SERVICIUDAD E.S.P.	Código SPOT-25	Versión 01
Política de seguridad y privacidad de la información	Página 1 de 22	

POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SERVICIUDAD E.S.P

DOSQUEBRADAS

Elaboró	Revisó	Aprobó
Harrison González Santa Técnico grado 3 sistemas	Diana Carolina Herrera C Subgerente Planeación	Fernando José Da Pena M Gerente
Fecha: 14-10-2021	Fecha: 15-10-2021	Fecha: 22-10-2021

TABLA DE CONTENIDO

INTRODUCCIÓN

La Seguridad y Privacidad de la Información presenta gran relevancia en la prestación de servicios de cada Entidad, debido al gran desarrollo y auge de nuevas tecnologías, plataformas de computación, aplicaciones, dispositivos de hardware e interconexión a través de redes, al mismo tiempo que surgen estos impactos positivos, traen inmersas amenazas que atentan contra los activos de información.

Se hace necesario adaptar y adoptar la Política de Seguridad y Privacidad de la Información, junto con actividades de socialización y sensibilización que orienten a todo el personal de la Entidad acerca del uso adecuado y seguro de los activos de información, con el fin de obtener el mayor provecho de la tecnología disponible y prevenir riesgos que impacten negativamente los procesos, como resultado de uso inadecuado en los bienes y servicios prestados por la Entidad.

En este sentido, La política de Seguridad y Privacidad de la Información se convierte en una herramienta efectiva para el uso adecuado de los recursos informáticos de SERVICIUDAD E.S.P.

1. DEFINICIONES

Política: Conjunto de directrices que indican la intención de la Alta Gerencia respecto a la operación y funcionamiento de la entidad, las cuales deben ser cumplidas por los funcionarios, empleados y terceros con vinculación a ésta.

Procedimiento: Documento que contiene las fases secuenciales donde se describe detalladamente cómo se lleva a cabo una actividad determinada.

Recurso Informático: Elementos informáticos (base de datos, sistemas operaciones, redes, sistemas de información y comunicaciones, equipos computacionales) que facilitan la prestación de servicios informáticos.

Seguridad de la información: Medidas preventivas y reactivas de la Entidad y de los sistemas tecnológicos que permiten resguardar y proteger la información.

Sistema de información: Es el conjunto de instrucciones, órdenes y reglas que un equipo de cómputo debe ejecutar, orientados al tratamiento y administración de datos e información. El concepto de *software* abarca todo lo intangible en una computadora o lo que no es físico ni se puede tocar. Ejemplos de *software* son los programas de computación o sistemas operativos de los equipos de cómputo

Usuario: Colaboradores, contratistas, pasantes universitarios y SENA, personal temporal y otras personas relacionadas a terceras partes, que utilicen recursos informáticos para desarrollar sus funciones y actividades asignadas.

ISO 27001:2018: Norma internacional que gestiona la seguridad de la información en una entidad, su eje central está enfocado en proteger la integridad, confidencialidad y disponibilidad de la información.

Incidente de seguridad de la información: Serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Activos de Información: Son los recursos que tiene el Sistema de Seguridad de la Información necesarios para que la Entidad logre los objetivos propuestos.

Acuerdo de Confidencialidad: Es un documento que debe suscribir todo usuario con el objeto de lograr el acceso a recursos informáticos de SERVICIUDAD E.S.P.

Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u entidad.

Backups o Copias de respaldo: Copia que se realiza a la información institucional definida como sensible o vulnerable según su impacto, con el fin de restablecer dicha información ante una eventual pérdida de datos, para continuar con las actividades rutinarias requeridas para el funcionamiento de los Procesos en la Entidad.

Contraseña: Clave de acceso a un recurso informático.

Riesgo: Posibilidad de ocurrencia de evento que conlleve a la irrupción del comportamiento normal de un proceso.

Control: Actividad preventiva para impactar la presencia de un riesgo, propiciando la mitigación y eliminación de éste.

Firewall: Conjunto de recursos de hardware y software que protegen recursos informáticos de accesos indebidos.

Clasificación de seguridad: Clasificación estratégica adoptada por el Sistema de Gestión de la Calidad, referente al mantenimiento de la seguridad de la información de acuerdo a su importancia para la Entidad, esta clasificación se define como:

- **Pública**: Información de dominio público que la Entidad puede dar a conocer a los usuarios interesados, Dicha información puede estar publicada en el sitio web de la Entidad.
- **Controlada**: Documentos de gestión de los procesos de la Entidad, que contienen los métodos de trabajo usados para su operación y/o para formación del personal. El acceso a esta información está restringido a los miembros de cada área o disponibles para los ejercicios de auditoría interna o externa de la Entidad.

