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

DIVISIÓN SISTEMAS
GESTIÓN INFORMÁTICA

POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
ACTUALIZADO 2026

Contenido

DESCRIPCIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las Políticas de Seguridad de la Información establecen el marco de referencia para la protección de la información y de los activos tecnológicos de La Sociedad Acueducto y Alcantarillado de Popayán S.A. E.S.P., con el fin de preservar la confidencialidad, integridad y disponibilidad de la información, así como asegurar la continuidad de los procesos misionales y de apoyo de la empresa.

A través de estas políticas se definen los lineamientos generales, responsabilidades y controles mínimos que deben ser adoptados por los trabajadores, contratistas, proveedores y terceros que tengan acceso a la información o a los sistemas de información de la entidad, promoviendo una gestión de la seguridad de la información coherente, consistente y alineada con las necesidades del negocio.

Las políticas se aplican de manera transversal en la empresa y buscan fortalecer la prevención, detección y respuesta frente a riesgos e incidentes de seguridad de la información, así como fomentar una cultura de uso responsable de la información y de los recursos tecnológicos, en concordancia con la normatividad vigente y las mejores prácticas aplicables.

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 TI), 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 diagnóstico 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 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.

Procedimientos asociados:

- P.GDI.007 Procedimiento Gestión de usuarios y contraseñas
- P.GDI.014 Procedimiento de Aseguramiento de Servicios en la Red
- P.GDI.016 Procedimiento Control de Acceso Físico al Centro de Datos

POLITICA 4: PROTECCION PARA EL ACCESO REMOTO A LA INFORMACION PERSONAL

La conexión remota a la red interna de Acueducto y Alcantarillado de Popayán S.A. E.S.P. deberá realizarse a través de una conexión VPN segura provista por La División Sistemas y accesible solo por usuarios autorizados, quienes deberán seguir los lineamientos establecidos para el uso adecuado de los servicios de VPN.

Lineamientos para el Servicio de Acceso Remoto (VPN)

Solicitudes de acceso a servicios VPN: Los servicios VPN deben ser solicitados por el jefe inmediato o supervisor de contrato, incluyendo el nombre completo del usuario que utilizará el servicio, la dependencia, el correo electrónico institucional del usuario, una descripción remota de las necesidades de acceso y fecha hasta va a estar activo el servicio y para contratistas, no más del tiempo de ejecución del contrato.

Condiciones de Uso del Servicio de VPN: Se asignarán en función de la disponibilidad de las licencias. Solo los usuarios previamente autorizados pueden utilizar el servicio de VPN y serán responsables del buen uso del acceso remoto.

- El Servicio de acceso remoto VPN solo se debe utilizar para tareas relacionadas con la funcionalidad o el cumplimiento de obligaciones contractuales y debe mantener la confidencialidad e integridad de la información a la que acceda a través de conexiones remotas.
- Los nombres de usuario y las contraseñas se proporcionarán al acceder al servicio VPN, estos nombres de usuario y contraseñas son solo para uso personal y no deben compartirse ni dejarse para que los vean terceros.
- Después de 10 minutos de inactividad, la sesión se desconecta automáticamente y el usuario debe autenticarse nuevamente para acceder al servicio VPN.
- Si los usuarios descubren que sus datos de acceso están siendo utilizados por personas no autorizadas o que existe un problema de seguridad, deben notificarlo División Sistemas de inmediato.
- La División Sistemas no se responsabiliza por cualquier pérdida de información debido a virus o mala manipulación de los computadores o equipos con el que accede el usuario.
- Los usuarios que no cumplan la política de acceso remoto (VPN) y los lineamientos para el servicio de VPN, se le bloqueará inmediatamente el acceso a este servicio.

Suspensión o cancelación del acceso al servicio VPN: El jefe inmediato o supervisor deberá solicitar la suspensión o cancelación del servicio VPN enviando un correo electrónico a la División Sistemas, explicando el motivo correspondiente.
A los usuarios que no utilicen el servicio VPN durante 2 meses consecutivos se les suspenderá el acceso y La División Sistemas notificará al usuario y al Jefe inmediato o supervisor del contrato por correo electrónico. Si no hay comunicación de activación de

acceso en el plazo de un mes desde la notificación, los datos de acceso al servicio VPN serán eliminados. Si se eliminan los datos de acceso al servicio VPN por inactividad o solicitud explícita, y el usuario necesita de nuevo el servicio VPN, deberá volver a realizar la solicitud.
Si el usuario se desvincula de la entidad, los datos de acceso al servicio VPN serán eliminados.

