POLITICA DE SEGURIDAD DE LA INFORMACIÓN

VIGENCIA 2022

Carrera 5ª No 4-88 – Telefax (098) 2479839 - Carmen de Apicalá, Tolima - Colombia.
http://daguassaesp.blogspot.com E-mail: daguassaesp@gmail.com

Contenido

1 INTRODUCCION

Los niveles de seguridad y la exigencia de la misma se han expandido exponencialmente en los últimos años por el avance tan drástico de la tecnología, dado a esto la protección de la información y bloqueo de intrusos son el objetivo a lograr para que la información y la estructura informática de la organización sea segura.

Los sistemas de almacenamiento de la información se expanden continuamente interconectando bases de dato, usuarios y demás, esto ha dado lugar a la aparición de nuevos problemas “amenazas” en los sistemas computarizados, al expandirse la cobertura del mismo modo se expande la vulnerabilidad de la misma.

Las empresas han dado prioridad y pie de fuerza para incentivar y mejorar el resguardo de la información de los proveedores y de las propias compañías, además del uso de adecuado de las tecnologías y hacen recomendación para aprovechar sus ventajas y minimizar los riesgos.

La **Política de Seguridad y Privacidad de la Información** es la declaración general que representa la posición de la administración de la de la Empresa de Distribución de Agua Potable, Alcantarillado y Aseo del Carmen de Apicalá S.A. E.S.P “DAGUAS S.A.E.S.P con respecto a la protección de los activos de información (los empleados, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la empresa y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

La de la Empresa de Distribución de Agua Potable, Alcantarillado y Aseo del Carmen de Apicalá S.A. E.S.P “DAGUAS S.A.E.S.P, para asegurar la dirección estratégica de la empresa, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la empresa.
- Cumplir con los principios de seguridad de la información.

- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los empleados, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los empleados, terceros, y clientes de la Empresa de Distribución de Agua Potable, Alcantarillado y Aseo del Carmen de Apicalá S.A. E.S.P "DAGUAS S.A.E.S.P Garantizar la continuidad del negocio frente a incidentes.

2 ALCANCE

La aplicación del manual de políticas de seguridad de DAGUAS S.A E.S.P, aplica a todo el personal que hagan uso de equipos y herramientas informáticas o estén conectados en la red interna de trabajo o manipulen información que está ligada con la base de datos central de la empresa, esta política de seguridad requiere de un gran compromiso por parte de todos los funcionarios de la institución, la capacidad para detectar anomalías y fallas generando una política cambiante y evolutiva.

3 RIESGOS NFORMÁTICOS

La ISO 27001 (Organización Internacional de Estandarización) define el riesgo informático como: "La posibilidad que una amenaza se materialice, utilizando vulnerabilidad existente en un activo o grupos de activos, generándose así pérdidas o daños."

En una empresa, los riesgos informáticos, son latentes día a día y pueden afectar gravemente la seguridad y la estabilidad de los sistemas de información, estos pueden presentarse en diversas áreas como lo ilustra la siguiente tabla.

Riesgos externos	Riesgos internos
Caída de la conexión a internet	Caída inesperada de algunos servicios del servidor, cambios bruscos en el fluido eléctrico de la institución
Errores en el suministro de la información.	Errores al utilizarlos recursos informáticos
Error en soporte técnico echo por terceros	Error en el diligenciamiento de la información de los usuarios dentro de la red de la institución
Eventos naturales que afecten la infraestructura de la institución afectando las redes y equipos informáticos.	Mal manejo de los equipos. Descargar software no autorizado Visitar sitios con contenido explicito

4 POLITICAS DE SEGURIDAD

Son las reglas y procedimientos que regulan la forma en que una organización mitiga los riesgos y busca establecer los estándares de seguridad a ser seguidos por todos los involucrados en el uso y mantenimiento de las herramientas tecnológicas.

Se consideran como el primer paso para aumentar la conciencia de seguridad de la información, están orientadas hacia la formación de buenos hábitos.

