Acueducto y Alcantarillado de Popayán S.A. E.S.P

DIVISION SISTEMAS
GESTION INFORMATICA

POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION
2022

POPAYÁN

DESCRIPCIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se agrupan las políticas de privacidad y seguridad de la información con el objetivo de continuar con la implementación transversal de Seguridad de la Información en La Sociedad Acueducto y Alcantarillado de Popayán S.A. E.S.P.

POLÍTICA 1: ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Esta política garantizará que existen responsabilidades claramente asignadas en todos los niveles organizacionales para la gestión de seguridad de los activos de la información; se contará con un comité de seguridad de la información conformado por personal idóneo (Comité de TICS), que apoyará como asesor interno de seguridad, con el objetivo de direccionar y hacer cumplir los lineamientos de la empresa, en la materia y revisar las posibles incidencias y acciones que se deben tomar.

Todos los trabajadores, contratistas, pasantes y externos con acceso a los activos de información de la empresa, tendrán el compromiso con la seguridad de cumplir las políticas y normas que la empresa dicte, así como reportar los incidentes que se pueda detectar.

- ✓ Los trabajadores, contratistas, y pasantes de La Sociedad Acueducto y Alcantarillado de Popayán S.A. E.S.P. son responsables de la información que manejan y deberán cumplir con los lineamientos generales y especiales dados por la empresa y por la ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

- ✓ Todo trabajador, contratista y/o pasante que labore en la empresa y detecte el mal uso de la información (copia indebida, transferencia a terceros sin autorización, daño, información oculta, adulteración o incumplimiento de la política), está en la obligación de reportar el hecho a la División Sistemas y/o la División Control Interno.

POLÍTICA 2: GESTIÓN DE ACTIVOS

Identificación y clasificación de activos:

- ✓ La empresa realizará la identificación, clasificación y actualización de los activos de información, de acuerdo a las directrices establecidas en el decreto 103 de 2015-Vigente "Por el cual se reglamenta parcialmente la ley 1712 de 2014 y se dictan otras disposiciones", Artículos 37 y 38, este se actualizará de acuerdo a los lineamientos establecidos en el programa de Gestión Documental.

- ✓ Toda la información de la empresa, así como los activos donde se procesa y se almacena deberá ser inventariada y asignada a un área responsable; se realizará y se publicará el inventario de activos de información, el índice de información clasificada y reservada y el esquema de publicación de acuerdo a las directrices de la Ley 1712 de 2014 del Ministerio de tecnologías y comunicaciones MINTIC- Vigente "por medio de la cual se crea la ley de

transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones" y decreto 103 de 2015.

- ✓ El inventario de activos de información, el índice de información clasificada y reservada y el esquema de publicación debe ser actualizada cuando se presenten cambios en la información o normatividad que pueda afectarla.

- ✓ Todo trabajador, contratista o pasante que utilice los sistemas de información, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.

Devolución de los Activos

Es deber de todo trabajador, contratista y/o pasante que labore en la empresa, al dejar de prestar sus servicios, entregar toda información del producto del trabajo realizado y hacer entrega de los equipos y recursos tecnológicos en perfecto estado, conforme al procedimiento correspondiente para los trabajadores, los contratistas y pasantes de acuerdo a las condiciones establecidas en el contrato o convenio. Una vez retirado, debe comprometerse a no utilizar, comercializar o divulgar la información generada o conocida durante la gestión en la empresa, directamente o a través de terceros.

Gestión de Medios Removibles

La empresa se reserva el derecho de restringir el uso de medios removibles; mientras esté permitido es responsabilidad de los trabajadores de contrato laboral, contratistas, pasante y/o terceros que el medio removible conectado esté libre de virus y/o código malicioso, que pueda poner en riesgo la Integridad, confidencialidad y disponibilidad de la información y de los recursos tecnológicos de la empresa.

Disposición de los Activos

- ✓ Ningún funcionario de la empresa por sus propios medios está autorizado para realizar labores de mantenimiento y/o reparación de los equipos de cómputo, redes, cámaras, GPS y demás dispositivos electrónicos, para tal fin se debe comunicar con la dependencia responsable.

- ✓ Los trabajadores, contratistas y/o pasantes deben velar por el buen uso de los recursos tecnológicos asignados, pues son los directamente responsables de cualquier daño. En caso de presentar falla física o lógica se deberá notificar a la División Sistemas por medio de escrito o al personal responsable de dar servicio a los mismos para que los revisen, corrijan la falla o de ser necesario ordenen la reparación de los mismos.

