos de seguridad de la tarjeta SIM para los dispositivos móviles institucionales antes de asignarlos a los usuarios y almacenar estos códigos en un lugar seguro.

TODOS LOS USUARIOS

- Los usuarios evitaran usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- Los usuarios no modificarán las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
- Los usuarios evitarán la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles organizaciones.
- Los usuarios deberán, cada vez que el sistema de sus dispositivos móviles institucionales notifique de una actualización disponible, aceptar y aplicar la nueva versión.
- Los usuarios evitaran hacer uso de redes inalámbricas de uso público, así como deberán desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.
- Los usuarios evitaran conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.

Los usuarios no deberán almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

3.3. POLITICA PARA USO DE CONEXIONES REMOTAS

La ORGANIZACIÓN SERVICIOS Y ASESORIAS establecerá las circunstancias y requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica de la organización; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

3.3.1. Medidas para uso de conexiones remotas dirigidas *a*:

GERENCIA DE GESTIÓN Y DIRECCION DE TECNOLOGIA

- La GERENCIA DE GESTIÓN, de manera conjunta con la Dirección de Tecnología, analizará y aprobar los métodos de conexión remota a la plataforma tecnológica dela organización

DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología implantará los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica de la ORGANIZACIÓN.
- La Dirección de Tecnología restringirá las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.
- La Dirección de Tecnología verificará la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica de la Organización de manera permanente.

GERENCIA DE GESTION

- La GERENCIA DE GESTIÓN, dentro de su autonomía, realizar auditorías sobre los controles implantados para las conexiones remotas a la plataforma tecnológica de la organización**.**

TODOS LOS USUARIOS

- Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de la Organización y deben acatar las condiciones de uso establecidas para dichas conexiones.

- Los usuarios únicamente deben establecer conexiones remotas en computadores previamente identificados y, bajo ninguna circunstancia, en computadores público, de hoteles o cafés internet, entre otros.

4. POLÍTICAS DE SEGURIDAD DEL PERSONAL

4.1. POLÍTICA RELACIONADA CON LA VINCULACIÓN DE EMPLEADOS

LA ORGANIZACIÓN SERVICIOS Y ASESORIAS, Considera de gran importancia el talento y capacidad de sus colaboradores, para lograr procesos eficientes que le permitan cumplir sus objetivos misionales, por lo cual realiza un proceso formal de selección de candidatos, orientado a las funciones y roles que cumplirán dentro de la organización, dicho proceso se ajusta a las políticas organizaciones.

4.1.1. Medidas relacionadas con la vinculación de EMPLEADOS

PROCESO DE SELECCIÓN Y CONTRATACIÓN

- Los profesionales vinculados al proceso de selección realizaran las verificaciones necesarias para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo dentro de la organización.

- Los profesionales vinculados al proceso de contratación garantizaran que los empleados de la organización firmen un Acuerdo y/o Cláusula de Confidencialidad y un documento de aceptación de Políticas de Seguridad de la Información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.

DIRECTIVOS DE LA ORGANIZACIÓN

- Todos los directivos de la organización deben garantizar que todos los empleados directos de la organización o proveedores que realicen algún tipo de actividad dentro de la misma, firmen un Acuerdo y/o Cláusula de Confidencialidad y un documento de aceptación de Políticas de Seguridad de la Información

GERENCIA DE GESTIÓN

- La Gerencia de Gestión diseñará y ejecutará de manera permanente un programa de concienciación en seguridad de la información, con el objetivo de apoyar la protección adecuada de la información y de los recursos de procesamiento la misma.
- La Gerencia de Gestión capacitará y entrenará a Los empleados de la organización en el programa de concienciación en seguridad de la información para evitar posibles riesgos de seguridad.
- La Gerencia de Gestión convocará a Los empleados a las charlas y eventos programados como parte del programa de concienciación en seguridad de la información, proveer los recursos para

la ejecución de las capacitaciones y controlar la asistencia a dichas charlas y eventos, aplicando las sanciones pertinentes por la falta de asistencia no justificada.

PROCESO JURIDICO

- El proceso jurídico aplicará el proceso disciplinario de la organización cuando se identifiquen violaciones o incumplimientos a las políticas de seguridad de la información**.**

TODOS LOS USUARIOS

- Todos los empleados y proveedores que por sus funciones hagan uso de la información de la Organización, darán cumplimiento a las políticas, Medidas y procedimientos de seguridad de la información, así como asistir a las capacitaciones que sean referentes a la seguridad de la información.

4.2. POLÍTICA DE DESVINCULACIÓN, LICENCIAS, VACACIONES O CAMBIO DE LABORES DE LOS EMPLEADOS Y PROVEEDORES

La organización asegurará que sus empleados y el personal provisto por terceros serán desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura.

4.2.1. Medidas para la desvinculación, licencias, vacaciones o cambios de labores de Los empleados proveedores

El proceso de nómina realizará el proceso de desvinculación, licencias, vacaciones o cambio de labores de los empleados de la organización llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin.

DIRECTIVOS DE LA ORGANIZACIÓN

- Todos los directivos de la organización monitorearan y reportar de manera inmediata la desvinculación o cambio de labores de Los empleados o proveedores a la GERENCIA DE GESTIÓN.

GERENCIA DE GESTIÓN

- La GERENCIA DE GESTIÓN verificará los reportes de desvinculación o cambio de labores y posteriormente debe solicitar la modificación o inhabilitación de usuarios a la Dirección de Tecnología.

5. POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

5.1. POLÍTICA DE RESPONSABILIDAD POR LOS ACTIVOS

La Organización como propietaria de la información física así como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen **el uso adecuado de la misma.**

La información, archivos físicos, los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y fases, entre otros) propiedad de la Organización, son activos de sus empresas y se proporcionan a Los empleados y proveedores autorizados, para cumplir con los propósitos del negocio.

Toda la información sensible de la Organización, así como los activos donde ésta se almacena y se procesa será asignada a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que dicte la GERENCIA DE GESTIÓN. Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas**.**

5.1.1. Medidas de responsabilidad por los activos

Medidas dirigidas a:

PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- Todos los directivos de la Organización actuaran como propietarias de la información física y electrónica de la entidad, ejerciendo así la facultad de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.
- Los propietarios de los activos de información deben generar un inventario de dichos activos para las áreas o procesos que lideran, acogiendo las indicaciones de las guías de clasificación de la información; así mismo, deben mantener actualizado el inventario de sus activos de información.
- Los propietarios de los activos de información deben monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información.
- Los propietarios de los activos de información deben ser conscientes que los recursos de procesamiento de información de la información, se encuentran sujetos a auditorías por parte de la GERENCIA DE GESTIÓN y a revisiones de cumplimiento por parte de la misma**.**

DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología es la propietaria de los activos de información correspondientes a la plataforma tecnológica de la Organización y, en consecuencia, debe asegurar su apropiada operación y administración. Y son quienes autorizan la instalación, cambio o eliminación de componentes de la plataforma tecnológica, previo aval de la gerencia general
- La Dirección de Tecnología debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.
- La Dirección de Tecnología es responsable de preparar las estaciones de trabajo fijas y/o portátiles de Los empleados y de hacer entrega de las mismas.
- La Dirección de Tecnología es responsable de recibir los equipos de trabajo fijo y/o portátil para su reasignación o disposición final, y generar copias de seguridad de la información de Los empleados que se retiran o cambian de labores, cuando les es formalmente solicitado.

GERENCIA DE GESTION

- La Gerencia de Gestión realizará un análisis de riesgos de seguridad de manera periódica, sobre los procesos de la Organización.
- La Gerencia de Gestión en acuerdo con la Gerencia General definirá las condiciones de uso y protección de los activos de información, tanto los tecnológicos como aquellos que no lo son.
- La Gerencia de Gestión realizará revisiones periódicas de los recursos de la plataforma tecnológica y los sistemas de información de la Organización.

DIRECTIVOS

- Los Directivos de la organización o quien ellos designen, deben autorizar a sus empleados el uso de los recursos tecnológicos, previamente preparados por la Dirección de Tecnología.
- Los Directivos de la Organización, o quien ellos designen, deben recibir los recursos tecnológicos asignados a sus colaboradores cuando estos se retiren de la organización son trasladados de área.

TODOS LOS USUARIOS

- Los recursos tecnológicos de la organización, deben ser utilizados de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen de la organización.
- Los recursos tecnológicos de la Organización provistos a empleados y/ o proveedores, son proporcionados con el único fin de llevar a cabo las labores de la Organización; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.
- Los empleados no deben utilizar sus equipos de cómputo y dispositivos móviles personales para desempeñar las actividades laborales.
- Los empleados no deben utilizar software no autorizado o de su propiedad en la plataforma tecnológica de la organización.
- Todas las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos son asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.

- En el momento de desvinculación o cambio de labores, los empleados deben realizar la entrega de su puesto de trabajo a su jefe o a quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

6. POLÍTICA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

La Organización definirá los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad, y generará una guía de Clasificación de la Información para que los propietarios de la misma la cataloguen y determinen los controles requeridos para su protección.

