PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Año 2023

emserfusa E.S.P.	**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El Manual de Políticas de Seguridad y Privacidad de la Información define los lineamientos y políticas que deben ser adoptadas todos los funcionarios, contratistas, proveedores, visitantes y todo personal externo que preste sus servicios o tenga algún intercambio de información con EMSERFUSA E.S.P

Las políticas de seguridad y privacidad descritas en este manual se encuentran enfocadas al cumplimiento de la normatividad legal colombiana vigente y siguiendo las buenas prácticas de seguridad de la información descritas en la norma ISO 27001:2013. A partir de las políticas descritas en este manual se promueve la implantación de controles, procedimientos y lineamientos para salvaguardar los activos de información de EMSERFUSA E.S.P

2. ALCANCE Y APLICABILIDAD

Las políticas y lineamientos descritos en este documento aplican a toda la Empresa de Servicios Públicos de Fusagasugá - EMSERFUSA E.S.P, sus funcionarios, contratistas, terceros y la ciudadanía en general, que en el desempeño de sus funciones y labores compartan, utilicen, recopilen, procesen, intercambien o consulten información de EMSERFUSA E.S.P. Se extiende la aplicabilidad a los entes de control y/o entidades relacionadas que accedan, ya sea interna o externamente a cualquier tipo de información, independientemente de su ubicación.

Las políticas y lineamientos dispuestos en este documento y su implementación son aplicables a toda la información creada, procesada o utilizada por EMSERFUSA E.S.P, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

Con la definición del presente Manual de Políticas de Seguridad y Privacidad de la Información no se contempla el control de incidentes a nivel de la ciudadanía, usuarios externos o entidades externas a EMSERFUSA E.S.P, sin embargo, con los medios disponibles se buscará promover la sensibilización sobre la existencia de la gestión de la

seguridad de la información dentro de la empresa de cara a la ciudadanía y otros actores externos.

3. GLOSARIO

- **Política:** Es una declaración de alto nivel que describe la posición de EMSERFUSA E.S.P sobre un tema específico, y para efectos de este documento, la posición sobre la seguridad y privacidad de la información.
- **Mejor Práctica:** Es un lineamiento específico o plataforma que es aceptada por la industria que proporciona un enfoque más efectivo para una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.
- **Guía:** Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas y buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.
- **Procedimiento:** Los procedimientos, definen específicamente como las políticas, mejores prácticas y guías serán implementadas en una situación dada. Los procedimientos son utilizados para definir los pasos que deben ser seguidos por un área o equipo de trabajo para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del área o la dependencia donde se aplican.
- **ISO 27001:2013:** Estándar internacional para la definición e implementación de un Sistema de Gestión de la Seguridad de la Información.

- **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).
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños 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).
- **Auditoría 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).
- **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**: Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética.
- **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.
- **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).
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- **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:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- **Parte interesada (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectad

4. OBJETIVO GENERAL

Establecer un Manual de Políticas de Seguridad y Privacidad de la Información junto con los mecanismos y controles que permitan asegurar la integridad, disponibilidad y

confidencialidad de los activos de información de la Empresa de Servicios Públicos de Fusagasugá – EMSERFUSA E.S.P

4.1 OBJETIVOS ESPECIFICOS

- Contribuir al incremento de la transparencia en la gestión pública.
- Dar lineamientos para la implementación de la gestión de la seguridad y privacidad de la información.
- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Alinear el Modelo de Seguridad y Privacidad de la Información con el Marco de Referencia de Arquitectura Empresarial de TI.
- Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas en las entidades.
- Contribuir a mejorar los procesos de intercambio de información pública.
- Orientar a las entidades en las mejores prácticas para la construcción de una política de privacidad respetuosa de los datos personales de los titulares.

5. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La gerencia de EMSERFUSA E.S.P entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) y el Sistema de Gestión de Seguridad de la Información (SGSI) buscando fortalecer la confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la empresa.

Para EMSERFUSA E.S.P, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad,

confidencialidad y la disponibilidad de la información, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a todos los funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones sobre seguridad de la información estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la empresa.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y funcionarios.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de EMSERFUSA E.S.P.
- Garantizar la continuidad del negocio frente a incidentes relacionados con seguridad de la información.

A continuación, se establecen los 11 lineamientos que soportan el **MSPI** (Modelo de Seguridad y Privacidad de la Información) y el **SGSI** (Sistema de Gestión de Seguridad de la Información) de EMSERFUSA E.S.P:

1. EMSERFUSA E.S.P ha decidido definir, implementar, operar y mejorar de forma continua un MSPI (Modelo de Seguridad y Privacidad de la Información) y en conjunto el SGSI (Sistema de Gestión de Seguridad de la Información), ambos soportados en lineamientos y criterios alineados con las necesidades del negocio, y con los requerimientos regulatorios que le aplican a su naturaleza.
2. Las responsabilidades, compromisos frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

