EMPRESA DE SERVICIOS PÚBLICOS E.S.P S.A.S

DIMENSION 3: GESTIÓN CON VALORES PARA RESULTADOS

POLITICA: SEGURIDAD DIGITAL

TABLA DE CONTENIDO

1. PRESENTACIÓN……3
2. INTRODUCCIÓN……4
3. JUSTIFICACIÓN……5
4. MARCO LEGAL……6
5. MARCO CONCEPTUAL……9
6. OBJETIVOS……16
6.1. OBJETIVO GENERAL……16
6.2. OBJETIVOS ESPECÍFICOS……16
7. ALCANCE ……17
8. APLICABILIDAD……17
9. NIVEL DE CUMPLIMIENTO……17
10. IMPLEMENTACIÓN ESTRATEGIAS……17
11. LINEAMIENTOS GENERALES DE LA POLITICA…… 19
12. POLITICA DE SEGURIDAD DIGITAL……20
12.1 PRIVACIDAD Y CONFIDENCIALIDAD……22
12.1.1 POLITICA DE TRATAMIENTO DE DATOS PERSONALES…… 22
12.1.2 TRATAMIENTO DE DATOS……23
12.1.3 DERECHO DE LOS TITULARES……23
12.1.4 AUTORIZACIÓN DEL TITULAR……24
12.1.5 ACUERDO DE CONFIDENCIALIDAD……24
12.2 LINEAMIENTOS PARA MEDIOS REMOVIBLES……24
12.3 SEGURIDAD DE COMPUTADORES Y PORTATILES……25
13. COMPROMISO DE LA ALTA DIRECCIÓN……27
14. ARMONIZACIÓN Y COMUNICACIÓN……28
15. COMUNICACIÓN……28
16. EVALUACIÓN Y SEGUIMIENTO……28
17. CONCLUSIONES……31
18. RECOMENDACIONES……32

1. PRESENTACIÓN

El Modelo Integrado de Planeación y Gestión MIPG es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio, según dispone el Decreto1499 de 2017.

El Objetivo de la puesta en marcha del Modelo Integrado de Planeación y Gestión MIPG, es Mejorar la capacidad del Estado para cumplirle a la ciudadanía, incrementando la confianza de la ciudadanía en sus entidades y en los servidores públicos, logrando mejores niveles de gobernabilidad y legitimidad del aparato público y generando resultados con valores a partir de una mejor coordinación interinstitucional, compromiso del servidor público, mayor presencia en el territorio y mejor aprovechamiento y difusión de información confiable y oportuna

El crecimiento en el uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, reflejado en la masificación de las redes de telecomunicaciones como base para cualquier actividad socioeconómica y el incremento en la oferta de servicios disponibles en línea, ha incrementado la participación digital de los ciudadanos, generando nuevas formas para atentar contra su seguridad y la del Estado, por ende, es necesario fortalecer las capacidades de las instituciones para identificar, gestionar el riesgo y atender las situaciones para brindar protección en el ciberespacio. A través de la política de seguridad digital se han propuesto estrategias que permiten resolver problemas, generar diagnósticos más rápidamente, así como comparar diferentes escenarios posibles para prevenir riesgos cibernéticos en la plataforma dispuesta para La Empresa de Servicios Públicos de Guatape.

Con la implementación de la Política de Seguridad Digital, La Empresa de Servicios Públicos de Guatape adopta un compromiso obligatorio de protección a la información frente a una amplia gama de amenazas. Contribuyendo a minimizar los riesgos asociados de daño y asegurar el eficiente cumplimiento de las funciones de la entidad apoyadas en un correcto uso de los Sistema de información.

2. INTRODUCCIÓN

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.

Por lo anterior, la Política de Seguridad Digital de La Empresa de Servicios Públicos de Guatape, pretende proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad los activos informáticos conectados o no a la red interna y a la información que ellos procesan o intercambien.

La Empresa de Servicios Públicos de Guatape**,** 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.

Este documento describe las políticas y normas de seguridad digital definidas por la Empresa. Para la elaboración del mismo, se toman como base las leyes y demás regulaciones aplicables.

La seguridad digital es una prioridad para la Empresa y por tanto el cumplimiento de esta política es responsabilidad de todos sus colaboradores.

