POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Empresa de Acueducto y Alcantarillado de Pereira S.A.S E.S.P
Dirección de Tecnologías de la Información
Pereira - Risaralda
Marzo de 2022

CONTENIDO

INTRODUCCIÓN

Actualmente la Seguridad de la información ha tomado gran importancia, debido al gran desarrollo y auge de nuevas tecnologías, nuevas plataformas de computación, nuevas aplicaciones, nuevos dispositivos de hardware e interconexión a través de redes. Pero al mismo tiempo surgen nuevas amenazas para los servicios de TI.

Se hace necesario desarrollar documentos con reglamentos y recomendaciones que orienten a todo el personal de la Empresa en el uso adecuado de los servicios de TI, con el fin de obtener el mayor provecho de la tecnología disponible y prevenir serios problemas como resultado de su uso inadecuado en los bienes y servicios prestados por ella.

En este sentido, las Políticas de Seguridad de la Información se convierten en una herramienta para el uso adecuado de los recursos informáticos de la **Empresa de Acueducto y Alcantarillado de Pereira S.A.S. E.S.P**, donde se desarrollan funciones y procedimientos de seguridad para concientizar a cada uno de los colaboradores de la organización en el uso adecuado de los recursos informáticos, permitiendo de esta manera obtener un mejor rendimiento y protección de los diversos servicios de TI y sus recursos asociados.

1 DEFINICIONES

Política: Instrucciones mandatarias que indican la intención de la alta gerencia respecto a la operación de la organización.

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

Servicios de TI: Elementos informáticos (base de datos, sistemas de información, programas, redes y comunicaciones, equipos de cómputo) que facilitan servicios de TI.

Seguridad de la información: Medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información, buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

Sistema de información: Conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo. Los elementos pueden ser personas, datos, actividades o técnicas de trabajo y Recursos materiales en general (generalmente recursos informáticos).

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

2 OBJETIVO

Definir parámetros de control para mantener y procurar la Seguridad de la Información de la **Empresa de Acueducto y Alcantarillado de Pereira S.A.S. E.S.P** en relación con los sistemas de información, utilización de los equipos de cómputo y el uso adecuado de los servicios de red, el servicio de Internet y correo electrónico.

ALCANCE DE LA POLÍTICA

Las políticas definidas en el presente documento aplican a todos los colaboradores de la **Empresa de Acueducto y Alcantarillado de Pereira S.A.S. E.S.P.,** contratistas, judicantes, pasantes universitarios y SENA y otras personas relacionadas a terceras partes, que utilicen recursos informáticos de la Empresa.

4 PRINCIPIOS DE LA POLÍTICA.

Los principios definidos para la política de Seguridad de la Información de la **Empresa de Acueducto y Alcantarillado de Pereira S.A.S 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 servicios de TI 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 Empresa para el uso de los servicios de TI, 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 servicios de TI, los cuales han sido destinados únicamente para los servicios prestados por la Empresa, respetando la propiedad intelectual del software, diseños e información, como también el adecuado uso de la información contenida en ellos.

Propiedad: La Empresa 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 Empresa 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 organización, 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 Empresa en caso de ser hallada durante una revisión.

5 ELEMENTOS DE LA POLÍTICA.

La política de seguridad de la información al interior de la **Empresa de Acueducto y Alcantarillado de Pereira S.A.S E.S.P.**consta de:

5.1 ASPECTOS GENERALES.

La filosofía de la política establece que los usuarios de la Empresa deben cumplir con los siguientes aspectos:

1. Usar los recursos informáticos únicamente para los servicios prestados por la Empresa.

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

3. Usar solo el **software autorizado** y asignado por la Empresa.

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 Empresa programas no licenciados ni autorizados por la Dirección de Tecnologías de la Información.

5. No instalar programas de cómputo por cuenta propia.

6. No usar los recursos informáticos para su propio beneficio o de terceros.

7. Proteger su usuario y su contraseña. No prestarlos ni divulgarlos.

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

9. No congestionar la red ni los equipos de cómputo de la Empresa con datos innecesarios, como fotos, videos, música y demás programas de entretenimiento o ajenos a la Empresa.

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

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

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

13. No trasladar los equipos de cómputo y sus componentes asignados a sitios diferentes a los autorizados.

5.2 RECURSO HUMANO.

La Empresa 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:

1. **Colaboradores directos e indirectos**, que participan en la ejecución de los servicios en la empresa.

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

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

5.2.1 En 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, papel, etc., contribuyendo de esta manera con la conservación del ambiente.

b. Los funcionarios solo podrán imprimir los trabajos asociados para el cumplimiento de los servicios asignados.