Recomendaciones para el Uso del Servicio de VPN: El computador o dispositivo con el que va a iniciar la conexión debe tener instalado un firewall o cortafuegos, antivirus actualizado, aplicaciones y sistema operativo actualizado, además debe estar configurada la activación automática del protector de pantalla con la contraseña de entrada, para que en caso de dejar abierta la sesión de manera involuntaria se pueda evitar el acceso al equipo por personal no autorizado.

- No usar el servicio de VPN en caso de que el computador o dispositivo con el que va a iniciar la conexión se encuentre infectado por virus o cualquier amenaza informática.
- El servicio de VPN no debe utilizarse desde computadores públicos y redes no confiables como cafés internet o redes inalámbricas públicas.
- En caso de pérdida o robo del equipo con el que accede al servicio de VPN, debe informar lo más pronto posible a la División Sistemas para bloquear la cuenta de acceso asignada.
- Cerrar sesión y desconectarse del servicio de VPN una vez finalizadas las labores realizadas en la conexión remota.
- En caso de presentar algún inconveniente con el uso del servicio de VPN, debe reportarlo a la División Sistemas.

POLÍTICA 5: SEGURIDAD DE LOS SERVICIOS INFORMÁTICOS

Uso del Correo Electrónico PO.GDI.001 V6.0

La Sociedad Acueducto y Alcantarillado de Popayán S.A. E.S.P. por medio de la División Sistemas suministra la dirección de correo electrónico institucional a los trabajadores y contratistas de la sociedad, así como los datos de acceso.
La cuenta de correo que proporciona LA EMPRESA se destinará a uso profesional, no pudiéndose utilizar para fines particulares, excepto en casos puntuales justificados.
La información de la empresa será enviada regularmente al correo electrónico para colaborar con el medio ambiente en el ahorro de papel, por esto se recomienda revisar regularmente el correo electrónico.

Autenticación y Acceso Seguro

- **Contraseñas fuertes:** los usuarios deberán crear sus contraseñas seguras (mínimo 12 caracteres con combinaciones de mayúsculas, minúsculas, números y símbolos).
- **Gestión de credenciales:** Se prohíbe compartir contraseñas y fomentar el uso de administradores de contraseñas para almacenar credenciales de forma segura.

Código de Conducta.

- **Reconocimiento de amenazas:** Reportar a la División Sistemas correos sospechosos, enlaces no confiables y archivos adjuntos potencialmente peligrosos.
- **Buenas prácticas:** El uso de correo institucional es exclusivamente para fines laborales y por lo tanto se debe evitar el uso de cuentas personales para actividades empresariales.

Está prohibida la suscripción del correo electrónico institucional a servicios de noticias no relacionados con la actividad profesional.

Todos los trabajadores y contratistas de La Sociedad que dispongan de una cuenta de correo institucional seguirán las siguientes buenas prácticas:

- No facilitar la cuenta de correo a personas no autorizadas.
- No utilizar la cuenta de correo como dirección de contacto en trámites personales.
- No utilizar el correo institucional con fines comerciales o financieros sin relación con La Sociedad.
- No participar en el envío de cadenas de correos.

- No distribuir mensajes con contenidos inapropiados (contenido ofensivo, homófobo, racista, discriminatorio, ...)

Verificación previa al envió del Correo Electrónico.

Se deberá verificar el destinatario y el contenido del mensaje antes de enviarlo. El usuario deberá incluir en sus correos su nombre completo y el cargo que ocupa.

La Sociedad Acueducto y Alcantarillado de Popayán S.A. E.S.P. podrá acceder a las cuentas corporativas de los usuarios en caso de enfermedad, vacaciones o despido de los empleados para continuar realizando las actividades propias de su puesto trabajo.

Ese acceso se realizará únicamente en caso de ser necesario, a solicitud del jefe inmediato del trabajador y con conocimiento del Jefe de la División Talento Humano de la sociedad.