4.1 CLASIFICACIÓN DE LAS POLÍTICAS DE SEGURIDAD

Para efectos de comprensión y estructuración de este documento, la oficina de Sistemas de Información de DAGUAS S.A E.S.P, ha clasificado las políticas de seguridad en los siguientes grupos:

- ✓ **Equipos:** Todo lo relacionado con el hardware, su uso y cuidado.
- ✓ **Usuarios:** Concerniente a las personas que utilizan los recursos informáticos de la institución.
- ✓ **Software**: los recursos lógicos tales como programas, aplicativos y demás.

- ✓ **Redes e Internet**: las medidas que se deben tomar a la hora de utilizar los recursos de telecomunicación.
- ✓ **Datos e Información**: Políticas que regulan la manipulación, transporte y almacenamiento de la información de la empresa.
- ✓ **Administración de seguridad Informática**: Establece la forma en que la Oficina de Sistemas de Información gestiona la seguridad de la infraestructura informática de DAGUAS S.A. E.S.P.

4.2 POLITICA DE SEGURIDAD DE EQUIPOS.

La ley 734 de 2002 en su artículo 48, considera una falta gravísima lo siguiente: **"Artículo 48. Faltas gravísimas. Son faltas gravísimas las siguientes: Causar daño a los equipos estatales de informática, alterar, falsificar, introducir, borrar, ocultar o desaparecer información en cualquiera de los sistemas de información oficial contenida en ellos o en los que se almacene o guarde la misma, o permitir el acceso a ella a personas no autorizadas."**

los equipos de cómputo son el centro más fundamental de la institución ya que se almacena y se gestiona la información, la función del funcionario de sistemas de información es velar que los equipos funcionen adecuadamente y establecer medidas preventivas y correctivas.

En caso de robo, incendio, desastres naturales, fallas eléctricas y cualquier otro factor que atente contra la infraestructura de la red y la informática se dan a comprender las siguientes políticas:

- ✓ Todo equipo de cómputo, periférico o accesorio que esté o sea conectado a la Red de DAGUAS S.A E.S.P. sea propiedad o no de la institución debe de sujetarse a las normas y procedimientos de instalación establecidos por la oficina de Sistemas de Información, de lo contrario no le será permitido conectar su equipo o dispositivo. Para los equipos que no sean propios de DAGUAS S.A E.S.P. debe diligenciar un formato donde su propietario asuma la total responsabilidad sobre su equipo mientras esté conectado a la red eléctrica y de datos de la institución, ya que esta no se hace responsable de daños físicos o lógicos que puedan sufrir los equipos o periféricos de terceros.
- ✓ El administrador de sistemas tendrá registro de todos los equipos que son propiedad de DAGUAS S.A E.S.P. si se requiere hacer un traslado de un computador, periférico o accesorio, debe contar con el consentimiento de la

oficina de sistemas, si el equipo necesita trasladarse en calidad de préstamo (periodo de días u horas), debe notificar al administrador de sistemas además de diligenciar un formato con el consentimiento de gerencia.