3. EMSERFUSA E.S.P protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de la información. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
4. EMSERFUSA E.S.P protegerá su información de las amenazas originadas por parte del personal.
5. EMSERFUSA E.S.P protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
6. EMSERFUSA E.S.P controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
7. EMSERFUSA E.S.P implementará control de acceso a la información, sistemas de información, aplicaciones y recursos de red.
8. EMSERFUSA E.S.P garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
9. EMSERFUSA E.S.P garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
10. EMSERFUSA E.S.P garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos de seguridad y debilidades asociadas.
11. EMSERFUSA E.S.P garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la presente política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de EMSERFUSA E.S.P, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

6. SEGUIMIENTO AL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

6.1 Seguimiento general

El seguimiento general se lleva a cabo con el documento Plan de Seguridad y Privacidad de la Información, donde se especifican las actividades que deben ser desarrolladas para la implementación de los controles requeridos de acuerdo con los resultados del análisis de riesgos del Modelo de Seguridad y Privacidad de la Información.

6.2 Plan de seguimiento apoyado en fechas y el tratamiento de los riesgos

Una vez se tiene la claridad de los riesgos de seguridad de la información a los que se encuentra expuesta la Empresa de Servicios Públicos de Fusagasugá - EMSERFUSA E.S.P, dentro de los procesos definidos formalmente, se procede con la evaluación, selección e implementación de los controles necesarios para el tratamiento acorde con la metodología de gestión de seguridad de la información. Este documento presenta la guía para que los responsables de la información, apoyados por la Oficina de Planeación e Informática - OPEI, oficina de Gestión Humana y la Secretaría Administrativa, cumplan con el plan de implementación de los controles para que cada uno de los riesgos identificados en las áreas responsables de los procesos del alcance del análisis de riesgos.

La Empresa de Servicios Públicos de Fusagasugá - EMSERFUSA E.S.P, requiere cumplir con los lineamientos del Modelo de Seguridad y Privacidad de la información (MSPI), aplicando la protección de la confidencialidad, integridad y disponibilidad de la información con base en los riesgos de seguridad de la información identificados; esto por supuesto incluye lo referente al cumplimiento del marco legal y regulatorio relacionado con seguridad de la información en Colombia, tal como lo establece MINTIC.

6.3 Referencia al Plan de Seguridad y Privacidad de la Información en el MSPI

A continuación, se referencian los puntos que exige el MSPI para el Plan de Seguridad y Privacidad de la Información, con la asociación a los correspondientes entregables del proyecto para La Empresa de Servicios Públicos de Fusagasugá – EMSERFUSA E.S.P.

Meta	resultados	MSPI	EMSERFUSA E.S.P – Fusagasugá
Política de seguridad general con Objetivos y alcance del MSPI. **Políticas de seguridad y privacidad de la información**	Capacitaciones por semestre al interior de la entidad acerca de la prevención y acción frente a la perdida de información u ocurrencia de delitos informáticos, buenas prácticas, dar a conocer el Modelo de Seguridad y Privacidad de la Información y su política, recomendaciones y otros emitidas por entidades u organismos de control.	Guía No 2 ISO 27001:2013 Numerales 4, 5, 6	Documentos y otros del Modelo de Seguridad y Privacidad de la Información (MSPI) de la Empresa de Servicios Públicos de Fusagasugá – EMSERFUSA E.S.P OPEI-MA-05 Manual de Políticas de Seguridad de la Información que incluye 11 políticas de seguridad, aprobado el 28 de Abril del 2023 por el Comité de Gestión y Desempeño Recomendaciones, circulares y otros emitidos por MINTIC y entidades de control. Política de Tratamiento de Datos Personales de la Empresa de Servicios Públicos de Fusagasugá – EMSERFUSA E.S.P, con el oficio, acta, resolución, memorando o decreto que aprueba el Manual de Políticas de Seguridad de la Información
Procesos y procedimientos, debidamente definidos	Formatos, procedimientos y otros debidamente definidos, establecidos y	Guía No 3	Oficio, acta, resolución, memorando o decreto que aprueba el Manual de Políticas de

	aprobados por la alta gerencia y calidad.		Seguridad de la Información **Tres formatos:** • Inventario de activos de información de EMSERFUSA E.S.P. • Matriz de riesgos de seguridad de la información. • Declaración de aplicabilidad. **Dos procedimientos:** • OPEI-P-11 Procedimiento de servicios tecnológicos. • OPEI-P-09 Procedimiento de mantenimiento preventivo y correctivo de equipos de computo Diseñar y enviar a aprobación nuevos documentos o actualizar los existentes, según la necesidad.
Inventario de activos de información	Identificación, clasificación y valoración de activos de información, revisado y aprobado por los líderes de cada proceso.	Guía 5	Inventario y Clasificación de Activos de Información Matriz Catalogo de Componentes de la información
Descripción de los de los activos de información que	Documento con la caracterización de los activos de información	Ley de protección de datos personales – Ley 1581 de 2012,	Inventario de Activos de seguridad y privacidad de la información

