PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

INTRODUCCIÓN

La información constituye uno de los activos más valiosos de cualquier organización. Por ello, es crucial garantizar su seguridad, preservando su confidencialidad, integridad y disponibilidad. Este documento se fundamenta en el Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y las mejores prácticas internacionales, como ISO/IEC 27001:2022.

El Plan de Seguridad y Privacidad de la Información busca fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI) en la Empresa de Acueducto, Alcantarillado y Aseo de El Espinal ESP (EAAA ESP), promoviendo una cultura de seguridad digital e implementando controles para mitigar riesgos.

1. ALCANCE

Este Plan aplica a todos los activos de información de la EAAA, incluyendo:

Sistemas críticos: GCI, GCIPRO, ORFEO, GLPI

Infraestructura: Servidores, Fortinet firewall, red LAN/WAN

Funcionarios: 100% administrativos + personal operativo clave

Terceros: Contratistas con acceso a datos sensibles

Meta 2026: Alcanzar 75/100 en Instrumento MSPI MinTIC (partiendo de 65/100 en 2025).

2. DEFINICIONES.

2.1. Seguridad de la Información

La seguridad y privacidad de la información se entiende como la preservación de las siguientes características:

- **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

- **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

- **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

- **Autenticidad:** busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

- **Auditabilidad:** define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

- **Protección a la duplicación:** consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

- **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta La Empresa de acueducto alcantarillado y aseo de El Espinal ESP.

- **Confiabilidad de la Información:** es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

- **Información:** Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

- **Sistema de Información:** Se refiere a un conjunto independiente de recursos de información organizados para la recopilación,

procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

- **Tecnología de la Información:** Se refiere al hardware y software operado por La Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP.. o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la misma, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

2.2. Evaluación de Riesgos

Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en el funcionamiento normal de La Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP..

2.3. Administración de Riesgos

Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

2.4. Comité de Seguridad de la Información

El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas de La Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP. destinado a garantizar el apoyo de la gerencia a las iniciativas de seguridad.

2.5. Responsable de Seguridad Informática

Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a

los integrantes. La Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP.. que así lo requieran, profesional con experiencia en seguridad informática.

2.6. Incidente de Seguridad

Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

2.7. Correo electrónico masivo

El correo electrónico masivo se refiere a cualquier mensaje de correo electrónico enviado a una larga lista de destinatarios que tiene un contacto idéntico para cada persona.

3. DIAGNÓSTICO ACTUAL (resumen mejorado)

Resultado MSPI 2025: 65/100 - NIVEL EFECTIVO

✓ Procesos y controles documentados y comunicados

⚠ Controles efectivos, pero aplicación inconsistente

⚠ Detección de desviaciones poco probable

Brechas críticas identificadas:

1. Sin procedimiento formal de incidentes de seguridad
2. Cultura de reporte de incidentes en desarrollo
3. Auditorías internas no sistematizadas

4. REQUISITOS PARA LA GESTIÓN DE LA SEGURIDAD Y PRIVACIDAD

4.1 Actividades clave para la implementación del SGSI

1. Institucionalizar la Política de Gobierno Digital.
2. Centrar la atención en el usuario.
3. Implementar un sistema de gestión de Tecnologías de Información.
4. Implementar un sistema de gestión de seguridad de la información (SGSI).

4.2 Factores clave para el éxito del SGSI

- Compromiso y apoyo de la dirección de la EAAA ESP.
- Concientización y capacitación de todos los funcionarios.
- Evaluación de riesgos adecuada a los procesos de la EAAA ESP.
- Compromiso de mejora continua.
- Desarrollo y aplicación de políticas en aspectos como uso de equipos, protección de datos personales y uso adecuado del internet.
- Mejora de la organización y comunicación interna.

4.3 Obstáculos para la implementación efectiva del SGSI

- Falta de sensibilización de los funcionarios sobre la importancia de la seguridad.
- Incumplimiento de acciones, planes y políticas.
- Descubrimiento continuo de no conformidades en comités de dirección.

- Resistencia al cambio por parte del personal.
- Planes de formación inadecuados.
- Definición poco clara del alcance del SGSI.
- Exceso de medidas técnicas en detrimento de la formación y concientización.
- Falta de comunicación de los progresos a la organización.

