PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

EMPRESA DE SERVICIOS PUBLICOS DE GUATAPE S.A.S E.S.P

2026

INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información tiene como objetivo identificar, evaluar y mitigar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información gestionada por Empresas de Servicios Públicos de Guatapé SAS ESP., en cumplimiento con la normativa vigente, como la Ley 1581 de 2012 (Protección de Datos Personales), la Ley 1266 de 2008 (Tratamiento de la Información Financiera) y las disposiciones establecidas por el MINTIC.

Actualmente, el creciente uso del entorno digital en Colombia para desarrollar actividades económicas y sociales, acarrea incertidumbres y riesgos inherentes de seguridad digital que deben ser gestionados permanentemente. No hacerlo, puede resultar en la materialización de amenazas o ataques cibernéticos, generando efectos no deseados de tipo económico o social para el país, y afectando la integridad de los ciudadanos en este entorno.

La Empresa de Servicios Públicos de Guatapé, identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la Entidad, por esta razón establece un modelo que asegura que la información es protegida de una manera adecuada para su recolección, manejo, procesamiento, transporte y almacenamiento.

JUSTIFICACION

La información es un activo estratégico para la empresa de servicios públicos, ya que soporta la operación, la atención al usuario y la toma de decisiones. Este plan busca proteger la confidencialidad, integridad y disponibilidad de la información, garantizando el cumplimiento normativo y la confianza de los usuarios.

Resulta fundamental la formulación e implementación de La Empresa de Servicios Públicos de Guatapé, esto debido a que es necesaria la protección de los activos de una amplia gama de amenazas, asegurar la continuidad de la operación de los servicios y funciones, minimizar los daños de la organización, maximizar la eficiencia de la administración pública y el mejoramiento continuo, aumentar la confianza ante ciudadanos, evitar los posibles riesgos en la seguridad de la información, reducir el tiempo de respuesta a los incidentes, proveer mejores prácticas en el aseguramiento de la información y finalmente, apoyar y controlar el cumplimiento de los requisitos legales, reglamentarios, contractuales y técnicos que haya lugar en su aplicación.

OBJETIVO GENERAL

Establecer lineamientos, controles y acciones para proteger la información de la empresa, asegurando su uso adecuado, la privacidad de los datos personales y la continuidad de los servicios.

OBJETIVOS ESPECIFICOS

- Proteger los datos personales de usuarios, empleados y proveedores.
- Prevenir accesos no autorizados, pérdidas o alteraciones de la información.
- Garantizar la continuidad operativa ante incidentes de seguridad.
- Promover la cultura de seguridad de la información en los colaboradores.
- Cumplir la normatividad vigente en protección de datos y seguridad digital.
- Establecer mecanismo de respuesta ante incidentes

ALCANCE

Aplica a:

- Información física y digital.
- Sistemas de información y bases de datos.
- Equipos tecnológicos, redes y aplicaciones.
- Todo el personal (planta, contratistas y terceros).

MARCO NORMATIVO Y LEGAL

- Acuerdo 03 de 2015 del AGN: Por el cual se establecen los lineamientos generales para las Entidades del Estado en cuanto a la gestión de documentos electrónicos generado como resultado del uso de medios tecnológicos de conformidad con lo establecido en el Capítulo IV de la Ley 1437 de 2011, se reglamenta el artículo 21 de la Ley 594 de 2000 y el Decreto 2609 de 2012.

- Decreto 2609 de 2012: Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos.

- Decreto 2693 de 2012: Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

- Decreto 212 de 2014 Por medio del cual se crea el comité de Gobierno en línea, Anti trámites y Eficiencia Administrativa

- Decreto Nacional 2573 de 2014: por el cual se establecen los lineamientos generales de la estrategia de gobierno en línea, se reglamenta parcialmente la ley 1341 de 2009 y se dictan otras disposiciones

- Decreto 1078 de 2015: Art. 2.2.9.1.2.2 contemplo los instrumentos para implementar la Estrategia de Gobierno en Línea, dentro de los cuales se exige la elaboración por parte de cada entidad un Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI, un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Seguridad y Privacidad de la Información

- Decreto 1499 de 2017 se crea el nuevo Modelo Integrado de Planeación y Gestión

Ley 1150 de 2007: Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos".