Toda la información de la Organización debe ser identificada, clasificada y documentada de acuerdo con las guías de Clasificación de la Información establecidas por la organización.

Una vez clasificada la información, la organización proporcionará los recursos necesarios para la aplicación de controles en busca de preservar la confidencialidad, integridad y disponibilidad de la misma, con el fin de promover el uso adecuado por parte de los empleados de la organización y proveedores que se encuentre autorizado y requiera de ella para la ejecución de sus actividades.

6.1. Medidas para la clasificación y manejo de la información

COMITÉ DE SEGURIDAD DE LA INFORMACION

El Comité de Seguridad de la Información (Conformado por la Gerencia General, la Gerencia de Gestión y el Coordinador de Gestión Documental recomendará los niveles de clasificación de la información propuestos por la Gerencia de Gestión y la guía de clasificación de la Información de Organización para que sean aprobados por la Junta Directiva.

Medidas dirigidas a:

GERENCIA DE GESTIÓN

- La GERENCIA DE GESTIÓN definirá los niveles de clasificación de la información para la organización y, posteriormente generará la guía de clasificación de la Información.
- La GERENCIA DE GESTIÓN socializará y divulgará la guía de clasificación de la Información a Los empleados de la Organización.
- La GERENCIA DE GESTIÓN monitoreará con una periodicidad establecida la aplicación de la guía de clasificación de la Información.

DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología proveerá los métodos de cifrado de la información, así como administrará el software o herramienta utilizado para tal fin.
- La Dirección de Tecnología debe efectuar la eliminación segura de la información, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son dados de baja o cambian de usuario.

DIRECCION DE TECNOLOGIA Y GERENCIA DE GESTIÓN

- La Dirección de Tecnología junto con la Gerencia de Gestión definirá los métodos de cifrado de la información de la Entidad de acuerdo al nivel de clasificación de los activo.

Medidas dirigidas a:

COORDINACION DE GESTION DOCUMENTAL

- La Coordinación de Gestión Documental debe utilizar los medios de los cuales está dotada para destruir o desechar correctamente la documentación física, con el fin de evitar la reconstrucción de la misma, acogiéndose a procedimiento establecido para tal fin.

- La Coordinación de Gestión Documental debe realizar la destrucción de información cuando se ha cumplido su tiempo de retención.

- La Coordinación de Gestión Documental debe administrar el contrato de almacenamiento y custodia de las cintas de backup, otros medios de almacenamiento y documentos físicos de la organización con el proveedor (Tial S.A.S.)

- La Coordinación de Gestión Documental verificará el cumplimiento de los Acuerdos de Niveles de Servicio (A.N.S) y Acuerdos de intercambio con el proveedor de custodia externo de los medios de almacenamiento y documentos de la organización.

PROPIETARIOS DE LA INFORMACIÓN

- Los propietarios de los activos de información deben clasificar su información de acuerdo con la guías de clasificación de la Información establecida.
- Los propietarios de los activos de información son responsables de monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar su re-clasificación.

TODOS LOS USUARIOS

- Los usuarios deben acatar los lineamientos guía de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la organización.
- La información física y digital debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de expiración, toda la información debe ser eliminada adecuadamente.
- Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias y envíes faxes: verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales;

asimismo, recoger de las impresoras, escáneres, fotocopiadoras y máquinas de fax, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.

- Tanto Los empleados como proveedores deben asegurarse que en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.
- La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo**.**

7. POLÍTICA DE USO DE PERIFERICOS Y MEDIOS DE ALMACENAMIENTO

El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica de la Organización será reglamentado por la Dirección de Tecnología, junto con la Gerencia de Gestión, considerando las labores realizadas por Los empleados y su necesidad de uso.

7.1. Medidas uso de periféricos y medios de almacenamiento

DIRECCION DE TECNOLOGIA Y GERENCIA DE GESTIÓN:

Medidas dirigidas a:

- La Dirección de Tecnología y la Gerencia de Gestión establecerán las condiciones de uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la organización.

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología implantará los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la organización, de acuerdo con los lineamientos y condiciones establecidas.

- La Dirección de Tecnología generará y aplicará lineamientos para la disposición segura de los medios de almacenamiento de la organización, ya sea cuando son dados de baja o re-asignados a un nuevo usuario.

GERENCIA GESTION

La GERENCIA GESTION, autorizará el uso de periféricos o medios de almacenamiento en la plataforma tecnológica de la Organización de acuerdo con el perfil del cargo del funcionario solicitante.

TODOS LOS USUARIOS

Los empleados y proveedores deben acoger las condiciones de uso de los periféricos y medios de almacenamiento establecidos por la Dirección de Tecnología.

Los Empleados y proveedores no deben modificar la configuración de periféricos y medios de almacenamiento establecidos por la Dirección de Tecnología.

Los empleados y proveedores son responsables por la custodia de los medios de almacenamiento institucionales asignados.

Los empleados y proveedores no deben utilizar medios de almacenamiento personales en la plataforma tecnológica de la Organización.

8. POLÍTICAS DE CONTROL DE ACCESO

8.1. POLÍTICA DE ACCESO A REDES Y RECURSOS DE RED

La Dirección de Tecnología, como responsable de las redes de datos y los recursos de red de la Organización, debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

8.1.1. Medidas de acceso a redes y recursos de red:

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA:

- La Dirección de Tecnología debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de la Organización
- La Dirección de Tecnología debe asegurar que las redes inalámbricas de la Organización cuenten con métodos de autenticación que evite accesos no autorizados.
- La Dirección de Tecnología, en conjunto con la GERENCIA GESTION, establecerá controles para la identificación y autenticación de los usuarios provistos por proveedores en las redes o recursos de red, y velará por la aceptación de las responsabilidades de dichos proveedores. Además, formalizará la aceptación de las Políticas de Seguridad de la Información por parte de estos.

Medidas dirigidas a:

GERENCIA GESTION

- Autorizará la creación o modificación de las cuentas de acceso a las redes o recursos de red
- Verificará periódicamente los controles de acceso para los usuarios provistos por proveedores, con el fin de revisar que dichos usuarios tengan acceso permitido únicamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.

TODOS LOS USUARIOS

- Los empleados y proveedores, antes de contar con acceso lógico por primera vez a la red de datos de la organización, contaran con el formato de creación de cuentas de usuario debidamente autorizado y el Acuerdo de Confidencialidad firmado previamente.
- Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de la Organización deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

8.2. POLÍTICA DE ADMINISTRACIÓN DE ACCESO DE USUARIOS

- La Organización establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la Organización. Así mismo, velará porque Los empleados y proveedores tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por Medidas y procedimientos establecidos para tal fin.

8.2.1. Medidas de administración de acceso de usuarios

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología establecerá un procedimiento formal para la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información de la Organización, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario.
- La Dirección de Tecnología, previa solicitud de los Jefes inmediatos de los solicitantes de las cuentas de usuario y aprobación tanto de los propietarios de los sistemas de información como de la GERENCIA GESTION, debe crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información administrados, acorde con el procedimiento establecido.

- La Dirección de Tecnología, en conjunto con la GERENCIA GESTION, definirán lineamientos para la configuración de contraseñas que aplicaran sobre la plataforma tecnológica, los servicios de red y los sistemas de información de la Organización; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.
- La Dirección de Tecnología establecerá un procedimiento que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando Los empleados se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.
- La Dirección de Tecnología se asegurará que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean inhabilitados o eliminados.

Medidas dirigidas a:

GERENCIA GESTION

- La **GERENCIA GESTION** autorizará la creación o modificación de las cuentas de acceso de los recursos tecnológicos y sistemas de información de la Organización.

- **Medidas dirigidas a:**

PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

- Es responsabilidad de los Propietarios de los activos de información, definir los perfiles de usuario y autorizar, conjuntamente con la GERENCIA GESTION, las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos.
- Los propietarios de los activos de información deben verificar y ratificar periódicamente todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

Medidas dirigidas a:

DIRECTIVOS

- Los Directivos de la Organización deben solicitar la creación, modificación, bloqueo y eliminación de cuentas de usuario, para Los empleados que laboran en sus áreas, acogiéndose al procedimiento establecidos para tal fin.

8.3. POLITICA DE RESPONSABILIDADES DE ACCESO DE LOS USUARIOS

Los usuarios de los recursos tecnológicos y los sistemas de información de la Organización realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.

8.3.1. Medidas de responsabilidades de acceso de los usuarios

Medidas dirigidas a:

TODOS LOS USUARIOS

- Todo funcionario de Organización Servicios y Asesorías debe poseer un usuario de acceso a la red, y su contraseña es de responsabilidad exclusiva del usuario. Es responsabilidad absoluta del usuario, el uso y buen funcionamiento de las herramientas de Hardware y/o Software que le han sido asignadas
- Las contraseñas asignadas a cada usuario para los diferentes aplicativos y servicios de la Organización Servicios y Asesorías son de responsabilidad exclusiva del trabajador a quien se haya adjudicado.
- El cambio de contraseña debe ser realizado por el usuario una vez esta sea asignada por el administrador del aplicativo o servicio, y debe ser realizado periódicamente.
- En el caso que no sea posible realizar el cambio por el usuario, el cambio de las contraseñas debe tramitarse ante el administrador del aplicativo o servicio, y su uso adecuado y custodia seguirá siendo responsabilidad exclusiva del usuario.

