PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Vigencia 2024

La versión vigente y controlada de este documento, solo podrá ser consultada a través de la página web www.edat.gov.co . La copia o impresión diferente a la publicada, será considerada como documento no controlado.

CONTENIDO

CONTENIDO 2
INTRODUCCIÓN 3
1. PRESENTACIÓN 4
2. OBJETIVO 7
3. DEFINICIONES 8
4. GESTIÓN DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. 12
5. ACTIVIDADES PROYECTADAS EN EL PLAN DE TRATAMIENTO DE RIESGOS 15
CONTROL DE CAMBIOS 16

INTRODUCCIÓN

El presente documento establece las acciones que la Empresa Departamental de Acueducto, Alcantarillado y Aseo del Tolima EDAT S.A. E.S.P. Oficial, ejecuta para implementar y socializar el componente de Gobierno Digital en el eje temático de la estrategia de gestionar los Riesgos de Privacidad y Seguridad de la Información, el cual busca manejar de la manera más adecuada los datos de los usuarios de los diferentes servicios que ofrece la entidad. Cabe mencionar que el presente plan corresponde al cumplimiento de lo establecido en la ley 152 de 1994 y el artículo 74 de la ley 1474 de 2011.

Además, se encuentra articulado con el plan de acción anual de conformidad con el decreto 612 de 2018.

1. PRESENTACIÓN

En Colombia se viene adelantando la implementación de la política de gobierno digital, tal como lo establece La Presidencia de la Republica y el Ministerio de Tecnologías de la Información y las Comunicaciones a través del Decreto 767 de 2022, cuyas disposiciones se compilan en el Decreto Único Reglamentario del Sector TIC, 1078 de 2015, específicamente en el capítulo 1, titulo 9, parte 2, libro 2, como un instrumento fundamental para mejorar la gestión pública y la relación del estado con los ciudadanos, la cual se ha articulado con el Modelo Integrado de Planeación y Gestión, como una herramienta dinamizadora para cumplir las metas de las políticas de desarrollo administrativo, articulada a otras políticas esenciales para la gestión pública en Colombia.

El Manual de la política de Gobierno Digital expedido por el MinTIC establece que la política tiene como propósito promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital. Según el manual, la implementación de la política de gobierno digital se ha definido en dos componentes: TIC para el estado y TIC para la sociedad, que son habilitados por cuatro elementos transversales: Arquitectura, Cultura y Apropiación, Seguridad y Privacidad de la Información y Servicios Ciudadanos Digitales.

Estos seis elementos, se desarrollan a través de lineamientos y estándares, que son requerimientos mínimos que todos los sujetos obligados deben cumplir para alcanzar los logros de la política. El manual en mención, precisa que el habilitador de Seguridad y Privacidad de la Información, busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, tramites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

No obstante, el Artículo 2.2.9.1.2.1 del Decreto Ministerial 1078 de 2015 establece que La Política de Gobierno Digital se desarrollará a través de un esquema que articula los elementos que la componen, a saber: gobernanza, innovación pública digital, habilitadores, líneas de acción, e iniciativas dinamizadoras, con el fin de lograr su objetivo.

En el mencionado artículo, en su numeral 3.2 resalta como habilitador, la Seguridad y Privacidad de la Información donde los sujetos obligados deben desarrollar capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

El documento denominado Modelo de Seguridad y Privacidad de la Información (MSPI), expedido por el Ministerio de Tecnologías de Información y de las Comunicaciones, expresa que la adopción de este, por las entidades del estado, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, apoyada en un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

La adopción, implementación y evaluación del modelo mencionado, es una actividad obligatoria según lo expresado en el artículo 2.2.9.1.3.2 del Decreto 767 de 2022. De igual manera es importante resaltar que es a través del Decreto Presidencial 612 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", en su artículo 1, adiciona al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto Presidencial 1083 de 2015, Único Reglamentario del Sector de Función Pública, agregando al anterior Decreto el artículo 2.2.22.3.14, por medio del cual se integran los planes institucionales y estratégicos al Plan de Acción, considerando en su numeral 11 y 12 como obligación la elaboración anual del "Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información" y del "Plan de Seguridad y Privacidad de la Información" respectivamente de cada Entidad.

Así mismo, la resolución 0500 de marzo 10 del 2021 expedida por el Ministerio de Tecnologías de Información y de las Comunicaciones, que tiene como objeto establecer los lineamientos generales para la implementación del Modelo de

Seguridad y Privacidad de la Información, la guía de gestión de riesgos de Seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y establecer los lineamientos y estándares para la estrategia de seguridad digital.

