POLITICA DE SEGURIDAD DIGITAL
AGUAS DEL HUILA S.A E.S.P

aguas del huila
...llevamos más que agua.

www.aguasdelhuila.gov.co

Contenido

INTRODUCCIÓN....3
MARCO NORMARTIVO....4
MARCO CONCEPTUAL....4
OBJETIVOS....7
OBJETIVO GENERAL....7
OBJETIVOS ESPECIFICOS....7
LINEAMIENTOS ESTRATÉGICOS....7
GESTION DE ACTIVOS....8
CONTROL DE ACCESO....8
INTEGRIDAD....8
SEGURIDAD DIGITAL....9
POLITICA DE SEGUIRDAD DIGITAL....9
DESARROLLO DE LA POLITICA....9
ALCANCE....10
VIGENCIA Y AVISO POLÍTICA DE SERVICIO AL CIUDADANO....10

INTRODUCCIÓN

La política de Seguridad Digital fomenta las buenas prácticas en el proceso de sistemas de la Empresa AGUAS DEL HUILA S.A.ES.P., buscando promover una adecuada gestión interna de las dependencias y mejorar la relación con el ciudadano a través de la participación y la prestación de servicios de calidad, brindando así información más precisa y protegida, debido a lo anterior es deber asegurarse que la información se proteja lo más pertinentemente en cuando a como se recolecta, como se administra y como se almacena. Por lo tanto, en el presente documento se describe la Política de Seguridad Digital para la cual se tomaron los lineamientos en base a ley y todas las regulaciones aplicables al tema, esta política hace parte de los procesos de gestión de la empresa y sirve para ejercer control, establecer todos los procedimientos y estándares que se necesitan.

En cumplimiento a lo estipulado en el Modelo Integrado de Planeación y Gestión MIPG, como 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, AGUAS DEL HUILA S.A.E.S.P, incorpora la política de seguridad digital en el marco de la tercera dimensión: Gestión con valores para resultados, La implementación de la política, se hará a través de la adopción e implementación del Modelo de Gestión de Riesgos de Seguridad Digital.

MARCO NORMARTIVO

- Guía lineamientos para la gestión de riesgos de seguridad digital en entidades públicas
- Ley 1928 de 2018 “Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest.
- Acuerdo 02 de 2018: Por el cual se crea el comité de Seguridad Digital.
- CONPES 3854 de 2016: POLÍTICA NACIONAL DE SEGURIDAD DIGITAL
- Decreto 1078 de 2015: “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”
- Ley 1712 de 2014 - Transparencia y Acceso a la Información Pública
- Ley estatutaria 1581 del 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 103 de 2015: por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 1499 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”. Presidencia de la República.
- Manual Operativo Modelo Integrado de Planeación y Gestión - MIPG Versión 4.
- Decreto 1083 de 2015 "Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales"

MARCO CONCEPTUAL

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.

Archivo

Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

Amenazas

Causa potencial de un incidente no deseado, que puede provocar danos a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoria

Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

Autorización:

Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

Bases de Datos Personales:

Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

Ciberseguridad

Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio

Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos:

Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

Datos Personales:

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos:

Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

Datos Personales Privados:

Es el dato que por su naturaleza intima o reservada solo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

Datos Personales Mixtos:

Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles:

Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como os datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

Declaración de aplicabilidad

Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Derecho a la Intimidad:

Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado del Tratamiento de Datos:

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

OBJETIVOS

OBJETIVO GENERAL

Establecer los componentes para proteger el sistema de información y los diferentes recursos tecnológicos de AGUAS DEL HUILA S.A. E.S.P., los cuales se deben conocer y cumplir por parte de todos los directivos, funcionarios, contratistas y terceros que presten su servicio o mantengan alguna relación con la entidad.

OBJETIVOS ESPECIFICOS

- Identificar, analizar y mitigar riesgos de seguridad digital.
- Garantizar en un alto grado la disponibilidad, integridad y confidencialidad de la información.
- Garantizar el correcto funcionamiento del plan de acción.
- Adoptar una metodología y procedimiento en la gestión del riesgo para el tratamiento de la información que permita una adecuada seguridad y privacidad de la misma que logre fortalecer y sostener un adecuado nivel de riesgos.

LINEAMIENTOS ESTRATÉGICOS

Se establecen los lineamientos, directrices y prohibiciones que rigen la Política de seguridad en los cuales se establece el derecho que tienen las personas que acceden a ella, el mecanismo de uso, transformación, defensa y responsabilidad del contenido y las prohibiciones que administran.

