EMPRESA MUNICIPAL DE ACUEDUCTO, ALCANTARILLADO Y ASEO DE FUNZA – EMAAF E.S.P.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ANDRES FELIPE RINCON DAMIAN
GERENTE

INTRODUCCIÓN

La Seguridad de la Información en la Empresa Municipal de Acueducto, Alcantarillado y Aseo de Funza EMAAF ESP, tiene como objetivo la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta y se logre alcanzar el máximo retorno de las inversiones en las oportunidades de negocio.

Los principios de protección de la información se enmarcan en:

Confidencialidad: Propiedad que la información sea concedida únicamente a quien esté autorizado.

Integridad: Propiedad que la información se mantenga exacta y completa.

Disponibilidad: propiedad que la información sea accesible y utilizable en el momento que se requiera.

OBJETIVO

Generar acciones frente a la gestión del riesgo bajo enfoque sistemático para una gestión que fortalezca la seguridad de la información en la Empresa Municipal de Acueducto, Alcantarillado y Aseo de Funza EMAAF ESP.

ALCANCE

La gestión de riesgos de seguridad de la información y su tratamiento, podrá ser aplicada sobre cualquier proceso de la Empresa que administre sistemas de información a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, tomando como base

la guía emitida por el DAFP y los requisitos de la Norma NTC-ISO/IEC 27001 Sistema de Gestión de Seguridad de Información.

Metodología de Análisis de Riesgos:

1- Identificar los activos de Información de cada proceso
2- Identificación de los responsables y dueños de la información(dependencia que produce el activo)
3- Identificar: Vulnerabilidades, Amenazas o Causas, Posibles consecuencias, Riesgo (Entrevistas, Observación directa, etc)
4- Determinar la probabilidad de ocurrencia para cada riesgo.
5- Determinar nivel de valoración del impacto para cada riesgo materializado.
6- Determinar el nivel de riesgo basados en la probabilidad de ocurrencia y la valoración del Impacto.

Definiciones:

Factor de Riesgo:

Aquellos que pueden afectar la confidencialidad, la integridad o la disponibilidad de la información

Factor de Riesgo	Descripción
Personas	Personal de la organización que se encuentra relacionado con la ejecución del proceso de forma directa o indirecta.
Procesos	Conjunto interrelacionado entre sí de actividades y tareas necesarias para llevar a cabo el proceso.
Tecnología	Conjunto de herramientas tecnológicas que intervienen de manera directa o indirecta en la ejecución del proceso.
Infraestructura	Conjunto de recursos físicos que apoyan el funcionamiento de la organización y de manera específica el proceso.
Factores Externos	Condiciones generadas por agentes externos, las cuales no son controlables por la administración y que afectan de manera directa o indirecta el proceso.

Tipos de Activos:

TIPO DE ACTIVOS	DESCRIPCIÓN
Activos Esenciales	**Datos importantes o vitales para la Administración de la Entidad:** Aquellos que son esenciales, imprescindibles para la continuidad de la entidad; es decir que su carencia o daño afectaría directamente a la entidad, permitiría reconstruir las misiones críticas o que sustancian la naturaleza legal de la organización o de sus usuarios. **Datos de carácter personal:** Cualquier información concerniente a personas físicas identificadas o identificables. Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su intimidad personal y familiar (Ley 1581 de 2012). **Datos Clasificados o Calificados:** Aquellos sometidos a normativa específica de control de acceso y distribución o cuya confidencialidad es tipificada por normativa interna o legislación nacional (Ley 1712 de 2014).
Datos / Información	**Que es almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.** Ejemplo: Copias de Respaldo, Ficheros, Datos de Gestión Interna, Datos de Configuración, Credenciales (Contraseñas), Datos de Validación de Credenciales (Autenticación), Datos de Control de Acceso, Registros de Actividad (Log), Matrices de Roles y Privilegios, Código Fuente, Código Ejecutable, Datos de Prueba.