A lo largo del documento al emplear el término seguridad digital se agrupan los conceptos de seguridad de la información, seguridad informática, ciberseguridad y la protección de los datos personales.

3. JUSTIFICACIÓN

Las Entidades Gubernamentales deben propender por el uso responsable de los activos informáticos y de igual manera minimizar los riesgos que propicien delitos informáticos a los que está expuesto un dispositivo al conectarse a una red o interactuar con otro dispositivo, máxime si no se tienen directrices, normas o lineamientos, riesgos como son uso indebido de información, interceptación, robo o suplantación de identidad, entre otros, se deben de contrarrestar y adoptar mecanismos de autenticación y control de acceso, atendiendo las prácticas del buen gobierno y como objetivo primordial; por lo tanto, se debe proveer una visión tecnológica y liderar el desarrollo e implantación de iniciativas que estén acordes con el entorno cambiante tecnológico, alineados con las metas institucionales y el cumplimiento de los fines esenciales del Estado.

Resulta fundamental la formulación e implementación de La Empresa de Servicios Públicos de Guatape, 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.

4. MARCO 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

- Decreto 612 de 2018: Por el cual se fijan las directrices para la integración de planes institucionales y estratégicos al plan de acción por parte de las entidades del estado

- Directiva Presidencial 04 de 2012: Eficiencia Administrativa y lineamientos de la política cero papeles en la Administración Pública

- ISO 27002:2005: Esta norma proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar e implantar o mantener sistemas de gestión de la seguridad de la información.

- ISO/IEC 27001:2005: Es la evolución certificable del código de buenas prácticas ISO 17799. Define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información.

- Ley 599 DE 2000: Por la cual se expide el Código Penal. Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa

- 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).

5. 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.

- Ciberamenaza 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.

- Sistema de información: es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de

información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por la Administración o de origen externo ya sea adquirido por la Entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.

- Sistemas de control ambiental: son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características del mismo, fundamentalmente humedad y temperatura y, de manera adicional, también permite controlar su pureza y su movimiento.

- Software malicioso: es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información

- Teletrabajo: Hace referencia a todas las formas de trabajo por fuera de la oficina, incluidos los entornos de trabajo no tradicionales, a los que se denomina "trabajo a distancia", "lugar de trabajo flexible", "trabajo remoto" y ambientes de "trabajo virtual".

- Terceros: todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la Entidad.

- Vulnerabilidad: Es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software; son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por el Instituto (amenazas), las cuales se constituyen en fuentes de riesgo.

6. OBJETIVOS

6.1. OBJETIVO GENERAL

Diseñar la Política de Seguridad Digital para fortalecer las capacidades e identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades, generando confianza digital y adaptación para el futuro digital

6.2. OBJETIVOS ESPECÍFICOS

- Diseñar estrategias que permitan la ejecución de la política

- Fortalecer la capacidad de La Empresa de Servicios Públicos de Guatape en materia de prevención de riesgos digitales

- Generar lineamientos para que partes interesadas gestionen el riesgo de seguridad digital en sus actividades

- Salvaguardar los activos tecnológicos y custodiar la información producida en La Empresa de Servicios Públicos de Guatape

- Generar confianza en el uso del entorno digital, estableciendo mecanismos de participación activa y permanente y promoviendo en las diferentes dependencias comportamientos responsables en el entorno digital

- Promover la cultura de la seguridad de la información a los Empleados, contratistas, ciudadanos y público en general

- Orientar a la ciudadanía en general sobre el uso responsable del medio digital

- Definir lineamientos en materia de seguridad de la información

- Capacitar al personal de la Empresa en buenas practicas digitales

7. ALCANCE

La Política de Seguridad Digital pretende identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades

6. APLICABILIDAD

Esta política aplica para todos los procesos institucionales, pues la eficiencia de todos y cada uno de los procesos afecta directa o indirectamente los recursos institucionales, por lo tanto, será aplicable a todos los empleados, contratistas, proveedores, visitantes y ciudadanos de La Empresa de Servicios Públicos de Guatape de acuerdo al nivel jerárquico se aplicarán las restricciones del caso.