- No se debe almacenar usuarios y/o contraseñas en los navegadores utilizados para ingresar a páginas web y las demás aplicaciones, ya que es un riesgo de seguridad y cualquier incidente que se detecte es responsabilidad directa de la persona a quien se haya asignado el usuario.
- Las contraseñas asignadas a cada usuario para los diferentes aplicativos y servicios de la Organización Servicios y Asesorías son de responsabilidad exclusiva del trabajador a quien se haya adjudicado.
- El cambio de contraseña debe ser realizado por el usuario una vez esta sea asignada por el administrador del aplicativo o servicio, y debe ser realizado periódicamente.
- En el caso que no sea posible realizar el cambio por el usuario, el cambio de las contraseñas debe tramitarse ante el administrador del aplicativo o servicio, y su uso adecuado y custodia seguirá siendo responsabilidad exclusiva del trabajador.
- No se debe almacenar usuarios y/o contraseñas en los navegadores utilizados para ingresar a páginas web y las demás aplicaciones, ya que es un riesgo de seguridad y cualquier incidente que se detecte es responsabilidad directa de la persona a quien se haya asignado el usuario.
- Los usuarios de la plataforma tecnológica, los servicios de red y los sistemas de información de la Organización deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.
- Los empleados no deben compartir sus cuentas de usuario y contraseñas con otros empleados o con proveedores.
- Los empleados y proveedores que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información de la Organización deben acogerse a lineamientos para la configuración de contraseñas implantados por la Organización.

8.4. POLÍTICA DE USO DE ALTOS PRIVILEGIOS Y UTILITARIOS DE ADMINISTRACION

La Dirección de Tecnología de la Organización velará porque los recursos de la plataforma tecnológica y los servicios de red de la Organización sean operados y administrados en condiciones controladas y de seguridad, que permitan un monitoreo posterior de la actividad de los usuarios administradores, poseedores de los más altos privilegios sobre dichos plataforma y servicios.

8.4.1. Medidas de uso de altos privilegios y utilitarios de administración

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA, ADMINISTRADORES DE LOS RECURSOS TECNOLOGICOS Y SERVICIOS DE RED

- La Dirección de Tecnología otorgará los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos empleados designados para dichas funciones.
- La Dirección de Tecnología establecerá cuentas personalizadas con altos privilegios para cada uno de los administradores de los recursos tecnológicos, servicios de red y sistemas de información.
- La Dirección de Tecnología verificará que los administradores de los recursos tecnológicos y servicios de red no tengan acceso a sistemas de información en producción.
- La Dirección de Tecnología restringirá las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado, de acuerdo con las labores desempeñadas.
- La Dirección de Tecnología se asegurará que los usuarios o perfiles de usuario que traen por defecto los sistemas operativos, el firmware y las bases de datos sean suspendidos o renombrados en sus autorizaciones y que las contraseñas que traen por defecto dichos usuarios o perfiles sean modificadas.
- La Dirección de Tecnología establecerá los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información no tengan instalados en sus equipos de cómputo utilitarios que permitan accesos privilegiados a dichos recursos, servicios o sistemas.
- Los administradores de los recursos tecnológicos y servicios de red, empleados de la Dirección de Tecnología, no deben hacer uso de los utilitarios que permiten acceso a los sistemas operativos, firmware o conexión a las bases de datos para pasar por alto la seguridad de los sistemas de información alojados sobre la plataforma tecnológica de la Organización
- Los administradores de los recursos tecnológicos deben deshabilitar las funcionalidades o servicios no utilizados de los sistemas operativos, el firmware y las bases de datos. Se debe configurar el conjunto mínimo requerido de funcionalidades, servicios y utilitarios.
- La Dirección de Tecnología debe generar y mantener actualizado un listado de las cuentas administrativas de los recursos de la plataforma tecnológica.

Medidas dirigidas a:

GERENCIA GESTION

- La GERENCIA GESTION validará que las políticas de contraseñas establecidas sobre la plataforma tecnológica, los servicios de red y los sistemas de información son aplicables a los usuarios administradores; así mismo, debe verificar que el cambio de contraseña de los usuarios administradores acoja el procedimiento definido para tal fin.
- La GERENCIA GESTION revisará periódicamente la actividad de los usuarios con altos privilegios en los registros de auditoría de la plataforma tecnológica y los sistemas de información.

8.5. POLÍTICA DE CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS

Los directivos de la Organización como propietarias de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.

La Dirección de Tecnología, como responsable de la administración de dichos sistemas de información y aplicativos, propenderá para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, velará porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

8.5.1. Medidas de control de acceso a sistemas y aplicativos

Medidas dirigidas a

PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

- Los propietarios de los activos de información autorizaran los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.
- Los propietarios de los activos de información monitorearan periódicamente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología establecerá un procedimiento para la asignación de accesos a los sistemas y aplicativos de la Organización.
- La Dirección de Tecnología establecerá ambientes separados a nivel físico y lógico para desarrollo, pruebas y producción, contando cada uno con su plataforma, servidores,

aplicaciones, dispositivos y versiones independientes de los otros ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.

- La Dirección de Tecnología asegurará, mediante los controles necesarios, que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción, y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.
- La Dirección de Tecnología establecerá el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, se asegurará que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
- La Dirección de Tecnología proporcionará repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.

Medidas dirigidas a:

DESARROLLADORES (INTERNOS Y EXTERNOS)

- Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.
- Los desarrolladores deben certificar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.
- Los desarrolladores deben certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.
- Los desarrolladores deben establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.
- Los desarrolladores deben asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como deben deshabilitar la funcionalidad de recordar campos de contraseñas. Los desarrolladores deben certificar que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.
- Los desarrolladores deben asegurar que si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico previamente registradas en los aplicativos, los cuales deben tener un periodo de validez establecido; se deben forzar el cambio de las contraseñas temporales después de su utilización.
- Los desarrolladores deben certificar que el último acceso (fallido o exitoso) sea reportado al usuario en su siguiente acceso exitoso a los sistemas de información.
- Los desarrolladores deben asegurar la re-autenticación de los usuarios antes de la realización de operaciones críticas en los aplicativos.
- Los desarrolladores deben, a nivel de los aplicativos, restringir acceso a archivos u otros recursos, a direcciones URL protegidas, a funciones protegidas, a servicios, a información de las aplicaciones, a atributos y políticas utilizadas por los controles de acceso y a la información relevante de la configuración, solamente a usuarios autorizados.

- Los desarrolladores deben establecer que periódicamente se re-valide la autorización de los usuarios en los aplicativos y se asegure que sus privilegios no han sido modificados.

9. POLÍTICAS DE CRIPTOGRAFIA

9.1. POLÍTICA DE CONTROLES CRIPTOGRAFICOS

La Organización velará porque la información de la Organización, clasificada como reservada o restringida, será cifrada al momento de almacenarse y/o transmitirse por cualquier medio.

9.1.1. Medidas de controles criptográficos

Medidas dirigidas a:

- La Dirección de Tecnología debe almacenará y/o transmitirá la información digital clasificada como reservada o restringida bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.
- La Dirección de Tecnología debe verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información reservada o restringida, cuente con mecanismos de cifrado de datos.
- La Dirección de Tecnología debe desarrollar y establecer un procedimiento para el manejo y la administración de llaves de cifrado.
- La Dirección de Tecnología, debe desarrollar y establecer estándares para la aplicación de controles criptográficos.

Medidas dirigidas a:

DESARROLLADORES (INTERNOS O EXTERNOS)

- Los desarrolladores deben cifrar la información reservada o restringida y certificar la confiabilidad de los sistemas de almacenamiento de dicha información.
- Los desarrolladores deben asegurarse que los controles criptográficos de los sistemas construidos cumplen con los estándares establecidos por la Dirección de Tecnología.

10. POLÍTICAS DE SEGURIDAD FISICA Y MEDIOAMBIENTAL

10.1. POLÍTICA DE AREAS SEGURAS

La Organización proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus sedes. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideras áreas de acceso restringido.

10.1.1. Medidas de áreas seguras

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA

- Las solicitudes de acceso al centro de cómputo o a los centros de cableado serán aprobadas por empleados de la Dirección de Tecnología autorizados; no obstante, los visitantes siempre deberán estar acompañados de un funcionario de dicha dirección durante su visita al centro de cómputo o los centros de cableado.
- La Dirección de Tecnología registrará el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia, en una bitácora ubicada en la entrada de estos lugares de forma visible.
- La Dirección de Tecnología descontinuará o modificará de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.
- La Dirección de Tecnología proveerá las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.
- La Dirección de Tecnología velará porque los recursos de la plataforma tecnológica de la Organización ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas.
- La Dirección de Tecnología certificará que el centro de cómputo y los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
- La Dirección de Tecnología asegurará que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, llevará control de la programación de los mantenimientos preventivos.

