emserfusa E.S.P.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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.

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.

2. ALCANCE Y APLICABILIDAD

Las políticas y lineamientos descritos en este documento aplican a toda la Empresa de Servicios Públicos de Fusagasugá - EMSERFUSA, 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. 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, 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, 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 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.

4. OBJETIVO

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

5. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La gerencia de EMSERFUSA, 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, 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.
- 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:

1. EMSERFUSA 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 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 protegerá su información de las amenazas originadas por parte del personal.
5. EMSERFUSA protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
6. EMSERFUSA controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
7. EMSERFUSA implementará control de acceso a la información, sistemas de información, aplicaciones y recursos de red.
8. EMSERFUSA garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

9. EMSERFUSA 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 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 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, 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. POLÍTICAS ESPECÍFICAS PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

6.1. Políticas para 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, 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.

6.2. Políticas para la Organización de la seguridad de la información

Organización interna: Es necesario que EMSERFUSA establezca los lineamientos para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.

- EMSERFUSA debe definir y asignar todas las responsabilidades de la seguridad de la información.
- Los deberes y áreas de responsabilidad que presenten conflicto de interés se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de información de la empresa.
- Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.

- La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.

Dispositivos móviles y teletrabajo: Entendiendo la regla de negocio de llevar a cabo el trabajo de manera presencial, frente a cualquier situación de riesgo que amenace la ejecución de las actividades de manera presencial y se deba recurrir a la opción de teletrabajo, EMSERFUSA debe garantizar la seguridad del teletrabajo, además de garantizar el uso correcto de los dispositivos móviles en cualquier escenario de trabajo.

- Se deben implementar medidas y lineamientos de seguridad y privacidad para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realizan labores en modalidad de teletrabajo.
- Se deben identificar y gestionar los riesgos introducidos por el uso de dispositivos móviles en cualquier escenario de trabajo.

6.3. Políticas para la Seguridad de los recursos humanos

Antes de asumir el empleo: EMSERFUSA debe asegurar que los funcionarios y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran, incluyendo las responsabilidades con respecto a la seguridad de la información.

- Los acuerdos contractuales con los funcionarios y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad y privacidad de la información.

Durante la ejecución del empleo: EMSERFUSA debe asegurar que los funcionarios y contratistas tomen conciencia de sus responsabilidades frente a la seguridad y privacidad de la información y las cumplan durante el desempeño de sus labores.

- La Oficina Jurídica de EMSERFUSA debe exigir a todos los funcionarios y contratistas la aplicación de la seguridad y privacidad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
- Todos los funcionarios de EMSERFUSA, y en donde sea pertinente, los contratistas, deberán recibir la educación y formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
- EMSERFUSA debe contar con un proceso disciplinario formal el cual debe ser comunicado, para emprender acciones contra funcionarios, contratistas, proveedores y partes externas que hayan cometido una violación a la seguridad y privacidad de la información.

Terminación o cambio de empleo: EMSERFUSA debe proteger sus intereses como parte del proceso de cambio o terminación del contrato de los funcionarios, contratistas, proveedores y partes externas.

- Las responsabilidades y deberes de seguridad y privacidad de la información que permanecen vigentes después de la terminación o cambio de un contrato se deben definir

y comunicar al funcionario, contratista, proveedor y partes externas, y se deben hacer cumplir. Se recomienda que la aceptación se dé desde antes del inicio del empleo.

6.4. Políticas para la Gestión de activos

Responsabilidad por los activos: EMSERFUSA debe identificar los activos organizacionales y activos de información y definir las responsabilidades de protección apropiadas para asegurar su uso y gestión adecuados.

- Se deben identificar los activos de información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
- Los activos mantenidos en el inventario deben tener un propietario asignado para asignar las responsabilidades sobre la protección, gestión y buen uso.
- Se deben identificar, documentar e implementar reglas para el uso aceptable de la información, los activos de información e instalaciones de procesamiento de información.
- Todos los funcionarios, contratistas, proveedores, y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

Clasificación de la información: EMSERFUSA debe asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia y relevancia para la empresa.