La resolución en mención precisa la necesidad de que los sujetos obligados deban adoptar las medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al Plan de Seguridad y Privacidad de la Información y así mitigar los riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital.

Es precisamente a través del artículo 5 de la resolución 0500 que se precisa la necesidad de adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital, e incluirla en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos del artículo 2.22.22.3.14 del capítulo 3 del título 22 de la parte 2 del libro 2 del decreto 1083 de 2015.

En atención a lo anterior, se presenta el plan de seguridad y privacidad de la información para la ***Empresa Departamental de Acueducto, Alcantarillado y Aseo del Tolima EDAT S.A. E.S.P. Oficial***.

2. OBJETIVO

Establecer un marco de acción orientado a la implementación del Modelo de Seguridad y Privacidad de la información, sobre los activos de información que soportan el cumplimiento de los objetivos organizacionales, conducente a preservar la confidencialidad, integridad y disponibilidad de la información institucional, en atención al contexto de la entidad, las capacidades y recursos disponibles, para fortalecer la confianza de los grupos de valor y de interés.

La planeación se enfocará en fortalecer la implementación de acciones de acuerdo con los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, orientados a mejorar las condiciones de seguridad y privacidad de la información en las diferentes dependencias adscritas a la Empresa Departamental de Acueducto, Alcantarillado y Aseo del Tolima EDAT S.A. E.S.P. Oficial en atención al logro de los objetivos organizacionales, teniendo en cuenta las capacidades y recursos disponibles, para mejorar la confianza de los grupos de valor y de interés.

3. DEFINICIONES

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen 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 de Información: Es toda aquella información que reside en un medio electrónico o físico, que tiene un significado y valor para la Empresa Departamental de Acueducto, Alcantarillado y Aseo del Tolima EDAT S.A. E.S.P. Oficial, y, por ende, necesita ser protegida.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización por completo.

Apetito del Riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección y del órgano de gobierno. El apetito del riesgo puede ser diferente para los diferentes tipos de riesgo que la entidad debe o desea gestionar.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material,

Auditoría: Proceso sistemático, independiente y documentado par 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).

Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, puede producir la materialización de un riesgo.

Causa Inmediata: Son las circunstancias sobre las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, corresponde a las razones por las cuales se puede presentar el riesgo.

Certificado SSL: Certificado que cifra bidireccionalmente toda conexión al sitio web para privacidad de la información y certifica el sitio web como "conexión segura", emitido por Cloudflare.

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3710).

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)

Confidencialidad: Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

Consecuencias: Los efectos y situaciones resultantes de la materialización del riesgo que impactan en el proceso, en la entidad, sus grupos de valor y demás partes interesadas.

CND Cloudflare: Red de distribución de contenido, que cuenta adicionalmente con caché de contenido, certificado SSL y protección DDoS.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. En este documento se habla de las Norma Técnica Colombiana ISO31000:2013.

Factores de Riesgo: Son las diferentes fuentes generadoras de riesgos.

Gestión del riesgo: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Impacto: Son las consecuencias que puede ocasionar a la Empresa Departamental de Acueducto, Alcantarillado y Aseo del Tolima EDAT S.A. E.S.P Oficial la materialización del riesgo.

Información: Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.

Integridad: propiedad de exactitud y completitud.

Nivel de Riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

Política de seguridad de información: Es el instrumento que adopta una entidad para definir las reglas de comportamiento aceptables en el uso y tratamiento de la información.

Probabilidad: Se entiende la posibilidad de ocurrencia de un riesgo. Estará asociada a la exposición del riesgo del proceso o actividad que se está analizando.

Riesgo: Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o de los procesos de la Empresa Departamental de Acueducto, Alcantarillado y Aseo del Tolima EDAT S.A. E.S.P. Oficial. Se expresa en términos de probabilidad y consecuencias.

Riesgo de Corrupción: Es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; *Estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información.* Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera.

Riesgo de Seguridad Digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los

intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgo de seguridad y privacidad: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. Se mide en términos de Contexto - Información sobre la evaluación de riesgos probabilidad y consecuencias.

Sistema de Gestión de Seguridad de la Información: Parte del sistema de gestión general de la Empresa Departamental de Acueducto, Alcantarillado y Aseo del Tolima EDAT S.A. E.S.P. Oficial, basada en un enfoque hacia los riesgos globales del negocio, cuyos fines son establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.

Titulares de la Información: Son las personas naturales cuyos datos personales sean objeto de Tratamiento (Ley 1581 de 2012, Art. 3).

