POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

EMPRESAS PUBLICAS DE PIAMONTE

AAA S.A.S E.S.P

YON FREDY CUELLAR LÓPEZ
GERENTE

"EMPRESAS PUBLICAS DE PIAMONTE AAA S.A.S E.S.P"
Dirección: Barrio Villa Los Prados / Diagonal al Parque Central
Celular: 3118287129 – Cod postal 195330
Página Web: https://empresaspublicaspiamonte.com.co/
Email: empresaspublicas@piamonte-cauca.gov.co

CONTENIDO

1. INTRODUCCION

De acuerdo con las directrices del Gobierno Nacional y MinTIC, la Política de la seguridad y privacidad de la información, Empresas Públicas de Piamonte AAA S.A.S. E.S.P, adopta dicha política donde manifiesta el MinTIC que la organización es la que establece la protección de los activos de información (funcionarios, contratistas, partes interesadas, la información, los procesos, las tecnologías de información incluido el hardware y el software) dando cumplimiento a los requisitos establecidos por las partes interesadas en la gestión de la Información.

Además, tiene como propósito salvaguardar la información generada dentro de la empresa garantizando así la seguridad de los datos y dando cumplimiento a la normatividad legal vigente, para lo cual se pretende realizar la Política de Seguridad y Privacidad de la información con el fin de que no se presenten daños, perdidas de información, accesos no autorizados y duplicación de información que puedan ocasionar afectaciones a los usuarios tanto internos como externos.

Empresas Públicas de Piamonte AAA S.A.S. E.S.P cumple con los tres pilares de la seguridad de la información en preservar la integridad, confidencialidad y disponibilidad de la información (2,30 ISO 27000):

- **Disponibilidad:** Propiedad que determina que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000).
- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. (2.13 ISO 27000).
- **Integridad:** Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000).

2. OBJETIVOS

2.1. Objetivos Generales

Constituir lineamientos para la implementación de políticas que garanticen la administración, manejo y control de la seguridad y privacidad de la información de Empresas Públicas de Piamonte AAA S.A.S. E.S.P.

2.2. Objetivos específicos

- Efectuar políticas y procedimientos enfocados en la de seguridad de la información.
- Mitigar los riesgos asociados a la seguridad de la Información que afecten la integridad, confidencialidad, disponibilidad y privacidad de la Información de Empresas Públicas de Piamonte AAA S.A.S. E.S.P.

2.3. Alcance

En cumplimiento a las disposiciones legales vigentes se pretende alcanzar la elaboración de la Política de Seguridad y Privacidad de la información de Empresas Públicas de Piamonte AAA S.A.S. E.S.P, teniendo como base los recursos, procesos, procedimientos, en su totalidad ya sean internos o externos vinculados a la empresa por contratos o acuerdo con terceros, y demás partes interesadas que usen los activos de información generados dentro de la empresa.

3. MARCO NORMATIVO

MARCO NORMATIVO	DESCRIPCION
Ley 527 de 1999	"Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".
Ley 1266 de 2008	"Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países".
Ley 1581 de 2012	"Por la cual se dictan disposiciones generales para la protección de datos personales".
Ley 1712 de 2014	"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".
Decreto 1499 del 11 de septiembre de 2017	"Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015".
Decreto 612 del 04 de abril de 2018	"Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado".
Decreto 1008 del 14 de junio de 2018	"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".

4. TERMINOS Y DEFINICIONES

- **Acceso a la Información Pública**: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- **Activo**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **Activo de Información**: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Confidencialidad**: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados (2.13 ISO 27000).
- **Disponibilidad**: Propiedad que determina que la información sea accesible y utilizable por solicitud de los autorizados (2.10 ISO 27000).
- **Integridad**: Propiedad de salvaguardar la exactitud y el estado completo de los activos (2.36 ISO 27000).
- **Partes interesadas (Stakeholder)**: Persona u organización que puede afectar a, ser afectada por, o percibirse a sí misma como afectada por una decisión o actividad.
- **Plan de tratamiento de riesgos**: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Privacidad**: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación.
- **Procedimiento**: Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles de Seguridad de la Información.
- **Riesgo**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Seguridad de la información**: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

5. RESPONSABLES

La empresa de servicios públicos "Empresas Públicas de Piamonte AAA S.A.S. E.S.P", tiene como responsables de la implementación, seguimiento y mantenimiento de la Política de Seguridad y Privacidad de la información en la empresa a los siguientes:

- El Secretario General y de las TIC quien será el delegado para velar la formulación e implementación de la Política de seguridad y privacidad de la información.