- Ley 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado “de la protección de la información y los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- Ley 1341 de 2009: Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones

- Ley 1474 de 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública

- 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.

- NTC 27001:2006: Sistema de Gestión de Seguridad de la Información (SGSI).

MARCO CONCEPTUAL

- Activo de Información: Es todo aquello que en la entidad es considerado importante o de alta validez para la misma ya que puede contener información importante como son en las Bases de Datos con usuarios, contraseñas, números de cuentas; cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la Empresa y en consecuencia, debe ser protegido

- Acuerdo de Confidencialidad: es un documento en los contratistas y personal provisto por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la Empresa comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

- Autenticación: es el procedimiento de comprobación de la Entidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información

- Análisis de riesgos de seguridad digital: proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

- Amenaza: Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo

- Centros de cableado: son habitaciones donde se deben instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

- Centro de cómputo: es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

- Ciber amenaza o amenaza cibernética: aparición de una situación potencial o actual que pudiera convertirse en un ciberataque.

- Ciberataque o ataque cibernético: acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de la misma o donde el ciberespacio es fuente o herramienta de comisión de un crimen.

- Ciberespacio: entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física.

- Ciberiesgo o riesgo cibernético: posibles resultados negativos derivados de fallas en la seguridad de los sistemas tecnológicos o asociados a ataques cibernéticos.

- Ciberseguridad: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la Entidad.

- Cifrado: es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, acceso no autorizado a los repositorios de información.

- Copias de respaldo: Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

- Componentes informáticos: Son todos aquellos recursos tecnológicos que hacen referencia a: aplicativos, software de sistemas, sistemas operativos, bases de datos, redes, correo electrónico, software ofimático, software de seguridad, hardware y equipos de comunicaciones

- Confidencialidad: es la garantía de que la información no es divulgada a personas, Entidades o procesos no autorizados.

- Control: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

- Criptografía: es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

- Custodio del activo de información: es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

- Dato: Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.

- Derechos de Autor: es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

- Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

- Equipo de cómputo: dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

- Evento de seguridad: ocurrencia de una situación que podría afectar la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio.

- Gestión de riesgos de seguridad digital: es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.

- Guías de clasificación de la información: directrices para catalogar la información de la Entidad y hacer una distinción entre la información que es calificada como pública clasificada o pública reservada y de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información

- Incidente de seguridad: ocurrencia de una situación que afecta la protección o el aseguramiento de los datos, sistemas y aplicaciones de la Entidad que son esenciales para el negocio.

- Información: Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

- Información en reposo: datos guardados en dispositivos de almacenamiento persistente (por ejemplo, cintas, copias de seguridad externas, dispositivos móviles, discos duros, entre otros).

- Integridad: es la protección de la exactitud y estado completo de los activos.

- Inventario de activos de información: es una lista ordenada y documentada de los activos de información pertenecientes a la Empresa

- Licencia de software: es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

- Medio removible: es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

- MSPI: Modelo de Seguridad y Privacidad de la Información

- Perfiles de usuario: son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

- Propiedad intelectual: es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

- Propietario de la información: es la unidad organizacional o proceso donde se crean los activos de información.

- Recursos tecnológicos: son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la Empresa

- Resiliencia: es la capacidad de un mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que pudo estar sometido.

- Responsabilidad: las múltiples partes interesadas deben asumir la responsabilidad de la gestión del riesgo de seguridad digital. Deben rendir cuentas sobre la base de sus funciones y su capacidad para actuar, teniendo en cuenta el posible impacto de sus decisiones sobre los demás. Deben también reconocer que un cierto nivel de riesgo de seguridad digital tiene que ser aceptado para lograr los objetivos económicos y sociales.

- Responsable por el activo de información: es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

- Riesgo: Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.

- Riesgo de seguridad digital: es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital.

- Sensibilización: es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.

- Servidor: Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia

- SGSI: Sistema de Gestión de Seguridad Digital.