TIPO DE ACTIVOS	DESCRIPCIÓN
Hardware / Infraestructura	**Medios físicos, destinados a soportar directa o indirectamente los servicios que presta la entidad, siendo depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.** Ejemplo: Servidores (host), Equipos de Escritorio (Pc), Equipos Portátiles (Laptop), Dispositivos Móviles, Equipos de Respaldo, Periféricos, Dispositivos Criptográficos, Dispositivos Biométricos, Servidores de Impresión, Impresoras, Escáneres, Equipos Virtuales (vhost), Soporte de la Red (Network), Módems, Concentradores, Conmutadores (switch), Encaminadores (router), Pasarelas (bridge), Firewall, Central Telefónica, Telefonía IP, Access Point.
Software / Aplicaciones Informáticas	**Que gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.** Ejemplo: Desarrollo Inhouse, Desarrollo Subcontratado, Estándar, Navegador, Servidor de Presentación (www), Servidor de Aplicaciones (app), Cliente de Correo Electrónico, Servidor de Correo Electrónico, Servidor de Ficheros (file), Sistemas de Gestión de Bases de Datos (dbms), Monitor Transaccional, Ofimática, Antivirus, Sistema Operativo (OS), Servidor de Terminales, Sistema de Backup o Respaldo, Gestor de Máquinas Virtuales.
Servicios	**Funciones que permiten suplir una necesidad de los usuarios (del servicio).** Ejemplo: Página Web, Correo Electrónico, Acceso Remoto, almacenamiento de ficheros, transferencia de ficheros, intercambio electrónico de datos, Gestión de Identidades (altas y bajas de usuarios del sistema), Gestión de Privilegios,

TIPO DE ACTIVOS	DESCRIPCIÓN
	Intercambio electrónico de datos, PKI (Infraestructura de Clave Pública).
Personas	Usuarios Internos, Usuarios Externos, Operadores, Administradores de Sistemas, Administradores de Comunicaciones, Administradores de Bases de Datos, Administradores de Seguridad, Programadores, Contratistas, Proveedores.
Soportes de Información	**Dispositivos físicos electrónicos o no que permiten almacenar información de forma permanente o durante largos periodos de tiempo.** Ejemplo: Discos, Discos Virtuales, Almacenamiento en Red (san), Memorias USB, CDROM, DVD, Cinta Magnética (tape), Tarjetas de Memoria, Tarjetas Inteligentes, Material Impreso, Microfilmaciones.
Redes de Comunicaciones	**Instalaciones dedicadas como servicios de comunicaciones contratados a terceros o medios de transporte de datos de un sitio a otro.** Ejemplo: Red Telefónica, Red Inalámbrica, Telefonía Móvil, Satelital, Red Local (LAN), Red Metropolitana (MAN), Internet, Radio Comunicaciones, Punto a Punto, ADSL, Red Digital (rdsi).
Claves Criptográficas	**Esenciales para garantizar el funcionamiento de los mecanismos criptográficos.** Ejemplo: Claves de Cifrado, Claves de Firma, Protección de Comunicaciones (Claves de Cifrado de Canal), Cifrado de Soportes de Información, Certificados Digitales, Certificados de Claves, Claves de Autenticación.

TIPO DE ACTIVOS	DESCRIPCIÓN
Equipos Auxiliares	**Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.** Ejemplo: Fuentes de alimentación, generadores eléctricos, equipos de climatización, sistemas de alimentación ininterrumpida (UPS), cableado, cable eléctrico, fibra óptica, equipos de destrucción de soportes de información, mobiliarios, armarios, cajas fuertes.
Instalaciones	Lugares donde albergan los sistemas de información y comunicaciones.

MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información.
Los riesgos son dinámicos de conformidad a la gestión de la empresa, por tanto podrán cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión continua que detecte:

(1) nuevos activos o modificaciones en el valor de los activos,
(2) nuevas amenazas
(3) cambios o aparición de nuevas vulnerabilidades
(4) aumento de las consecuencias o impactos,
(5) incidentes de seguridad de la información.

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y medición que permitan contextualizar una toma de decisiones de manera oportuna.

CRONOGRAMA VALORACION DE RIESGOS DE SEGURIDAD DE LA INFORMACION

Se definirá y mantendrá un cronograma de actividades para la realización de la valoración de los riesgos de seguridad de la información en los procesos de la

organización, basado con su criticidad y su valor para el cumplimiento del objeto misional de la EMAAF E.S.P.

ID	ACTIVIDAD	FECHA INICIO	FECHA FINAL
1	Sensibilización institucional sobre política de seguridad de la información.	01/04/2022	30/04/2022
2	Desarrollar y/o actualizar el inventario de activos de información.	01/02/2022	31/05/2022
3	Elaborar procedimiento gestión de riesgos de seguridad de la información.	01/03/2022	30/04/2022
4	Diligenciar herramienta del análisis de Riesgo de seguridad de la Información para la implementación del riesgo.	18/01/2022	30/01/2022
5	Ejecutar Plan de riesgos de seguridad y privacidad de la información.	01/02/2022	30/11/2022
6	Seguimiento a través de auditorías por parte de la oficina asesora de control interno conforme a la guía suministrada por el DAFP.	01/06/2022	30/09/2022

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2022

El presente plan tiene por objetivo comprender e implementar las acciones tendientes a proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.