Es un compromiso y responsabilidad de todos conocer la Política y es su deber cumplirla y respetarla para el desarrollo de cualquier actividad o consulta

9. NIVEL DE CUMPLIMIENTO

La política será objeto de evaluación aplicando mecanismos de mejoramiento continuo que involucren participación, compromiso, cooperación, adaptación e inversión.

La Política de Seguridad Digital de la Empresa será de obligatorio cumplimiento para todos los Empleados de planta, contratistas, practicantes, proveedores y terceros.

La política abarca también a clientes internos que son las dependencias que componen la estructura de la Empresa.

10. IMPLEMENTACIÓN DE ESTRATEGIAS

Para la implementación de la Política, la, ha definido las siguientes estrategias:

- Empoderar a los ciudadanos a través de la consolidación de un Estado Abierto

- Elaborar procedimientos de acuerdo a la normatividad que permitan minimizar los riesgos que puedan generar los eventos

- Habilitar y mejorar la provisión de servicios digitales de confianza y calidad

- Implementar iniciativas apropiadas para prevenir, coordinar, atender, controlar, generar recomendaciones y regular los incidentes o emergencias digitales para afrontar las amenazas y los riesgos que atentan contra la seguridad digital.

- Tomar decisiones basadas en datos a partir del aumento en el aprovechamiento de la información

- Adoptar una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información e implementar estrategias de mejoramiento continuo

- Lograr procesos internos seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías procesos e información

- Brindar capacitación especializada en seguridad de la información y seguridad digital

- Implementar controles de acceso a la información, sistemas y recursos de red.

- Definir, implementar, operar y mejorar de forma continua el Plan de Seguridad y privacidad de la información, soportado en lineamientos claros alineados a las necesidades, a la normatividad y a los requerimientos regulatorios.

- Realizar ejercicios de auditoria y monitoreo de la operación de sus procesos que involucren la plataforma tecnológica para minimizar los riesgos asociados al manejo de los recursos tecnológicos y las redes de datos

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los usuarios, o terceros.

- Aplicar controles de acuerdo con la clasificación de la información salvaguardada y en custodia por cada uno de los funcionarios, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta

11. LINEAMIENTOS GENERALES DE LA POLITICA

La Empresa de Servicios Públicos de Guatape, se encargará de:

- Minimizar el uso de dispositivos extraíbles para compartir archivos aprovechando los recursos compartidos del servidor de la entidad o haciendo uso del servicio de internet

- Asignar responsabilidades frente a la seguridad de la información que serán definidas, compartidas, publicadas y aceptadas por cada uno de los proveedores, socios de la Entidad o terceros

- Verificar que la seguridad sea parte integral del ciclo de vida de los sistemas de información

- Proteger la información creada, procesada, transmitida o resguardada por los procesos de la Entidad, con el fin de minimizar los impactos financieros, operativos o legales a causa de los usos de esta y las amenazas originadas por parte del personal.

La Empresa de Servicios Públicos de, velara por qué:

- Todo usuario de los recursos TIC debe advertir e informar al Área de Sistemas o quien haga sus veces, de las medidas específicas de protección para evitar el

acceso a personal no autorizado, y/o establecer el sistema de respaldo para la misma.

- Toda información que provenga de un archivo externo de la Entidad o que deba ser descargado tiene que ser analizado con el antivirus institucional vigente.

- Todo usuario de los recursos TIC, No debe visitar sitios restringidos de manera explícita o implícita, o sitios que afecten la productividad de la Institución; como el acceso desde la Entidad a sitios relacionados con la pornografía, juegos, redes sociales no autorizadas, etc

12. POLITICA DE SEGURIDAD DIGITAL

La Empresa de Servicios Públicos de Guatape, con el fin de abordar las incertidumbres, los riesgos, las amenazas, las vulnerabilidades y los incidentes digitales, adoptará esta política que en su conjunto tendrá como fin contrarrestar el incremento de las amenazas informáticas que pueden afectar significativamente la institución y el correcto desarrollo normativo y legal de las mismas fortaleciendo la institucionalidad de la entidad.

La Entidad Se compromete a administrar los riesgos de seguridad y privacidad de la información para generar, implementar y monitorear los controles que permitan mantener la confidencialidad, integridad y disponibilidad de sus activos de información en cumplimiento de los requisitos aplicables.