- ✓ Cualquier equipo, periférico o accesorio de propiedad de DAGUAS S.A E.S.P. que necesite ser retirado de la institución tendrá que ser autorizado por el administrador de almacén, visto bueno de gerencia y visto bueno del administrador de sistemas.
- ✓ Todo equipo de la institución debe estar ubicado en el área que cumpla con los requerimientos de: seguridad física, condiciones ambientales adecuadas, seguridad y estabilidad en la parte eléctrica, garantías que deben proporcionarse en conjunto con el área de mantenimiento de DAGUAS S.A E.S.P. en general todos los equipos.
- ✓ Todos los equipos de cómputos, periféricos y demás deben estar lejos de los siguientes factores principales: la luz directa del sol y la humedad, filtraciones, fallas eléctricas, instrumentos que emitan campos magnéticos u radiación.
- ✓ Todos los equipos o periféricos pertenecientes a la red de DAGUAS S.A E.S.P. deberá contar con dispositivo de protección eléctrica ya sea un estabilizador o una UPS, que resguarde los equipos ante un cambio repentino en la corriente eléctrica.
- ✓ Todo equipo de cómputo, periférico o accesorio que esté o sea conectado a la Red de DAGUAS S.A E.S.P. sea propiedad o no de la institución debe de sujetarse a las normas y procedimientos de instalación establecidos por la oficina de Sistemas de Información, de lo contrario no le será permitido conectar su equipo o dispositivo. Para los equipos que no sean propios de DAGUAS S.A E.S.P, debe diligenciar un formato donde su propietario asuma la total responsabilidad sobre su equipo mientras esté conectado a la red eléctrica y de datos de la institución, ya que esta no se hace responsable de daños físicos o lógicos que puedan sufrir los equipos o periféricos de terceros.
- ✓ El administrador de sistemas tendrá registro de todos los equipos que son propiedad DAGUAS S.A E.S.P, si se requiere hacer un traslado de un computador, periférico o accesorio, debe contar con el consentimiento de la oficina de sistemas, si el equipo necesita trasladarse en calidad de préstamo (periodo de días u horas), debe notificar al administrador de sistemas además de diligenciar un formato con el consentimiento de gerencia.
- ✓ Cualquier equipo, periférico o accesorio de propiedad DAGUAS S.A E.S.P, que necesite ser retirado de la institución tendrá que ser autorizado por el

administrador de almacén, visto bueno de gerencia y visto bueno del administrador de sistemas.

- ✓ Todo equipo de la institución debe estar ubicado en el área que cumpla con los requerimientos de: seguridad física, condiciones ambientales adecuada, seguridad y estabilidad en la parte eléctrica, garantías que deben proporcionarse en conjunto con el área de mantenimiento de DAGUAS S.A E.S.P. en general todos los equipos.
- ✓ Todos los equipos de cómputos, periféricos y demás deben estar lejos de los siguientes factores principales: la luz directa del sol y la humedad, filtraciones, fallas eléctricas, instrumentos que emitan campos magnéticos u radiación.
- ✓ Todos los equipos o periféricos pertenecientes a la red de DAGUAS S.A E.S.P deberá contar con dispositivo de protección eléctrica ya sea un estabilizador o una UPS, que resguarde los equipos ante un cambio repentino en la corriente eléctrica. Todo equipo propiedad de la empresa, y que no cuente con alguno de estos dispositivos de protección, no puede colocarse en funcionamiento. Si el funcionario conectara el equipo, será el directo responsable de los daños que puedan ocurrirle a este, y se le aplicará ley 734. Régimen Único Disciplinario.
- ✓ En caso que se necesite poner en funcionamiento un equipo que no tenga UPS o estabilizador, podrá hacerse de manera temporal y con el acompañamiento de un funcionario de la oficina de Sistemas.
- ✓ Los usuarios responsables de los equipos en cada dependencia deberán dar cumplimiento con las normas y estándares de instalación con las que fue entregado el equipo, y deberán pedir aprobación de actualización o instalación de cualquier software, reubicación del equipo, reasignación, y todo aquello que implique cambios respecto a su instalación, asignación, función y misión original. Los equipos de cómputo no deben moverse o reubicarse sin la aprobación previa de la oficina de Sistemas de Información, que evaluará la viabilidad de dicho cambio.
- ✓ La protección física y la limpieza externa de los equipos corresponde al funcionario de sistemas al que se le asigne la tarea, y la custodia y cuidado en el sitio de trabajo le corresponde al funcionario que lo manipula y quien debe notificar las eventualidades, tales como daños, pérdidas y demás en el menor tiempo posible a la oficina de Sistemas de Información de DAGUAS S.A E.S.P. Está totalmente prohibido el consumo o ubicación de alimentos cerca de los equipos e impresoras, así como pegar distintivos, calcomanías y demás.