---

5. POLÍTICAS ACTUALIZADAS

5.1 Seguridad Tecnológica y Organizacional

- Control de Acceso: Uso obligatorio de contraseñas robustas y autenticación multifactor (MFA).
- Protección contra Amenazas: Implementación de sistemas avanzados de detección de intrusos (IDS) y protección contra ransomware.
- Actualizaciones y parches: Garantizar que todos los sistemas operativos y aplicaciones estén actualizados regularmente.

5.2 Cultura Organizacional

- Capacitación: Realizar talleres trimestrales sobre ciberseguridad.
- Campañas: Divulgar buenas prácticas mediante boletines y afiches.

5.3 Gestión de Riesgos

- Evaluación Periódica: Revisar riesgos semestralmente.
- Planes de Continuidad: Diseñar escenarios de recuperación ante desastres.

---

6. RESPONSABILIDADES

Comité de Seguridad de la Información

- Revisar y actualizar anualmente las políticas de seguridad.
- Aprobar los lineamientos de capacitación y comunicación.

Grupo de Apoyo a la Seguridad

- Supervisar la implementación de controles técnicos y organizativos.
- Gestionar incidentes y reportes de seguridad.

Funcionarios y Contratistas

- Cumplir las políticas establecidas.
- Reportar incidentes o brechas de seguridad.

6. FASE DE DIAGNÓSTICO

El proceso de gestión tecnológica en la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP, es un proceso de apoyo, conformado por el área de Tecnologías de Información y comunicación que tiene como objeto garantizar el efectivo apoyo tecnológico a las diferentes áreas de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP, mediante la asignación, administración y mejora de los recursos tecnológicos disponibles (hardware, software, redes y comunicaciones).

6.1 ACTIVIDADES

A la fecha de elaboración de este diagnóstico, el proceso de gestión tecnológica tiene las siguientes actividades en su proceso:

6.1.1 ADMINISTRAR REDES Y COMUNICACIONES.

Esta actividad permite gestionar y administrar las comunicaciones entre los distintos dispositivos que se conectan a las redes LAN y WAN de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP, mediante la administración de un dispositivo firewall marca FORTINET, y Access point marca SYMANTEC.

6.1.2. REALIZAR ADMINISTRACIÓN, SOPORTE DE SOFTWARE.

En esta actividad se atienden los requerimientos de software para la gestión de la información. Se maneja el siguiente software:

- Software GCI y GCIPRO(Gestión Comercial Integrada).
- Software de gestión documental ORFEO.
- Soporte de aplicaciones de ofimática.
- Software para dispositivos móviles de los funcionarios operativos
- Software de gestión de Tecnologías (GLPI)
- Software para aplicación para dispositivos móviles para los usuarios.

6.1.3. BRINDAR SOPORTE A USUARIOS INTERNOS (HARDWARE).

En esta actividad se emplea la metodología para garantizar el adecuado funcionamiento de los computadores, servidores y periféricos de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP, de forma que su rendimiento sea adecuado y el almacenamiento de la información sea confiable. Se realizan las siguientes acciones:

- Instalación y configuración de computadores y periféricos

- Mantenimiento de equipos correctivo y preventivo.

Para la realización de las actividades del soporte realizado se basa en los acuerdo de nivel de servicio establecidos por LA OFICINA ASESORA DE PLENACIÓN Y TIC y se utiliza la plataforma GLPI, lo que permite tener un mayor control de las actividades realizadas y el cumplimiento de los ANS

6.1.4. REALIZAR MANTENIMIENTO EN LA PAGINA WEB Y CORREOS INSTITUCIONALES.

En esta actividad se emplea la metodología que permite mantener actualizados los procedimientos en la página web de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP, así como la información que en ella se publica. Esto con el fin de garantizar su adecuado funcionamiento en cumplimiento de los requerimientos normativos. Así mismo la gestión de los correos institucionales con el fin de garantizar su adecuado funcionamiento.

Para estas actividades se implementó el desarrollo de los niveles de accesibilidad web que son requeridos por el Ministerio de Tecnologías De Información Y Comunicación.

6.1.5. REALIZAR ADMINISTRACIÓN DE BASES DE DATOS Y SEGURIDAD DE LA INFORMACIÓN.

Esta actividad se emplea la metodología que permite garantizar un adecuado almacenamiento de la información en bases de datos de las distintas aplicaciones y software que tiene la Acueducto Alcantarillado y Aseo de El Espinal ESP, el control al acceso que se ejerce sobre los datos que en ella se tienen.