contengan datos personales	que contengan datos personales.		
Acciones para tratar riesgos y oportunidades de seguridad de la información: identificación, valoración y tratamiento de riesgos.	Documento con el informe de análisis de riesgos, matriz de riesgos, plan de tratamiento de riesgos, revisado y aprobado.	Guía 7 Guía 8 Guía 9	Actualización Plan de Tratamiento de Riesgos de Seguridad de la Información.
Toma de conciencia	Informe y evidencias de actividades que se integran entre el MSPI y el plan anticorrupción con: El resultado de las capacitaciones brindadas a los funcionarios, número de acciones ejecutadas por proceso en temas de seguridad informática como apropiación, actualización de infraestructura tecnológica, física y/o servicios de seguridad y de TI; y número de acciones ejecutadas para prevenir delitos informáticos en las operaciones realizadas en la entidad	Guía 14	Capacitación a los funcionarios para la prevención y acción frente a la perdida de información u ocurrencia de delitos informáticos, buenas prácticas, dar a conocer el Modelo de Seguridad y privacidad de la información y sus políticas. Acciones ejecutadas de seguridad informática como apropiación, actualización de infraestructura tecnológica, física y/o servicios de seguridad y de TI.

Tabla Referencia al MSPI

6.4 Plan de tratamiento

De acuerdo con los resultados del análisis de riesgos se identifican vulnerabilidades que deben ser corregidas para los procesos de la Empresa de Servicios Públicos de Fusagasugá - EMSERFUSA E.S.P, lo que conlleva a un plan de tratamiento base que debe ser aplicado y que se describe en este documento. A continuación, se aborda el plan de tratamiento con base en los dominios de la Norma ISO 27001 base fundamental del Modelo de Seguridad y Privacidad de la Información MSPI.

Las actividades implican la responsabilidad de todos los servidores públicos y los procesos frente a la participación en las capacitaciones y toma de conciencia con relación a las buenas prácticas, recomendaciones y el MSPI; generando una cultura de cambio en la entidad y la apropiación del MSPI.

Basados en el plan de tratamiento de riesgos se proponen responsables y fechas

6.5 Liderazgo y compromiso

N°	ACTIVIDAD	RESPONSABLE	FECHA DE EJECUCIÓN
1	Sensibilización a todos los funcionarios y contratistas frente al cumplimiento obligatorio de las políticas, procedimientos, formatos, manuales, guías y demás que estén definidos en el MSPI	Jefe de cada oficina	semestral
2	Realizar una acción o actividad que permita evidenciar la mejora en la seguridad de la información o informática, como apropiación, actualización de infraestructura tecnológica, física y/o servicios de seguridad y de TI.	Jefe Oficina de Planeación e Informática OPEI	Una vez al año
3	Realizar acciones que permitan prevenir la ocurrencia de delitos informáticos, aplicar las recomendaciones emitidas por los entes de control y vigilancia, así como, las políticas y demás lineamientos de la empresa de servicios públicos de Fusagasugá – EMSERFUSA E.S.P; vincular a las entidades bancarias para validar la infraestructura y servicios que permitan garantizar la seguridad en las operaciones o transacciones que comprometen recursos públicos a través de los portales o plataformas bancarias virtuales como: consultas, pagos y transferencias electrónicas	Jefe división financiera	Trimestralmente
4	Incluir dentro del plan de capacitación, sensibilización y formación semestral a los funcionarios en temas de seguridad de la información, seguridad informática y prevención de delitos informáticos.	Gestión y talento humano	Semestral

6.6 Diagnóstico de seguridad informática

N°	ACTIVIDAD	RESPONSABLE	FECHA DE EJECUCIÓN
1	Analizar la información relacionada con modelo de seguridad y privacidad de la información (MSPI)	Agente de seguridad de la información - P.U Sistemas y Redes – P.U Sistemas y Catastro	Semestral
2	Analizar y Actualizar la Política de Seguridad y Privacidad de la Información	Agente de seguridad de la información - P.U Sistemas y Redes – P.U Sistemas y Catastro	Semestral
3	Revisar y actualizar el Manual de Políticas de Seguridad y Privacidad de la Información	Agente de seguridad de la información - P.U Sistemas y Redes – P.U Sistemas y Catastro	Semestral
4	Publicar la Política de Seguridad y Privacidad de la Información y Manual de Políticas de Seguridad y Privacidad de la Información	Agente de seguridad de la información - P.U Sistemas y Redes – P.U Sistemas y Catastro	Semestral
5	Realizar acciones encaminadas al mejoramiento de la plataforma de seguridad perimetral – Firewall	Oficina de Planeación e Informática	Semestral
6	Realizar técnicas de Hacking Ético	Oficina de Planeación e Informática - Agente de seguridad de la información	Semestral

6.7 Organización para la seguridad de la información

6.7.1 Contacto con las autoridades

Control requerido para dar parte a las autoridades en caso de la ocurrencia de un incidente de seguridad de la información o delitos informáticos, procedimiento que debe ser llevado a cabo por medio de la Oficina de Planeación e Informática -OPEI.