Medidas dirigidas a:

DIRECTIVOS DE LA ORGANIZACIÓN

- Los Directivos de la Organización que se encuentren en áreas restringidas velaran mediante monitoreo por la efectividad de los controles de acceso físico y equipos de vigilancia implantados en su áreas.
- Los Directivos de la Organización que se encuentren en áreas restringidas autorizaran cualquier ingreso temporal a sus áreas, evaluando la pertinencia del ingreso; así mismo, delegaran al personal del área el registro y supervisión de cada ingreso a sus áreas.
- Los Directivos de la Organización velaran porque las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a sus áreas solo sean utilizadas por Los empleados autorizados y, salvo situaciones de emergencia u otro tipo de eventos que por su naturaleza lo requieran, estos no sean transferidos a otros empleados de la Organización.

Medidas dirigidas a:

GERENCIAS REGIONALES – RECURSOS FISICOS

- Las Gerencias regionales proporcionaran los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones de la Organización.
- Las Gerencias Regionales identificaran mejoras a los mecanismos implantados y, de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones de la Organización.
- Las Gerencias Regionales almacenaran y custodiar los registros del sistema de control de acceso a las instalaciones de la Organización.
- Las Gerencias Regionales certificaran la efectividad de los mecanismos de seguridad física y control de acceso al centro de cómputo, centros de cableado y demás áreas de procesamiento de información.
- Las Gerencias Regionales controlaran el ingreso de los visitantes a los centros de cableado que están bajo su custodia.
- Las Gerencias Regionales se cercioraran de que los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
- Las Gerencias Regionales, con el acompañamiento de la Dirección de Tecnología, deben verificar que el cableado se encuentra protegido con el fin de disminuir las intercepciones o daños.

Medidas dirigidas a:

TODOS LOS USUARIOS

- Los ingresos y egresos de personal a las instalaciones de la Organización deben ser registrados; por consiguiente, Los empleados y proveedores deben cumplir completamente con los controles físicos implantados.

- Los empleados deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de la Organización; en caso de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible.
- Aquellos empleados o proveedores para los que aplique, en razón del servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.
- Empleados y proveedores no deben intentar ingresar a áreas a las cuales no tengan autorización.

10.2. POLÍTICA DE SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES

La Organización para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la Organización que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

10.2.1. Medidas de seguridad para los equipos institucionales

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA:

- La Dirección de Tecnología proveerá los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de la Organización. La Dirección de Tecnología realizará mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la Organización.
- La Dirección de Tecnología, en conjunto con las Gerencias Regionales propenderá porque las áreas de carga y descarga de equipos de cómputo se encuentren aisladas del centro de cómputo y otras áreas de procesamiento de información.
- La Dirección de Tecnología generará estándares de configuración segura para los equipos de cómputo de Los empleados de la Organización y configurar dichos equipos acogiendo los estándares generados.
- La Dirección de Tecnología establecerá las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos de la Organización y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.
- La Dirección de Tecnología aislará los equipos de áreas sensibles, como la Dirección de Tesorería para proteger su acceso de los demás empleados de la red de la empresa.

La Dirección de Tecnología generará y aplicar lineamientos para la disposición segura de los equipos de cómputo de Los empleados de la Organización, ya sea cuando son dados de baja o cambian de usuario.

Medidas dirigidas a:

GERENCIA DE GESTION

- La GERENCIA DE GESTION tiene la responsabilidad de incluir dentro del plan anual de auditorías la verificación aleatoria a los equipos de cómputo de todas las dependencias y puntos de atención de la entidad.
- La GERENCIA GESTION debe evaluar y analizar los informes de verificación de equipos de cómputo de las diferentes áreas de la Organización, en particular de las áreas sensibles.

Medidas dirigidas a:

GERENCIAS REGIONALES:

- Las Gerencias Regionales revisaran los accesos físicos en horas no hábiles a las áreas donde se procesa información.
- Las Gerencias Regionales restringirán el acceso físico a los equipos de cómputo de áreas donde se procesa información sensible.
- Las Gerencias Regionales velaran porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos institucionales de las instalaciones de la Organización cuente con la autorización documentada y aprobada previamente por el Gerente Regional.
- Las Gerencias Regionales velaran porque los equipos que se encuentran sujetos a traslados físicos fuera de la Organización, posean pólizas de seguro.

Medidas dirigidas a:

TODOS LOS USUARIOS

- La Dirección de Tecnología es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de la Organización.
- Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a Los empleados y proveedores deben acoger las instrucciones técnicas de proporcione la Dirección de Tecnología.
- Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico propiedad de la Organización el usuario responsable debe informar a la Mesa de Ayuda en donde se atenderá o escalará al interior de la Dirección de Tecnología, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.
- La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la Organización, solo puede ser realizado por Los empleados de la Dirección de Tecnología, o por el proveedor autorizado por dicha dirección.
- Los empleados de la Organización y proveedores deben bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo.
- Empleados y proveedores no deben dejar encendidas las estaciones de trabajo u otros recursos tecnológicos en horas no laborables.

- Los equipos de cómputo, bajo ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.
- Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.
- Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.
- En caso de pérdida o robo de un equipo de cómputo de la Organización, se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.
- Los empleados de la Organización y proveedores deben asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

11. POLITICAS DE SEGURIDAD EN LAS OPERACIONES

11.1. POLÍTICA DE ASIGNACIÓN DE RESPONSABILIDADES OPERATIVAS

La Dirección de Tecnología, encargada de la operación y administración de los recursos tecnológicos que apoyan los procesos de la Organización, asignará funciones específicas a sus empleados, quienes deben efectuar la operación y administración de dichos recursos tecnológicos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de las actividades. Así mismo, velará por la eficiencia de los controles implantados en los procesos operativos asociados a los recursos tecnológicos con el objeto de proteger la confidencialidad, la integridad y la disponibilidad de la información manejada y asegurará que los cambios efectuados sobre los recursos tecnológicos, serán adecuadamente controlados y debidamente autorizados.

La Dirección de Tecnología proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información de la Organización, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica con una periodicidad definida.

11.1.1. Medidas de asignación de responsabilidades operativas

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología efectuará, a través de sus empleados, la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica de la Organización.

- La Dirección de Tecnología proporcionará a sus empleados manuales de configuración y operación de los sistemas operativos, firmware, servicios de red, bases de datos y sistemas de información que conforman la plataforma tecnológica de la Organización.
- La Dirección de Tecnología proveerá los recursos necesarios para la implantación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de desarrollo y producción, la inexistencia de compiladores, editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.
- La Dirección de Tecnología, a través de sus empleados, realizará estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados (capacity planning) de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica. Estos estudios y proyecciones deben considerar aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, anchos de banda, internet y tráfico de las redes de datos, entre otros.

Medidas dirigidas a:

GERENCIA GESTION

- La GERENCIA GESTION debe emitir concepto y generar recomendaciones acerca de las soluciones de seguridad seleccionadas para la plataforma tecnológica de la Organización.

11.2. POLÍTICA DE PROTECCIÓN FRENTE A VIRUS:

La Organización proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso (virus). Además, proporcionará los mecanismos para generar cultura de seguridad entre sus empleados y proveedores frente a los ataques de software malicioso.

11.2.1. Medidas de protección frente a VIRUS

Medidas dirigidas a:

DIRECCIÓN DE TECNOLOGIA

- La Dirección de Tecnología proveerá herramientas tales como antivirus, antimalware, anti spam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de la Organización y los servicios que se ejecutan en la misma.
- La Dirección de Tecnología asegurará que el software de antivirus, antimalware, anti spam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.

- La Dirección de Tecnología certificará que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.
- La Dirección de Tecnología, a través de sus empleados, se asegurará que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, anti spam, antimalware.
- La Dirección de Tecnología, a través de sus empleados, debe certificar que el software de antivirus, antispyware, anti spam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.