- **Reservada**: Documentos estratégicos con información descriptiva de claves y datos técnicos de funcionamiento de los procesos de la Entidad. Esta información se encuentra disponible solo para el personal autorizado para su uso y/o para atender solicitudes derivadas de los procesos de auditorías internas o externas.

Monitoreo: Verificación de las actividades de un usuario con respecto al uso de los recursos informáticos de SERVICIUDAD E.S.P.

Vulnerabilidad: Debilidad de un activo o grupo de activos que puede ser impactada por una o más amenazas.

2. NORMATIVIDAD RELACIONADA

LEY 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.

Ley 44 de 1993: por la cual se modifica y adiciona la ley 23 de 1982 "Sobre los Derechos de Autor" y se modifica la ley 29 de 1944.

ISO 27001: Norma de la Seguridad de la Información

Decreto 1008 de 2018: "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"

3. OBJETIVO

Establecer parámetros de riesgos y controles para proteger de posibles riesgos de daño, pérdida y uso indebido de la información, los equipos y demás recursos informáticos de SERVICIUDAD E.S.P, los cuales están en constante cambio y evolución de acuerdo con el avance de la tecnología y los requerimientos de la Entidad.

4. ALCANCE

La Política de Seguridad y privacidad de la Información de SERVICIUDAD E.S.P está dirigida a todos aquellos usuarios que posean algún tipo de contacto con los activos de información. Los usuarios de los activos de información de la Entidad deberán diligenciar un acuerdo de confidencialidad, que los compromete con el cumplimiento de la política acá descrita.

5. PRINCIPIOS DE LA POLÍTICA

Los principios definidos para la Política de Seguridad y Privacidad de la Información de **SERVICIUDAD E.S.P** son los siguientes:

Responsabilidad: Todos los usuarios, sin excepción, son responsables por los accesos, acciones y demás situaciones que se realicen en los diferentes sistemas de información donde se implique el uso de código de usuario y contraseña, así como en el uso de las cuentas de correo electrónico corporativo.

Cumplimiento: Es deber de los usuarios acatar las normas, procedimientos administrativos y técnicos establecidos por la Entidad para el uso de los sistemas de información, así como la aplicación de las instrucciones para la protección de la información.

Ética: Se debe mostrar y aplicar una buena conducta en la utilización de los sistemas de información, los cuales han sido destinados únicamente para los servicios prestados por la Entidad, respetando la propiedad intelectual del software, diseños e información, como también el adecuado uso de la información contenida en ellos.

Propiedad: La Entidad es la propietaria de todos los recursos informáticos instalados y entregados a los usuarios para su utilización, entre los que se destacan los siguientes: computadores de escritorio y/o portátiles, dispositivos móviles (celular Smartphone, Tablet, entre otros), correo electrónico y la información resultante en los servicios prestados sobre ellos.

Vigilancia: La Entidad se reserva el derecho de vigilar el uso de los recursos informáticos y acceder a la información contenida en los mismos de ser necesario,

procurando la no violación de las normas y principios establecidos por la entidad, en especial la información que no tenga relación con las funciones inherentes al cargo del usuario o aquella que no esté debidamente autorizada para su acceso, la cual podrá ser retenida por la Entidad en caso de ser hallada durante una revisión.

Confidencialidad: La Entidad busca que la información se encuentre únicamente disponible a las personas que cuentan con la debida autorización, evitando la fuga de datos e información de alto impacto.

Integridad: SERVICIUDAD E.S.P busca garantizar que los datos no se modifiquen desde su creación, para brindar garantías de transparencia y acceso a la Información funcional, como insumo para procesos requeridos.

Disponibilidad: SERVICIUDAD E.S.P busca garantizar que la información estará disponible para el usuario en el momento requerido.

6. ELEMENTOS DE LA POLÍTICA

La política de seguridad y privacidad de la información de SERVICIUDAD E.S.P consta de:

6.1. ASPECTOS GENERALES.

La política descrita establece que los usuarios de la Entidad deben cumplir con los siguientes aspectos:

1. Usar los recursos informáticos únicamente para los servicios prestados por la Entidad y en el cumplimiento de sus objetos contractuales.