- ✓ Cualquier cambio que se requiera realizar en los equipos de cómputo de la empresa (cambios de procesador, adición de memoria, discos duros o tarjetas) debe tener

previamente un diagnostico técnico avalando el cambio y este se debe realizar únicamente por la División Sistemas o con apoyo autorizado por el jefe de la División Sistemas.

- ✓ La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal autorizado.

- ✓ Los computadores corporativos son asignados a los trabajadores de contrato laboral, contratista o pasante, con el propósito de mejorar su ambiente de trabajo, mecanizar funciones y procesar información oficial, por lo cual se prohíbe el uso de los mismos para fines personales.

- ✓ Los usuarios sólo podrán utilizar los programas con que cuenta el computador que se le asignó, toda modificación del sistema será realizada bajo supervisión de la División Sistemas.

- ✓ Todo recurso tecnológico cuando cumpla su vida útil ya sea por obsolescencia o daño debe ser reintegrado a la oficina de Almacén con visto bueno de la División Sistemas.

- ✓ Se debe cerrar las sesiones abiertas de los diferentes Sistemas de Información, Correo Electrónico y demás aplicaciones al finalizar la jornada de trabajo y apagar el computador, estación de trabajo, portátil, etc., a excepción de los servidores y equipos del área de servidores, los cuales deben permanecer activos las 24 horas.

POLÍTICA 3: CONTROL DE ACCESO

- ✓ En el caso de personas ajenas a la empresa deban ingresar a algún activo informático, la Gerencia y Jefes de Oficina deben autorizar sólo el acceso indispensable de acuerdo con el trabajo a realizar por estas personas, previa justificación y autorización.

- ✓ En todos los contratos deberá hacerse taxativa la cláusula de confidencialidad, responsabilidad, integridad, buen uso, etc., sobre la información institucional que el funcionario en desarrollo de su trabajo deba utilizar.

- ✓ El otorgamiento de acceso a la información está regulado mediante el procedimiento de administración de cuentas de usuario.

- ✓ Todos los accesos y permisos para el uso de los sistemas de información de la empresa deben terminar inmediatamente después de que el trabajador, contratista o pasante cesa de prestar sus servicios a la empresa.

- ✓ Los proveedores o terceras personas solamente deben tener privilegios durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas y debe estar supervisado por el personal División Sistemas cuando el acceso se realice a un Servidor.

- ✓ Todo usuario de los sistemas de información deberá tener asignado una cuenta y una contraseña para su utilización, de acuerdo a los estándares que maneja la División Sistemas, previa solicitud de la División de Talento Humano para trabajadores y/o pasantes y del Supervisor para contratistas. El uso de la misma es responsabilidad de la persona o la que está asignada, es de carácter personal e intransferible.

- ✓ La cuenta de usuario administrador dispone a todos los privilegios y características que le permiten administrar completamente el equipo, por tal motivo dicha cuenta debe manejarse únicamente por el personal de la División Sistemas.

- ✓ Se debe reportar oportunamente los eventos relacionados con traslados, vacaciones, ingresos, retiros de trabajadores, contratistas y/o pasantes de la entidad que ameriten activar y/o desactivar códigos de usuario, crear y/o modificar perfiles y roles de otros existentes, activar y/o desactivar servicios, etc.

POLÍTICA 4: SEGURIDAD DE LOS SERVICIOS INFORMÁTICOS

Uso del Correo Electrónico PO.GDI.014 V4.0

- ✓ Los buzones de Correo electrónico asignados a los trabajadores, contratista, pasantes o dependencias, deben ser usados solamente para el envío o recepción de documentos relacionados con las actividades propias del cumplimiento de las funciones institucionales.

- ✓ El usuario titular de la cuenta de correo es el único y directo responsable de todas las acciones y mensajes que se envíen a través de dicha cuenta.

- ✓ Los usuarios del servicio de Correo Electrónico de la empresa no pueden enviar, distribuir, difundir y participar en la propagación de “cadenas” de mensajes o propaganda comercial.

- ✓ El Correo Electrónico no se debe utilizar para enviar o distribuir ningún mensaje que pueda ser considerado difamatorio, acosador, o explícitamente sexual, o que pueda ofender a alguien con base en su raza, religión, género, nacionalidad, orientación sexual, política o discapacidad.

- ✓ Los mensajes masivos solamente podrán ser enviados siempre y cuando se trate de temas de carácter oficial y de interés general evitando en lo posible enviar archivos anexos de gran tamaño y solamente por personas autorizadas para tal fin. Esto debe hacerse con la autorización del Jefe de Oficina.

- ✓ La empresa se reserva el derecho de acceder y develar todos los mensajes enviados por medio del sistema de correo electrónico Institucional para cualquier propósito. Para este efecto el funcionario, contratista o pasante autorizará a la empresa para realizar las revisiones y/o auditorias respectivas directamente o a través de terceros.