N°	ACTIVIDAD	RESPONSABLE	FECHA DE EJECUCIÓN
1	Reportar a las entidades competentes los eventos o incidentes de seguridad identificados o reportados por los	Agente de seguridad de la información - P.U	Según la necesidad

	funcionarios, de acuerdo al caso a: Centro Cibernético Policial, Col-Sert, Comando Conjunto Cibernético, CSIRT	Sistemas y Redes – P.U Sistemas y Catastro	

7. FUNCIONARIOS PÚBLICOS, CONTRATISTAS Y PARTICULARES CON ACCESO A INFORMACIÓN DE LA EMPRESA DE SERVICIOS PÚBLICOS DE FUSAGASUGÁ – EMSERFUSA E.S.P

- Cumplir con todas las Políticas de Seguridad y Privacidad de la información adoptadas por la Empresa de Servicios Públicos de Fusagasugá – EMSERFUSA E.S.P.
- Actualizarse en los temas propios de Seguridad y Privacidad de la información aplicados en la Empresa de Servicios Públicos de Fusagasugá – EMSERFUSA E.S.P.
- Todos los funcionarios, contratistas y personal externo deben aceptar los acuerdos de confidencialidad definidos por la entidad, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.
- Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de la entidad a personas o entidades externas. Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso contractual, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hará parte integral de cada uno de los contratos

7.1 Cumplimiento

El cumplimiento de las Políticas de Seguridad y Privacidad de la Información es obligatorio. Si los funcionarios de la Empresa de Servicios Públicos de Fusagasugá – EMSERFUSA E.S.P o terceros violan este plan, la entidad, se reserva el derecho de tomar las medidas correspondientes.

7.2 Comunicación

Mediante socialización a todos los funcionarios y contratistas de la Empresa de Servicios Públicos de Fusagasugá – EMSERFUSA E.S.P, se dará a conocer el contenido del documento Manual de Políticas de Seguridad y Privacidad de la Información, así mismo se deberá informar a los funcionarios y contratistas en el momento que se requiera con el propósito de realizar los ajustes y la retroalimentación necesaria para dar cumplimiento efectivo al plan.

Todos los funcionarios y contratistas de la entidad deben conocer la existencia de las políticas y la obligatoriedad de su cumplimiento, la ubicación física del documento estará a cargo de la Oficina de Planeación e Informática - OPEI para que sea consultado en el momento que se requiera, igualmente estarán alojados en la plataforma de la entidad www.kawak.com.co.

7.3 Monitoreo

Se crearán los mecanismos y los indicadores correspondientes a la política de seguridad con el fin de determinar el cumplimiento de las mismas para establecer qué modificaciones o adiciones deben hacerse, este monitoreo debe realizarse como mínimo una vez al año o cuando sea necesario.

8. POLÍTICAS ESPECÍFICAS PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

8.1 Políticas para la Seguridad de la información

Las políticas específicas relacionadas con la seguridad y privacidad de la información deben brindar orientación y apoyo por parte de la gerencia de EMSERFUSA E.S.P, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.

- Se deben definir un conjunto de políticas específicas para la seguridad y privacidad de la información, aprobadas por la gerencia, publicadas y comunicadas a los funcionarios y partes externas pertinentes.
- Las políticas específicas para la seguridad y privacidad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas. Como buena práctica se recomienda realizar dicha revisión como mínimo cada año.
- La Empresa de Servicios Públicos de Fusagasugá – EMSERFUSA E.S.P, define sus políticas de seguridad y privacidad fundamentada en los dominios de controles señalados en la norma NTC/IEC ISO 27001 - NTC/IEC ISO 27002 y que se transcriben a continuación.

8.1.1 POLÍTICA DE CONTROL DE ACCESO A LA INFORMACIÓN

8.1.1.2 Objetivo General de la Política de Control de Acceso a la Información

La Política de Control de Acceso a la información de la Empresa de Servicios Públicos de Fusagasugá – EMSERFUSA E.S.P, provee las pautas para que la información únicamente sea accedida por los funcionarios, contratistas y partes autorizadas con base en las funciones de su rol frente a los procesos formalmente definidos por el Sistema Integrado de Gestión.

Condiciones de las cuentas de usuario

N°	ACTIVIDAD	RESPONSABLE	FECHA DE EJECUCIÓN
1	Verificar, definir y autorizar la creación e inactivación de las cuentas de usuario de red, roles y permisos a los sistemas de información, red, correo electrónico institucional y otros que requieren los servidores públicos para el ejercicio de sus funciones u obligaciones.	Jefe de cada oficina	Semestral
2	Realizar una socialización para revisar los permisos y acceso y/o gestión de cuentas de	Jefe de cada oficina	Semestral

	usuario en lo pertinente a los sistemas de información, aplicativos, plataformas y correos electrónicos institucionales que se encuentren bajo la responsabilidad del área correspondiente, con el fin de actualizar los roles y privilegios e informar a los administradores.		