Medidas dirigidas a:

TODOS LOS USUARIOS

- Es responsabilidad absoluta del usuario, el uso y buen funcionamiento de las herramientas de software que le han sido asignadas.
- Ningún funcionario puede tener en su poder instaladores de programas licenciados o producidos por Organización Servicios y Asesorías a menos que sean autorizados por la Jefatura de Tecnología Informática y Comunicaciones.
- Está terminantemente prohibido instalar cualquier tipo de software sin el consentimiento expreso del departamento de Tecnología Informática y Comunicaciones y siempre teniendo en cuenta el esquema y la cantidad de licencias disponibles para los diferentes aplicativos utilizados en Organización Servicios y Asesorías
- Todo empleado que copie software ilegalmente cometerá falta grave y quedara sujeto a sanción disciplinaria por la Empresa. Todo empleado que copie software ilegalmente para entregarlo a terceros, incluyendo clientes, también estará cometiendo falta grave y quedará sujeto a sanción disciplinaria por la Empresa.
- Todo equipo dentro de la red de Organización Servicios y Asesorías, independientemente del propietario del activo, deberá tener licenciamiento adecuado referente todo Software instalado en él (Sistema Operativo, Herramienta Ofimática, Antivirus, Compresores, etc.) y tener su soporte de licenciamiento. Si alguno de los trabajadores está utilizando elementos propios en la infraestructura de la Organización, deberá diligenciar y firmar el documento de responsabilidad sobre uso de licencias de software excluyendo a Organización Servicios y Asesorías de cualquier acción legal o jurídica respecto a licenciamiento de Software. Si el trabajador no puede demostrar la legalidad del software instalado en su equipo dentro de las instalaciones de la organización, no podrá utilizarlo con los recursos de TI de la Organización.
- La Empresa no permitirá que empleado alguno realice copias no autorizadas de software.
- Los usuarios de recursos tecnológicos no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, anti spam definida por la Dirección de Tecnología; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.
- Los usuarios de recursos tecnológicos deben ejecutar el software de antivirus, antispyware, anti spam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico. Los usuarios deben asegurarse que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.

- Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar a la Mesa de Ayuda, para que a través de ella, la Dirección de Tecnología tome las medidas de control correspondientes.

11.3. POLÍTICA DE COPIAS DE RESPALDO DE LA INFORMACIÓN

La Organización certificará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades. Las áreas propietarias de la información, con el apoyo de la Dirección de Tecnología, encargada de la generación de copias de respaldo, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.

De otra parte la Organización velará porque los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

11.3.1. Medidas de copias de respaldo de la información

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología, a través de sus empleados, generara y adoptará los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.
- La Dirección de Tecnología dispondrá de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.
- La Dirección de Tecnología, a través de sus empleados, llevará a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario. La Dirección de Tecnología debe definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.
- La Dirección de Tecnología proporcionará apoyo para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de la los activos información de la Organización.

Medidas dirigidas a:

PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- Los propietarios de los recursos tecnológicos y sistemas de información definirán, en conjunto con la Dirección de Tecnología, las estrategias para la generación, retención y rotación de las copias de respaldo de los activos de información.

Medidas dirigidas a:

TODOS LOS USUARIOS

- Es responsabilidad de los usuarios de la plataforma tecnológica de la Organización identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

11.4. POLÍTICA DE REGISTRO DE EVENTOS Y MONITOREO DE LOS RECURSOS TECNOLÓGICOS Y LOS SISTEMAS DE INFORMACIÓN

- La Organización realizará monitoreo permanente del uso que dan Los empleados y proveedores a los recursos de la plataforma tecnológica y los sistemas de información de la Organización. Además, velará por la custodia de los registros de auditoría cumpliendo con los periodos de retención establecidos para dichos registros.
- La Dirección de Tecnología y la GERENCIA GESTION definirán la realización de monitoreo de los registros de auditoria sobre los aplicativos donde se opera los procesos misionales de la Organización. El Comité de revisión de logs mensualmente se reunirá a analizar los resultados del monitoreo efectuado.

11.4.1. Medidas de registro de eventos y monitoreo de los recursos tecnológicos y los sistemas de información

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA Y GERENCIA GESTION

- La Dirección de Tecnología, en conjunto con la GERENCIA GESTION, debe determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información de la Organización.
- La Dirección de Tecnología y la GERENCIA GESTION, revisará logs, deben definir de manera mensual cuáles monitoreos se realizarán de los registros de auditoria sobre los aplicativos donde se opera los procesos misionales de la Organización. Así mismo, se deben reunir para analizar los resultados de cada monitoreo efectuado.

- La Dirección de Tecnología, a través de sus empleados, habilitará los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con los eventos a auditar establecidos.
- La Dirección de Tecnología certificará la integridad y disponibilidad de los registros de auditoria generados en la plataforma tecnológica y los sistemas de información de la Organización. Estos registros deben ser almacenados y solo deben ser accedidos por personal autorizado.

Medidas dirigidas a:

GERENCIA DE GESTIÓN:

- La GERENCIA DE GESTION debe determinar los periodos de retención de los registros (logs) de auditoria de los recursos tecnológicos y los sistemas de información de la Organización.
- La GERENCIA DE GESTION debe revisar periódicamente los registros de auditoria de la plataforma tecnológica y los sistemas de información con el fin de identificar brechas de seguridad y otras actividades propias del monitoreo.

Medidas dirigidas a:

DESARROLLADORES (INTERNOS Y EXTERNOS)

- Los desarrolladores deben generar registros (logs) de auditoría de las actividades realizadas por los usuarios finales y administradores en los sistemas de información desarrollados. Se deben utilizar controles de integridad sobre dichos registros.
- Los desarrolladores deben registrar en los logs de auditoría eventos como: fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, entre otros, de acuerdo con las directrices establecidas por la Dirección de Tecnología y la GERENCIA GESTION. Los desarrolladores deben evitar almacenar datos innecesarios de los sistemas construidos en los logs de auditoría que brinden información adicional a la estrictamente requerida.

11.5. POLITICA DE CONTROL AL SOFTWARE OPERATIVO

La Organización, a través de la Dirección de Tecnología, designará responsables y establecerá procedimientos para controlar la instalación de software operativo, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software operativo es actualizado.

11.5.1. Medidas de control al software operativo

Medidas dirigidas a:

DIRECCIÓN DE TECNOLOGIA

- La Dirección de Tecnología se asegurará que el software operativo instalado en la plataforma tecnológica de la Organización cuente con soporte de los proveedores.
- La Dirección de Tecnología establecerá responsabilidades y procedimientos para controlar la instalación del software operativo, que interactúen con el procedimiento de control de cambios existente en la organización.

- La Dirección de Tecnología se asegurará que el software operativo instalado en la plataforma tecnológica de la Organización cuente con soporte de los proveedores.
- La Dirección de Tecnología concederá accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.
- La Dirección de Tecnología validará los riesgos que genera la migración hacia nuevas versiones del software operativo. Se debe asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.
- La Dirección de Tecnología establecerá las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo de la Organización.

11.5.2. Medidas para la gestión de vulnerabilidades

Medidas dirigidas a:

GERENCIA GESTION

- La GERENCIA GESTION adelantará los trámites correspondientes para la realización de pruebas de vulnerabilidades y hacking ético con una periodicidad establecida, por un ente independiente al área objeto de las pruebas, con el fin de garantizar la objetividad del desarrollo de las mismas.
- La GERENCIA GESTION generará los lineamientos y recomendaciones para la mitigación de vulnerabilidades, resultado de las pruebas de vulnerabilidades y hacking ético.

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología revisará periódicamente la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de prevenir la exposición al riesgo de estos.
- La Dirección de Tecnología, a través de sus empleados, debe generar y ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA Y GERENCIA GESTION

La Dirección de Tecnología y la GERENCIA GESTION, a través del Comité de vulnerabilidades, revisaran, valoraran, y gestionaran las vulnerabilidades técnicas encontradas, apoyándose en herramientas tecnológicas para su identificación.

12. POLÍTICAS DE SEGURIDAD EN LAS COMUNICACIONES

12.1. POLÍTICA DE GESTION Y ASEGURAMIENTO DE LAS REDES DE DATOS

La Organización establecerá, a través de la Dirección de Tecnología, los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.

De igual manera, propenderá por el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información reservada y restringida de la Organización.

12.1.1. Medidas de gestión y aseguramiento de las redes de datos

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología adoptará medidas para asegurar la disponibilidad de los recursos y servicios de red de la Organización.
- La Dirección de Tecnología implantará controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.
- La Dirección de Tecnología mantendrá las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para el organización.
- La Dirección de Tecnología identificará los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios de red, cuando estos se contraten externamente.
- La Dirección de Tecnología establecerá los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica de la Organización, acogiendo buenas prácticas de configuración segura.
- La Dirección de Tecnología, a través de sus empleados, identificará, justificará y documentará los servicios, protocolos y puertos permitidos por la Organización en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.
- La Dirección de Tecnología debe instalar protección entre las redes internas de la Organización y cualquier red externa, que este fuera de la capacidad de control y administración de la Organización.
- La Dirección de Tecnología velará por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos de la organización.

12.2. POLÍTICA DE USO DEL CORREO ELECTRONICO

La Organización, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre empleados, clientes, proveedores, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

12.2.1. Medidas de uso del correo electrónico

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA Y GERENCIA GESTION

- La Dirección de Tecnología generará y divulgará un procedimiento para la administración de cuentas de correo electrónico.
- La Dirección de Tecnología diseñará y divulgará las directrices técnicas para el uso de los servicios de correo electrónico.
- La Dirección de Tecnología proveerá un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico.
- La Dirección de Tecnología establecerá procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.
- La Dirección de Tecnología, con el apoyo de la GERENCIA GESTION, generará campañas para concientizar tanto a Los empleados internos, como proveedores, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio del correo electrónico.