Es obligación del trabajador borrar todos los mensajes de carácter personal que pudieran estar contenidos en su buzón de correo periódicamente.

> **El almacenamiento en el servidor de correo tiene un espacio limitado, por lo que es importante gestionar de manera eficiente el uso del correo electrónico. Se recomienda no almacenar ni duplicar correos electrónicos que incluyan archivos adjuntos de gran tamaño, ya que esto puede ocupar espacio innecesario y afectar el rendimiento del sistema. Además, es fundamental evitar el uso del correo interno para guardar información personal o confidencial, ya que esto podría comprometer la seguridad de los datos. Optar por soluciones de almacenamiento externas o respaldos organizados puede ayudar a mantener el sistema eficiente y seguro.**

Uso y manejo de Internet PO.GDI.001 V6.0

La Sociedad Acueducto y Alcantarillado de Popayán S.A. E.S.P. por medio de la División Sistemas controla por motivos de seguridad los accesos a Internet realizados desde sus instalaciones y monitoriza el uso de este. Consultar páginas no autorizadas y realizar descargas de sitios no controlados puede suponer un peligro para los sistemas de información de la Empresa. **El acceso a Internet en horario de trabajo y desde equipos de la Empresa será moderado y alineado con las tareas y responsabilidades de cada trabajador no afectando en ningún caso a la productividad de la empresa.**

Está prohibido:

- El acceso a sitios web no relacionados con las actividades de la empresa (por ejemplo, plataformas de streaming, juegos en línea o redes sociales específicas).

- El acceso a páginas de contenido ilícito o que atenten contra la dignidad humana: aquellas que realizan apología del terrorismo, pornográficos, páginas con contenido xenófobo, racista, o antisemita, etc…
- La participación en foros o chats de discusión.
- La descarga de ficheros, programas o documentos que pueda afectar el ancho de banda o introducir riesgos de seguridad y que contravengan las normas de la empresa sobre instalación de software y propiedad intelectual.
- El uso de YouTube y plataformas para reproducir música y/o emisoras que afecten el ancho de banda.

Acceso controlado: Se permite el uso de YouTube, Vimeo o plataformas similares únicamente para fines educativos, capacitación o actividades laborales específicas.

Ejemplos de páginas web autorizadas son aquellas que:

- Faciliten un contenido relacionado con la función del trabajador en la empresa (por ejemplo, sitios institucionales, revistas especializadas, etc…)
- Faciliten noticias de interés general (como periódicos digitales, etc…)
- Faciliten servicios de guías telefónicas, callejeros, meteorología, etc…
- Faciliten el aprendizaje, la capacitación y el desarrollo profesional.

En todo caso, la consulta de estas páginas no podrá resultar abusiva.

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.

Documentos asociados:

- P.GDI.007 Procedimiento Gestión de usuarios y contraseñas
- P.GDI.014 Procedimiento de Aseguramiento de Servicios en la Red
- P.GDI.015 Procedimiento de Capacitación y Sensibilización del Personal en TIC
- P.GDI.016 Procedimiento Control de Acceso Físico al Centro de Datos
- P.GDI.017 Procedimiento de Gestión de Incidentes de Seguridad de la Información
- PO.GDI.001 Políticas de Seguridad de los Servicios Informáticos (Software, Internet y Correo Electrónico)

POLÍTICA 6: 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.

Procedimientos asociados:

- P.GDI.007 Procedimiento Gestión de usuarios y contraseñas
- P.GDI.014 Procedimiento de Aseguramiento de Servicios en la Red
- P.GDI.015 Procedimiento de Capacitación y Sensibilización del Personal en TIC
- P.GDI.016 Procedimiento Control de Acceso Físico al Centro de Datos
- P.GDI.017 Procedimiento de Gestión de Incidentes de Seguridad de la Información

POLÍTICA 7: 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.

Documentos asociados:

- PO.GDI.001 Políticas de Seguridad de los Servicios Informáticos (Software, Internet y Correo Electrónico)
- P.GDI.013 Procedimiento Administración de licencias de software

POLÍTICA 8: 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.

- ✓ La información está respaldada tanto en servidores, Copias de Seguridad en físicos y en la nube de manera automática.