Acceso a redes y servicios de red

N°	ACTIVIDAD	RESPONSABLE	FECHA DE EJECUCIÓN
1	Creación de formato de Control de acceso al Centro de Computo de la entidad, para llevar a cabo un control y registro de entradas, salidas y actividades	Oficina de Planeación e Informática - P.U Sistemas y Redes- Sistemas y Catastro	Una vez al año
2	Aplicar políticas o directivas de seguridad en el directorio activo o firewall, generando una restricción para que los funcionarios no puedan observar las contraseñas de las redes inalámbricas (WIFI) instaladas en la entidad	Oficina de Planeación e Informática - P.U Sistemas y Redes- Sistemas y Catastro	Una vez al año
3	Contratar un servicio de internet de respaldo con diferente operador y medio de transmisión para mitigar el riesgo de suspensión del servicio de internet sin previo aviso por el operador actual en la empresa de servicios públicos de Fusagasugá – EMSERFUSA E.S.P	ADMINISTRATIVA	Una vez al año
4	Realizar las configuraciones lógicas y/o físicas para mejorar la seguridad de las redes telemáticas y garantizar el servicio.	Oficina de Planeación e Informática - P.U Sistemas y Redes- Sistemas y Catastro	Una vez al año

8.1.2 POLÍTICA DE BLOQUEO DE PUERTOS USB

8.1.2.1 Objetivo General de la Política de Bloqueo de Puertos USB

La política de bloqueo de puertos USB de la Empresa de Servicios Públicos de Fusagasugá – EMSERFUSA E.S.P busca proteger la información que se encuentran dentro de un computador, ya sea de contagio de virus o plagio de esta.

Permisos para el uso de los puertos USB

N°	ACTIVIDAD	RESPONSABLE	FECHA DE EJECUCIÓN
1	Generar formato de solicitud de activación de puertos USB, para una actividad determinada	Oficina de Planeación e Informática - P.U Sistemas y Redes-Sistemas y Catastro	Cuando se requiera

Bloqueo de puertos USB

N°	ACTIVIDAD	RESPONSABLE	FECHA DE EJECUCIÓN
1	Realizar la configuración del directorio activo – firewall y antivirus de la entidad para bloquear los puertos USB de todos los equipos de la entidad (Formato 140-F47 Solicitud de Servicios tecnológicos - V2)	Oficina de Planeación e Informática - P.U Sistemas y Redes-Sistemas y Catastro	Trimestralmente
2	Instalación de un software de protección Antivirus, para proteger todos los dispositivos de la entidad	Oficina de Planeación e Informática - P.U Sistemas y Redes-Sistemas y Catastro	Trimestralmente

8.1.3 POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA

8.1.3.1 Objetivo General de la Política de Escritorio y Pantalla Limpia

La Política de Escritorio y Pantalla Limpia de la Empresa de Servicios Públicos de Fusagasugá – EMSERFUSA E.S.P busca asegurar que sus funcionarios y contratistas adopten mejores prácticas de seguridad de la información en cuanto al uso de los espacios de trabajo y las herramientas y provistas por la Entidad.

Escritorio limpio

N°	ACTIVIDAD	RESPONSABLE	FECHA DE EJECUCIÓN
1	Almacenamiento de toda la información impresa o dispositivos de almacenamiento, en sitios indicados para eso, como estanterías o cajones de escritorio.	Jefe de cada oficina	Semestral

2	Ordenamiento de los sitios de trabajo, que no quede información expuesta de ningún tipo sobre los escritorios de cada funcionario	Jefe de cada oficina	Semestral

Cierre de sección y pantalla limpia

N°	ACTIVIDAD	RESPONSABLE	FECHA DE EJECUCIÓN
1	Configuración del directorio activo, para bloqueo de sesión después de inactividad en un computador	Oficina de Planeación e Informática - P.U Sistemas y Redes- Sistemas y Catastro	Trimestralmente
2	Ocultar o no guardar información en el escritorio del computador, para protección de la misma.	Todos los funcionarios de la entidad	Trimestralmente

8.1.4 POLÍTICA DE USO ACEPTABLE DE LOS ACTIVOS

8.1.4.1 Objetivo General de la Política de Uso Aceptable de los Activos

La Política de Uso Aceptable de los Activos de Información de la Empresa de Servicios Públicos de Fusagasugá – EMSERFUSA E.S.P establece las especificaciones de seguridad para el uso aceptable de los activos de información, la cual garantiza que todos los empleados de la entidad apliquen practicas aceptables para el uso de la misma, garantizando que todos los activos de información estén clasificados, protegidos y gestionados.

N°	ACTIVIDAD	RESPONSABLE	FECHA DE EJECUCIÓN
1	Actualizar el inventario de activos de información como un documento de referencia permanente, teniendo claro los roles de responsable, criticidad de la información, principios de la seguridad de la información y custodio, que refleje la realidad de todos los procesos que ejecutan como parte de la misionalidad y funciones, aplicar los lineamientos de la Ley 1712 de 2014 sobre Transparencia y Acceso a la Información Pública Nacional, identificando los activos de información que contienen datos personales y otros que establece la normatividad concordante.	Jefe división administrativa	1 Vez al año