Se realiza adicionalmente un mínimo de dos mantenimientos lógicos a las bases de datos de las aplicaciones principales utilizadas en la entidad.

6.1.6. REALIZAR ADMINISTRACIÓN DE SERVIDORES

Se administra las diferentes aplicaciones que permite la gestión de información con el software que se maneja dentro de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP.

6.1.7 ADMINISTRACIÓN DE REDES SOCIALES

Se administran las cuentas de redes sociales de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP, con el fin de informar a la comunidad las labores realizadas por los funcionarios, y noticias que se presenten relacionadas con la funcionalidad de la entidad. Así mismo se busca aumentar la buena imagen de la entidad en la comunidad.

6.2 ANÁLISIS DEL PROCESO DE GESTIÓN TECNOLÓGICA

Realizando una lectura y análisis de las actividades del proceso de gestión tecnológica, se observa que se encuentra en proceso el desarrollo e implementación de actividades y/o soportes documentales sobre la seguridad y privacidad de la información, igualmente los elementos relacionados a los análisis de riesgo, no solo a nivel de Tecnologías de la Información (TI), sino también a la infraestructura física que aloja los activos. Se evidencia el desarrollo documental de procesos, actividades y/o buenas prácticas de Seguridad de la Información, esto se realiza de acuerdo a las acciones de mejora establecidas en diagnósticos anteriores y la necesidad

de implementar un Sistema de Gestión de Seguridad SGSI, así como de documentar las buenas prácticas sugeridas por los estándares (ISO 27001:2013) y otras normas que tienen relevancia en Seguridad de la Información.

Se observa que la gestión ante los problemas de seguridad en el proceso de gestión tecnológica es proactiva y reactiva, las brechas en la seguridad, si son detectadas, son controladas por acciones de momento o acciones de recuperación de desastres, a su vez existe una gestión del riesgo que permite preservar la confidencialidad, integridad y disponibilidad de la información. Así mismo las responsabilidades para proteger la seguridad, confidencialidad e integridad han sido asignadas a cada funcionario, y se han implementado medidas para soportar la administración de la misma.

En la lectura del proceso de gestión tecnológica, se encuentra en proceso de desarrollo procedimientos, actividades y responsables, relacionados con los registros que generan los dispositivos implementados en la arquitectura tecnológica en la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP.

Teniendo en cuenta que la información es unos de los activos más valiosos en una entidad, independiente de su naturaleza pública o privada, y que es fundamental para el desarrollo de los procesos que se adelantan al interior de una organización, se debería tener una valoración de estos activos, con el fin de analizar los impactos económicos que generaría una brecha de seguridad y con base en esto, crear controles y políticas que permitan garantizar la seguridad y privacidad de la información en la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP.

La constante evolución de las Tecnologías de la información y las comunicaciones, genera un aumento en las amenazas que se puedan encontrar en un ambiente organizacional, es por esto que periódicamente el comité de seguridad de la información, deberá evaluar, revisar y ajustar los controles para garantizar la efectividad ante la evolución de las TICS; esta serie de actividades deberá garantizar la protección de la información, evitar su pérdida, garantizar la confidencialidad y la accesibilidad que se

requiera por parte de los funcionarios de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP, contratistas y partes interesadas.

En el comité de seguridad de la información conscientes de las vulnerabilidades en la gestión de la seguridad relacionados protección de la información, los activos que la resguardan y el fortalecimiento de la cultura de seguridad y privacidad de la información en los funcionarios, contratistas y terceros, se compromete al fortalecimiento de su proceso en el sistema integrado de gestión, a realizar e implementar las acciones necesarias, con el fin de disminuir el impacto generado por las brechas de seguridad y a mantener un nivel de seguridad adecuado, de acuerdo con las necesidades de los distintos grupos de interés en la Acueducto Alcantarillado y Aseo de El Espinal ESP, esto con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones, la adopción de las buenas prácticas de los estándares ISO/ IEC 27001:2013 y el marco jurídico vigente y aplicables a empresa del Sector de los Servicios Públicos.