Tolerancia del Riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito del riesgo determinado por la entidad.

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad (ISO/IEC 27000).

Vulnerabilidad: Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

4. GESTIÓN DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La gestión de Riesgo de Seguridad y Privacidad de la Información del presente plan obedece a la estructura y etapas definidas en la “Guía para la Administración de Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en las Entidades Públicas” del Ministerio de Tecnologías de la Información y las Comunicaciones y el Departamento Administrativo de la Función Pública.

Además de tener en cuenta las políticas de administración de Riesgo de Colombia Compra Eficiente.

PROCESO	ACTIVO	DESCRIPCIÓN	DUEÑO DEL ACTIVO	TIPO DE ACTIVO	LEY 1712 DE 2014	LEY 1581 DE 2012	CRITICIDAD RESPECTO A SU CONFIDENCIALIDAD	CRITICIDAD RESPECTO A COMPLETITUD O INTEGRIDAD	CRITICIDAD RESPECTO A SU DISPONIBILIDAD	NIVEL DE CRITICIDAD
GESTIÓN HUMANA Y SST	BASE DE DATOS DE CONTRATISTAS Y EMPLEADOS DE PLANTA	Bases de datos con la información de los empleados de planta y los contratistas que trabajan en la entidad	Secretaria General	Información	Información Reservada	Contiene datos personales	ALTA	ALTA	ALTA	ALTA
GESTIÓN FNANCIERA	BASE DE DATOS DE NÓMINA	Base de datos con información de la nómina de la entidad	Dirección Financiera y Tesorería	Información	Información Reservada	No contiene datos personales	ALTA	ALTA	ALTA	ALTA
GESTIÓN FINANCIERA	APLICATIVO CONTABLE	Servidor Web que contiene Syscafe de la entidad	Dirección Financiera y Tesorería	Software	N/A	N/A	BAJA	MEDIA	BAJA	MEDIA

ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN	AMENAZAS	CONTROLES EXISTENTES	VULNERABILIDADES	ACCIONES DE TRATAMIENTO
Servicios Web	Posibles ataques por parte de piratas electrónicos	Protocolos de seguridad informática, políticas de tratamiento de datos personales	Formulario de PQRS que intentan ingresar como personas sin autenticarse	Formularios protegidos mediante reCAPTCHA v2.0 para prevenir el acceso de robots de SPAM ('spammers').
Redes	Líneas de comunicación sin la debida protección	Organización de la mejor manera posible del cableado.	Daño en los cables de red, por desprotección	Montaje de canaleta adecuada para le protección de los cables de red
Información Física o Digital	Daño físico de los documentos	Se esta realizando la digitalización y control de la documentación	Perdida y daño de información importante para la entidad	Reconstrucción de documentación y digitalización acorde a los reglamentos del archivo general de la nación.
Tecnología de Información TI	Ausencia de copias de seguridad	No existen controles al momento	Perdida importante de información de contratistas que ya no laboran en la entidad.	Compra de discos duros externos de gran capacidad para guardar esta información
Tecnologías de Operación TO	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información.	No existen al momento.	Abuso de los derechos	Crear a largo plazo los procedimientos adecuados para mejorar este aspecto

5. ACTIVIDADES PROYECTADAS EN EL PLAN DE TRATAMIENTO DE RIESGOS

CRONOGRAMA DE ACTIVIDADES PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN 2024 - 2025

ACTIVIDAD	ABRIL JUNIO				JULIO SEPTIEMBRE				OCTUBRE DICIEMBRE				ENERO MARZO				ABRIL JUNIO			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Realizar diagnóstico de la entidad para actualizar los riesgos																				
Actualización de la política de Seguridad y Privacidad de la Información																				
Valoración del riesgo residual																				
Socialización de la política de seguridad y privacidad de la información																				
Seguimiento y Control																				

CONTROL DE CAMBIOS

FECHA	DESCRIPCIÓN DEL CAMBIO	VERSIÓN
Diciembre de 2020	• Edición de documento	01
2022/01/31	• Actualización del documento, teniendo en cuenta los lineamientos para la vigencia 2022 y la programación de nuevas actividades	02
2023/01/31	• Actualización del documento, teniendo en cuenta la normatividad vigente.	03
2024/01/31	• Actualización del documento, de acuerdo con lo definido en la normatividad vigente y las recomendaciones de mejora identificadas en el marco del Sistema Integrado de Gestión, a partir de las Auditorías Internas y demás instrumentos de evaluación.	04