2	Verificar, cotejar y actualizar el inventario de los activos tecnológicos correspondientes a cada proceso, incluir las características mínimas de cada activo.	Jefe división administrativa	1 Vez al año
3	Diseñar el mecanismo y/o procedimiento para indicar a los dueños de proceso como se deben salvaguardar las cuentas de usuario tipo Administrador y la contraseña de las plataformas en la nube, sistemas de información, aplicaciones servidores, dominós, redes telemáticas, entre otros.	Oficina de Planeación e Informática - P.U Sistemas y Redes- Sistemas y Catastro	1 Vez al año
4	Manejo de un sistema de copias de seguridad para salvaguardar la información de todos los funcionarios de la entidad	Oficina de Planeación e Informática - P.U Sistemas y Redes- Sistemas y Catastro	Trimestralmente
5	Configuración del directorio activo, para eliminar permisos de descarga, instalación y eliminación de software en los equipos de la entidad	Oficina de Planeación e Informática - P.U Sistemas y Redes- Sistemas y Catastro	Trimestralmente
6	Creación de un formato para el control de acceso al data center de la entidad para manejar un control de registro de ingreso de todas las personas que hacen uso del mismo.	Oficina de Planeación e Informática - P.U Sistemas y Redes- Sistemas y Catastro	Trimestralmente
7	Configuración del firewall de la entidad, para bloquear sitios de internet, que no son de interés productico en los funcionarios de la entidad	Oficina de Planeación e Informática - P.U Sistemas y Redes- Sistemas y Catastro	Trimestralmente
8	Creación de un sistema de comunicación institucional, correo electrónico para todos los funcionarios de la entidad, con un sistema de seguridad que requiera una contraseña segura y robusta para su apertura y funcionamiento.	Oficina de Planeación e Informática - P.U Sistemas y Redes- Sistemas y Catastro	Cada vez que se requiera

8.1.5 POLÍTICA DE GENERACIÓN DE COPIAS DE SEGURIDAD

8.1.5.1 Objetivo General de la Política Generación de Copias de Seguridad

Proporcionar medios de respaldo adecuados para asegurar que toda la información de la Empresa de Servicios Públicos de Fusagasugá – EMSERFUSA E.S.P es esencial, así como lo es el software, se pueda recuperar después de una falla, garantizando que la información

y la infraestructura de software crítica de la entidad, sean respaldadas y puedan ser restauradas en caso de una falla o desastre

N°	ACTIVIDAD	RESPONSABLE	FECHA DE EJECUCIÓN
1	A la hora de la firma del contrato, firmar los siguientes documentos Anexo 01 Acta de Aceptación de Políticas de Seguridad y Compromisitos de Confidencialidad, Anexo 02 Acta de Aceptación de Políticas Para uso de Recursos Informáticos, Manual de Uso de los Servicios y Recursos Informáticos, aplicando los lineamientos de Seguridad de la entidad y demás normatividad aplicable, teniendo en cuenta que la responsabilidad penal es individual	Todos los funcionarios y contratistas	1 vez al año
2	Realizar copias de seguridad de la información de cada funcionario, en el espacio indicado por la OPEI, aclarando que la información guardada es netamente laboral	Todos los funcionarios y contratistas	Semestralmente
3	Realizar copias de seguridad de la información de servidores de información, aplicaciones web y de red de la entidad	Oficina de Planeación e Informática - P.U Sistemas y Redes-Sistemas y Catastro	Trimestralmente
4	Recibir y custodiar las copias de seguridad de la información que entregan los funcionarios y contratistas	Oficina de Planeación e Informática - P.U Sistemas y Redes-Sistemas y Catastro	Cuando se requiera

Obligatoriedad del respaldo

Es responsabilidad de cada propietario de la información realizar continuamente la copia de respaldo, ya que en el escenario de un incidente ocasionado por la falla en el equipo de cómputo o de en una copia de seguridad, la responsabilidad es del propietario de dicha información más no de la Oficina de Planeación e Informática - OPEI.

8.1.6 POLÍTICA PARA LA SEGURIDAD FÍSICA Y DEL ENTORNO

8.1.6.1 Objetivo General de la Política de Seguridad Física y del Entorno

Prevenir el acceso físico no autorizado a todas las áreas de la entidad, para evitar el robo, daño o perdida de los activos de información en la Empresa de Servicios Públicos de Fusagasugá – EMSERFUSA E.S.P, teniendo en cuenta que toda la información sensible que se maneja dentro de la compañía debe estar ubicada en una zona segura dentro de un perímetro de seguridad, así de esta manera se pueden evitar las interrupciones a las actividades diarias de todos los funcionarios, contratistas y terceros.

N°	ACTIVIDAD	RESPONSABLE	FECHA DE EJECUCIÓN
1	Supervisión de las zonas seguras por parte de los funcionarios que autorizaron los respectivos accesos a personal ajeno a la entidad	Todos los funcionarios y contratistas	Cuando se requiera
2	Solicitar el porte del carnet a los funcionarios de planta a la hora de ingreso en la entidad para identificar quienes son de planta y quienes contratistas.	Oficina de recursos humanos – Gestión Humana	Cuando se requiera
3	Brindar sistemas de seguridad en zonas donde se manejen activos críticos como los data center de la entidad	Oficina de Planeación e Informática	Trimestralmente
4	Manejar sistemas de protección, para salvaguardar la información de todos los sistemas de la entidad y la información de los funcionarios y contratistas.	Oficina de Planeación e Informática	Trimestralmente
5	Sistemas de protección en el Data center de la entidad como sistema de acceso, puerta de seguridad, barra de apertura entre otros	División de administrativa - Oficina de Planeación e Informática	1 vez al año
6	Revisión en la zona de carga por parte de la compañía de vigilancia de todos los elementos que ingresan, para evidenciar que no ingresan elementos peligrosos que puedan afectar la integridad de los funcionarios y los activos de información de la entidad	División de administrativa	Cuando se requiera
7	Inventario de equipos de cómputo actualizados, marcados con placas de seguridad, para evidenciar cuantos equipos	División de administrativa	Trimestralmente