- El profesional encargado de la gestión de TICS, será el encargado de desarrollar la implementación de la Política de seguridad y privacidad de la información.

- Todos los funcionarios y/o contratistas y demás partes interesadas de Empresas Públicas de Piamonte AAA S.A.S. E.S.P, son responsables del cumplimiento obligatorio de la Política de seguridad y Privacidad de la Información y en caso de no cumplir se reserva el derecho de tomar las medidas correspondientes según el caso.

- Para comunicar esta política se hará mediante socialización con todos los funcionarios, contratista y partes interesadas de Empresas Públicas de Piamonte AAA S.A.S. E.S.P, el cual dará a conocer la existencia, contenido y obligatoriedad de dicho documento. La custodia y ubicación física del documento estará a cargo del Sistema Integrado de Gestión y el líder de TIC.

6. POLITICAS

Empresas Públicas de Piamonte AAA S.A.S. E.S.P divulga los objetivos y alcances de la seguridad de la información dentro de la empresa, que son efectivos por medio de controles de seguridad, con el fin de mantener, gestionar y mitigar el riesgo como se estable en el Plan de Tratamiento de Riesgos, garantizando así la continuidad de los servicios y disminuyendo la probabilidad de amenazas que puedan afectar los procesos internos para el cumplimiento de la prestación del servicio.

6.1. Identificación, clasificación y valoración de activos de información.

Cada proceso, bajo supervisión y con base en el inventario de activos de Empresas Públicas de Piamonte AAA S.A.S. E.S.P siempre se debe estar actualizando en donde se incorpore la clasificación, valoración, ubicación y acceso de la información y demás características identificas por la Alta dirección permitiendo así la administración eficiente de cada proceso garantizando la disponibilidad, integridad y confidencialidad de dicha información.

6.2. Seguridad de la información en el Talento Humano

Todas y todos los empleados de Empresas Públicas de Piamonte AAA S.A.S. E.S.P, independiente del tipo de vinculación laboral o contractual, o de los procesos al que pertenezca y del nivel de funciones o actividades que desempeñe deben contar con un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. Por ende, se debe contar con un directorio completo y actualizado de los perfiles creados.

La responsabilidad de custodia de cualquier documento o archivo generado dentro de la empresa, usado o producido por algún funcionario y/o contratista que se retira, o cambia de cargo, recae en la Gerencia con funciones de talento humano, demás secretarios o dependencia o supervisor del contrato; Aclarando que el proceso de cadena de custodia de la información debe ser parte integral de un procedimiento de terminación de la relación contractual o de cambio de cargo.

6.3. Usuarios invitados y servicios de acceso público

El acceso de usuarios no registrados solo debe estar autorizado por la Alta dirección, de manera de información institucional, igualmente el servicio de internet al que puedan acceder debe estar protegido con una contraseña, contando con una restricción de sitios web no autorizados. Si los usuarios invitados no realizaron el debido proceso de registro, no se permitirá el acceso a cualquier otro tipo de recursos de información, aplicación y/o herramientas TIC.

6.4. Seguridad Física y del entorno

Seguridad en los equipos: Los servidores o equipos de cómputo que contengan información institucional deben estar en un ambiente seguro y protegido por lo menos con:

- Controles de acceso y seguridad física.
- Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

Además, toda información institucional en formato digital debe ser mantenida en los servidores y/o unidades extraíbles aprobados por la Secretaria General y de la TIC.

También se debe asegurar que la infraestructura esté cubierta, con mantenimiento y soporte adecuados tanto para el hardware como para el software y las estaciones de trabajo deben ser operadas por funcionarios de la institución el cual deben estar capacitados acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información institucional. Se deben incluir los medios que alojan copias de seguridad el cual deben ser conservados de forma correcta de acuerdo a las políticas y estándares establecidos.

6.5. Administración de las comunicaciones y operaciones

Reporte y revisión de incidentes de seguridad: El personal vinculado a Empresas Públicas de Piamonte AAA S.A.S. E.S.P, debe realizar el reporte de una manera eficiente y con responsabilidad de las presuntas violaciones de seguridad detectadas y se deben reportar a través de su jefe de dependencia o su supervisor, a la Gerencia de la empresa con funciones de talento humano o cuando la ocasión lo amerite si es un caso especial y podrá realizarse directamente por la persona que encuentre el incidente o novedad.