6.3 INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD.

Para determinar el estado actual de seguridad y privacidad de la información se empleó como herramienta de diagnóstico el Instrumento de Evaluación MSPI establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). En esta etapa fue necesario identificar cómo se está garantizando la privacidad sobre todo el ciclo de la información que se tiene en la entidad verificando la implantación o no de medidas que dan cumplimiento a los requerimientos de las normas sobre la protección de datos personales y que adicionalmente contribuya a identificar la información pública sometida a reserva o clasificada en los términos de la ley. (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016)

6.4 EVALUACIÓN DE LOS CONTROLES DE EFECTIVIDAD

Resultado de la Fase de Diagnóstico: Teniendo en cuenta la herramienta de diagnóstico, se obtuvieron los siguientes resultados:

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	70	100	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	50	100	EFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	70	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	60	100	EFECTIVO
A.9	CONTROL DE ACCESO	60	100	EFECTIVO
A.10	CRIPTOGRAFÍA	50	100	EFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	80	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	80	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	80	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	60	100	EFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	60	100	EFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	50	100	EFECTIVO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	70	100	GESTIONADO
A.18	CUMPLIMIENTO	70	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		**65**	**100**	GESTIONADO

La Acueducto Alcantarillado y Aseo de El Espinal ESP obtuvo un puntaje de 65 sobre 100, es decir, que se encuentra en un nivel **EFECTIVO**, esto significa que, *Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.*

7. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD PARA LA ACUEDUCTO ALCANTARILLADO Y ASEO DE EL ESPINAL ESP

La Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP, define sus políticas de seguridad y privacidad fundamentada en los dominios de controles señalados en la norma NTC/IEC ISO 27001 - NTC/IEC ISO 27002 y que se transcriben a continuación.

7.1. Política de seguridad.

Controles para proporcionar directivas y consejos de gestión para mejorar y preservar la Seguridad y privacidad de la Información de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP, para lo cual dispondrá de los recursos necesarios para garantizar el correcto desarrollo de los lineamientos planteados en cada política propuesta.

7.2. Organización de la Seguridad

Controles para facilitar la gestión de la seguridad de la información en el seno de la organización. Garantizar que existan responsabilidades claramente asignadas en todos los niveles de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP, para la gestión de la seguridad y Privacidad de la Información y contar con un Comité de Seguridad de la Información conformado por personal de alto nivel de cada dependencia.

Todos los servidores públicos, contratistas y particulares que tengan acceso a los activos de información del organismo, tendrán el compromiso de cumplir las políticas y normas que se dicten en materia de seguridad de la información así, como reportar los incidentes que detecten.

7.3. Gestión de Activos.

Controles para catalogar los activos y protegerlos eficazmente. Toda la información sensible de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP, así como los activos donde esta se almacena o procesa, deberán ser inventariados, asignárseles un responsable y clasificarlos de acuerdo con los requerimientos en materia de seguridad de la información y los criterios que dicte el Comité de Seguridad de la Información del organismo, de acuerdo con esta clasificación se deben establecer los niveles de protección orientados a determinar, a quién se le permite el manejo de la información, el nivel de acceso a la misma y los procedimientos para su manipulación. La clasificación deberá revisarse

periódicamente y atender a los cambios que se presenten en la información o la estructura que puedan afectarla.

LA OFICINA ASESORA DE PLANEACIÓN Y TIC debe brindar herramientas que permitan la administración del inventario por cada dependencia, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

7.4. Seguridad de los Recursos Humanos.

Controles para reducir los riesgos de error humano, robo, fraude y utilización abusiva de los equipamientos. Desde la vinculación de los funcionarios se deben tener controles que permitan verificar la idoneidad e identidad, ética profesional y conducta. Los términos y condiciones de empleo o trabajo deberán establecer la responsabilidad de los funcionarios y contratistas, por la Seguridad de la Información, que van más allá de la finalización de la relación laboral o contractual, por lo que se debe firmar un acuerdo de confidencialidad que se hace extensivo a los contratistas y terceros que tengan acceso a la información.

Deberán existir mecanismos de información y capacitación para los usuarios en materia de seguridad, así como de reporte de incidentes que puedan afectarla. Los funcionarios deben cooperar con los esfuerzos por proteger la INFORMACIÓN y ser responsables de actualizarse en cada materia, así como consultar con el encargado de la seguridad de la información, en caso de duda o desconocimiento de un procedimiento formal, ya que esto no lo exonera de una acción disciplinaria que deberá llevarse a cabo cuando se incurra en violaciones a las políticas o normas de seguridad.

Para el caso de los contratistas, la responsabilidad de custodia de cualquier archivo mantenido, usado o producido por el personal que se retira, o cambio de cargo, recae en el supervisor del contrato y para el personal de planta el jefe inmediato; en todo caso el proceso de cambio en la cadena de custodia de la información debe hacer parte integral del procedimiento de terminación de la relación contractual o de cambio de cargo.