	tiene la entidad, en qué lugar se encuentra y quien es el responsable del mismo.		
8	Se deben tener extintores de incendios debidamente probados, y con capacidad de detener fuego generado por equipo eléctrico, papel o químicos especiales	División de administrativa	1 vez al año
9	Instalación del sistema de cableado estructurado, bajo la norma EIA/TIA 568-A	División de administrativa	1 vez al año
10	Elaboración de un plan de mantenimiento preventivo/correctivo de los equipos de cómputo de la entidad	Oficina de Planeación e Informática	Semestralmente

8.1.7 POLÍTICA DE DISPOSITIVOS MÓVILES

8.1.7.1 Objetivo General de la Política de Dispositivos Móviles

Establecer las condiciones para el manejo de los dispositivos móviles institucionales o personales que acceden y manejan información de la Empresa de servicios públicos de Fusagasugá – EMSERFUSA E.S.P y velar por el uso responsable de estos por parte del personal, evitando que estos dispositivos sean causales de infección o distribución de código malicioso.

N°	ACTIVIDAD	RESPONSABLE	FECHA DE EJECUCIÓN
1	Toda compra de quipos tecnológicos debe ser analizada y revisada por la OPEI	Oficina de Jurídica - Oficina de Planeación e Informática	1 vez al año
2	Configuraciones de seguridad a todos los equipos de la entidad, en software y permisos administrativos	Oficina de Planeación e Informática	Trimestralmente
3	Inventario de equipos de cómputo actualizados, marcados con placas de seguridad, para evidenciar cuantos equipos tiene la entidad, en que ligar se encuentra y quien es el responsable del mismo.	División de administrativa	Trimestralmente
4	Revisión periódica de los equipos tecnológicos de la entidad, para evidenciar que no se encuentre software no licenciado y autorizado instalado en los equipos	Oficina de Planeación e Informática - P.U Sistemas y Redes- Sistemas y Catastro	Trimestralmente

5	Instalación de un software de protección Antivirus, para proteger todos los dispositivos de la entidad	Oficina de Planeación e Informática - P.U Sistemas y Redes-Sistemas y Catastro	Trimestralmente
6	Configuración de bloqueo de pantalla automático, para prevenir fugas o perdida de la información cuando el equipo este solo	Oficina de Planeación e Informática - P.U Sistemas y Redes-Sistemas y Catastro	Trimestralmente
7	Configuración de un software de seguridad para borrado seguro de dispositivos, en caso de pérdida o robo	Oficina de Planeación e Informática - P.U Sistemas y Redes-Sistemas y Catastro	1 Vez al año
8	Informar a la OPEI los incidentes o eventos de malware que afectan los equipos tecnológicos, indicando desde donde se generó y cuando se presentó el incidente de seguridad	Todos los funcionarios y contratistas	Cuando se requiera
9	Utilización de software libre o licenciado en todos los equipos de la entidad	Oficina de Planeación e Informática - P.U Sistemas y Redes-Sistemas y Catastro	Trimestralmente
10	Configuración de redes VPN, aplicaciones de acceso remoto solicitas mediante el formato correspondiente	Oficina de Planeación e Informática - P.U Sistemas y Redes-Sistemas y Catastro	Cuando se requiera
11	Bloqueo de sitios web para uso personal en los dispositivos móviles institucionales. Igualmente, sitios o aplicaciones web de dudosa procedencia, con contenido inapropiado o confuso	Oficina de Planeación e Informática - P.U Sistemas y Redes-Sistemas y Catastro	Cuando se requiera
12	Firma de formatos para la Aceptación de las Políticas de Seguridad y Compromisos de Confidencialidad de la Información y la Aceptación de las Políticas Para Uso de los Recursos Informáticos	Todos los funcionarios y contratistas	1 Vez al año
13	Eliminación de las aplicaciones que sean consideradas maliciosas o inapropiadas.	Oficina de Planeación e Informática - P.U Sistemas y Redes-Sistemas y Catastro	Cuando se requiera

8.1.8 POLÍTICA DE TRANSFERENCIA DE LA INFORMACIÓN

8.1.8.1 Objetivo General de la Política de Trasferencia de la Información

Mantener y asegurar la seguridad de la información y el software cuando sean intercambiados o transferidos dentro y fuera de la entidad mediante el uso de todo tipo de

instalaciones de comunicación, como lo son correo electrónico, VPN, SFTP, dispositivos móviles, equipos computacionales, servicios web, plataformas digitales entre otros.