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

c. El sistema de correo electrónico, herramientas de chat y demás utilidades asociadas, deben ser usadas según los lineamientos adoptados por la Empresa 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.

d. Se prohíbe el uso de cualquier programa chat que no sea el institucional. En caso de requerir un programa diferente para estar en contacto directo con clientes y proveedores, se debe enviar por escrito a la Dirección de Tecnologías de la Información, por intermedio del subgerente o director de área del usuario solicitante, justificando la razón por la cual es necesaria la instalación del mismo para su análisis y aprobación.

e. 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 Empresa.

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

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

g. Si los usuarios sospechan de alguna infección causada por un virus informático, deben comunicarlo inmediatamente a la Dirección de Tecnologías de la Información para tomar las acciones pertinentes.

h. Los usuarios deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En caso de personas ajenas a la Empresa, los subgerentes o directores de área son los responsables de autorizar el acceso a los recursos informáticos de la organización, de acuerdo al trabajo que estas personas realizarán y con previa justificación a la Dirección de Tecnologías de la Información mediante el sistema de Gestión de Usuarios.

5.2.2 En relación con los recursos informáticos.

El uso de los recursos informáticos deberá estar regulado por:

- **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.

- **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. Deberán permitir la asignación a cada usuario de posibles y diferentes roles.

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

a. El control de acceso a todos los sistemas de cómputo de la entidad debe realizarse por medio de nombre de usuario o de identificación y contraseñas únicos para cada colaborador.

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 o compartidas a ninguna persona.

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

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

5.2.3 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 Empresa y deban ser ubicados y administrados por ésta, deben garantizar la legalidad en hardware y software del recurso para su funcionamiento dentro de la Empresa.

b. Cuando se requiera utilizar recursos informáticos que no sean propios de la Empresa y deban ubicarse en sus instalaciones, estos serán administrados por la Dirección de Tecnologías de la Información.

c. Los usuarios terceros tendrán acceso limitado y supervisado a los recursos informáticos necesarios para el cumplimiento de su función dentro de la Empresa. La autorización para acceder a esos servicios deben ser aprobadas por el subgerente o director de área y por el Director de Tecnologías de la Información.

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 Empresa. Adicional a ello

debe diligenciarse el acta de responsabilidad 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 Empresa y terceros debe ser aprobada y certificada por la Dirección de Tecnologías de la Información, con el fin de no comprometer la seguridad de la información de la Empresa.

f. Como requisito para interconectar las redes de la entidad con terceros, sus sistemas de comunicación deben cumplir con los requisitos establecidos por la Empresa. La Empresa 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 organización.

5.3 LUGARES FISICOS.

Los lugares físicos incluyen:

Instalaciones: edificios, salones y oficinas.

Sistemas de control de acceso físico a los diferentes lugares de la empresa.

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

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

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

5.3.1 En relación con la seguridad física del edificio.

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

a. La empresa deberá contar con mecanismos de control de acceso, tales como puertas de seguridad, sistemas de control con tarjetas inteligentes, sistemas de alarmas, entre otros. Además, se debe contar con un circuito cerrado de televisión en las dependencias que la entidad considere críticas (por ejemplo, el Data Center).

b. Las áreas consideradas críticas por la Empresa, 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.

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

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

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

f. Cuando un usuario detecte un visitante sin compañía de un colaborador 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.

5.4 SEGURIDAD DE LA RED.

5.4.1 Usos de la red.

El usuario se compromete a aceptar las condiciones estipuladas por la Empresa en las que se señala el uso de los servicios con fines netamente laborales, excluyendo cualquier uso comercial de la red, así como prácticas desleales (hacking) o cualquier otra actividad que voluntariamente tienda a afectar a otros usuarios de la red, tanto en las prestaciones de ésta como en la privacidad de su información.

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

a. Tratar de causar daño a servicios de TI o equipos conectados a la red corporativa de la Empresa y a otras redes a las que se proporcione acceso.

b. Esparcir, o permitir que se esparzan, "virus", "gusanos", "troyanos" u otros tipos de programas dañinos para sistemas de procesamiento de la información.

c. Utilizar los medios de la red corporativa con fines propagandísticos o comerciales no concernientes a los procesos de la Empresa.

d. Congestionar intencionalmente o no, enlaces de comunicaciones o servicios de TI mediante el envío o recepción de información o programas concebidos para tal fin.

e. Congestionar enlaces de comunicaciones servicios de TI mediante la transferencia o ejecución de archivos o programas no propios del ambiente laboral.

f. Realizar acciones donde se disminuya el desempeño de los servicios de TI o interfieran con los procesos de los sistemas propios o de cualquier otro servicio de TI.