- EMSERFUSA debe clasificar la información y activos de información en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
- Se debe desarrollar e implementar un procedimiento para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la empresa.
- Se debe desarrollar e implementar un procedimiento para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la empresa.
- Se debe implementar un procedimiento para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la empresa.
- Se debe disponer en forma segura de los medios cuando ya no sean requeridos, utilizando procedimientos formales.
- Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.

6.5. Políticas para el Control de acceso

Requisitos del negocio para control de acceso: En EMSERFUSA se debe limitar el acceso a información y a instalaciones de procesamiento de información.

- Se debe establecer, documentar y revisar los lineamientos de control de acceso con base en los requisitos del negocio y de seguridad de la información.
- Solo se debe permitir el acceso a la red y a los servicios de red para los usuarios (internos, externos) que hayan sido autorizados específicamente.

Gestión de acceso de usuarios: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.

- Se debe implementar un procedimiento de gestión de accesos para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
- Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado, por medio de un procedimiento de gestión de accesos
- Los propietarios de los sistemas y servicios deben revisar los derechos de acceso de los usuarios, a intervalos regulares, preferiblemente cada año.
- Los derechos de acceso de todos los funcionarios y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios a la contratación.

Responsabilidades de los usuarios: EMSERFUSA debe hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.

- Se debe exigir a los usuarios que cumplan las prácticas y lineamientos de la empresa para mantener confidencial cualquier información de autenticación (tales como credenciales de acceso, etc).

Control de acceso a sistemas y aplicaciones: En EMSERFUSA se debe evitar el acceso no autorizado a sistemas y aplicaciones.

- El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con los lineamientos y procedimiento de gestión de acceso, que asegure asignación de credenciales para el ingreso seguro. Como mínimo se debe considerar: Control de acceso basado en roles, niveles de acceso, permisos para leer, escribir, eliminar y actualizar información.
- Garantizar que las credenciales (usuario y contraseña) sean de calidad, que cumplan con el nivel requerido y se apliquen de manera consistente para garantizar niveles óptimos de seguridad y protección.

6.6. Políticas para la Seguridad física y del entorno

Áreas seguras: Se debe prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la empresa.

- Se debe asegurar que solamente se permite el acceso a personal autorizado mediante controles de entrada apropiados para las instalaciones de la empresa, que incluya la asignación de credenciales temporales y registro en un sistema de información.
- Se deben establecer controles de ingreso y permanencia en instalaciones y centros de datos. El centro de datos debe contar preferiblemente con control de acceso biométrico para evitar ingreso de personal no autorizado.

- Se debe restringir el ingreso y uso de equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, a menos que se cuente con autorización para ello.
- Las áreas con acceso restringido deben estar claramente demarcadas para evitar ingresos no autorizados.

Equipos: Se debe prevenir la pérdida, daño, robo o compromiso de activos de información, y la interrupción de las operaciones de la empresa.

- Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, asimismo se debe evitar comer, beber y fumar cerca del equipo para evitar daños o evitar que los funcionarios estén en contacto con los equipos si no están trabajando en ellos.
- En el centro de datos e instalaciones de tecnología el cableado de potencia y de telecomunicaciones deben estar separados para evitar interferencias, asimismo, el cableado alrededor del centro de datos debe estar aislado de forma segura para evitar la conexión de dispositivos no autorizados.
- Se deben seguir las recomendaciones del fabricante y realizar mantenimiento a los equipos para asegurar su disponibilidad e integridad continuas, esto incluye que solo el personal autorizado debe realizar dicho mantenimiento y se debe llevar registro del mantenimiento. Cuando sea necesario, la información sensible debe mantenerse a salvo antes de realizar el mantenimiento a un equipo.
- Los equipos, información o software no se deben retirar de su sitio sin autorización previa. En caso de requerirse el retiro temporal se debe identificar claramente al personal autorizado para realizar el retiro, y llevar registro de los equipos, información o software retirados.
- Se deben mantener el escritorio limpio de documentos y medios de almacenamiento removibles, y mantener la pantalla limpia en los equipos; además de bloquear pantalla y sesiones de aplicaciones cuando no estén en uso.