- ✓ Se cuenta con un servicio de nube corporativa (servicio de almacenamiento) para que los usuarios internos compartan su información, así como respaldarla. Este servicio está controlado por medio de usuarios y contraseña.

Documentos asociados:

- P.GDI.011 Procedimiento Copias de Seguridad Bases de Datos y Aplicaciones
- F.GDI.005 Control de Copias de Seguridad

POLITICA 9: POLÍTICA DE GESTIÓN DE VULNERABILIDADES Y ACTUALIZACIONES DE SEGURIDAD

Esta política aplica a todos los sistemas de información, aplicaciones, equipos, dispositivos, redes, infraestructura tecnológica y servicios tecnológicos utilizados por La Sociedad, independientemente de si son administrados internamente o por terceros.

Lineamientos generales

- La empresa deberá identificar y evaluar periódicamente las vulnerabilidades de seguridad que puedan afectar sus activos tecnológicos, de acuerdo con su nivel de criticidad y exposición al riesgo.
- Las actualizaciones y parches de seguridad deberán ser aplicados de manera oportuna, priorizando los sistemas críticos y aquellos expuestos a redes públicas o externas.
- Las vulnerabilidades identificadas deberán ser analizadas para determinar su impacto y probabilidad, definiendo acciones de mitigación, corrección o aceptación del riesgo, según corresponda.
- Cuando no sea posible aplicar una actualización o parche de forma inmediata, se deberán implementar controles compensatorios que reduzcan el riesgo.
- Las actividades de actualización y aplicación de parches deberán planificarse y ejecutarse procurando minimizar el impacto en la operación del negocio.
- Los proveedores y terceros que administren sistemas o servicios tecnológicos de la empresa deberán cumplir con los lineamientos definidos en esta política.
- Las vulnerabilidades y actualizaciones relevantes deberán ser registradas y seguidas hasta su cierre.

Responsabilidades

- **División Sistemas:** Coordinar la identificación de vulnerabilidades, la aplicación de actualizaciones y el seguimiento de las acciones definidas.
- **Usuarios:** Facilitar la aplicación de actualizaciones en los equipos que utilicen y reportar cualquier comportamiento anómalo.

- **Proveedores y terceros:** Aplicar las actualizaciones y parches de seguridad en los sistemas bajo su responsabilidad, conforme a los acuerdos contractuales.
- **División Control Interno:** Apoyar la verificación del cumplimiento de la presente política.

Cumplimiento

El incumplimiento de esta política podrá dar lugar a la aplicación de las acciones administrativas, disciplinarias o contractuales correspondientes, de acuerdo con la normatividad interna vigente.

POLÍTICA 10: 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.

POLITICA 11: POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Esta política aplica a todos los trabajadores, contratistas, proveedores y terceros que tengan acceso a los activos de información, sistemas de información, infraestructura tecnológica o información de la empresa.

Definición de incidente de seguridad de la información

Se considera incidente de seguridad de la información cualquier evento real o potencial que comprometa o pueda comprometer la confidencialidad, integridad o disponibilidad de la información, los sistemas de información o los servicios tecnológicos de la empresa.

Lineamientos generales

- Todo incidente de seguridad de la información, real o sospechado, debe ser reportado de manera inmediata a la División Sistemas.
- Los incidentes deben ser gestionados de forma oportuna, ordenada y documentada, priorizando la reducción del impacto operativo, legal, reputacional y financiero.
- Se deberán definir y aplicar acciones de contención, corrección y recuperación, según la naturaleza y severidad del incidente.
- La información relacionada con los incidentes será tratada de manera confidencial y solo será divulgada a las partes autorizadas.
- Cuando el incidente involucre información sensible, datos personales o servicios críticos, se deberá escalar oportunamente a la alta dirección y a las áreas correspondientes.
- La empresa deberá realizar análisis posteriores a los incidentes, con el fin de identificar causas raíz y definir acciones de mejora que eviten su recurrencia.