ACTIVOS DE INFORMACIÓN CRÍTICOS

- Base de datos de usuarios (facturación y PQR).
- Información de redes de acueducto y alcantarillado.
- Planos y mapas de infraestructura.
- Información de plantas de tratamiento.
- Rutas y frecuencias de recolección de residuos.
- Información financiera y contable.
- Información contractual.
- Datos de empleados y contratistas.
- Sistemas de monitoreo y control operativo.

PRINCIPIOS DE SEGURIDAD

- Confidencialidad
- Integridad
- Disponibilidad
- Legalidad
- Responsabilidad
- Continuidad del servicio público

ROLES Y RESPONSABILIDADES

(Se mantienen los roles: Gerencia, Responsable de Seguridad de la Información, Sistemas, Talento Humano, funcionarios y Contratistas, con énfasis en personal operativo y técnico)

CLASIFICACIÓN DE LA INFORMACIÓN

- Pública: Informes, tarifas, planes.
- Uso interno: Procedimientos, reportes.
- Confidencial: Infraestructura crítica, claves, contratos.
- Datos personales: Usuarios y empleados.
- Datos sensibles: Información de salud laboral, vulnerabilidad social.

IDENTIFICACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Riesgos Tecnológicos

- Pérdida de información por fallas eléctricas.
- Ataques informáticos (virus, ransomware).
- Accesos no autorizados a sistemas.
- Uso de contraseñas débiles.
- Falta de copias de seguridad.
- Obsolescencia tecnológica.
- Uso de software no autorizado.

Riesgos Operativos (Acueducto y Alcantarillado)

- Divulgación de planos de redes.
- Manipulación indebida de datos operativos.
- Pérdida de registros de calidad del agua.
- Acceso no autorizado a información de plantas.
- Errores en sistemas de control y monitoreo.

Riesgos Operativos (Aseo)

- Divulgación de rutas y horarios de recolección.
- Pérdida de información sobre disposición final.
- Alteración de registros ambientales.
- Uso indebido de dispositivos móviles del personal operativo.

Riesgos Humanos

- Falta de capacitación.
- Error humano.
- Uso indebido de información.
- Fuga de información por exfuncionarios.
- Ingeniería social.

Riesgos Físicos

- Robo de equipos.
- Daños por incendios o inundaciones.
- Acceso no autorizado a archivos físicos.
- Falta de control en áreas críticas.

Riesgos Legales

- Incumplimiento de la Ley 1581.
- Uso indebido de datos personales.
- Sanciones de entes de control.
- Demandas de usuarios.

Riesgos Reputacionales

- Pérdida de confianza ciudadana.
- Publicación de información errónea.
- Filtración de datos de usuarios.
- Interrupción del servicio por incidentes de información.

CONTROLES Y MEDIDAS DE SEGURIDAD

Administrativos

- Políticas institucionales.
- Acuerdos de confidencialidad.
- Manuales de procedimiento.
- Gestión de riesgos.
- Control de accesos por roles.

Técnicos

- Antivirus y firewall.
- Copias de seguridad automáticas.
- Control de usuarios.
- Cifrado de información sensible.
- Restricción de dispositivos externos.
- Sistemas de respaldo alterno.

Físicos

- Control de ingreso a plantas y oficinas.
- Custodia de planos y archivos.
- Archivadores con llave.
- Eliminación segura de documentos.

PROTECCIÓN DE DATOS PERSONALES

- Autorización expresa del usuario.
- Uso limitado y legítimo.
- Confidencialidad obligatoria.
- Atención de consultas y reclamos.
- Registro de bases de datos.

GESTIÓN DE INCIDENTES

- Identificación y reporte inmediato.
- Activación del protocolo.
- Registro del incidente.
- Análisis de impacto.
- Medidas correctivas.
- Informe a autoridades si aplica.

CONTINUIDAD DEL SERVICIO

- Plan de respaldo de información crítica.
- Procedimientos de recuperación.
- Responsables asignados.
- Pruebas periódicas.
- Priorización de sistemas esenciales**.**

CAPACITACIÓN

- Inducción y reinducción.
- Capacitación al personal operativo.
- Buenas prácticas digitales.
- Manejo seguro de información.