6.7. Políticas para la Seguridad de las operaciones

Procedimientos operacionales y responsabilidades: Se deben asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

- El procedimiento para la operación, uso y responsabilidad de los equipos debe estar documentado y ser socializado con todos los usuarios que tengan equipos a su disposición.
- Para asegurar el desempeño requerido de la infraestructura, sistemas de información y redes de datos, se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones sobre la capacidad futura. Se recomienda que se haga seguimiento anual.

Protección contra códigos maliciosos: Debe asegurarse que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

- Se deben implementar controles y/o herramientas para la detección, prevención y recuperación, incluyendo la toma de conciencia y socialización de las responsabilidades de los usuarios para la protección contra códigos maliciosos.
- Se debe restringir la conexión de medios extraíbles u otros dispositivos no autorizados para evitar la introducción de códigos maliciosos o material riesgoso.

Copias de respaldo: Se debe asegurar la protección contra la pérdida de datos.

- Se deben hacer copias de respaldo de la información de los usuarios, y ponerlas a prueba regularmente de acuerdo con las necesidades de recuperación de cada tipo de información.
- La ubicación de las copias de seguridad debe ser diferente a la ubicación original de la información para aumentar la seguridad ante posibles riesgos.
- Se debe mantener un registro de las copias de seguridad realizadas para asegurar que la información salvada se mantiene vigente.

Registro y seguimiento: Se debe llevar registro de los eventos sobre los sistemas de información y redes de datos.

- Se debe contar con una herramienta / sistema / procedimiento de monitoreo de sistemas de información y redes de datos que permita generar, conservar y revisar regularmente los registros sobre las actividades de los usuarios y administradores, excepciones, fallas y eventos de seguridad de la información. Se recomienda la revisión de registros cada dos meses para analizar tendencias, detectar potenciales actividades fraudulentas, o detectar el origen de fallos de funcionamiento.

Gestión de vulnerabilidades técnicas: EMSERFUSA debe prevenir la explotación de las vulnerabilidades técnicas que afecten la seguridad y privacidad de la información.

- Se deben identificar oportunamente las vulnerabilidades técnicas de los sistemas de información y redes de datos; evaluar la exposición de la empresa a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado. Se recomienda que la identificación de vulnerabilidades técnicas se realice cada año.
- Solo los funcionarios autorizados deben realizar instalación de software y configuraciones en los equipos de los usuarios. Cualquier instalación de software y/o configuración no autorizada deberá tramitarse como un proceso disciplinario por la Oficina de Control Disciplinario y demás que se consideren apropiadas.

Consideraciones sobre auditorías de sistemas de información: Se deben realizar auditorías a los sistemas de información para asegurar que son adecuados al uso y propósito.

- Se deben establecer actividades de auditoría previamente planificadas para la verificación de los sistemas de información. Debe incluir la revisión de: la correcta asignación de privilegios para los usuarios, estabilidad y confiabilidad de la infraestructura que soporta los sistemas de información, suficiente capacidad de los sistemas de

información e infraestructura que los soporta (memoria, procesamiento, almacenamiento, ancho de banda, etc.), oportunidades de mejora, desempeño, disponibilidad, mantenimiento, monitoreo.

6.8. Políticas para la Seguridad de las comunicaciones

Seguridad de las redes: Se deben gestionar las redes de datos de la empresa.