La protección de la información; busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con el objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados

Para dar cumplimiento a la política de seguridad digital, La Empresa de Servicios Públicos de Guatape ha definido los siguientes parámetros:

- Los equipos de cómputo y de comunicaciones de la Entidad deben utilizarse únicamente para asuntos de carácter institucional

- El correo electrónico, claves de internet, y chat son de carácter personal e intransferible, es deber de cada uno de los usuarios mantener el uso de estas y de sus contraseñas, por ningún motivo se debe permitir a otra persona acceder a estos recursos

- Toda información que se publique o divulgue por cualquier medio de internet de cualquier empleado, contratista o colaborador que sea creado a nombre personal como redes sociales, se considera fuera del dominio de la Empresa, por lo tanto, su integridad, confiabilidad, disponibilidad y daños y perjuicios que se puedan generar, serán de completa responsabilidad de la persona que las haya generado

- El uso e información de cada equipo es responsabilidad del empleado asignado.

- Cada empleado de La Empresa de Servicios Públicos de Guatape, tendrá un usuario con contraseña personal e intransferible de los aplicativos, correo electrónico, plataformas institucionales y demás para el desempeño de sus funciones

- No debe descargarse juegos ni aplicativos en ninguno de los equipos de la administración.

- Tendrán acceso a redes sociales un grupo de usuario, teniendo en cuenta sus funciones

- La entidad deberá restringir el acceso a los sitios relacionados con redes sociales, con el fin de aumentar la velocidad de acceso y el riesgo de virus. Si algún empleado por motivos de trabajo requiere acceso a ellos, deberá enviarla solicitud al Área de Sistemas

- La contraseña definida por cada usuario debe contener los estándares de seguridad definidos en el plan de seguridad y privacidad de la información.

12.1 PRIVACIDAD Y CONFIDENCIALIDAD

12.1.1 POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

- Los datos personales que los ciudadanos, usuarios, empleados, proveedores que se suministren a La Empresa de Servicios Públicos de Guatape, en cualquiera de sus procesos, serán utilizados para la prestación del servicio solicitado y serán incorporados en una base de datos cuya responsabilidad y manejo está a cargo de la Empresa.

- Los datos personales suministrados serán administrados de forma confidencial y con la finalidad de brindar los servicios y el soporte requerido por el usuario, con las debidas garantías constitucionales, legales y demás normas aplicables a la protección de datos personales.

La Empresa de Servicios Públicos de Guatape:

- No responderá en ningún caso y bajo ninguna circunstancia, por los ataques o incidentes contra la seguridad de su sitio web o contra sus sistemas de información; o por cualquier exposición o acceso no autorizado, fraudulento o ilícito a su sitio web y que afecten la confidencialidad, integridad o autenticidad de la información publicada o asociada con los contenidos y servicios que se ofrecen en él.

- Transferirá la información a un tercero únicamente si está obligado a hacerlo por orden de autoridad administrativa o judicial

- Se abstiene de ceder, vender o compartir los datos de carácter personal recolectados, sin la expresa autorización del usuario

12.1.2 TRATAMIENTO DE LOS DATOS:

El Tratamiento de los datos se realizará para:

- Para los fines relacionados con el desarrollo el proceso de gestión contractual de productos o servicios que la entidad requiera para su funcionamiento de acuerdo a la normatividad vigente

- La vinculación, desempeño de funciones o prestación de servicios, retiro o terminación.

- Para seguridad de las personas, los bienes e instalaciones de gobierno

12.1.3 DERECHOS DE LOS TITULARES

- La revocatoria y/o supresión procederá cuando la Empresa haya determinado que en el tratamiento el responsable o encargado han incurrido en conductas contrarias a la Ley 1581 de 2012 y a la Constitución

- Conocer, actualizar y rectificar sus datos personales frente al responsable y encargado del tratamiento. Este derecho se podrá ejercer entre otros ante datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado

- Revocar la autorización y/o solicitar la supresión del dato personal cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.

- Solicitar prueba de la autorización otorgada a la Empresa como responsable y encargado del tratamiento, salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la Ley 1581 de 2012

- Presentar ante la Empresa quejas por infracciones a lo dispuesto en la Ley 1581 de 2012 y las demás normas que la modifiquen, adicionen o complementen

- Ser informado por la Empresa como responsable del tratamiento y encargado del tratamiento, previa solicitud, respecto del uso que les ha dado a los datos personales del Titular.