g. Realizar acciones tendientes a burlar la seguridad de los servicios de TI, ni usar su cuenta para intentar burlar la seguridad de otros servicios de TI.

h. Intentar cambiar la configuración de los programas ni alterar archivos o información del sistema de información.

i. Los archivos, dispositivos y programas tienen privilegios de acceso asignados por el administrador del sistema. Por tanto, el usuario no puede intentar leer, escribir, copiar o alterar de cualquier manera información que no ha sido autorizada dentro de sus funciones.

j. Intentar o realizar accesos a cuentas de usuario diferentes a la asignada (utilizando cualquier protocolo: telnet, ftp, etc.), aunque no se consiga ingresar al sistema de información.

k. Exportar los archivos de contraseñas o realizar cualquier manipulación sobre los mismos, en concreto, intentar averiguar las contraseñas de otros usuarios.

l. Afectar o paralizar algún servicio ofrecido por la Dirección de Tecnologías de la Información.

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

n. Acceder, analizar o exportar archivos que sean accesibles a todo el mundo, pero sin ser propiedad del usuario, salvo que se encuentren en una localización destinada para uso público.

o. 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 Empresa. De ser necesario su uso, la dirección o subgerencia del área correspondiente deberá hacer la solicitud por escrito ante la Dirección de Tecnologías de la Información, 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 resultantes del mal uso dado a estos dispositivos.

5.4.2 Política de acceso a la información.

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

a. Todos los usuarios deben tener acceso sólo a la información necesaria para el desarrollo los procesos asignados

b. En el caso de personas ajenas a la Empresa, los subgerentes o directores de área son los responsables de autorizar sólo el acceso indispensable de acuerdo con el trabajo realizado por estas personas, con previa justificación.

c. Para dar acceso a la información se tendrán en cuenta la clasificación de ésta al interior de la Empresa, la cual deberá realizarse de acuerdo con la importancia de la información en la operación normal de la organización.

d. El otorgamiento de acceso a la información está regulado mediante las normas/reglas y procedimientos definidos para tal fin.

e. Todos los privilegios para el uso de los servicios de TI de la Empresa deben terminar inmediatamente después del cese de actividades del trabajador en la organización. Proveedores o terceras personas solamente deben tenerlos durante el periodo del tiempo requerido para llevar a cabo las labores asignadas.

f. Mediante el registro de eventos de los diversos recursos informáticos integrados en la plataforma tecnológica, se hará disponible la ejecución de un seguimiento de los accesos realizados por los usuarios a los sistemas de información y servicios de TI de la organización, con el objeto de minimizar el riesgo de pérdida de integridad de la información.

g. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información se deberán documentar y realizar las acciones tendientes a su solución.

5.4.3 Política de uso de software.

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

a. La Empresa de Acueducto y Alcantarillado de Pereira S.A.S E.S.P. respeta los derechos de propiedad intelectuales asociados con su propio hardware, software y documentación; en consecuencia, ningún usuario de sus servicios de TI ni cualquier otra persona puede reproducirlos por cualquier medio, comercializarlos o hacerlos públicos.

b. Si los derechos de propiedad intelectual se infringen por medio de un abuso deliberado o por negligencia, la persona involucrada puede ser procesada según las leyes aplicables.

c. Se considera como software autorizado, tanto los Sistemas Ofimáticos como Sistemas de gestión empresarial, los instalados por la Dirección de Tecnologías de la Información, previo visto bueno para su adquisición por el Director de Tecnologías de la Información y con la autorización legal del proveedor para su uso.

d. Toda área podrá utilizar UNICAMENTE el software que la Dirección de Tecnologías de la Información haya instalado en sus equipos de cómputo para el desarrollo de sus funciones.

e. Toda necesidad de software adicional, debe ser solicitada por escrito la Dirección de Tecnologías de la Información por intermedio de la dirección o subgerencia del área solicitante.

f. Todo software que utilice la Empresa será adquirido con normatividad vigente y siguiendo los procedimientos específicos de la organización.

g. Sin excepción, no se permitirá la instalación de software sin la debida autorización y/o participación de la Dirección de Tecnologías de la Información. De hacerlo, la acción será considerada como una violación a las normas.

h. Todo el software de manejo de datos utilizado por la Empresa dentro de su infraestructura informática, deberá contar con la

recomendación y/o aprobación de la Dirección de Tecnologías de la Información, siendo ésta la única responsable de su instalación y verificación del cumplimiento de las políticas de Seguridad de la Información.

i. Debe existir una cultura de seguridad de la información al interior de la organización para garantizar el conocimiento, por parte de los usuarios, de las implicaciones que tiene instalar software ilegal en los computadores de la Empresa.

j. Llevar un inventario de las licencias del software instalado en la empresa, permitiendo su adecuada administración y control y evitar, de esta manera, posibles sanciones por instalación de software no licenciado.