- ✓ Todo uso indebido del correo electrónico, acarrea suspensión temporal de la cuenta de acuerdo al nivel de la falta cometida.

Uso y manejo de Internet PO.GDI.014 V4.0

- ✓ Los trabajadores, contratistas y/o pasantes de la empresa no deben descargar archivos que puedan ser nocivos para los sistemas como virus, software espía, programas maliciosos capaces de alojarse en computadores permitiendo el acceso a usuarios externos y atacantes que pongan en riesgo la seguridad de la información, así mismo no deben acceder a sitios desconocidos o de baja confianza, ni aceptar los mensajes sobre instalación de software que ofrezcan las diferentes páginas sin la debida autorización de la División Sistemas.

- ✓ Para evitar la congestión en los canales de comunicación, la empresa se reserva el derecho de restringir el acceso a ciertas páginas (no oficiales, categorías maliciosas y otras), aplicar limitación de ancho de banda a páginas web, como redes sociales y almacenamiento en la nube no oficial. Si por requerimiento del trabajo se requiere utilizar algunas de las páginas restringidas se debe solicitar la autorización a el área sistemas, por medio de comunicado oficial.

- ✓ Se prohíbe el uso de software que omita las políticas de seguridad de la información, como proxy, Túnel, VPN no autorizada, entre otros.

Uso Red Inalámbrica

- ✓ La Red Inalámbrica de la empresa permitirá el acceso solo al personal autorizado, ya sean trabajadores, contratistas, pasantes o usuarios invitados.

- ✓ La gerencia y el área de sistemas se reserva el derecho de negar el acceso a la Red Inalámbrica en caso que se requiera.

Escritorios Limpios

- ✓ Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel.

- ✓ Todo trabajador, contratista, pasante y/o colaborador de la empresa que se retire de su escritorio por un tiempo prolongado, deberá garantizar el bloqueo de la pantalla del computador, PC, estación de trabajo, servidor u otro equipo con el fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información.

POLÍTICA 5: SEGURIDAD DE COMUNICACIONES Y OPERACIONES

- ✓ Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la empresa, deberán ser consideradas y tratadas como información confidencial. Su diseño, administración,

operación y mantenimiento está a cargo del Proceso de Gestión Informática de la División Sistemas.

- ✓ Todas las conexiones a redes externas de tiempo real que accedan a la red interna de la empresa, deben pasar a través de los sistemas de defensa electrónica que incluyen servicios de cifrado y verificación de datos, detección de ataques cibernéticos, detección de intentos de intrusión, administración de permisos de circulación y autenticación de usuarios.

- ✓ Todo intercambio electrónico de información o interacción entre sistemas de información con entidades externas deberá estar autorizado por la División Sistemas.

- ✓ Los equipos, Servidores, Equipos de Comunicaciones no deben moverse o reubicarse sin la aprobación previa de la División Sistemas.

- ✓ Para seguridad de los equipos tecnológicos (Computadores) debe tenerse en cuenta que la conexión eléctrica debe realizarse a las tomas de corriente regulada (identificadas con color naranja).

- ✓ Los trabajadores, contratistas y pasantes se comprometen a **NO** utilizar la red regulada de energía para conectar equipos eléctricos diferentes a su equipo de cómputo, como impresoras, cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras y en general cualquier equipo que genere caídas de la energía.

- ✓ Los particulares en general, entre ellos, los familiares de todos los trabajadores, contratistas y/o pasantes, no están autorizados para utilizar los recursos informáticos de la empresa.

- ✓ Los equipos de usuarios terceros que deban estar conectados a la Red, deben cumplir con todas las normas de seguridad vigentes en la empresa. La Sociedad Acueducto y Alcantarillado de Popayán S.A. E.S.P. se reserva el derecho de cancelar y terminar la conexión a sistemas de terceros que no cumplan con los requerimientos internos establecidos.

- ✓ La División Sistemas se reserva el derecho de monitorear el tráfico de la red con el fin de garantizar el uso productivo del espacio (ancho de banda), detectar y prevenir fallas, estudiar tendencias de tráfico y detectar y prevenir el acceso no autorizado a los diferentes sistemas de información.

Adquisición de Recursos Tecnológicos

- ✓ Toda adquisición de recursos tecnológicos debe estar avalado por el Comité TI siguiendo los lineamientos del manual de contratación de la empresa, quienes deberán participar en todo el proceso para garantizar las características tecnológicas mínimas, su compatibilidad, confiabilidad y adaptabilidad de los mismos con la infraestructura tecnológica de la empresa.