Roles y responsabilidades

- **Usuarios:** Reportar oportunamente cualquier incidente o situación anómala relacionada con la seguridad de la información.
- **División Sistemas:** Coordinar la gestión de los incidentes, ejecutar las acciones técnicas necesarias y mantener el registro de los mismos.
- **División Control Interno:** Verificar el cumplimiento de la política y apoyar el seguimiento a las acciones correctivas.
- **Gerencia:** Tomar decisiones estratégicas cuando la gravedad del incidente lo requiera.

Registro y seguimiento

Todos los incidentes de seguridad de la información deberán ser registrados, documentados y seguidos hasta su cierre, incluyendo las acciones implementadas y las lecciones aprendidas, con el fin de fortalecer continuamente los controles de seguridad.

Cumplimiento

El incumplimiento de la presente política podrá dar lugar a las acciones administrativas, disciplinarias o contractuales que correspondan, de acuerdo con la normatividad interna vigente.

POLÍTICA 12: 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.

Procedimiento asociado:

- P.GDI.005 Procedimiento Restablecimiento del Sistema y Bases de Datos

POLÍTICA 13: 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.

Procedimientos asociados:

- P.GDI.007 Procedimiento Gestión de usuarios y contraseñas
- P.GDI.014 Procedimiento de Aseguramiento de Servicios en la Red
- P.GDI.015 Procedimiento de Capacitación y Sensibilización del Personal en TIC
- P.GDI.017 Procedimiento de Gestión de Incidentes de Seguridad de la Información.

POLITICA 14: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA PROVEEDORES Y TERCEROS

Esta política aplica a todos los proveedores, contratistas y terceros que, directa o indirectamente, tengan acceso a información de la empresa o participen en la operación, soporte, desarrollo, mantenimiento o administración de servicios tecnológicos y de información.

Lineamientos generales

- Todo proveedor o tercero deberá cumplir con los lineamientos de seguridad de la información definidos por la empresa, de acuerdo con el nivel de acceso y criticidad del servicio prestado.
- El acceso a la información o a los sistemas de la empresa deberá otorgarse únicamente cuando sea estrictamente necesario y bajo el principio de mínimo privilegio.
- Los proveedores y terceros deberán comprometerse a mantener la confidencialidad de la información a la que tengan acceso, incluso después de finalizada la relación contractual.
- Los accesos otorgados a proveedores y terceros deberán ser controlados, monitoreados y revocados oportunamente una vez finalice el contrato o servicio.
- Cuando un proveedor gestione o almacene información de la empresa, deberá implementar controles razonables de seguridad para su protección.
- Los incidentes de seguridad de la información que involucren a proveedores o terceros deberán ser reportados de manera inmediata a la empresa y gestionados conforme a la Política de Gestión de Incidentes de Seguridad de la Información.
- La empresa podrá realizar verificaciones razonables del cumplimiento de esta política, de acuerdo con la criticidad del servicio y los recursos disponibles.

Responsabilidades

- **Proveedores y terceros:** Cumplir los lineamientos de esta política y reportar cualquier incidente de seguridad de la información que afecte o pueda afectar a la empresa.
- **Área responsable del contrato:** Verificar que los proveedores y terceros conozcan y acepten los requisitos de seguridad de la información.
- **División Sistemas:** Definir los accesos, controles técnicos y lineamientos de seguridad aplicables a proveedores y terceros.
- **División Control Interno:** Apoyar el seguimiento y verificación del cumplimiento de la presente política.

Cumplimiento

El incumplimiento de esta política por parte de proveedores o terceros podrá dar lugar a la aplicación de las medidas contractuales, legales o administrativas correspondientes, conforme a lo establecido en los contratos y la normatividad vigente.

POLITICA 15: POLITICA DE TRANSFERENCIA DE INFORMACION

Para el cumplimiento de sus obligaciones la Sociedad Acueducto y Alcantarillado de Popayán S.A. E.S.P. intercambia información con el Municipio de Popayán, y con le empresa del Servicio Aseo Urbaser Popayán S.A. E.S.P. por diferentes medios electrónicos cumpliendo con los principios de confidencialidad, integridad y disponibilidad.
Los lineamientos que se establecieron para garantizar que el intercambio de información se realice bajo altos niveles de protección siempre que se vaya a transferir información de nuestros usuarios se deberá cumplir con lo siguiente:

Intercambio de Información entre trabajadores y/o contratistas del Acueducto y Alcantarillado de Popayán S.A. E.S.P.