Medidas dirigidas a:

TODOS LOS USUARIOS

- La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario de la Organización, cliente o proveedor, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya. El usuario es la única persona autorizada para leer su cuenta de correo electrónico corporativo, a menos que él mismo autorice explícitamente a otra persona para hacerlo, o bien, que su cuenta esté involucrada en un incidente de seguridad o proceso administrativo. Es responsabilidad exclusiva del usuario el correcto uso de la cuenta de correo corporativa.
- Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional de la Organización. La cuenta de correo corporativa únicamente debe ser utilizada para las comunicaciones internas de Organización Servicios y Asesorías y las comunicaciones externas a las que sean necesarias para cumplir con el perfil del cargo del usuario. El correo institucional no debe ser utilizado para actividades personales.

- Los mensajes y la información contenida en los buzones de correo son propiedad de la Organización y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

- Los usuarios de correo electrónico institucional tienen prohibido él envió de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para Los empleados de la Organización y proveedores.
- No es permitido el envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.
- Los programas malignos (MalWare) y el SPAM (Correo electrónico no deseado) ingresados a las redes de Organización Servicios y Asesorías son de responsabilidad absoluta del usuario a la que corresponde la cuenta de correo.
- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por la Organización y deben conservar en todos los caso.
- El mensaje legal corporativo de confidencialidad.
- La creación de la cuenta de correo electrónico corporativa de usuario debe hacerse expresamente por el director del departamento o unidad o área al cual el usuario esta adscrito y autorizada por la Gerencia Administrativa o en su defecto la Jefatura de Tecnología Informática y Comunicaciones.
- El uso del correo electrónico está ligado a el uso del software antivirus licenciado por la Organización Servicios y Asesorías Esta terminantemente prohibido utilizar clientes de correo electrónico sin tener activado el software antivirus.

12.3. POLÍTICA DE USO ADECUADO DE INTERNET

La Organización consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias.

12.3.1. Medidas de uso adecuado de internet

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología proporcionará los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.
- La Dirección de Tecnología diseñará e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
- La Dirección de Tecnología monitoreará continuamente el canal o canales del servicio de Internet.

- La Dirección de Tecnología establecerá procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.
- La Dirección de Tecnología generará registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.

Medidas dirigidas a:

GERENCIA GESTION

La GERENCIA GESTION generará campañas para concientizar tanto a Los empleados internos, como a proveedores, respecto a las precauciones que deben tener en cuenta cuando utilicen el servicio de Internet.

Medidas dirigidas a:

TODOS LOS USUARIOS

- Los usuarios del servicio de Internet de la Organización deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.
- Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.
- No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.
- Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN, Yahoo, Sype, Net2phome y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio de la Organización.
- No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el jefe respectivo y la Dirección de Tecnología, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.
- No está permitido el intercambio no autorizado de información de propiedad de la Organización, de sus clientes y/o de sus empleados, con terceros.
- Todo empleado que entregue Datos de la empresa a terceros sin el previo conocimiento y aprobación de las gerencias, estará cometiendo falta grave y quedará sujeto a sanción disciplinaria por la Empresa y las acciones legales que corresponda.

12.4. POLÍTICA DE INTERCAMBIO DE INFORMACIÓN

La Organización asegurará la protección de la información en el momento de ser transferida o intercambiada con otras entidades y establecerá los procedimientos y controles necesarios para el intercambio de información; así mismo, se establecerán Acuerdos de Confidencialidad y/o de Intercambio de Información con los proveedores con quienes se realice dicho intercambio. El organización propenderá por el uso de tecnologías informáticas y de telecomunicaciones para llevar a cabo el intercambio de información; sin embargo, establecerá directrices para el intercambio de información en medio físico.

12.4.1. Medidas de intercambio de información

Medidas dirigidas a:

PROCESO JURIDICO – GERENCIA DE GESTION- PROCESO DE CONTRATACION

- El **Proceso Jurídico - Gerencia de Gestión - Proceso Contratación**, en acompañamiento con la GERENCIA GESTION, definirá los modelos de Acuerdos de Confidencialidad y/o de Intercambio de Información entre el organización y tercera partes incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos. Entre los aspectos a considerar se debe incluir la prohibición de divulgar la información entregada por la Organización a los terceros con quienes se establecen estos acuerdos y la destrucción de dicha información una vez cumpla su cometido.
- El **Proceso Jurídico - Gerencia de Gestión - Proceso Contratación** establecerá en los contratos que se establezcan con proveedores, los Acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de información de beneficiarios de la Organización que les ha sido entregada en razón del cumplimiento de los objetivos misionales de la Organización.

Medidas dirigidas a:

GERENCIA GESTION

- La GERENCIA GESTION definirá y establecerá el procedimiento de intercambio de información con los diferentes terceros que, hacen parte de la operación de la Organización, reciben o envían información de los beneficiarios de la Organización, que contemple la utilización de medios de transmisión confiables y la adopción de controles, con el fin de proteger la confidencialidad e integridad de la misma.
- La GERENCIA GESTION velará porque el intercambio de información de la Organización con entidades externas se realice en cumplimiento de las Políticas de seguridad para el intercambio de información aquí descritas, los Acuerdos de Intercambio de Información y el procedimiento definido para dicho intercambio de información.

- La GERENCIA GESTION autorizará el establecimiento del vínculo de transmisión de información con proveedores, para que posteriormente las áreas funcionales realicen las actividades de transmisión requeridas en cada caso.

Medidas dirigidas a:

PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

- Los propietarios de los activos de información velarán porque la información de la Organización o de sus beneficiarios sea protegida de divulgación no autorizada por parte de los terceros a quienes se entrega esta información, verificando el cumplimiento de las clausulas relacionadas en los contratos, Acuerdos de confidencialidad o Acuerdos de intercambio establecidos.
- Los propietarios de los activos de información aseguraran que los datos requeridos de los beneficiarios sólo puedan ser entregada a terceros, previo consentimiento de los titulares de los mismos, salvo en los casos que lo disponga una ley o sea una solicitud de los entes de control.
- Los propietarios de los activos de información, o a quien ellos deleguen, verificaran que el intercambio de información con terceros deje registro del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.
- Los propietarios de los activos de información autorizaran los requerimientos de solicitud/envío de información de la Organización por/a proveedores, salvo que se trate de solicitudes de entes de control o de cumplimiento de la legislación vigente.
- Los propietarios de los activos de información se aseguraran que el Intercambio de información (digital) solamente se realice si se encuentra autorizada y dando cumplimiento a las Políticas de administración de redes, de acceso lógico y de protección de datos personales de la Organización así como del procedimiento de intercambio de información.
- Los propietarios de los activos de información verificará la destrucción de la información suministrada a los terceros, realizada por ellos una vez esta ha cumplido el cometido por el cual fue enviada.

Medidas dirigidas a:

GERENCIA DE GESTIÓN

- La GERENCIA DE GESTION acogerá el procedimiento para el intercambio, de información (medios de almacenamiento y documentos) con proveedores y la adopción de controles a fin de proteger la información sensible contra divulgación, pérdida o modificaciones.
- La GERENCIA DE GESTIÓN certificará que todo envió de información física a terceros (documento o medio magnético) utilice únicamente los servicios de transporte o servicios de mensajería autorizados por la Organización, y que estos permitan ejecutar rastreo de las entregas.

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología ofrecerá servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de información, que permitan el cumplimiento del procedimiento para el intercambio de información (digital o medio

magnético), con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.

Medidas dirigidas a:

TERCEROS CON QUIENES SE INTERCAMBIA INFORMACION DE LA ORGANIZACIÓN

- Los terceros con quienes se intercambia información De la Organización deben darle manejo adecuado a la información recibida, en cumplimiento de las Políticas de seguridad de la Organización, de las condiciones contractuales establecidas y del Procedimiento de intercambio de información.
- Los terceros con quienes se intercambia información de la Organización deben destruir de manera segura la información suministrada, una vez esta cumpla con la función para la cual fue enviada y demostrar la realización de las actividades de destrucción.

Medidas dirigidas a:

TODOS LOS USUARIOS:

- Los usuarios no deben utilizar el correo electrónico como medio para enviar o recibir información sensible de la Organización o de sus beneficiarios.
- No está permitido el intercambio de información sensible de la Organización por vía telefónica.

13. POLÍTICA DE GESTIÓN DE VULNERABILIDADES

La Organización, a través de la Dirección de Tecnología y la GERENCIA GESTION, revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de plataforma tecnológica por medio de la realización periódica de pruebas de vulnerabilidades, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas. Estas dos áreas conforman en Comité de vulnerabilidades encargado de revisar, valorar y gestionar las vulnerabilidades técnicas encontradas.