Acceso al centro de datos

- ✓ Para el ingreso al cuarto de servidores del personal encargado de actividades como: mantenimiento del aire acondicionado, UPS, instalación y mantenimiento de servidores, instalación y mantenimiento de software, los visitantes y el personal de limpieza deberán estar identificados plenamente en sus actividades, y deberá registrar el motivo del ingreso y estar acompañada permanentemente por el personal de la División Sistemas.

- ✓ Todo cambio relacionado con modificación de acceso, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.

- ✓ Las áreas de cableados que la empresa considere críticas como por ejemplo el cuarto de servidores, deben ser lugares de acceso restringido.

POLÍTICA 6: SOFTWARE

- ✓ Está prohibida la descarga y uso de software no autorizado.

- ✓ Los usuarios no pueden descargar y/o emplear archivos de imagen, sonido o similares que estén o puedan estar protegidos por derechos de autor de terceros sin la previa autorización de los mismos.

- ✓ Se realizará seguimiento o revisión para ejercer control sobre el uso de Software legalmente adquirido y licenciado por la empresa.

- ✓ Está prohibida la reproducción de cualquier software perteneciente a la empresa, bien sea que se haya adquirido o desarrollado internamente, para beneficio personal de cualquiera de sus usuarios o de terceras partes.

- ✓ La entrega de software desarrollado (en caso tal de que sea desarrollado en la empresa) a otras entidades debe estar autorizado por la Gerencia de la empresa.

- ✓ Antes de que un nuevo sistema se desarrolle o se adquiera, el Comité TI, deberán definir las especificaciones y requerimientos de seguridad necesarios.

POLÍTICA 7: ALMACENAMIENTO Y RESPALDO

- ✓ La información que es soportada por la infraestructura de tecnología de La Sociedad Acueducto y Alcantarillado de Popayán S.A. E.S.P. deberá ser almacenada y respaldada de acuerdo a lo establecido en el procedimiento "***P.GDI.011 PROCEDIMIENTO COPIAS DE SEGURIDAD BASES DE DATOS Y APLICACIONES***", de tal forma que se garantice su disponibilidad.

- ✓ Los trabajadores, contratistas y pasantes son responsables de los respaldos de la información almacenada localmente en el computador asignado.

POLÍTICA 8: REGISTRO Y AUDITORIA

- ✓ Todos los sistemas automáticos que operen y administren información sensitiva, valiosa o crítica para la empresa, como son sistemas de información en ambiente productivo, sistemas operativos, sistemas de bases de datos y telecomunicaciones deben generar registros de auditoría.

- ✓ Todos los archivos de auditorías deben proporcionar suficiente información para apoyar el monitoreo, control y seguimiento que se requiera y preservarse por períodos definidos según su criticidad y de acuerdo a las exigencias legales para cada caso.

POLÍTICA 9: DISPONIBILIDAD DEL SERVICIO DE LA INFORMACIÓN (PLAN DE CONTINUIDAD)

- ✓ El Proceso de Sistemas definirá, preparará, mantendrá actualizado y probado de forma periódica el Plan de Contingencia, de tal manera que permita a las aplicaciones críticas y sistemas de información, sistemas de cómputo y comunicación, garantizar la continuidad del negocio en el evento de un desastre de grandes proporciones como terremoto, explosión, terrorismo, inundación, fallas eléctricas u otros riesgos que se puedan cristalizar.

POLÍTICA 10: CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

- ✓ Es responsabilidad del Comité TI evaluar, actualizar, verificar y socializar las políticas de seguridad de la información, conforme a esto, el presente documento tendrá una revisión anual, o antes en caso de ser necesario.

- ✓ Estas políticas deben ser socializada de acuerdo a las actualizaciones que puedan llevarse a cabo, y publicarla en el sitio web de la empresa para conocimiento de todo el personal objetivo e incluirla en el proceso de inducción de nuevos trabajadores, contratistas y/o pasantes.

- ✓ El líder del Proceso de Gestión Informática a través de los trabajadores responsables de administrar la infraestructura de las Tecnologías de la Información y las Comunicaciones será el responsable de efectuar el seguimiento al cumplimiento de las Políticas de Seguridad de la Información con el fin de verificar y controlar que se esté aplicando adecuadamente. Los casos de incumplimiento serán reportados a la Gerencia, para ser aplicadas las sanciones a que haya lugar.

Descripción	Elaboró	Revisó	Aprobó
Nombre: Cargo: Fecha: Firma:	Carlos Andrés Silva G Jefe División Sistemas 21/01/2022	Alex Ortega Certuche Subgerente Planeación Estudios (E). 28/01/2022	Hernando Alfonso Pérez Gerente 28/01/2022