7.5. Seguridad Física.

Controles para impedir la violación, deterioro y la perturbación de las instalaciones y los datos. Deberán establecerse áreas seguras para la gestión, almacenamiento y procesamiento de información en la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP, estas deberán contar con protecciones físicas y ambientales acordes a los activos que protegen, incluyendo perímetros de seguridad, controles de acceso físicos, controles especiales en áreas de mayor sensibilidad, seguridad de los equipos, seguridad en el suministro eléctrico y cableado, condiciones ambientales de operación y sistemas de contención, detección y extinción de incendios adecuados que preserven el medio ambiente.

Esta seguridad debe mantenerse en los momentos de mantenimiento, cuando la información o los equipos que la contienen deben salir de la entidad o cuando se deben eliminar o dar de baja, para lo cual deben existir procedimientos especiales.

Toda información de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP, en formato digital debe ser mantenida en servidores aprobados a través de la Oficina de tecnologías de información y comunicación. No se permite el alojamiento de información institucional en servidores externos sin que medie una aprobación por escrito del Comité de Seguridad de la Información.

Los Equipos claves de comunicaciones deben se alimentados por sistemas de potencia eléctrica regulados y estar protegidos por UPS.

El área administrativa a través de la oficina de tecnología de información y comunicación debe asegurar que la infraestructura de servicios de TI esté cubierta por mantenimiento y soporte adecuados de hardware y software.

Las estaciones de trabajo deben estar correctamente aseguradas y operadas por personal de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP, el cual debe estar capacitado acerca del contenido de

esta política y de las responsabilidades personales en el uso y administración de la información institucional.

Los medios que alojan copias de seguridad deben ser conservados de forma correcta de acuerdo a las políticas y estándares.

7.6. Gestión de las Telecomunicaciones y Operaciones.

Controles para garantizar un funcionamiento seguro y adecuado de los dispositivos de tratamiento de la información. Deben documentarse los procedimientos y responsabilidades de administración y seguridad que sean necesarios en cada ambiente tecnológico y físico, garantizando un adecuado control de cambios y el seguimiento a estándares de seguridad que deben definirse, así como el seguimiento a los incidentes de seguridad que puedan presentarse. Debe buscarse una adecuada segregación de funciones.

Debe garantizarse una adecuada planificación y aprobación de los sistemas de información que consideren o provean las necesidades de capacidad futura.

Deben considerarse protecciones contra software malicioso y un adecuado mantenimiento y administración de la red, y protección contra el acceso no autorizado o amenazas de acceso externas, así como un adecuado cuidado de los medios de almacenamiento y seguridad en el intercambio de información.

En todo caso y como control mínimo, las estaciones de trabajo de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP, deben estar protegidas por software antivirus con capacidad de actualización automática en cuanto a firmas de virus. Los usuarios de las estaciones no están autorizados a deshabilitar este control, de la misma forma tener activa la licencia del firewall físico que protege la entidad contra accesos no autorizados y e intentos de ataque por parte de ciber-delincuentes.

Toda información que pertenezca al inventario de activos de información de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP, que sea de interés para un proceso comercial, jurídico, operativo o de misión crítica debe ser respaldada por copias de seguridad. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

La Oficina de tecnologías de información y comunicación debe garantizar la ejecución de las copias de seguridad automatizando el procedimiento por medio de herramientas software.

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios. Los usuarios deben cumplir con las directrices para el desarrollo de las copias de seguridad establecidas por LA OFICINA ASESORA DE PLENACIÓN Y TIC, en caso de no cumplir con las directrices impartidas serán responsables de cualquier perdida de información que se produzca por daños físicos, lógicos, y/o ataques informáticos que se puedan presentar y a su vez serán responsables por los perjuicios económicos, administrativos y fiscales que se puedan generar por la pérdida de información.

La configuración de enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red; debe ser documentada, respaldada por copia de seguridad y mantenida por la Oficina de tecnologías de información y comunicación.

Todo equipo de TI debe ser revisado, registrado y aprobado por La Oficina de tecnologías de información y comunicación antes de conectarse a cualquier nodo de la Red de comunicaciones y datos de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP. Dicha área debe desconectar aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad a ser investigado.