GESTION DE ACTIVOS

AGUAS DEL HUILA S.A.E.S.P., se compromete a realizar los debidos controles del uso y seguridad de la información digital, para proteger la publicada o resguardada y evitar lo impactos en la entidad por el uso indebido de la misma. Bajo las siguientes pautas: se hará un control y supervisión de datos teniendo en cuenta la responsabilidad, la reserva, sensibilidad. Los cambios en los aplicativos se harán por el personal autorizado. Los activos de información estarán inventariados y se deberá velar por su cuidado para no sufrir por daño o pérdida. Se velará por la modernización de recursos tecnológicos para mejorar, así mismo todo material que se cree, envíe o se reciba lo resguardará la entidad y por último los usuarios darán su consentimiento a los funcionarios para revisar material que creen, almacenen, envíen o reciban por equipo de cómputo o por internet.

No se podrá divulgar o retirar información no autorizada ya sea en medios físicos como celulares, memorias o en papel. Tampoco usar los medios tecnológicos para propagar contenido no autorizado. Desperdiciar recursos tecnológicos tanto como copiar software o hasta contratar, descargar sin previa autorización.

CONTROL DE ACCESO

Se respetarán las contraseñas que restrinjan la manipulación por parte de agentes externos, Igualmente proteger la información generada, procesada o resguardada por los procesos, de esta forma los usuarios son responsables de salvaguardar sus contraseñas y por lo tanto proteger la información, utilizar el acceso a internet para uso laboral, como también evitar el acceso no autorizado a sistemas y aplicaciones.

INTEGRIDAD

Todo usuario debe utilizar los activos de información de forma responsable, ética y legal. De deberá mantener la privacidad de la información y usada para el cumplimiento de metas, objetivos y propósitos.

SEGURIDAD DIGITAL

La entidad se compromete a robustecer la seguridad digital, de modo que el usuario de los activos de información desarrolle la confianza en las aplicaciones digitales, que son implementadas para la prosperidad del servicio y frenar los tipos de crímenes que atentan contra la seguridad de la entidad.

POLITICA DE SEGUIRDAD DIGITAL

AGUAS DEL HUILA S.A.E.S.P., establece estrategias para el amparo de los activos de información, legitimar la confidencialidad, integridad y disponibilidad de los mismos, emitiendo los lineamientos con respecto a la protección de los activos de información incluido el hardware y el software, que soportan los procesos y que apoyan la implementación del Sistema de Gestión de Seguridad.

DESARROLLO DE LA POLITICA

La implementación de la política de seguridad digital en AGUAS DEL HUILA S.A. E.S.P., se basa en el cumplimiento de las siguientes actividades:

A. Definir, implementar, operar y mejorar de forma continua el Plan de Seguridad y privacidad de la información.
B. Brindar capacitación constante en seguridad de la información y seguridad digital en las diferentes consultas técnicas de los usuarios, incentivándolos en el mejor uso y operación de las tecnologías de la información.
C. Concientizar a los funcionarios y contratistas sobre sus responsabilidades frente a la seguridad de la información mediante la ejecución de un plan de sensibilización.
D. Elaborar procedimientos de acuerdo a la normatividad que permitan minimizar los riesgos como copias de seguridad, cuentas de correo electrónico, usuarios y contraseñas, entre otros.

PRICIPIOS

Confidencialidad de la información

Según www.unir.net “la privacidad, hace referencia a que la información sólo debe ser conocida por las personas que necesitan conocerla y que han sido autorizadas para ello. Este principio asegura que la información no va a ser divulgada de manera fortuita o intencionada”.

Integridad de la información

Hace referencia a que la información que se encuentra almacenada en los dispositivos o la que se ha transmitido por cualquier canal de comunicación no ha sido manipulada por terceros de manera malintencionada. Esto garantiza que la información no será modificada por personas no autorizadas.

Disponibilidad de la información

Según www.unir.net “Se refiere a que la información debe estar disponible siempre para las personas autorizadas para accederla y tratarla, y además puede recuperarse en caso de que ocurra un incidente de seguridad que cause su pérdida o corrupción. Es decir, permite que la información esté disponible cuando sea necesario”.

APLICABILIAD

La presente política aplica en el desarrollo en todos los procesos y de la Entidad a todos los servidores que procesan y manejan información incluida la recopilación, análisis, procesamiento, disponibilidad, custodia, conservación y recuperación y deben preservar la confidencialidad de la información que por razones de su cargo o responsabilidades designada esté bajo su custodia.

VIGENCIA Y AVISO POLÍTICA DE SERVICIO AL CIUDADANO

La Política de Servicio al Ciudadano de Aguas del Huila S.A. E.S.P., la cual será divulgada y publicada en la página web, www.aguasdelhuila.gov.co.

GENARO LOZADA MENDIETA
Gerente