2. Acceder bajo su responsabilidad solo a sus datos, programas y demás recursos asignados, necesarios para realizar sus funciones y brindar el servicio designado.

3. Hacer uso solo del software autorizado y asignado por la Entidad y en caso de utilizar equipos que no son de propiedad de la Entidad presentar el debido licenciamiento legal del software utilizado.

4. Respetar las leyes de derecho de autor contempladas en la **Ley 23 de 1982, Ley 44 de 1993** y **ley 603 de 2000**; por lo tanto, no se permite instalar en los

computadores de la Entidad programas no licenciados ni autorizados por la Oficina de TI

5. Proteger las credenciales de acceso a los sistemas de Información. No prestarlos ni divulgarlos.

6. Mantener la confidencialidad y reserva de la información a su cargo, no divulgando ésta a personas extrañas a la Entidad.

7. No monopolizar la red ni los computadores de la Entidad con datos ajenos a la naturaleza de los procesos atendidos e inherentes a SERVICIUDAD E.S.P

8. Respetar y cumplir a cabalidad con las medidas de seguridad de los sistemas de información, recursos informáticos y red corporativa de la Entidad, obligando a mantener protegida la información y recursos asignados.

9. Hacer buen uso de la red corporativa y de sus recursos, como las impresoras, el papel, los medios de almacenamiento y seguridad, los canales de comunicación, entre otros.

10. No compartir o difundir en la red información sensible que pueda atentar contra la seguridad de la información de la Entidad, como infecciones por virus informáticos y demás programas que intenten violar la seguridad de la misma.

11. No trasladar los computadores y sus componentes asignados a sitios diferentes a los autorizados.

6.2 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

6.2.1 Recurso Humano

La Entidad considera a las personas como elemento clave de los procesos de gestión de información y como usuarios de tecnología. Se pueden identificar los siguientes tipos de usuario:

a. **Colaboradores directos e indirectos**, que participan en la ejecución de los servicios en la entidad.

b. **Clientes y proveedores**, autorizados para el acceso a los recursos de tecnología de la entidad.

c. **Demás terceros**, autorizados por la Entidad, para acceder a la información y demás recursos informáticos.

6.2.2 Con relación a los servicios informáticos

Se considera como falta SIMPLE el incumplimiento de las siguientes consideraciones:

a. Los usuarios deberán velar por el adecuado uso de las impresoras, donde se realicen impresiones sólo de información realmente necesaria para el desempeño de sus servicios asignados, y lograr el eficiente uso de los recursos: tinta, papel, etc., contribuyendo de esta manera con la conservación del ambiente.
Se considera como falta MEDIA el incumplimiento de las siguientes consideraciones:

b. El sistema de correo electrónico, herramientas de chat y demás aplicaciones, deben ser usadas según los lineamientos adoptados por la entidad para el uso de cada una de ellas y únicamente para el ejercicio de las funciones delegadas a cada colaborador y servicios contratados a terceros.

c. Los usuarios no deben utilizar el servicio de chat para fines tales como realización de encuestas, concursos, o cualquier otro tipo de mensajes no solicitados (Comerciales o de otro tipo); solamente se debe utilizar para fines pertinentes a la labor en la Entidad.

d. Para hacer uso de la herramienta chat institucional, se debe gestionar el acceso directamente con la Oficina de TI, por intermedio del subgerente o director de área del usuario solicitante.

Se considera como falta GRAVE el incumplimiento de las siguientes consideraciones:

e. Los usuarios autorizados para acceder al Internet deberán aceptar, respetar y aplicar las políticas y prácticas del uso adecuado de este servicio en sus labores desarrolladas al interior de la Entidad.

f. Si los usuarios sospechan de alguna infección causada por un virus informático, deben comunicarlo inmediatamente a la Oficina de TI para tomar las acciones pertinentes.

g. Los usuarios deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En caso de personas ajenas a la Entidad, los subgerentes o directores de área son los responsables de autorizar el acceso a los recursos informáticos de la entidad, de acuerdo al trabajo que estas personas realizarán y con previa justificación a la Oficina de TI.

6.2.3 En relación con los recursos informáticos.

El uso de los recursos informáticos deberá estar regulado por:

1. **Administración de usuarios:** Establece como deben ser utilizadas las claves de acceso a los recursos informáticos, los parámetros de longitud mínima de la contraseña, la frecuencia de cambio de contraseña por parte de los usuarios, entre otras.