Las normas de uso de Internet y de los servicios de correo electrónico serán elaboradas, mantenidas y actualizadas por el Comité de Seguridad de la Información y en todo caso este comité debe velar por el cumplimiento del

código de ética vigente y el manejo responsable de los recursos de tecnologías de la información.

El sistema de correo electrónico institucional de la Empresa de Acueducto Alcantarillado Y Aseo de El Espinal ESP. debe ser usado únicamente para propósitos laborales.

Los usuarios del correo electrónico institucional no deben enviar mensajes personales u ofensivos; injuriosos, cadenas de mensajes o mensajes que se relacionen con actividades ilegales y no éticas, o que atenten contra el buen nombre de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP.

Los usuarios no deben utilizar una cuenta de correo electrónico que pertenezca a otra persona. En caso de ausencias o vacaciones, se debe recurrir a mecanismos alternos como redirección de mensajes.

Cualquier información de carácter institucional debe ser enviada a través de una cuenta institucional, correos personales no serán tenidos en cuenta.

La difusión masiva de comunicaciones debe estar aprobada por la Gerencia, directores de área y OFICINA ASESORA DE PLANEACIÓN Y TIC.

El área de Tecnologías realiza procesos de inducción y reinducción a los funcionarios, contratistas con el fin de divulgar la política seguridad de la información.

Con relación al software GCI Y GCIPRO que se tienen actualmente en la Empresa de Acueducto, Alcantarillado y Aseo de El Espinal ESP y que es considerado el activo más importante en la empresa, este software tiene la arquitectura cliente servidor, en donde un cliente (usuario) realiza peticiones mediante un programa o un navegador que se encuentra en una computadora para leer, editar o eliminar datos, y el servidor responde a las peticiones a través del mismo programa. Esta arquitectura de trabajo permite gestionar los permisos de los usuarios que utilizan el software, minimizando el riesgo de errores intencionales o de uso indebido por parte

de los funcionarios de la empresa o partes interesadas de los activos de información.

Con relación a la conexión de los computadores hacia el servidor del software GCI y GCIPRO, en la Empresa de Acueducto, Alcantarillado y Aseo de El Espinal ESP se tienen configuradas las computadoras en una red de DOMINIO DE WINDOWS, el cual permite centralizar la administración de cada una de ellas mediante la asignación de políticas de seguridad y acceso.

Con relación al acceso físico a los servidores donde se tienen los datos del software GCI y GCPRO, este cuarto es protegido con llave y el acceso debe ser autorizado por el líder del área de Tecnologías De Información Y Comunicación.

La Empresa de Acueducto, Alcantarillado y Aseo de El Espinal ESP no tienen instructivos y/o procedimientos documentados relacionados con los incidentes de seguridad. Si se genera un hecho de violación de la seguridad que involucre información se realiza la DENUNCIA ante la oficina de control disciplinario para que inicie el proceso investigativo.

7.7. Control de Acceso a los Datos.

Medios para impedir accesos no autorizados y registro de los accesos efectuados: Debe establecerse medidas de control de acceso a las áreas de la Empresa de Acueducto Alcantarillado Y Aseo de El Espinal ESP y a los diferentes niveles de la plataforma tecnológica, tales como la red, sistema operativo y aplicaciones; así como a la información física que tenga un componente de seguridad.

Estas medidas estarán soportadas en el desarrollo de la cultura de seguridad y privacidad de las personas que laboran en la entidad y buscarán limitar y monitorear el acceso a los activos de información requeridos para el trabajo, de acuerdo con su clasificación y manejando controles, en dispositivos y servicios que permitan identificar los niveles de acceso que los usuarios deben tener.

El control de las contraseñas de red y uso de equipos es responsabilidad de la de la oficina de tecnologías de información y comunicación. Dichas contraseñas deben ser codificadas y almacenadas de forma segura.

Las claves de administrador de los aplicativos deben ser conservadas por la de la oficina de tecnologías de información y comunicación y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal cambie.

7.8. Adquisición, Desarrollo y Mantenimiento de Software.

Controles para garantizar que la Política de Seguridad y privacidad esté incorporada a los sistemas de información: Asegurar que se haga un adecuado análisis e implementación de los requerimientos de seguridad del software desde su diseño, ya sea interno o adquirido, que incluya garantías de validación de usuarios y datos de entrada y salida, así como de los procesos mismos, de acuerdo con la clasificación de los activos a gestionar en la herramienta. Además, se establecerán controles para cifrar la información confidencial y se buscará evitar la posibilidad de una acción indebida por parte de un usuario del sistema. Igualmente, se deberán asegurar los archivos del sistema y mantener un control adecuado de los cambios que puedan presentarse.