13.1. Medidas para la gestión de vulnerabilidades

Medidas dirigidas a:

GERENCIA GESTION

- La GERENCIA GESTION adelantará los trámites correspondientes para la realización de pruebas de vulnerabilidades y hacking ético con una periodicidad establecida, por un ente independiente al área objeto de las pruebas, con el fin de garantizar la objetividad del desarrollo de las mismas.
- La GERENCIA GESTION generará los lineamientos y recomendaciones para la mitigación de vulnerabilidades, resultado de las pruebas de vulnerabilidades y hacking ético.

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología revisará periódicamente la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de prevenir la exposición al riesgo de estos.
- La Dirección de Tecnología, a través de sus empleados, generará y ejecutará o monitoreará planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA Y GERENCIA GESTION

- La Dirección de Tecnología y la GERENCIA GESTION, a través del Comité de vulnerabilidades, revisará, valorará y gestionará las vulnerabilidades técnicas encontradas, apoyándose en herramientas tecnológicas para su identificación.

14. POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

14.1. POLÍTICA PARA EL ESTABLECIMIENTO DE REQUISITOS DE SEGURIDAD

La Organización asegurará que el software adquirido y desarrollado tanto al interior de la Organización, como por proveedores, cumplirá con los requisitos de seguridad y calidad establecidos por él. Las áreas propietarias de sistemas de información, la Dirección de Tecnología y la GERENCIA GESTION incluirán requisitos de seguridad en la definición de requerimientos y, posteriormente se asegurarán que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.

14.1.1. Medidas para el establecimiento de requisitos de seguridad

Medidas dirigidas a:

PROPIETARIOS DE LOS SISTEMAS DE INFORMACIÓN, DIRECCION DE TECNOLOGIA Y GERENCIA GESTION

- Todos los sistemas de información o desarrollos de software deben tener un área propietaria dentro de la Organización formalmente asignada.
- La Dirección de Tecnología establecerá metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.
- Los procesos propietarios de los sistemas de información, en acompañamiento con la Dirección de Tecnología y la GERENCIA GESTION establecerán las especificaciones de adquisición o

desarrollo de sistemas de información, considerando requerimientos de seguridad de la información.

- Los procesos propietarios de los sistemas de información definirán qué información sensible puede ser eliminada de sus sistemas y solicitar que estos soporten la eliminación de dicha información, como es el caso de los datos personales o financieros, cuando estos ya no son requeridos.
- La GERENCIA GESTION liderará la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.

Medidas dirigidas a:

DESARROLLADORES (INTERNOS O EXTERNOS)

- Los desarrolladores documentaran los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.
- Los desarrolladores certificaran que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas y reconocidas en el mercado.
- Los desarrolladores deshabilitaran las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.
- Los desarrolladores establecerán el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.
- Los desarrolladores aseguraran que no se permitan conexiones recurrentes a los sistemas de información construidos con el mismo usuario.
- Los desarrolladores utilizaran usar los protocolos sugeridos por la Dirección de Tecnología y la GERENCIA GESTION en los aplicativos desarrollados.
- Los desarrolladores certificaran la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros.

14.2. POLÍTICA DE DESARROLLO SEGURO, REALIZACION DE PRUEBAS Y SOPORTE DE LOS SISTEMAS

La Organización velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por la Organización.

14.2.1. Medidas de desarrollo seguro, realización de pruebas y soporte de los sistemas

Medidas dirigidas a:

PROPIETARIOS DE LOS SISTEMAS DE INFORMACIÓN

- Los propietarios de los sistemas de información son responsables de realizar las pruebas para asegurar que cumplen con los requerimientos de seguridad establecidos antes del paso a

producción de los sistemas, utilizando metodologías establecidas para este fin, documentado las pruebas realizadas y aprobando los pasos a producción. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.

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

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología implantará los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.
- La Dirección de Tecnología contará con sistemas de control de versiones para administrar los cambios de los sistemas de información de la Organización.
- La Dirección de Tecnología asegurará que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
- La Dirección de Tecnología generará metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación
- La Dirección de Tecnología, a través de sus empleados, se asegurará que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.
- La Dirección de Tecnología incluirá dentro del procedimiento y los controles de gestión de cambios el manejo de los cambios en el software aplicativo y los sistemas de información de la Organización.

Medidas dirigidas a:

DESARROLLADORES (INTERNOS O EXTERNOS)

- Los desarrolladores de los sistemas de información considerarán las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.
- Los desarrolladores deben proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el software aplicativo de la Organización; dicho soporte debe contemplar tiempos de respuesta aceptables.
- Los desarrolladores construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.
- Los desarrolladores se aseguraran que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.

- Los desarrolladores suministraran opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.
- Los desarrolladores aseguraran el manejo de operaciones sensibles o críticas en los aplicativos desarrollados permitiendo el uso de dispositivos adicionales como tokens o el ingreso de parámetros adicionales de verificación.
- Los desarrolladores aseguraran que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.
- Los desarrolladores garantizaran que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.
- Los desarrolladores removerán todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.
- Los desarrolladores deben prevenir la revelación de la estructura de directorios de los sistemas de información construidos.
- Los desarrolladores removerán información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
- Los desarrolladores evitaran incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.
- Los desarrolladores certificaran el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.
- Los desarrolladores desarrollaran los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.
- Los desarrolladores protegerán el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.
- Los desarrolladores asegurarán que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

Medidas dirigidas a:

GERENCIA GESTION

- La GERENCIA GESTION verificará que las pruebas de seguridad sobre los sistemas de información se realicen de acuerdo con las metodologías definidas, contando con pruebas debidamente documentadas.

14.3. POLÍTICA PARA LA PROTECCION DE LOS DATOS DE PRUEBA

La Dirección de Tecnología de la Organización protegerá los datos de prueba que se entregarán a los desarrolladores, asegurando que no revelan información confidencial de los ambientes de producción.

14.3.1. Medidas para la protección de los datos de prueba

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología certificará que la información a ser entregada a los desarrolladores para sus pruebas será enmascarada y no revelará información confidencial de los ambientes de producción.
- La Dirección de Tecnología eliminará la información de los ambientes de pruebas, una vez estas han concluido.

15. POLÍTICAS QUE RIGEN DE LA RELACION CON PROVEEDORES

15.1. POLÍTICA DE INCLUSION DE CONDICIONES DE SEGURIDAD EN LA RELACIÓN CON PROVEEDORES

La Organización establecerá mecanismos de control en sus relaciones con proveedores, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, Medidas y procedimientos de seguridad de la información.
Los empleados responsables de la realización y/o firma de contratos o convenios con proveedores se asegurarán de la divulgación de las políticas, Medidas y procedimientos de seguridad de la información a dichas partes.

15.1.1. Medidas de inclusión de condiciones de seguridad en la relación con proveedores

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA, OFICINA ASESORA JURIDICA Y GERENCIA GESTION

- La Dirección de Tecnología, la Oficina Asesora Jurídica y la GERENCIA GESTION generaran un modelo base para los Acuerdos de Niveles de Servicio y requisitos de Seguridad de la Información, con los que deben cumplir proveedores o proveedores de servicios; dicho modelo, debe ser divulgado a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos.
- La Dirección de Tecnología, la Oficina Asesora Jurídica y la GERENCIA GESTION elaboraran modelos de Acuerdos de Confidencialidad y Acuerdos de Intercambio de Información con proveedores. De dichos acuerdos deberá derivarse una responsabilidad tanto civil como penal para la tercera parte contratada.

Medidas dirigidas a:

DIRECCIÓN DE TECNOLOGIA

La Dirección de Tecnología establecerá las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la Organización.

La Dirección de Tecnología establecerá las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.

La Dirección de Tecnología mitigará los riesgos relacionados con proveedores que tengan acceso a los sistemas de información y la plataforma tecnológica de la Organización

Medidas dirigidas a:

GERENCIA GESTION

La GERENCIA GESTION evaluará y aprobar los accesos a la información de la Organización requeridos por proveedores.

La GERENCIA GESTION identificará y monitorear los riesgos relacionados con proveedores o los servicios provistos por ellas, haciendo extensiva esta actividad a la cadena de suministro de los servicios de tecnología o comunicaciones provistos.

Medidas dirigidas a:

SUPERVISORES DE CONTRATOS CON PROVEEDORES

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

15.2. POLÍTICA DE GESTION DE LA PRESTACION DE SERVICIOS DE PROVEEDORES

La Organización propenderá por mantener los niveles acordados de seguridad de la información y de prestación de los servicios de los proveedores, en concordancia con los acuerdos establecidos con estos. Así mismo, velará por la adecuada gestión de cambios en la prestación de servicios de dichos proveedores.

15.2.1. Medidas de gestión de la prestación de servicios de proveedores

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA Y GERENCIA GESTION

- La Dirección de Tecnología verificará en el momento de la conexión y, cuando se considere pertinente, el cumplimiento de las condiciones de conexión de los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la Organización.
- La Dirección de Tecnologías y la GERENCIA GESTION verificaran las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.