La definición del marco de seguridad y privacidad de la información y de los sistemas de información en la empresa, define el estado actual del nivel de seguridad y privacidad y las acciones a implementar.

DIAGNÓSTICO DE SEGURIDAD Y PRIVACIDAD

La Empresa Municipal de Acueducto, Alcantarillado y Aseo de Funza EMAAF E.S.P., busca determinar el estado actual del nivel de seguridad y privacidad de la información y de los sistemas de información, basándose en el MSPI Modelo de Seguridad y Privacidad de la Información para GOBIERNO DIGITAL. Para lo cual cuenta con un diagnóstico de seguridad y privacidad e identifica y analiza los

riesgos, definiendo y gestionando las respectivas acciones a nivel de seguridad y privacidad, así como acciones de mitigación del riesgo.

IMPLEMENTACIÓN

La Empresa Municipal de Acueducto, Alcantarillado y Aseo de Funza EMAAF E.S.P., implementa el plan de seguridad y privacidad de la información y de los sistemas de información desarrollando las estrategias de Gestión de riesgos de seguridad y privacidad de la información, buscando proteger los derechos de los usuarios y mejorar los niveles de confianza en los mismos a través de la identificación, valoración, tratamiento y mitigación de los riesgos de los sistemas de información, para lo cual toma como base el MSPI Modelo de Seguridad y Privacidad de la Información para GOBIERNO DIGITAL del cual describe sus directrices en el “Plan de tratamiento de riesgos de seguridad y privacidad de la información vigencia 2021”.

MONITOREO Y MEJORAMIENTO CONTINUO

El plan de seguridad y privacidad de la información, busca desarrollar actividades para la evaluación y mejora de los niveles de seguridad y privacidad de la información y los sistemas de información con los que cuenta la EMAAF E.S.P., realizando las mediciones necesarias para calificar la operación y efectividad de los controles, estableciendo niveles de cumplimiento y de protección de los principios de seguridad y privacidad de la información, para lo cual se toma como base el M.SPI Modelo de Seguridad y Privacidad de la Información para GOBIERNO DIGITAL

La Empresa Municipal de Acueducto, Alcantarillado y Aseo de Funza EMAAF E.S.P. cuenta con actividades para el seguimiento, medición, análisis y evaluación del desempeño de la seguridad y privacidad, con el fin de generar los ajustes o cambios pertinentes y oportunos.

De igual forma se revisa e implementa acciones de mejora continua que garanticen el cumplimiento del plan de seguridad y privacidad de la información.

PLAN DE ACCIÓN PARA LA VIGENCIA

De acuerdo con el autodiagnóstico realizado en la vigencia 2021, se estiman puntos de priorización en el desarrollo de actividades que permitan avanzar en la fase de implementación del MSPI, contempladas y aprobadas previamente en el marco de los comités de Gobierno Digital.

Calle 16 No. 16-04 Funza (Cundinamarca)
P.B.X. 822 14 50 FAX: 822 01 67 CEL. 3118875844
e-mail: info@emaafesp.gov.co
C.P. 250020 www.emaafesp.gov.co

ID	ACTIVIDAD	FECHA INICIO	FECHA FINAL
1.	Política de seguridad de la información	18/01/2022	18/02/2022
2.	Políticas de la organización de la seguridad de la información	19/02/2022	18/03/2022
3.	Políticas de seguridad del personal	16/05/2022	31/05/2022
4.	Políticas de gestión de activos de información	01/02/2022	18/03/2022
5.	Políticas de control de acceso	02/09/2022	16/09/2022
6.	Política de criptografía	01/11/2022	30/11/2022
7.	Políticas de seguridad física y del entorno	19/09/2022	30/09/2022
8.	Políticas de seguridad en las operaciones	01/10/2022	31/10/2022
9.	Políticas de seguridad en las comunicaciones	18/09/2022	30/09/2022
10.	Políticas de adquisición, desarrollo y mantenimiento de sistemas de información	02/08/2022	22/08/2022
11.	Políticas de relación con proveedores, terceras partes y/o contratistas	02/08/2022	22/08/2022
12.	Política de gestión de incidentes de seguridad	01/11/2022	24/11/2022
13.	Políticas de continuidad del negocio	01/06/2022	05/07/2022
14.	Políticas de cumplimiento	01/12/2022	16/12/2022

Original firmado

Andrés Felipe Rincón Damián
Gerente

Revisión	Nombre	Cargo	Firma
Aprobó	Ricardo Lagos Jiménez	Jefe Oficina Asesora de Planeación	
Proyectó	John Edwin Sánchez Sánchez	Profesional Apoyo Seguridad Información	