12.1.4 AUTORIZACIÓN DEL TITULAR

Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa, expresa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta y verificación posterior.

Casos en que no se requiere la autorización: La autorización del Titular no será necesaria cuando se trate de:

- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos

- Datos de naturaleza pública

- Datos relacionados con el Registro Civil de las Personas

- Información requerida por la Empresa en ejercicio de sus funciones legales o por orden judicial

- Casos de urgencia médica o sanitaria

12.1.5 ACUERDO DE CONFIDENCIALIDAD

Implica que la información conocida por todo empleado, contratista y/o tercero, bajo ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente, sin contar con previa autorización.

12.2 LINEAMIENTOS PARA MEDIOS REMOVIBLES

Son medios removibles todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores, para lo cual se establecen los siguientes lineamientos:

- Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera encriptado y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones.

- El servicio de acceso a Internet, Intranet, Sistemas de información, medio de almacenamiento, aplicaciones (Software), cuentas de red, navegadores y equipos de cómputo son propiedad de La Empresa de Servicios Públicos de Guatape y deben ser usados únicamente para el cumplimiento de la misión de la Entidad.

- Cuando un empleado que tiene asignada una cuenta de correo de la entidad, deberá entregar al Area de Sistemas los usuarios y password asignados, de igual manera dicha información debe entregarse cuando exista un proceso de empalme

- Está restringida la copia de archivos en medios removibles de almacenamiento, por lo cual se deshabilita la opción de escritura en dispositivos USB, unidades ópticas de grabación en todos los equipos de cómputo institucionales.

- Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor

- El manejo, configuración, y actualización de la página institucional es exclusivamente del Área de Sistemas para tal fin.

- Los usuarios deben tratar los mensajes de correo electrónico, chat y archivos adjuntos como información de propiedad de La Empresa de Servicios Públicos de Guatape.

12.3 SEGURIDAD DE COMPUTADORES Y PORTATILES

Para lograr un alto rendimiento y salvaguarda de computadores y portátiles, La Empresa de Servicios Públicos de Guatape ha definido los siguientes parámetros.

- Los recursos de Gobierno en Línea, utilizados para el procesamiento de la información deben ser ubicados en sitios estratégicos, que faciliten el trabajo compartido, el trabajo colaborativo, la optimización de recursos

- Los computadores de mesa, portátiles, y cualquier activo de tecnología de información, podrán salir de las instalaciones únicamente con la aprobación del Jefe del área.

- Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en computadores que tengan también conexión a la red local

- Se prohíben que los equipos estén en contacto con piso, el usuario debe disponerlo (computador y/o Portátil) sobre el escritorio

- El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones de La Empresa de Servicios Públicos de Guatape.

- Los equipos de La Empresa de Servicios Públicos de Guatape, sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos

- El Área de Sistemas no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información) a equipos que no sean de La Empresa de Servicios Públicos de Guatape

- Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario.

- El personal que utiliza un computador portátil que contenga información confidencial de la institución, no debe dejarlo desatendido, sobre todo cuando esté de viaje.

- Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente a la oficina de las TIC y poner el computador en cuarentena hasta que el problema sea resuelto

- Debe respetarse y no modificar la configuración de hardware y software establecida por el Area de Sistemas

- Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del computador

- A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la Empresa está protegido por derechos de autor y requiere licencia de uso. Por tal razón, es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

- Los usuarios deberán asegurarse de respaldar la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previniendo así la pérdida involuntaria de información, derivada del proceso de reparación

- No debe utilizarse software descargado de Internet y en general software que provenga de una fuente no confiable, a menos que haya sido comprobado en forma rigurosa y que esté aprobado su uso por el Área de Sistemas de la Empresa

13. COMPROMISO DE LA ALTA DIRECCIÓN

La Empresa de Servicios Públicos de Guatape, aprueba esta Política de Seguridad Digital como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad digital de la Entidad

la Alta Dirección de la Empresa demuestra su compromiso a través de:

- El aseguramiento de los recursos adecuados para implementar y mantener la política de seguridad digital.