- ✓ En caso que ocurra un incidente producido por el derrame de algún tipo de alimentos sobre un equipo, periférico o accesorio, este debe apagarse y desconectarse de inmediato e informar oportunamente a la oficina de Sistemas de Información quien hará un diagnóstico del equipo y evaluara el daño y notificara a gerencia las respectivas sanciones.
- ✓ Además, el funcionario se hace cargo de la reparación del equipo u daño de impresoras por mal uso.
- ✓ No se permite el uso de dispositivos de almacenamiento extraíble tales como memorias USB, CD o DVD, nuevas tecnologías en los equipos de DAGUAS S.A E.S.P salvo en aquellos casos en donde por fuerza mayor se requiera y previamente evaluado y aprobado por la oficina de Sistemas de Información
- ✓ Los equipos de cómputo de la empresa, no deben ser alterados ni mejorados (cambios de procesador, adición de memoria o tarjetas) bajo ninguna causa. (Ley 734). Está totalmente prohibido a los usuarios destapar o desarmar los equipos o impresoras bajo cualquier motivo, sin exclusión. El único personal autorizado para esta labor es el de la oficina de Sistemas de Información. De detectarse que se está presentando esta conducta se informara y se tomaran las medidas correctivas necesarias.
- ✓ No se puede dar mantenimiento o soporte técnico a nivel de hardware a un equipo de cómputo que no es propiedad de DAGUAS S.A E.S.P Los funcionarios de La oficina de Sistemas de Información DAGUAS S.A E.S.P, son los únicos autorizados para manejar, mantener y velar por la integridad y seguridad de los servidores centrales de la institución, a su vez de mantener las claves de estos.
- ✓ El servidor central de la red de DAGUAS S.A E.S.P. debe estar ubicado en un lugar exclusivo, sin acceso de personas ajenas a la oficina de Sistemas de Información, y con las condiciones adecuadas de espacio, temperatura, iluminación, entre otras.
- ✓ Solo puede tener llaves del servidor el administrador de sistemas y gerencia, bajo ningún motivo se puede prestar llaves a terceros.
- ✓ La adquisición de nueva infraestructura de procesamiento de la información (hardware, software, aplicaciones e instalaciones físicas) o la actualización de la existente, deberá ser autorizada por la Oficina de Sistemas de Información y gerencia.
- ✓ Todo equipo que sea asignado a un funcionario o contratista, deberá ser entregado al responsable de este, en las mismas condiciones en que lo recibió, como parte de las actividades definidas en la terminación del contrato o cambio de cargo

- ✓ Todo funcionario debe firmar un acta de entrega de los equipos, verificar las condiciones del equipo y en esas mismas condiciones debe ser entregados al administrador de sistemas y al administrador de almacén.
- ✓ El administrador en todos los equipos tendrá bloqueados las redes sociales, YouTube, sitios porno y demás que se usen a fines de ocio.
- ✓ Todos los funcionarios tienen prohibido compartir las claves, contraseñas de equipos y wifi.
- ✓ Todos los empleados y contratistas deben apagar y dejar desconectados los equipos y periféricos al culminar la jornada laboral.
- ✓ Solo el administrador de sistemas puede establecer o dar conexión a escritorio remoto los demás funcionarios tienen prohibido hacer esto sin la aprobación del administrador de sistemas.

4.3 POLÍTICA DE SEGURIDAD EN USUARIOS

- ✓ Los usuarios son las personas que utilizan la estructura tecnológica de la Institución, ya sean equipos, recursos de red o gestión de la información. La oficina de Sistemas de Información establece normas que buscan reducir los riesgos a la información o infraestructura informática. Estas normas incluyen, restricciones, autorizaciones, denegaciones, perfiles de usuario, protocolos y todo lo necesario que permita un buen nivel de seguridad informática.
- ✓ Todos los funcionarios y contratistas de la empresa, deberán cumplir con estos requerimientos de seguridad de la Información. Igualmente, durante el proceso de vinculación deberán recibir inducción sobre lo establecido en este documento y sobre la responsabilidad del cumplimiento de las políticas, procedimientos y estándares definidos por la empresa.
- ✓ La información almacenada en los equipos de cómputo de DAGUAS S.A E.S.P y cada usuario es responsable por proteger su integridad, confidencialidad y disponibilidad. No es permitido divulgar, alterar, borrar, eliminar información sin la debida autorización
- ✓ Toda información en formato electrónico o impreso de la empresa debe estar debidamente identificada mediante rótulos o etiquetas, lo que permitirá su identificación y clasificación. Con esto se alimenta el inventario y clasificación de los archivos de información.
- ✓ Las claves o los permisos de acceso que les sean asignados a los funcionarios y/o contratista, son responsabilidad exclusiva de cada uno de ellos y no deben utilizar la identificación o contraseña de otro usuario,

excepto cuando los funcionarios de Sistemas la soliciten para la reparación o el mantenimiento de algún servicio o equipo.