SEGUIMIENTO Y MEJORA CONTINUA

- Auditorías internas.
- Indicadores de riesgo.
- Reportes periódicos.
- Actualización anual del plan.

SANCIONES

El incumplimiento dará lugar a sanciones disciplinarias y legales conforme a la normativa vigente.

RESULTADOS ESPERADOS

- Información protegida.
- Continuidad del servicio.
- Reducción de riesgos.
- Cumplimiento legal.
- Confianza de los usuarios.

MATRIZ DE RIESGOS POR PROCESOS

PROCESO	ACTIVO DE INFORMACION	RIESGO IDENTIFICADO	CAUSA	IMPACTO	P	I	NIVEL	CONTROLES EXISTENTES	ACCIONES DE TRATAMIENTO
FACTURACION ATENCION AL USUARIO	Base de datos usuarios	Acceso no autorizado	Contraseñas débiles	Sanciones legales				Usuarios y claves	Políticas de contraseñas seguras, doble autenticación, control de perfiles
SISTEMAS	servidor	Perdida de información	Fallas eléctricas	Interrupción del servicio				UPS	Copias de seguridad
ACUEDUCTO	Planos de redes	Divulgación indebida	Falta de control físico	Riesgo infraestructura				archivadores	Control de acceso a formato de prestamos
OPERACION	Datos de calidad del agua	Alteración de datos	Error humano	Riesgo sanitario				procedimientos	Doble validación
ASEO	Rutas de recolección	Fuga de información	Uso móvil de personal	Riesgo operativo				supervison	Equipos institucionales
TALENTO HUMANO	Datos empleados-historias laborales	Uso indebido-perdida o divulgación de	Falta copias de seguridad	Sanciones legales				contratos	Implementar backups automáticos y pruebas de recuperación

		información financiera							
ARCHIVO Y DOCUMENTACION	Archivo físico	Deterioro o perdida de documentos	Almacenamiento inadecuado	Sanciones legales				Cerraduras en archivo central	Control de acceso a los archivos
SISTEMA	Servidores y equipos	Ataques informáticos	Falta de actualizaciones de software	Daño sistema				Antivirus y firewall	Actualización periódica de sistemas y parches de seguridad
CONTRATACION	Información contractual	divulgación	Falta confidencialidad	Riesgo legal				clausulas	Acuerdos y políticas de confidencialidad

MATRIZ DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
Empresa de Acueducto, Alcantarillado y Aseo

CRITERIOS DE VALORACIÓN

Probabilidad (P)

- 1 – Baja: Ocurre raramente
- 2 – Media: Puede ocurrir ocasionalmente
- 3 – Alta: Ocurre con frecuencia

Impacto (I)

- 1 – Bajo: Afectación mínima
- 2 – Medio: Afectación operativa o administrativa
- 3 – Alto: Afectación grave, sanciones o interrupción del servicio

Nivel de Riesgo = P x I

- 1–2: Bajo
- 3–4: Medio
- 6–9: Alto

MATRIZ DE RIESGOS

MATRIZ DE RIESGOS ESPECÍFICOS POR SERVICIO

Acueducto y Alcantarillado

- Pérdida de registros de calidad del agua
- Alteración de datos de plantas de tratamiento
- Acceso no autorizado a sistemas de monitoreo
- Divulgación de mapas de redes

Aseo

- Fuga de información de rutas y horarios
- Alteración de registros ambientales
- Uso indebido de dispositivos móviles
- Pérdida de reportes de disposición final

PLAN DE TRATAMIENTO DEL RIESGO

- Evitar: Eliminar procesos inseguros.
- Mitigar: Implementar controles.
- Transferir: Seguros o terceros.
- Aceptar: Riesgos bajos documentados.

RESPONSABLES

- Gerencia
- Responsable Seguridad Información
- Sistemas
- Coordinadores Operativos
- Talento Humano

SEGUIMIENTO

- Revisión semestral.
- Actualización ante cambios tecnológicos.
- Reporte a control interno.

CONCLUSIÓN

La matriz permite identificar, evaluar y tratar los riesgos de seguridad y privacidad de la información, garantizando la continuidad de los servicios de acueducto, alcantarillado y aseo y el cumplimiento normativo.