Se debe diseñar, mantener y difundir las normas, procesos y guías para el reporte y revisión de incidentes de seguridad el cual se mantendrá procedimientos escritos para la operación de dichas actividades sin afectar el desarrollo normal de la prestación del servicio y asegurando la confiabilidad de la información.

6.6. Protección contra software malicioso y hacking

Se debe proteger todos los sistemas de información que involucre los controles humanos, físicos técnicos y administrativos para no incurrir en daños, se elaborará y mantendrá un conjunto de políticas, normas, estándares, procedimientos que garanticen la mitigación de riesgos asociados a amenazas de software malicioso y técnicas de hacking que pueda afectar la prestación del servicio.

Como control básico, todas las estaciones de trabajo de Empresas Públicas de Piamonte AAA S.A.S. E.S.P, deben estar protegidas por software antivirus con capacidad de actualización automática en cuanto a firmas de virus.

6.7. Copias de Seguridad

Toda información que se encuentre contenida en el inventario de activos de información o que sea de interés para un proceso siempre debe estar o ser respaldada con copias de seguridad tomadas de acuerdo a los procedimientos documentados y probados por el Sistema Integrado de Gestión.

El procedimiento debe incluir actividades de almacenamiento, administración y custodia de las copias de seguridad incluyendo lugares seguros y control de registros de dichas copias. Dentro del procedimiento debe quedar claro que se deben efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad.

Tener en cuenta que la creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios, es decir la responsabilidad de realizar las copias y mantenerlas actualizadas, recae directamente sobre cada dueño de los activos de la información de la Empresa.

6.8. Intercambio de Información con Entidades Externas

Las peticiones o solicitudes de información por parte de entes externos deben ser aprobadas por la Alta dirección, y ser redireccionados a los responsables del manejo y custodia dicha información. Tener en cuenta que la información solicitada por parte de los entes externos debe ser realizada por un medio valido que permita el registro de la solicitud, donde se pueda identificar el remitente, el asunto y la fecha aclarando que toda información institucional debe ser manejada de acuerdo a la normatividad legal vigente.

6.9. Instalación de Software

Todas las instalaciones de software que se realicen sobre sistemas operativos previamente instalados en Empresas Públicas de Piamonte AAA S.A.S. E.S.P, deben ser aprobadas por la Alta dirección, de acuerdo a los procedimientos establecidos para tal fin.

El funcionario encargado en la Gestión de las TIC debe desinstalar cualquier software ilegal y registrar este hecho como un incidente de seguridad para su respectiva investigación además debe tener un inventario del software autorizado para su uso institucional.

6.10. Control de Claves y Nombres de Usuario

Las claves de administrador de los diferentes sistemas deben ser conservadas por la Gerencia de la empresa con funciones de talento humano y el funcionario encargado en la Gestión de las TIC y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie. Adicionalmente se debe elaborar, mantener y actualizar el procedimiento para la correcta definición, uso y complejidad de las claves de usuario.

Una vez se termine la relación contractual o laboral del personal con Empresas Públicas de Piamonte AAA S.A.S. E.S.P, se debe expedir un certificado de suspensión y/o cancelación de las cuentas creadas al respectivo usuario, en todos y cada uno de los sistemas de información en los cuales estuviera activo (correo electrónico, sistemas de información automatizados, plataformas, entre otros); se determinara cual será el tiempo prudencial para la posible renovación de la relación contractual o laboral, o una vez transcurrido el tiempo se dará de baja las cuentas si no hay renovación ninguna.

6.11. Uso adecuado de Internet

Empresas Públicas de Piamonte AAA S.A.S. E.S.P es consciente de la importancia del servicio de Internet como una herramienta fundamental para el desempeño de labores que proporcionará los recursos necesarios para asegurar su disponibilidad a los servidores públicos y demás partes de interés que así lo requieran.

- El proceso de TIC debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.
- El proceso de TIC debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
- El proceso de TIC debe monitorear continuamente el canal o canales del servicio de Internet.
- El proceso de TIC debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar el monitoreo sobre la utilización del servicio de Internet.

YON FREDY CUELLAR LOPEZ
Gerente Empresas Públicas de Piamonte AAA S.A.S. E.S.P

Proyectó/Aprobó: Ing. Yon Fredy Cuellar López – Gerente Empresas Públicas de Piamonte AAA S.A.S. E.S.P.