5.4.4 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, sin excepción alguna, ante la Dirección de Tecnologías de la Información.

b. Cualquier cambio para mejorar el rendimiento en alguno de los equipos de cómputo de la entidad (procesador, adición de memoria RAM, tarjeta o discos), debe tener previamente una evaluación técnica y autorización de la Dirección de Tecnologías de la Información.

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, únicamente 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 la Dirección de Tecnologías de la Información.

5.4.5 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 organización, deberán ser consideradas y tratadas como información confidencial.

b. Todas las conexiones a redes externas de tiempo real con acceso a la red interna de la Empresa, debe pasar a través de los sistemas firewall, de redes y autenticación de usuarios.

c. Todo intercambio electrónico de información o interacción entre servicios de TI con entidades externas deberá estar soportado con un acuerdo o documentos de formalización, y preferentemente este intercambio generarlo con información cifrada y haciendo uso de conexiones VPN.

d. Los equipos de la organización que requieran conexión de manera directa con computadores de entidades externas, lo realizaran con previa autorización y supervisión o ejecución de la Dirección de Tecnologías de la Información.

e. El acceso remoto a los recursos informáticos de la Empresa 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.

Nota aclaratoria:
Toda información secreta y/o confidencial que se transmita por las redes de comunicación de la Empresa e Internet deberá estar cifrada.

5.4.6 Acceso al servicio de Internet y cuentas de correo electrónico.

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

a. Para hacer uso de este tipo de herramientas se debe gestionar el acceso directamente con la Dirección de Tecnologías de la Información por escrito y por intermedio de la dirección del área del usuario solicitante.

b. El servicio de Internet y correo electrónico estará disponible únicamente para propósitos corporativos concernientes a la Empresa.

c. Está estrictamente prohibido cualquier uso con fines comerciales, políticos, particulares o cualquier otro diferente al laboral que dio origen a la habilitación del servicio.

d. Está prohibido transmitir cualquier material que viole cualquier regulación de la Empresa y en general de la República de Colombia; esto incluye: derechos de autor, amenazas, mensajes ofensivos, mensajes en cadena, mensajes intencionales que no contengan información o que contengan basura informática, material obsceno o información protegida por secreto comercial.

e. El usuario de Internet o cuenta de correo no tiene permitido acceder o intentar acceder a la cuenta o a los datos de otros usuarios.

f. El usuario de Internet o cuenta de correo no tiene permitido autorizar a otras personas a utilizar su cuenta.

g. Cualquier evidencia de acceso no autorizado a la cuenta o a los datos tiene que ser informada inmediatamente a la Dirección de Tecnologías de la Información.

5.5 SEGURIDAD DE DATOS

5.5.1 Política de seguridad de almacenamiento y respaldo.

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

a. La información soportada por la infraestructura de tecnología informática de la Empresa deberá ser almacenada y respaldada de acuerdo con las normas emitidas, de tal forma que se garantice su disponibilidad.

b. Debe existir una definición formal de la estrategia de generación, retención y rotación de las copias de respaldo, establecida en normas y procedimientos.

c. La empresa definirá la custodia de los respaldos de la información que se llevará al exterior de la Empresa con una compañía especializada en el tema.

d. La Dirección de Tecnologías de la Información definirá la estrategia a seguir para el respaldo de la información y la socializará con los colabdores de la Empresa.

e. Los usuarios son responsables de acatar las indicaciones técnicas dictadas por la Dirección de Tecnologías de la Información con respecto al almacenamiento de la información sujeta de backup.

5.5.2 Política de 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 los lineamientos generales y especiales regulados por la Empresa para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida da la misma.

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 acatar el cumplimiento de la seguridad de la información, la confidencialidad y buen manejo de la información.

d. Cuando un trabajador deja de prestar sus servicios a la Empresa, 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 o dirección de área correspondiente.

e. Cuando un colaborador vaya iniciar sus vacaciones, el Depto de Gestión Humana debe informar a la Dirección de Tecnologías de la Información el inicio y terminación de éstas, periodo en el cual se restringirá el acceso a los recursos informáticos asignados al usuario.

f. En caso de suplencia en algún cargo por motivo de vacaciones de un colaborador, se notificará a la Dirección de Tecnologías de la Información del reemplazo para proceder a activar el respectivo encargo en los servicios de TI y accesos a los recursos informáticos que le serán asignados. Bajo ninguna circunstancia un código de usuario puede ser usado por otro colaborador 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, según se requiera.