Solo se puede realizar intercambio de información entre los trabajadores y contratistas cuando dicho intercambio corresponda a actividades relacionadas con el desarrollo de sus labores.
Siempre que se realice intercambio de información catalogada como pública clasificada o pública reservada, dicho intercambio debe ser aprobado por el jefe inmediato o supervisor de contrato.

Intercambio de información con terceros.

Todo intercambio de información electrónica perteneciente al Acueducto y Alcantarillado de Popayán S.A. E.S.P. con terceros, debe ser respaldado con un acuerdo (convenio o contrato), incluyendo una cláusula de confidencialidad y no divulgación de la información proporcionada.

La solicitud de intercambio de información puede ser por requerimientos de la Sociedad Acueducto y Alcantarillado de Popayán S.A. E.S.P., de un organismo externo, ente de control o incluso de un tercero que, ante disposiciones legales o directrices del gobierno hacen necesaria dicha interoperabilidad.
La excepción en la entrega de información debe estar regida por lo establecido según legislación vigente.
La información recibida de otra entidad en Colombia se debe salvaguardar a un nivel igual o mayor que el aplicado por la entidad que originó el documento.
El intercambio de información digital pública clasificada y pública reservada, debe realizarse por canales cifrados que garanticen la protección de la confidencialidad de la información y que cumpla con la política de controles criptográficos, esto debe quedar registrado en los convenios o acuerdos de intercambio de información que firmen las partes.

Intercambio de Información Física

El intercambio de información que se encuentre en formatos físicos debe estar debidamente etiquetada, en caso de que sea catalogada como pública clasificada o pública reservada, el intercambio debe realizarse en un sobre sellado para ser enviada a terceros.
Para el transporte de medios físicos de información sensibles, se debe generar una bitácora de entrega de estos medios y recepción de estos.
Se debe transportar en un dispositivo con un sello de seguridad que garantice que en su desplazamiento no ha sido intervenido por un tercero.

Intercambio de información vía correo electrónico institucional

Toda información enviada desde la Sociedad Acueducto y Alcantarillado de Popayán S.A. E.S.P a través de correos electrónicos deberá incluir en su pie de página la siguiente advertencia:
Este mensaje y cualquier archivo que se adjunte al mismo es confidencial y podría contener información clasificada y reservada de la Sociedad Acueducto y Alcantarillado de Popayán S.A. E.S.P, para el uso exclusivo de su destinatario. Si usted no es el receptor autorizado, cualquier retención, difusión, distribución o copia de este mensaje es prohibida y sancionada por la ley. Si por error recibe este mensaje, por favor reenviarlo al remitente y borrar el mensaje recibido inmediatamente.

Documento asociado:

- ACUERDO DE CONFIDENCIALIDAD AAPSA

POLITICA 16: POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

Esta política aplica a todos los trabajadores, contratistas, proveedores y terceros que, en el ejercicio de sus funciones, tengan acceso, traten o administren datos personales de la empresa, independientemente del medio o formato en el que se encuentren.

Lineamientos generales

- La empresa contará con un documento específico que establece la Política de Protección de Datos Personales, el cual define los principios, derechos, deberes y procedimientos aplicables al tratamiento de datos personales.
- El tratamiento de datos personales deberá realizarse conforme a lo establecido en la Política de Protección de Datos Personales vigente y a la normatividad legal aplicable.
- Los datos personales serán considerados información sensible o crítica, según corresponda, y deberán ser protegidos mediante los controles de seguridad definidos en la Política de Seguridad de la Información.
- Los incidentes de seguridad que involucren datos personales deberán ser gestionados conforme a la Política de Gestión de Incidentes de Seguridad de la Información.
- Los proveedores y terceros que tengan acceso a datos personales deberán cumplir tanto la Política de Seguridad de la Información como la Política de Protección de Datos Personales de la empresa.

Documento asociado

- **Política de Protección de Datos Personales** (documento vigente)

Cumplimiento

El incumplimiento de lo dispuesto en la presente política podrá dar lugar a las acciones administrativas, disciplinarias o contractuales correspondientes, de acuerdo con la normatividad interna y legal vigente.