2. **Rol de Usuario:** Los sistemas operacionales, bases de datos y aplicativos deberán contar con los roles predefinidos o con un módulo que permita definir roles, definiendo las acciones permitidas por cada uno de estos.

Se considera como falta GRAVE el incumplimiento de las siguientes consideraciones:

a. El control de acceso a todos los sistemas de computación de la entidad debe realizarse por medio de códigos de identificación y contraseñas únicos para cada usuario.

b. Todo sistema de información debe tener definidos los perfiles de usuario de acuerdo con los servicios a su cargo y de los usuarios que acceden a ellos.

c. Las contraseñas de acceso a los recursos informáticos que se asignen a los usuarios son su responsabilidad exclusiva y éstas no deben ser divulgadas a ninguna persona.

d. El usuario debe cambiar la contraseña regularmente, mediante los mecanismos y procedimientos dispuestos para tal fin.

e. Los usuarios son responsables de todas las actividades realizadas en los sistemas de información al cual tengan acceso y donde se lleve registro de uso de código de identificación de usuario y clave personal.

6.2.4 En relación con usuarios terceros.

Se considera como falta GRAVE el incumplimiento de las siguientes consideraciones:

a. Los dueños de los recursos informáticos que no sean propiedad de la Entidad y deban ser ubicados y administrados por ésta, deben garantizar la legalidad en hardware y software del recurso para su funcionamiento dentro de la entidad.

b. Cuando se requiera utilizar recursos informáticos que no sean propios de la Entidad y deban ubicarse en sus instalaciones, estos serán administrados por la Oficina de TI.

c. Los usuarios terceros tendrán acceso limitado y supervisado a los recursos informáticos necesarios para el cumplimiento de su función dentro de la Entidad. La autorización para acceder a esos servicios debe ser aprobada por el subgerente o director de área y por el Oficina de TI.

d. Los equipos de usuarios terceros que deban tener acceso a la red interna, deben cumplir con todas las normas de seguridad de la información vigentes establecidas por la Entidad. Adicional a ello, debe diligenciarse el acta respectiva donde queda plasmada la información del equipo de cómputo con sus respectivas autorizaciones.

e. La conexión entre los sistemas de información internos de la Entidad y terceros debe ser aprobada y certificada por la Oficina de TI, con el fin de no comprometer la seguridad de la información de la Entidad.

f. Como requisito para interconectar las redes de la entidad con terceros, sus sistemas de comunicación deben cumplir con los requisitos establecidos por la Entidad. La Entidad se reserva el derecho de monitorear estos sistemas de terceros sin previo aviso para evaluar la seguridad de los mismos. Así como se reserva el derecho de cancelar y terminar la conexión a sistemas de terceros que no cumplan con los requerimientos internos establecidos por la entidad.

6.2.5 Lugares Físicos

Los lugares físicos incluyen:

Instalaciones: Sede Administrativa y Técnica.

1. Sistemas de control de acceso físico a los diferentes lugares de la Entidad.

2. Sistemas de detección de fuego, agua, humedad y temperatura, instalados como mecanismos preventivos.

3. Centros de almacenamiento de información, magnética e impresa, que la entidad ha dispuesto para tal fin.

4. Toda la estructura física de equipos de procesamiento, como computadores, UPS, impresoras, equipos de comunicación, entre otros.

6.2.6 En relación con la seguridad física del edificio.

Se considera como falta GRAVE el incumplimiento de las siguientes consideraciones:

a. La entidad deberá contar con mecanismos de control de acceso, tales como puertas de seguridad, sistemas de alarmas y las demás que la entidad considere como impacto de control a riesgos críticos.

b. Las áreas consideradas críticas por la Entidad, deben ser lugares de acceso restringido. Si una persona no autorizada requiere ingresar a ellos, deberá registrar el motivo del ingreso y estar acompañada permanentemente por un usuario con acceso autorizado para estar en esa área específica.

b. Las áreas consideradas críticas por la Entidad deberán contar con elementos de control de incendio, inundación, humedad y temperatura.

c. Las áreas consideradas críticas por la Entidad deberán estar demarcadas con zonas de circulación definidas para visitantes y delimitar las zonas con acceso restringido.

d. Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con acceso restringido a personal no autorizado.

e. Cuando un usuario detecte un visitante sin compañía de un funcionario y sea sorprendido en alguna área restringida de la entidad, debe ser cuestionado inmediatamente, solicitando las razones por las cuales se encontraba en un área restringida e informar de inmediato al subgerente o director del área donde ocurra el incidente.