5.6 Gestión de accesos y contraseñas

5.6.1 Gestión de Accesos

Remítase a la Directiva 078 de 2022: Gestión de accesos

5.6.2 Gestión de Contraseñas

Para las políticas de contraseñas configuradas mediante la administración de directivas de grupo a través del controlador de dominio, se definen los siguientes parámetros:

- Exigir historial de contraseñas: **(20 contraseñas recordadas)**

  Esta configuración de seguridad determina el número de nuevas contraseñas únicas que deben asociarse a una cuenta de usuario antes de poder reutilizar una contraseña antigua. El valor debe estar comprendido entre 0 y 24 contraseñas.

- La contraseña debe cumplir con los requisitos de complejidad: **(habilitada)**

  Con la habilitación de esta directiva, las contraseñas deben cumplir los siguientes requisitos mínimos:

  - No contener el nombre de cuenta del usuario o partes del nombre completo del usuario en más de dos caracteres consecutivos.
  - Tener una longitud mínima de 8 caracteres
  - Incluir caracteres de tres de las siguientes categorías:
    - Mayúsculas (de la A a la Z)
    - Minúsculas (de la a a la z)
    - Dígitos de base 10 (del 0 al 9)
    - Caracteres no alfanuméricos (por ejemplo, !, $, #, %)
  - Estos requisitos de complejidad se exigen al cambiar o crear contraseñas.

- Longitud mínima de la contraseña **8 caracteres**

  Esta configuración de seguridad determina el número mínimo de caracteres que debe contener la contraseña de un usuario.

- Vigencia máxima de la contraseña: **60 días**

  Esta configuración de seguridad determina el período de tiempo (en días) en que puede usarse una contraseña antes de que el sistema solicite al usuario que la cambie.

- Vigencia mínima de la contraseña **1Dia**

Esta configuración de seguridad determina el período de tiempo (en días) en que puede usarse una contraseña antes de que el usuario pueda cambiarla.

5.6.3 Almacenamiento de Contraseñas

Todas las contraseñas de los sistemas operativos de servidores, servicios de TI, bases de datos y dispositivos de red deberán ser cambiadas en periodos de cuatro meses a excepción de la contraseña de administrador de dominio la cual cambia con las políticas anteriormente descritas.

El compilado de todas las contraseñas debe ser impreso periodicamente, y deberá ser entregado en sobre cerrado al Director de TI o a la Gerencia de la Empresa para su respectiva custodia.

SANCIONES POR INCUMPLIMIENTO DE LA POLÍTICA

a. En caso de infracción debidamente comprobada de alguna de las normas anteriores o de cualquier abuso efectuado por el usuario de los recursos informáticos de la Empresa, el subgerente o director de la Dirección de Tecnologías de la Información puede tomar acciones que van, desde una simple advertencia hasta la restricción completa del uso de los servicios computacionales y de red de la Empresa hasta no efectuar proceso de descargos con el área del usuario infractor. Todo este proceso será informado directamente a la dirección de área del usuario infractor.

b. 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 en el contrato de trabajo de la Empresa de Acueducto y Alcantarillado de Pereira S.A. E.S.P, conforme a las normas del Régimen Laboral, y de la legislación colombiana e internacional. En estos casos, la aplicación de sanciones se delega a la subgerencia o dirección de área del usuario implicado.

c. Cuando por consecuencia de una violación de las normas se suspendan privilegios de los servicios computacionales a un usuario, para reactivar los servicios la dirección de área del usuario infractor debe solicitar por escrito el levantamiento de la restricción ante la Dirección de Tecnologías de la Información.

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

7 CONSIDERACIONES FINALES

Por todo lo anterior, se solicita el compromiso y la gestión de todos los colaboradores para conservar un ambiente seguro en los servicios de TI y recursos informáticos de la Empresa, informando de cualquier irregularidad observada en los procesos que se lleve en los servicios de TI, o al uso dado a los recursos informáticos, procurando el aseguramiento de calidad y mejora continua en la ejecución de los servicios prestados.

No olvidemos que la Empresa es de todos y todos somos responsables de su seguridad.

DOCUMENTOS RELACIONADOS

- **Ley 1273 de 2009** sobre la protección de la información y de los datos.

- **Ley 1581 del 17 octubre 2012** sobre Protección de datos personales.

- **Ley 23 de 1982** sobre derechos de autor
  - **Ley 44 de 1993.** Modifica Ley 23
  - **Ley 603 2000.** Gestión de software, modifica Ley 23