- ✓ Los permisos a usuarios son personales e intransferibles y serán acordes a las funciones que desempeñen y no deberán tener permisos adicionales a estos. Estos permisos se conceden a solicitud escrita del administrador de sistemas.
- ✓ Los usuarios deben renovar periódicamente su clave de acceso al sistema, esto deben solicitarlo a la oficina de Sistemas de Información quienes le facilitarán el acceso y lo acompañarán en el proceso. Está totalmente prohibido: El intento o violación de los controles de seguridad establecidos; El uso sin autorización de los activos informáticos; El uso no autorizado o impropio de la conexión al Sistema; el uso indebido de la las contraseñas, firmas, o dispositivos de autenticación e identificación; acceder a servicios informáticos utilizando cuentas, claves, contraseñas de otros usuarios. Aún con la autorización expresa del usuario propietario de la misma
- ✓ El usuario será el directo responsable de cualquier daño producido por medidas o decisiones mal tomadas, mantenimientos, reparaciones o instalaciones realizados por él que no fueran informadas o consultadas al administrador de sistemas de DAGUAS S.A E.S.P
- ✓ Los usuarios son responsables de todas las actividades llevadas a cabo con su código de usuario. Si detectan actividades irregulares con su código, tienen que solicitar una auditoría a la oficina de Sistemas de Información que se encargará de dar soporte e informar al usuario la actividad completa en el período y módulos solicitados y de igual manera informara qué medidas se deben tomar al respecto. (Investigación preliminar, cambio de usuario, proceso disciplinario).
- ✓ Informar inmediatamente a la oficina de Sistemas de Información cualquier anomalía, aparición de virus o programas sospechosos e intentos de intromisión y no intente distribuir este tipo de información interna o externamente.
- ✓ A cualquier infracción a la política de seguridad informática cometida por un funcionario y/o contratista de la empresa, se le aplicará lo estipulado en el Código Único Disciplinario (Ley 734 de 2002) Art. 34 Núm. 24: “Son deberes de todo servidor público: Denunciar los delitos, contravenciones y faltas disciplinarias de los cuales tuviere conocimiento, salvo las excepciones de ley.”
- ✓ En caso de presentarse un problema crítico a nivel informático en horario no laboral afectando el normal funcionamiento de DAGUAS S.A E.S.P., el

Administrador de sistemas reportara en la oficina de Talento Humano quien es el encargado de localizarlo.

- ✓ Está prohibido intentar sobrepasar los controles de los sistemas, o tratar de saltar los bloqueos de acceso a internet (cambio de dirección IP, cambio de nombre de equipo, etc.) o introducir intencionalmente software malintencionado que impida el normal funcionamiento de los sistemas. En este caso se le aplicara lo estipulado en el Código Único Disciplinario (Ley 734 de 2002) Art. 34 núm.24: "Son deberes de todo servidor público: Denunciar los delitos, contravenciones y faltas disciplinarias de los cuales tuviere conocimiento, salvo las excepciones de ley."
- ✓ Todo funcionario que utilice los recursos informáticos, tiene la responsabilidad de velar por su integridad, confidencialidad y disponibilidad de la información que Maneje, especialmente si dicha información es crítica. Código Único Disciplinario (Ley 734 de 2002) Art. 34 núm. 22: "Son deberes de todo servidor público: Responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización."
- ✓ El administrador de sistemas es la única encargada y responsable de capacitar a los usuarios en el manejo de las herramientas informáticas que son exclusivas de la misión y función de la empresa.
- ✓ No se permitirá el almacenamiento y/o procesamiento de información propiedad DAGUAS S.A E.S.P, en equipos o dispositivos de propiedad de los funcionarios o contratistas. Todos los contratistas y funcionarios deben firmar una cláusula de confidencialidad, que permita a la empresa proteger la información.