- La promoción activa de una cultura de seguridad

- La verificación del cumplimiento de la política aquí mencionada

- Facilitar la divulgación de esta política a todos los empleados de la Entidad

- La revisión y aprobación de la Política de Seguridad Digital contenida en este documento.

14. ARMONIZACION Y COORDINACIÓN

La política de Seguridad Digital, se armonizará en concordancia con los lineamientos que imparte la función pública, que al interior de la entidad la implementará el Área de Sistemas o a quien se delegue; el MIPG coordinado por el Asesor del mismo y los demás procesos desarrollados por La Empresa de Servicios Públicos de Guatape.

15. COMUNICACIÓN

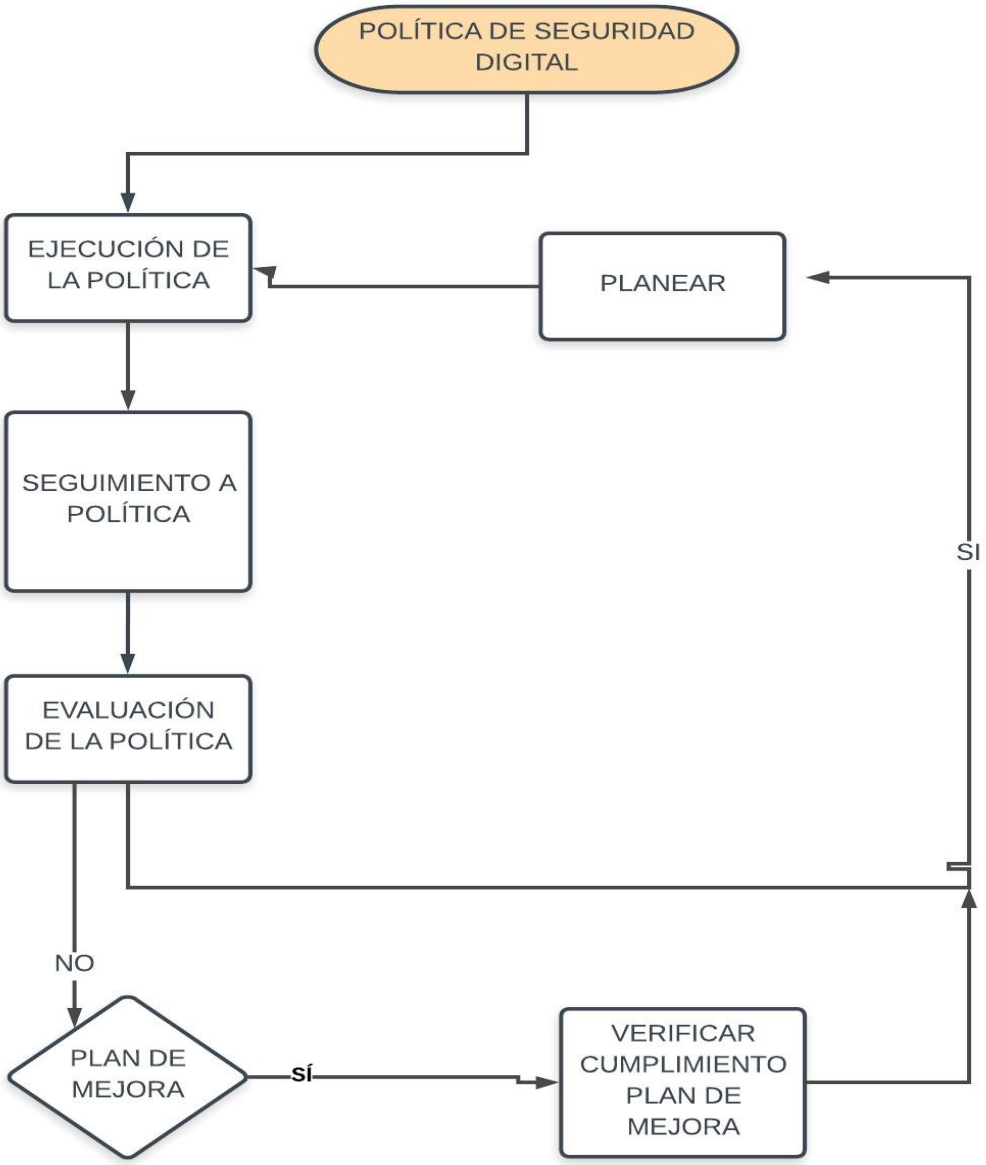
La divulgación de la Política debe ser transmitida e implementada a través de las diferentes dependencias que conforman la estructura organizacional y jerarquía de La Empresa de Servicios Públicos de Guatape