Medidas dirigidas a:

GERENCIA GESTION Y SUPERVISORES DE CONTRATOS CON TERCEROS

- La GERENCIA GESTION y los Supervisores de contratos con proveedores deben monitorear periódicamente, el cumplimiento de los Acuerdos de Niveles de Servicio, Acuerdos de Confidencialidad, Acuerdos de Intercambio de información y los requisitos de Seguridad de la Información de parte de los terceros proveedores de servicios.
- Los Supervisores de contratos con proveedores, con el apoyo de la GERENCIA GESTION, deben administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad establecidos con ellos y monitoreando la aparición de nuevos riesgos.

16. POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD

16.1. POLÍTICA PARA EL REPORTE Y TRATAMIENTO DE INCIDENTES DE SEGURIDAD

La Organización promoverá entre Los empleados y proveedores el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas.

De igual manera, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.

Los directivos de la organización o a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

16.1.1. Medidas para el reporte y tratamiento de incidentes de seguridad

Medidas dirigidas a:

PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- Los propietarios de los activos de información deben informar a la GERENCIA GESTION, los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.

Medidas dirigidas a:

GERENCIA GESTION

- La GERENCIA GESTION establecerá responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.
- La GERENCIA GESTION evaluará todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y escalar al Comité de Seguridad de la Información aquellos en los que se considere pertinente.
- La GERENCIA GESTION designará personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su re-ocurrencia.
- La GERENCIA GESTION , con el apoyo con la Dirección de Tecnología y el proceso jurídico, creará bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.

Medidas dirigidas a:

COMITÉ DE SEGURIDAD DE LA INFORMACION

El Comité de Seguridad de la Información analizará los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.

Medidas dirigidas a:

TODOS LOS USUARIOS

- Es responsabilidad de empleados y de proveedores reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible.
- En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, Los empleados deben notificarlo a la Oficina de Riesgo para que se registre y se le dé el trámite necesario.

17. POLÍTICAS DE INCLUSION DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

17.1. POLÍTICA DE CONTINUIDAD, CONTINGENCIA, RECUPERACIÓN Y RETORNO A LA NORMALIDAD CON CONSIDERACIONES DE SEGURIDAD DE LA INFORMACION

La Organización proporcionará los recursos suficientes para proporcionar una respuesta efectiva de empleados y procesos en caso de contingencia o eventos catastróficos que se presenten en el organización y que afecten la continuidad de su operación.

Además, responderá de manera efectiva ante eventos catastróficos según la magnitud y el grado de afectación de los mismos; se restablecerán las operaciones con el menor costo y pérdidas posibles, manteniendo la seguridad de la información durante dichos eventos. La Organización mantendrá canales de comunicación adecuados hacia empleados, proveedores y proveedores interesadas.

17.1.1. Medidas de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad de la información

Medidas dirigidas a:

COMITE SARO-SARLAFT Y GERENCIA GESTION

- El Comité SARO-SARLAFT, junto con la GERENCIA GESTION, reconocerá las situaciones que serán identificadas como emergencia o desastre para la organización, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.
- El Comité SARO-SARLAFT, junto con la GERENCIA GESTION, liderará los temas relacionados con la continuidad del negocio y la recuperación ante desastres
- La GERENCIA GESTION realizará los análisis de impacto al negocio y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.
- El Comité SARO-SARLAFT, junto con la GERENCIA GESTION, producto del análisis BIA seleccionará las estrategias de recuperación más convenientes para la organización.
- La GERENCIA GESTION validará que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información.
- El Comité SARO-SARLAFT, junto con la GERENCIA GESTION, deben asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de negocio, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA Y GERENCIA GESTION

La GERENCIA GESTION, en conjunto con la Dirección de Tecnología, elaborara un plan de recuperación ante desastres para el centro de cómputo y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados.

La Dirección de Tecnología y la GERENCIA GESTION participará activamente en las pruebas de recuperación ante desastres y notificar los resultados al Comité SARO-SARLAFT.

Medidas dirigidas a:

DIRECTIVOS

- Los Directivos de la Organización identificaran y, al interior de sus procesos, generar la documentación de los procedimientos de continuidad que podrían ser utilizados en caso de un evento adverso, teniendo en cuenta la seguridad de la información. Estos documentos deben ser probados para certificar su efectividad.

17.2. POLÍTICA DE REDUNDANCIA

La Organización propenderá por la existencia de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para la organización.

2.1. Medidas de redundancia

Medidas dirigidas a:

DIRECCION DE TECNOLOGIA Y GERENCIA GESTION

- La Dirección de Tecnología y la GERENCIA GESTION analizará y establecer los requerimientos de redundancia para los sistemas de información críticos para la organización y la plataforma tecnológica que los apoya.
- La Dirección de Tecnología evaluará y probará soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos de la Organización.
- La Dirección de Tecnología, a través de sus empleados, debe administrar las soluciones de redundancia tecnológica y realizar pruebas periódicas sobre dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad de la Organización.

18. POLÍTICAS DE CUMPLIMIENTO

18.1. POLÍTICA DE CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES

La Organización velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ella la referente a 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.

1.1. Medidas de cumplimiento con requisitos legales y contractuales

Medidas dirigidas a:

OFICINA ASESORA JURIDICA Y GERENCIA GESTION

- El proceso jurídico y la GERENCIA GESTION deben identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la organización y relacionados con seguridad de la información.

Medidas dirigidas a:

DIRECCIÓN DE TECNOLOGIA

- La Dirección de Tecnología certificará que todo el software que se ejecuta en la organización esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.
- La Dirección de Tecnología establecerá un inventario con el software y sistemas de información que se encuentran permitidos en las estaciones de trabajo o equipos móviles de la Organización para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo o equipos móviles corresponda únicamente al permitido.

Medidas dirigidas a:

TODOS LOS USUARIOS

- Los usuarios no instalaran software o sistemas de información en sus estaciones de trabajo o equipos móviles suministrados para el desarrollo de sus actividades.
- Los usuarios cumplirán con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada.

18.2. POLÍTICA DE PRIVACIDAD Y PROTECCION DE DATOS PERSONALES

En cumplimiento de la de Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales, la Organización a través de la GERENCIA GESTION, propenderá por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información.

Se establecerán los términos, condiciones y finalidades para las cuales la Organización, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información

de todas las personas que en algún momento, por razones de la actividad que desarrolla la organización, hayan suministrado datos personales.

En caso de delegar a un tercero el tratamiento de datos personales, la Organización exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales.

Así mismo, buscará proteger la privacidad de la información personal de sus empleados, estableciendo los controles necesarios para preservar aquella información que la organización conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la Organización y no sea publicada, revelada o entregada a empleados o proveedores sin autorización.

1.1. Medidas de privacidad y protección de datos personales

Medidas dirigidas a:

PROCESOS QUE PROCESAN DATOS PERSONALES

- Las procesos que manejan datos personales de beneficiarios, empleados, proveedores u otros deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la Organización.
- Los procesos que manejan datos personales de beneficiarios, empleados, proveedores u otros proveedores deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.
- Los procesos que manejan datos personales de beneficiarios, empleados, proveedores u otros proveedores deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.
- Los procesos que manejan datos personales de beneficiarios, empleados, proveedores u otros proveedores deben acoger las directrices técnicas y procedimientos establecidos para el intercambio de estos datos con los terceros delegados para el tratamiento de dichos datos personales.
- Los procesos que manejan datos personales de beneficiarios, proveedores u otros proveedores deben acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.

Medidas dirigidas a:

GERENCIA GESTION

- La GERENCIA GESTION establecerá los controles para el tratamiento y protección de los datos personales de los beneficiarios, empleados, proveedores y demás terceros de la Organización de los cuales reciba y administre información.

Medidas dirigidas a:

DIRECCIÓN DE TECNOLOGIA

- La Dirección de Tecnología implantará los controles necesarios para proteger la información personal de los beneficiarios, empleados, proveedores u otros proveedores almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.

Medidas dirigidas a:

TODOS LOS USUARIOS

- Los usuarios guardarán la discreción correspondiente, o la reserva absoluta con respecto a la información de la Organización o de sus empleados de cual tengan conocimiento en el ejercicio de sus funciones.

- Es deber de los usuarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.

Medidas dirigidas a:

USUARIOS DE LOS PORTALES DE LA ORGANIZACIÓN

- Los usuarios de los portales de la Organización asumirán la responsabilidad individual sobre la clave de acceso a dichos portales que les es suministrada; así mismo, deben cambiar de manera periódica esta clave de acceso.
- Los usuarios de los portales de la Organización contarán con controles de seguridad en sus equipos de cómputo o redes privadas para acceder a los portales de la Organización.
- Los usuarios de los portales de la Organización aceptarán el suministro de datos personales que pueda hacer el organización a los terceros delegados para el tratamiento de datos personales, a entidades judiciales y demás entes del Estado que, en ejercicio de sus funciones, solicitan esta información; de igual manera, deben aceptar que pueden ser objeto de procesos de auditoria interna o externa.

Elaboro: María Teresa Herrera Gerente de Gestión	Aprobó: RAFAEL A. TARAZONA OREJARENA Gerente General