4.4 POLITICA DE SEGURDAD DE SOFTWARE

- ✓ La oficina de Sistemas de Información es la única responsable de la instalación de software informático y de telecomunicaciones.
- ✓ En los equipos de cómputo de DAGUAS S.A E.S.P. no se permite la instalación de software que no cuente con el licenciamiento apropiado. Está prohibido el uso de aplicaciones ilegales y el uso de "Cracs", "Keygens" y demás aplicativos.
- ✓ Está totalmente prohibido la instalación de juegos, programas de mensajería o aplicativos que no estén relacionados con las labores institucionales que se realizan en la empresa.
- ✓ Con el propósito de proteger la integridad de los equipos y sistemas informáticos y de telecomunicaciones, es obligatorio que todos y cada uno

de estos dispongan de software de seguridad (antivirus, filtros de contenido web, controles de acceso, entre otros). Equipo que no cuente con estos aplicativos de seguridad, no puede conectarse a la red de la institución.

- ✓ las medidas de protección lógica (a nivel de software) son responsabilidad del personal de sistemas de información y el correcto uso de los sistemas corresponde a quienes se les asigna y les compete notificar cualquier eventualidad a la oficina de Sistemas de Información.
- ✓ La adquisición y actualización de software para los equipos de cómputo y de telecomunicaciones se llevará a cabo de acuerdo al calendario y requerimientos que sean propuestos por la oficina de Sistemas de Información y a la disponibilidad presupuestal con el que se cuente.
- ✓ Es obligación de todos los usuarios que manejen información masiva y/o crítica, solicitar respaldo correspondiente a la Oficina de sistemas sobre la generación copias de seguridad ya que se considera como un activo de la institución que debe preservarse. Las copias de respaldo a la información generada por el personal y los recursos informáticos de la institución deben estar resguardados en sitios debidamente adecuados para tal fin.
- ✓ La oficina de Sistemas de Información administrará los diferentes tipos de licencias de software con la que cuenta la empresa y vigilará su vigencia de acuerdo a sus fechas de caducidad.

4.5 POLITICAS DE SEGURIDAD DE LA RED E INTERNET

- ✓ Toda cuenta de acceso al sistema, a la red y direcciones IP, será asignada por la oficina de Sistemas de Información de DAGUAS S.A E.S.P, previa solicitud por escrito.
- ✓ Se prohíbe utilizar la red y los equipos de DAGUAS S.A E.S.P, para cualquier actividad que sea lucrativa o comercial de carácter individual, privado o para negocio particular. En este caso se le aplicara lo estipulado en el Código Único Disciplinario (Ley 734 de2002) Art. 34 Núm. 24: **"Son deberes de todo servidor público: Denunciar los delitos, contravenciones y faltas disciplinarias de los cuales tuviere conocimiento, salvo las excepciones de ley."**
- ✓ En lo relacionado con el uso de correo electrónico, no está permitido el uso del correo personal. Los correos institucionales deben ser para uso exclusivo de las actividades de DAGUAS S.A E.S.P.

- ✓ Para garantizar la seguridad de la información y el equipo informático, la oficina de Sistemas de Información establece filtros y medidas para regular el acceso a contenidos en el cumplimiento de esta normatividad:

Se prohíbe:

- ✓ Utilizar los servicios de comunicación, incluyendo el correo electrónico o cualquier otro recurso, para intimidar o insultar a otras personas, o interferir con el trabajo de los demás.
- ✓ Utilizar los recursos DAGUAS S.A E.S.P, para el acceso no autorizado a redes y sistemas remotos.
- ✓ Acceder remotamente a los equipos de DAGUAS S.A E.S.P , los únicos funcionarios autorizados para realizar estas prácticas son los de la oficina de Sistemas de Información, al momento de dar soporte a los usuarios en horario extra laboral.
- ✓ Provocar deliberadamente el mal funcionamiento de computadoras, estaciones o terminales periféricos de redes y sistemas, mediante técnicas, comandos o programas a través de la red.
- ✓ Monopolizar los recursos en perjuicio de otros usuarios, incluyendo: el envío de mensajes masivamente a todos los usuarios de la red, iniciación y facilitaciones de cadenas, creación de procesos innecesarios, generar impresiones en masa, uso de recursos de impresión no autorizado.
- ✓ Poner información en la red que infrinja el derecho a la intimidad de los demás funcionarios y/o contratistas.
- ✓ Utilizar los servicios de la red para la descarga, uso, intercambio y/o instalación de juegos, música, películas, imágenes protectoras o fondos de pantalla, software de libre distribución, información y/o productos que de alguna manera atenten contra la propiedad intelectual de sus actores o que contenga archivos ejecutables.
- ✓ El intercambio no autorizado de información de propiedad de DAGUAS S.A E.S.P Utilizar los servicios para acceder a páginas de radio o TV en línea, descargar archivos de música o video, visitar sitios de pornografía, ocio, entre otros que estén fuera de las funciones del usuario. Código Único Disciplinario (Ley 734 de 2002) Art. 35 Núm. 9: “A todo servidor público le está prohibido: Ejecutar en el lugar de trabajo actos que atenten contra la moral o las buenas costumbres.”
- ✓ La oficina de Sistemas de Información tiene habilitado un equipo con acceso total a internet, en el cual, los usuarios puedan realizar consultas o actividades personales, de corta duración. La oficina de Sistemas de

Información no se responsabiliza por pérdidas de información en ese equipo, ya que es de uso público y periódicamente se está eliminando información ajena a la institución. La oficina de sistemas realizará monitoreo permanente de tiempos de navegación y actividades realizadas a páginas vistas por parte de los funcionarios y/o contratistas

- ✓ Los servicios bancarios vía web a nombre de DAGUAS S.A E.S.P, solamente podrán ser utilizados por la jefe financiera y la Gerencia únicamente en el equipo que este tenga asignado. La oficina de Sistemas de Información, tendrá habilitado otro equipo para esta tarea a fin de dar apoyo y soporte cuando se solicite.
- ✓ El acceso a la red interna, se permitirá siempre y cuando se cumpla con los requisitos de seguridad necesarios, y éste será permitido únicamente por la oficina de Sistemas de Información.
- ✓ El uso de carpetas compartidas está prohibido para todos los funcionarios y/o contratistas, ya que en caso de infiltrase un virus o programa malicioso, usa este medio para propagarse. Las únicas carpetas compartidas que pueden existir en la red de DAGUAS S.A E.S.P, son las copias de seguridad programadas, tanto de base de datos como de información de los usuarios. Está prohibido el uso abusivo de estos recursos por parte de los usuarios en forma tal que afecte negativamente el rendimiento de la red.
- ✓ Para posibilitar el uso compartido de archivos, la oficina de Sistemas de Información tiene habilitado un servidor FTP en el cual se pueden almacenar y compartir la información Pública y Privada de cada dependencia. La información Pública puede ser accedida por cualquier funcionario de cualquier dependencia. La información Privada solo está disponible para los funcionarios de la misma dependencia.
- ✓ Cualquier alteración del tráfico entrante o saliente a través de los dispositivos de acceso a la red, será motivo de verificación y tendrá como resultado directo la realización de una auditoría de seguridad y un reporte de los hallazgos a la oficina De Control Interno para que se tomen las medidas pertinentes.
- ✓ Los mensajes y la información contenida en los buzones de correo son de propiedad de DAGUAS S.A E.S.P Los buzones no deberán contener mensajes con más de un año de antigüedad. Pero se debe dejar un histórico del registro de los mensajes. Todos los mensajes enviados deben respetar los formatos de imagen corporativa definidos por el Sistema de Gestión Documental y conservar todas las normas de legalidad de los documentos.