N°	ACTIVIDAD	RESPONSABLE	FECHA DE EJECUCIÓN
1	Manejo del correo institucional dentro de los procesos contractuales en la entidad	Todos los funcionarios y contratistas	1 Vez al año
2	Correcto uso del Drive del correo para la transferencia de la información	Todos los funcionarios y contratistas	1 Vez al año
3	Bloque de puertos USB para protección de los equipos y de la información	Oficina de Planeación e Informática - P.U Sistemas y Redes-Sistemas y Catastro	Trimestralmente

8.1.9 POLÍTICA DE INSTALACIÓN DE SOFTWARE

8.1.9.1 Objetivo General de la Política de Instalación de Software

Establecer las restricciones para la instalación de programas en los computadores de las oficinas, debido a la probabilidad de que los programas sean descargados desde páginas dudosas y realicen acciones como ocupar una puerta trasera o backdoor mediante el cual realizan sus acciones. Se debe prestar especial atención a la instalación de los programas en los computadores ya que algunos de estos pueden representar una amenaza para la empresa a través del computador en el cual se encuentra alojado.

N°	ACTIVIDAD	RESPONSABLE	FECHA DE EJECUCIÓN
1	Instalación de software licenciado	Oficina de Planeación e Informática - P.U Sistemas y Redes-Sistemas y Catastro	Semestralmente
2	Creación de un repositorio para el almacenamiento de todas las licencias de software que maneja la entidad	Oficina de Planeación e Informática - P.U Sistemas y Redes-Sistemas y Catastro	Semestralmente
3	Inventario de equipos y revisión de programas de cómputo instalados en cada equipo para garantizar que ningún funcionario tenga instalado un programa de cómputo sin su respectiva licencia.	Oficina de Planeación e Informática - P.U Sistemas y Redes-Sistemas y Catastro	Trimestralmente
4	Plan de actualización de software para todos los equipos de la entidad	Oficina de Planeación e Informática - P.U	Semestralmente

		Sistemas y Redes- Sistemas y Catastro	

8.1.10 POLÍTICA DE MANEJO DE REDES Y MEDIOS SOCIALES

8.1.10.1 Objetivo General de la Política de Manejo de Redes y Medios Sociales

Establecer las restricciones y/o permisos para el uso de las redes sociales en la empresa de servicios públicos de Fusagasugá – EMSERFUSA E.S.P, durante la jornada laboral, dejando claro que no se puede utilizar la red de internet de la compañía para dicho uso.

N°	ACTIVIDAD	RESPONSABLE	FECHA DE EJECUCIÓN
1	Bloqueo de páginas web de utilización de redes sociales	Oficina de Planeación e Informática - P.U Sistemas y Redes-Sistemas y Catastro	Trimestralmente
2	Firma del acuerdo de confidencialidad al inicio del contrato laboral	Todos los funcionarios y contratistas	1 Vez al año
3	Configuración de los puntos de acceso a Internet inalámbrico (Access Point) con contraseñas robustas para la no saturación del canal de internet.	Oficina de Planeación e Informática - P.U Sistemas y Redes-Sistemas y Catastro	Trimestralmente
4	Configuración de acceso a ciertas páginas de Internet por medio de un oficio generado por el jede de cada dependencia para temas de capacitación o reuniones de carácter laboral.	Jefes de área - Oficina de Planeación e Informática - P.U Sistemas y Redes-Sistemas y Catastro	Cuando se requiera

8.1.11 POLÍTICA DE SEGURIDAD DE PROVEEDORES

8.1.11.1 Objetivo General de la Política de Seguridad de Proveedores

Establecer mecanismos de control en las relaciones de la Empresa de Servicios Públicos de Fusagasugá – EMSERFUSA E.S.P, con sus proveedores de servicios, con el objetivo de asegurar que la información a la que tengan acceso y los servicios que sean provistos por ellos, cumplan con las políticas y procedimientos de seguridad de la información establecidos por la entidad.

N°	ACTIVIDAD	RESPONSABLE	FECHA DE EJECUCIÓN
1	Firmar acuerdo de confidencialidad, ya que van a manejar y observar información sensible de la entidad	Oficina de jurídica	Cuando se requiera
2	Actas de auditoria para evidenciar el cumplimiento de la ejecución del contratos	Oficina de jurídica	Cuando se requiera
3	Base de datos actualizada con la información de los proveedores que brindan un servicio para la empresa EMSERFUSA E.S.P	Jefes de cada oficina - Oficina de Planeación e Informática - P.U Sistemas y Redes- Sistemas y Catastro	Trimestralmente

9. CONTROL DE VERSIONES

CONTROL DE VERSIONES			
FECHA	**VERSIÓN**	**DESCRIPCIÓN DE ACTIVIDADES**	**APROBADO**
XX/XX/XXXX	1	Creación del documento con el Plan de Seguridad y Privacidad de la Información, para que sea revisado y aprobado por la alta gerencia de la Empresa de Servicios Públicos de Fusagasugá – EMSERFUSA E.S.P	Comité Institucional de Gestión y Desempeño