6.2.7 Seguridad De La Red

6.2.7.1 Usos de la red

En particular quedan expresamente prohibidas las siguientes acciones, de manera tal que su incumplimiento es considerado como falta GRAVE:

a. Instalar o implantar "virus", "gusanos", "troyanos" u otros tipos de programas dañinos para sistemas de proceso de la información.

b. Utilizar los medios de la red corporativa con fines comerciales no concernientes a los procesos de la Entidad.

c. Congestionar intencionalmente o no, enlaces de comunicaciones o sistemas de información mediante el envío o recepción de información o programas concebidos para tal fin.

d. Congestionar enlaces de comunicaciones o sistemas de información mediante la transferencia o ejecución de archivos o programas no propios del ambiente laboral.

e. El usuario no puede realizar acciones donde se disminuya el desempeño de los sistemas de información o interfieran con los procesos del sistema propio o de cualquier otro sistema de información.

f. El usuario no puede intentar cambiar la configuración de los programas ni alterar archivos o información del sistema de información.

g. Afectar o paralizar algún servicio ofrecido por la Oficina de TI.

h. Modificar archivos que no sean propiedad del usuario, aunque cuente con los permisos de escritura.

i. Se prohíbe el uso de dispositivos USB (memorias, discos duros externos, discos ópticos externos y similares) que no estén asociados a las labores realizadas por el usuario al interior de la Entidad. De ser necesario su uso, la dirección o Subgerencia del área correspondiente deberá hacer la solicitud por escrito ante la Oficina de TI, donde se justifiquen las razones para su utilización. Una vez se considere viable la solicitud, la dirección del área solicitante es la responsable de las acciones inadecuadas.

6.2.8 Seguridad de la Información.

Se considera como falta GRAVE el incumplimiento de las siguientes consideraciones:

a. Los usuarios son responsables de la información a su cargo y deberán cumplir las directrices establecidas en la política.

b. Todo usuario que utilice los recursos informáticos tiene la responsabilidad de velar por la integridad, confidencialidad y disponibilidad de la información a su cargo, en especial si dicha información está protegida por reserva legal o ha sido clasificada como crítica.

c. Los usuarios deberán firmar un acuerdo de cumplimiento de la seguridad de la información, la confidencialidad y buen manejo de la información.

d. Cuando un colaborador deja de prestar sus servicios a la Entidad, se compromete a entregar toda la información correspondiente a los servicios designados. Una vez retirado, el usuario debe comprometerse a no utilizar, comercializar o divulgar los productos o la información generada o conocida durante la gestión en la entidad, directamente o a través de terceros; así mismo, los usuarios que detecten el mal uso de la información, están en la obligación de reportar el hecho ante de la Subgerencia de área correspondiente.

e. Cuando un funcionario vaya iniciar sus vacaciones, el proceso de Gestión del Talento Humano debe informar a la Oficina de TI, el inicio y terminación de éstas, periodo en el cual se restringirá el acceso a los recursos informáticos asignados a su código y clave de usuario.

f. En caso de suplencia en algún cargo por motivo de vacaciones de un funcionario, se notificará a la Oficina de TI del reemplazo para proceder a activar el respectivo cargo en los sistemas de información y accesos a los recursos informáticos que le serán asignados. Bajo ninguna circunstancia un código puede ser usado por otro funcionario distinto; los privilegios de acceso serán limitados para las personas que realizan un reemplazo.

g. Como regla general, la información de políticas, normas y procedimientos de seguridad de la información se deben revelar únicamente a usuarios y entes externos que lo requieran, de acuerdo con su competencia y servicios a prestar.

6.2.9 Política de actualización de hardware.

Se considera como falta MEDIA el incumplimiento de las siguientes consideraciones:

a. En caso de necesitarse un nuevo dispositivo, éste debe gestionarse técnica y funcionalmente, sin excepción alguna, ante la Oficina de TI.

b. Cualquier cambio para mejorar el rendimiento en alguno de los equipos de cómputo de la Entidad debe tener previamente una evaluación técnica y autorización de la Oficina de TI.

Se considera como falta GRAVE el incumplimiento de las siguientes consideraciones:

c. La reparación técnica de algún equipo de cómputo donde se implique su apertura. Esta actividad solo puede ser realizada por personal autorizado.

d. Los recursos tecnológicos no deben ser movidos o reubicados sin la aprobación previa del subgerente o director de área involucrada, en acuerdo con el Director de la Oficina de TI.