16. EVALUACIÓN Y SEGUIMIENTO

El seguimiento es un instrumento indispensable para la implementación adecuada de la política. Se trata de contar con la opción de supervisar el avance o, en su caso, los problemas que registre el desarrollo de la misma para de manera oportuna tomar acciones o medidas correctivas

ESTRATEGIAS	UNIDAD DE MEDIDA	INDICADOR	RESPONSABLE	PERIODICIDAD
Implementar estrategias para afrontar las amenazas y los riesgos que atentan contra la seguridad digital.	Estrategias para minimizar riesgos	Estrategias para minimizar riesgos implementada	Todas las dependencias	Diciembre de cada año
Brindar capacitación especializada en seguridad de la información	Capacitación en seguridad de la información	Capacitación en seguridad de la información realizada	Todas las dependencias	Diciembre de cada año
Definir, implementar, operar y mejorar de forma continua el plan de Seguridad y privacidad de la información,	Plan de Seguridady privacidad de la Información	Plan de Seguridad y privacidad de la Información formulado e implementado	Todas las dependencias	Diciembre de cada año

Definir responsabilidades frentea la seguridad de la información	Responsabilidades definidas	Responsabilidades definidas frente a seguridad de la información	Todas las dependencias	Diciembre de cada año
Aplicar controles de acuerdo con la clasificación de la información salvaguardada y en custodia por cada uno de los funcionarios	Controles aplicados	Controles aplicados	Todas las dependencias	Diciembre de cada año
Realizar ejercicios de auditoria y monitoreo de la operación de sus procesos que involucren la plataforma tecnológica para minimizar los riesgos asociados al manejo de los recursos tecnológicos y las redes de datos.	Auditorías realizadas	Auditorías realizadas	Todas las dependencias	Diciembre de cada año
Implementar controles de acceso a la información, sistemas y recursos de red.	Controles realizados	Controles realizados	Todas las dependencias	Diciembre de cada año
Adoptar una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información e implementar estrategias de mejoramiento continuo.	Estrategias de mejoramiento continuo	Estrategias de mejoramiento continuo adoptadas	Todas las dependencias	Diciembre de cada año
Elaborar procedimientos de acuerdo a la normatividad que permitan minimizar los riesgos que puedan generar los eventos.	Procedimientos	Procedimientos elaborados	Todas las dependencias	Diciembre de cada año


POLÍTICA DE SEGURIDAD DIGITAL
EJECUCIÓN DE LA POLÍTICA
PLANEAR
SEGUIMIENTO A POLÍTICA
EVALUACIÓN DE LA POLÍTICA
SI
NO
PLAN DE MEJORA
SÍ
VERIFICAR CUMPLIMIENTO PLAN DE MEJORA

17. CONCLUSIONES

- El desarrollo de las estrategias de la Política de Seguridad Digital buscan contrarrestar el incremento de las amenazas informáticas que pueden afectar significativamente la Empresa y el correcto desarrollo normativo y legal de las mismas fortaleciendo la institucionalidad de la entidad.

- La implementación de esta política permite establecer reglas, lineamientos y buenas prácticas que coadyuven a la confidencialidad, seguridad y disponibilidad de la información digital que permita minimizar el riesgo de pérdida de datos, accesos no autorizados, divulgación no controlada y duplicación e interrupción intencional de la información.

18. RECOMENDACIONES

- Es necesario que todos los Empleados de la entidad puedan entender la importancia de su labor en función de los propósitos misionales de la entidad, conozcan y se apropien de esta política 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, el mejoramiento continuo y aumentar la confianza ante ciudadanos.

- Implementar la política de Seguridad Digital para establecer lineamientos y estrategias para que los recursos TIC obedezcan a las directrices de seguridad y evitar que se creen vulnerabilidades que impacten la Entidad.

- Se requiere retroalimentación constante y mejoramiento continuo para rediseñar los instrumentos, herramientas y estrategias que permitan 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.