5 POLITICAS DE SEGURIDAD DE DATOS E INFORMACIÓN

- ✓ La información es en uno de los elementos más importantes dentro de una organización. La seguridad informática debe evitar que usuarios externos y no autorizados puedan acceder a ella sin autorización. De lo contrario la empresa corre el riesgo de que la información sea utilizada maliciosamente para obtener ventajas de ella o que sea manipulada, ocasionando datos errados o incompletos. El objetivo de esta política es la de asegurar el acceso a la información en el momento oportuno.
- ✓ Toda información de relevancia debe contar con copia de seguridad y un tiempo de retención determinado, por lo cual, la información no se debe guardar indefinidamente en un archivo activo ocupando espacio innecesario de almacenamiento, el usuario debe establecer cuándo su información pasará a ser inactiva. Aplicación de la Ley 594 de 2000 Ley de Archivos. Tablas de Retención Documental.
- ✓ La copia de seguridad de la base de datos central de DAGUAS S.A E.S.P., se genera así: copias diarias en equipos diferentes al servidor; Una copia semanal en disco, que será almacenada de acuerdo a los requerimientos necesarios para dicho fin ubicado en un sitio distante del área de trabajo. Estas copias deben ser monitoreadas a diario con el objetivo de garantizar la correcta realización y funcionamiento de las mismas. La ubicación de los medios de almacenamiento, deberá estar alejada del polvo, humedad o cualquier contacto con material que produzca corrosión.

A continuación, se establecen las 12 políticas de seguridad que soportan el SGSI de la Empresa de Distribución de Agua Potable, Alcantarillado y Aseo del Carmen de Apicalá S.A. E.S.P “DAGUAS S.A.E.S.P:

- ✓ La Empresa de Distribución de Agua Potable, Alcantarillado y Aseo del Carmen de Apicalá S.A. E.S.P “DAGUAS S.A.E.S.P , ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
- ✓ Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

- ✓ La Empresa de Distribución de Agua Potable, Alcantarillado y Aseo del Carmen de Apicalá S.A. E.S.P "DAGUAS S.A.E.S.P protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.

- ✓ La Empresa de Distribución de Agua Potable, Alcantarillado y Aseo del Carmen de Apicalá S.A. E.S.P "DAGUAS S.A.E.S.P protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- ✓ La Empresa de Distribución de Agua Potable, Alcantarillado y Aseo del Carmen de Apicalá S.A. E.S.P "DAGUAS S.A.E.S.P protegerá su información de las amenazas originadas por parte del personal.

- ✓ La Empresa de Distribución de Agua Potable, Alcantarillado y Aseo del Carmen de Apicalá S.A. E.S.P "DAGUAS S.A.E.S.P protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- ✓ La Empresa de Distribución de Agua Potable, Alcantarillado y Aseo del Carmen de Apicalá S.A. E.S.P "DAGUAS S.A.E.S.P controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- ✓ La Empresa de Distribución de Agua Potable, Alcantarillado y Aseo del Carmen de Apicalá S.A. E.S.P "DAGUAS S.A.E.S.P implementará control de acceso a la información, sistemas y recursos de red.

- ✓ La Empresa de Distribución de Agua Potable, Alcantarillado y Aseo del Carmen de Apicalá S.A. E.S.P "DAGUAS S.A.E.S.P garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- ✓ La Empresa de Distribución de Agua Potable, Alcantarillado y Aseo del Carmen de Apicalá S.A. E.S.P "DAGUAS S.A.E.S.P garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades

asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- ✓ La Empresa de Distribución de Agua Potable, Alcantarillado y Aseo del Carmen de Apicalá S.A. E.S.P "DAGUAS S.A.E.S.P garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.

- ✓ La Empresa de Distribución de Agua Potable, Alcantarillado y Aseo del Carmen de Apicalá S.A. E.S.P "DAGUAS S.A.E.S.P garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
- ✓ El incumplimiento a la **política de Seguridad y Privacidad de la Información** traerá consigo, las consecuencias legales que apliquen a la normativa de la empresa, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

OSCAR IVAN CARABALI COLLANTES
Gerente

MELIDA LEAL
Jefe División Administrativa

PROYECTÓ / CONTRATISTA MIPG