6.2.10 Políticas de seguridad en comunicaciones.

Se considera como falta GRAVE el incumplimiento de las siguientes consideraciones:

a. Las direcciones internas (IP), topologías, configuraciones e información relacionadas con el diseño, la arquitectura y seguridad de la entidad, deberán ser consideradas y tratadas como información confidencial.

b. Todas las conexiones a redes externas en tiempo real con acceso a la red interna de la Entidad, deben tener filtro a través de los sistemas firewall, administración de permisos de circulación y autenticación de usuarios.

c. Todo intercambio electrónico de información o interacción entre sistemas de información con entidades externas deberá estar soportado con un acuerdo o documentos de formalización, y preferentemente este intercambio generarlo con información cifrada.

d. Los equipos de la entidad que requieran conexión de manera directa con computadores de entidades externas, lo realizaran con previa autorización y supervisión o ejecución de la Oficina de TI.

e. El acceso remoto a los recursos informáticos de la Entidad estará restringido SÓLO para personal autorizado. Cualquier intento de acceder o violar la seguridad de los recursos informáticos, como el uso e instalación de herramientas para este fin, será catalogado como una falta GRAVE.

6.2.11 Políticas De Backup

6.2.11.1. Período de almacenamiento de registros de auditoria

Registros de aplicación que contengan eventos relevantes de seguridad deben ser almacenados por un período no menor a tres (3) meses. Durante este período los

registros deben ser asegurados para evitar modificaciones y para que puedan ser vistos solo por personal autorizado. Estos registros son importantes para la corrección de errores, auditoría forense, investigaciones sobre fallas u omisiones de seguridad y demás esfuerzos relacionados.

6.2.11.2. Tipo de datos y frecuencia de backup

La información sensible y software crítico de SERVICIUDAD E.S.P presente en los recursos informáticos, se le debe hacer backup con la frecuencia necesaria validada por el procedimiento de copias de seguridad. Se deben hacer pruebas periódicas para garantizar el buen estado de la información almacenada.

7. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN SERVICIUDAD E.S.P

SERVICIUDAD E.S.P reconoce la importancia de la seguridad de la información, así como la necesidad de su protección para constituir un activo estratégico de la entidad y todas las partes interesadas, identificando el inadecuado uso de los activos de información como un peligro hacia la continuidad del negocio.

Los funcionarios, terceros y usuarios en general deberán conocer el presente documento, normas, reglas, estándares y procedimientos que apliquen según las funciones que realicen para la entidad, el desconocimiento que conlleve a la violación de lo anteriormente mencionado representará para la persona involucrada las sanciones disciplinarias que apliquen según el incidente presentado.

8. RESPONSABLE

Los responsables de velar por el cumplimiento de la Política de Seguridad y Privacidad de la Información son el director de la Oficina de TI y Control Interno, los cuales tendrán como responsabilidad lo siguiente:

- Compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de los mecanismos para asegurar la información al interior de la Entidad.
- Realizar procesos de socialización y sensibilización a los colaboradores de la Entidad, sobre la importancia de cumplir los objetivos de seguridad de la información, las responsabilidades legales, y la necesidad de la mejora continua.
- Realizar seguimiento y control sobre los planes de acción diseñados a partir de las auditorías internas ejecutadas en los procesos de TI.
- Realizar las debidas sanciones disciplinarias de acuerdo a los hallazgos identificados en las auditorias.

SANCIONES POR INCUMPLIMIENTO DE LA POLÍTICA

a. Cuando se trate de una falta que afecte directamente el normal funcionamiento del recurso tecnológico o infrinja leyes del ámbito jurídico, se aplicarán también todas las normas vigentes, informando por escrito al Área del usuario infractor y la Oficina de control interno Disciplinario para tomar las medidas y sanciones correspondientes.

b. Cuando por consecuencia de una violación de las normas se suspendan privilegios de los servicios computacionales a un usuario, para reactivar los servicios la Subgerencia de área del usuario infractor debe solicitar por escrito el levantamiento de la restricción ante la Oficina de TI.

c. La reincidencia de una falta SIMPLE la convierte en GRAVE.

CONSIDERACIONES FINALES

Por todo lo anterior, se solicita la gestión de todos los colaboradores para conservar un ambiente seguro en los sistemas de información y recursos informáticos de la Entidad, informando de cualquier irregularidad observada en los procesos que se lleve en los sistemas de información, o al uso dado de los recursos informáticos.