- Se deben aplicar controles para gestionar la seguridad de las redes de datos, tales como el inventario de los elementos físicos de red, monitoreo de las redes de datos, y control de los privilegios de acceso a la red para establecer medidas correctivas.
- Se deben establecer y monitorear Acuerdos de Nivel de Servicio para los servicios de red (aunque sean subcontratados con un proveedor externo), con el fin de monitorear la disponibilidad de la red y evaluar los riesgos a los que estamos expuestos con dichos servicios ya que de ellos depende la operatividad de los sistemas de información.

Intercambio de información: Se debe mantener la seguridad de la información transferida dentro de la empresa y la información intercambiada con cualquier Entidad externa (contratista, proveedor, etc.)

- Se debe contar con un procedimiento que permita proteger la transferencia / entrega / intercambio de información considerando los requisitos legales que sean aplicables (p.e. Ley de tratamiento de datos o acuerdos de confidencialidad).
- Todos los funcionarios deben acceder a su correo electrónico corporativo desde las redes de datos de EMSERFUSA, en caso que algún usuario requiera acceso externo o desde redes públicas externas, debe ser notificado a la OPEI para dar el tratamiento necesario.
- Se deben firmar los acuerdos de confidencialidad y de deber de secreto antes de iniciar una transferencia de información y/o ejecución de labores. Esto es aplicable para todos los funcionarios de la empresa, contratistas, practicantes, proveedores, y cualquier ente externo.

6.9. Políticas para la Adquisición, desarrollo y mantenimiento de sistemas

Requisitos de seguridad de los sistemas de información: Se debe asegurar que la seguridad de la información es parte integral al adquirir o contratar sistemas de información.

- Desde el Manual de contratación se deben considerar requisitos de seguridad al adquirir o contratar sistemas de información, tales como: criterios de evaluación de riesgos, períodos de prueba de producto, configuraciones adicionales requeridas, homologación y aceptación de producto.
- Se debe contar con certificados de seguridad en los sistemas de información, aplicaciones y/o pasarelas de pago que operen o sean accedidos desde redes públicas externas por los usuarios de la empresa, y que manejen información sensible como datos personales o financieros.

Seguridad en los procesos de desarrollo y soporte: EMSERFUSA debe asegurar que la seguridad de la información sea implementada por los proveedores o contratistas externos que suministran sistemas de información, aplicaciones o servicios de tecnología.

- Se debe asegurar que el proveedor o contratista externo cuenta con una política y/o procedimiento de seguridad de la información en el desarrollo, mantenimiento y soporte de software y sistemas.
- Se debe asegurar que el proveedor o contratista externo cuenta con un procedimiento de gestión de cambios a los sistemas de información, aplicaciones o servicios de tecnología, que incluya plazos de respuesta y escalamientos si aplican.
- Cuando el proveedor o contratista externo aplique cambios a sistemas de información, aplicaciones o servicios de tecnología, se debe realizar pruebas para garantizar que los cambios no afecten la operación de EMSERFUSA. Estas pruebas deben ser planeadas y coordinadas previamente con la OPEI y áreas/departamentos que se vean impactados por el cambio.
- La OPEI en conjunto con la Oficina Jurídica deben designar un funcionario, equipo, área o departamento que realice seguimiento a la actividad de desarrollo, soporte, operación, mantenimiento, actualización de sistemas de información, aplicaciones o servicios de tecnología que sean contratados externamente.
- Antes de implementar actualizaciones o nuevos sistemas de información, aplicaciones o servicios de tecnología, en conjunto con el proveedor o contratista se debe establecer un cronograma de pruebas para la aceptación y de esta manera evitar fallos en la operación.

6.10. Políticas para la Relación con los proveedores

Seguridad de la información en las relaciones con los proveedores: Se debe asegurar la protección de los activos de información que sean accesibles por los proveedores o contratistas externos.