La implantación de nuevas herramientas de Hardware y Software, de sistemas de información y de otros recursos informáticos, deben cumplir con las políticas definidas.

7.9. Cumplimiento y Normatividad Legal.

Controles para prevenir los incumplimientos de las leyes penales o civiles, de las obligaciones reglamentarias o contractuales y de las exigencias de seguridad: Garantizar que la gestión de la seguridad dé cumplimiento adecuado a la legislación vigente para lo cual analizará los requisitos legales aplicables a la información que se gestiona incluyendo los derechos de propiedad intelectual, los tiempos de retención de registros, privacidad

de la información, uso inadecuado de recursos de procesamiento de información, uso de criptografía y recolección de evidencias.

Así mismo deberá garantizarse que el direccionamiento y los controles relacionados con la seguridad de la información se cumplen y son compatibles técnicamente con los diferentes ambientes y tecnologías. Se debe garantizar la posibilidad de llevar a cabo auditorias, manteniendo los registros necesarios, para que éstas respondan adecuadamente a la disminución del riesgo de discontinuidad de cada tarea o servicio propio de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP.

8. ORGANIZACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN.

La Empresa de acueducto alcantarillado y aseo de El Espinal ESP. garantiza el apoyo al proceso de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de la Seguridad y privacidad de la Información, del cual hace parte integral la presente política, por medio de la creación de una comisión técnica denominada Comité de Seguridad de la Información cuya composición y funciones serán reglamentadas por una mesa de trabajo compuesta por:

- Representante legal de la entidad o un delegado de este.
- Jefe de la Oficina Asesora de Planeación y TIC – 006-05
- Profesional Universitario - 219-03 - Gestión TIC
- Técnico Administrativo 367-03
- Director (a) Oficina Jurídica o su delegado
- Un Representante del Área de Archivo

8. RESPONSABILIDADES

8.1. Comité de Seguridad de la Información.

- Garantizar la existencia de una dirección y apoyo gerencial que soporte la administración y el desarrollo de iniciativas sobre seguridad

y privacidad de la información, a través de compromisos y uso adecuado de los recursos en el organismo.

- Formular y mantener una política de seguridad y privacidad de la información que aplique a toda la organización conforme con lo dispuesto por la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP.
- En todo caso, dicho comité o la mesa de trabajo, deberá revisar y actualizar anualmente esta política presentando las propuestas a la alta gerencia de la Empresa de Acueducto Alcantarillado y Aseo de El Espinal ESP, para su aprobación mediante resolución o acto jurídico correspondiente.

8.2. Grupo de Apoyo a la Seguridad.

- Desarrollar, mantener y administrar operativa y técnicamente la seguridad y privacidad de la información conforme con las políticas de seguridad adoptadas por la Empresa de acueducto alcantarillado y aseo de El Espinal ESP.
- Materializar las medidas de largo, mediano y corto plazo que permitan el desarrollo efectivo, estratégico y armónico de las políticas planteadas.
- Estará conformado por los integrantes del área de tecnologías de información y comunicación.

8.3. Funcionarios, contratistas y particulares con acceso a información de la Empresa de acueducto alcantarillado y aseo de El Espinal ESP.

- Cumplir con todas las políticas de seguridad y privacidad y directrices adoptadas por la Empresa de Acueducto Alcantarillado Y Aseo de El Espinal ESP.

- Actualizarse en los temas propios de seguridad y privacidad de activos de la información aplicados en la Empresa de acueducto alcantarillado y aseo de El Espinal ESP.

- Todos los funcionarios de la Empresa de acueducto alcantarillado y aseo de El Espinal ESP., contratistas y/o terceros deben aceptar los acuerdos de confidencialidad definidos por la entidad, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

- Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de la Empresa de acueducto alcantarillado y aseo de El Espinal ESP. a personas o entidades externas. Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso contractual, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hará parte integral de cada uno de los contratos

CONTROL DE CAMBIOS

FECHA	DESCRIPCIÓN DEL CAMBIO	VERSIÓN
2023/01/02	Emisión original del documento	01
2024/01/16	Actualización de información para vigencia 2024	02
2025/01/07	Actualización de información para vigencia 2025	03
2026/01/19	Actualización de información para vigencia 2026	04