- En los contratos con proveedores o contratistas externos se deben establecer las condiciones y cláusulas de confidencialidad para el manejo adecuado de la información de EMSERFUSA de acuerdo con los requisitos de seguridad definidos en el presente Manual de políticas.
- En caso que el proveedor o contratista externo incumpla con las condiciones y cláusulas de confidencialidad descritas anteriormente, se debe iniciar un proceso legal desde la Oficina Jurídica, por lo que el funcionario, equipo, área o departamento que identifique el incumplimiento debe notificarlo inmediatamente a la OPEI y a la Oficina Jurídica.
- En caso que el proveedor o contratista externo identifique algún riesgo al incumplimiento en las condiciones y cláusulas de confidencialidad en su cadena de suministro debe notificarlo inmediatamente a la OPEI y a la Oficina Jurídica para iniciar el proceso legal correspondiente.

Gestión de la prestación de servicios con los proveedores: EMSERFUSA debe verificar que el proveedor o contratista externo cumple y mantiene el nivel acordado de seguridad de la información y de prestación del servicio de acuerdo a los compromisos contractuales.

- Desde la Oficina Jurídica y en conjunto con el funcionario, equipo, área o departamento que mantenga relación con el proveedor o contratista externo, se debe establecer una revisión frecuente a los contratos, condiciones y cláusulas pactadas, incluyendo la solicitud de informes mensuales al proveedor o contratista externo sobre el nivel de servicio prestado.

6.11. Políticas para la Gestión de incidentes de seguridad de la información

Gestión de incidentes y mejoras en la seguridad de la información: Se debe realizar una gestión adecuada de los incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y vulnerabilidades.

- Se debe contar con un procedimiento de seguridad que defina los roles y responsabilidades, y las actividades detalladas para la gestión de los incidentes de seguridad de la información que incluya reporte de eventos, análisis y diagnóstico, mecanismos de respuesta a incidentes, y gestión del conocimiento relacionado con los incidentes de seguridad de la información.
- Todos los funcionarios, contratistas, practicantes de EMSERFUSA que usan los servicios y sistemas de información de la empresa, deben informar cualquier debilidad o situación sospechosa que pueda afectar los sistemas o servicios de EMSERFUSA.
- Anualmente se debe realizar un análisis de vulnerabilidades técnicas que permita identificar los riesgos a los que se encuentran expuestos los sistemas de información y redes de datos, de manera que se puedan definir las medidas correctivas y preventivas que reduzcan los incidentes de seguridad de la información.

6.12. Políticas para Aspectos de seguridad de la información en la gestión de continuidad de negocio

Continuidad de seguridad de la información: Se debe considerar la continuidad de la seguridad de la información ante alguna situación que pueda afectar la continuidad de negocio de la empresa.

- Se debe definir un plan con las medidas que permitan restablecer la disponibilidad, integridad y confidencialidad de la información ante una situación de parada o de emergencia que pueda afectar los distintos servicios (energía, comunicaciones, red de datos, colapso de infraestructuras, etc.)
- Ante una situación de parada de los distintos servicios se debe realizar un análisis de impacto en los requisitos de seguridad de la información, para activar las medidas de respuesta y restablecimiento.
- Anualmente se deben revisar y poner a prueba el plan para restablecer la disponibilidad, integridad y confidencialidad de la información, y revisar las medidas de respuesta

definidas anteriormente, para asegurar la vigencia y correspondencia con las necesidades de la empresa.

Redundancias: Se debe asegurar la disponibilidad de instalaciones de procesamiento de información.

- Se debe identificar qué sistemas de información, software, aplicaciones, redes de datos, infraestructura y servicios de tecnología deben contar con redundancia para asegurar la continuidad de negocio, luego se debe analizar la viabilidad de las redundancias y realizar pruebas del buen funcionamiento de las mismas.

7. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

Se debe garantizar que las políticas de seguridad y privacidad de la información son implementadas y operadas de acuerdo con las demás políticas y procedimientos organizacionales, para ello se establecen controles basados en la norma ISO 27001, y el MSPI, los cuales se encuentran en el Anexo *Instrumento de evaluación de MSPI - ISO 27001*, dichos controles deben ser evaluados de preferencia anualmente por la Oficina de Control Interno.