PROCEDIMIENTO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

1. OBJETIVO

Establecer las actividades necesarias para atender los requerimientos relacionados con la seguridad de la información y de la gestión de activos, aplicando la política de seguridad en todos los procesos de la empresa, garantizando la confidencialidad, integridad y disponibilidad de la información, para asegurar la continuidad en la prestación de servicios de los usuarios.

2. ALCANCE

Este procedimiento es aplicable para todas Oficinas y Divisiones de la Empresa de Servicios Públicos de Fusagasugá (EMSERFUSA E.S.P.),incluidos los contratistas, proveedores y terceros con acceso autorizado a las instalaciones, equipos y/o sistemas de información de la empresa.

3. DEFINICIONES

Confidencialidad: impedir que la información se divulgue o se ponga a disposición de entidades no autorizadas.

Disponibilidad: característica de la información que garantiza que pueda ser utilizada cuando se necesite.

Integridad: una garantía de que la información es exacta y sólo puede ser modificada por el personal autorizado.

Autenticación: verificación de que una característica o atributo que parece o se afirma como verdadero, es de hecho verdadero.

No repudio: proporcionar una prueba innegable de que un supuesto evento ocurrió, o una supuesta acción se llevó a cabo, y que este evento o acción fue realizado por una entidad en particular.

Activo: un activo es cualquier cosa que tenga valor para una organización.

Amenaza: es cualquier evento potencial que podría tener un impacto negativo en un activo.

Actor de la amenaza: es cualquier persona u organización que supone una amenaza.

Vulnerabilidad: es cualquier debilidad en un activo o control que podría ser explotada por una amenaza.

Acceso no autorizado: es un incidente que involucra a una persona, sistema o código malicioso que obtiene acceso lógico o físico sin autorización adecuada del dueño a un sistema, aplicación, información o un activo de información.

Modificación de recursos no autorizados: un incidente que involucra a una persona, sistema o código malicioso que afecta la integridad de la información o de un sistema de procesamiento.

Uso inapropiado de recursos: un incidente que involucra a una persona que viola alguna política de uso de recursos.

No disponibilidad de los recursos: un incidente que involucra a una persona, sistema o código malicioso que impide el uso autorizado de un activo de información.

4. DOCUMENTOS DE REFERENCIA

Marco de trabajo ITIL 4
Anexo 1.6 Política de seguridad de la información
Modelo de Seguridad y Privacidad de la Información – MSPI
Anexo 2.1 Procedimiento de gestión de incidentes y problemas
NTC-ISO/IEC Colombiana 27001:2013

5. CONSIDERACIONES

- Garantizar la gestión de seguridad, con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información necesaria, para que la empresa desarrolle sus actividades laborales, y, en consecuencia, el encargado de seguridad revisa, administra y monitorea las políticas relacionadas con la seguridad, guardando evidencia, para garantizar su seguimiento.
- Es responsabilidad de EMSERFUSA establecer la estrategia de seguridad de la información para la empresa, considerando las estrategias comerciales y los riesgos que podrían llegar a afectar el desarrollo normal de sus operaciones.
- Dentro del procedimiento de gestión de seguridad se incluye el desarrollo de las actividades para la gestión de incidentes de seguridad y el desarrollo de las actividades de gestión de auditoría y de revisión.
- Para prestar el servicio de soporte técnico es necesario que el equipo esté registrado en el inventario de las Oficinas o Divisiones que hacen parte de EMSERFUSA.
- Una vez se detecte o sospeche sobre una fuga de un incidentes de información por parte de funcionarios, proveedores o terceros con acceso autorizado a los recursos tecnológicos o a los activos de información de EMSERFUSA, se debe realizar una investigación del incidente que involucre a las partes implicadas y se toman acciones de detención del mismo, inmediatamente se debe inactivar el usuario y restringir el acceso a los servicios; un vez, finalizada la diligencia, se determina la acción final bien sea inhabilitar el usuario o debe ser reactivado.
- EMSERFUSA debe garantizar la adopción y proporcionar la información de protección suficiente para evitar impactos adversos en la capacidad de los servicios; asegurando un flujo de comunicación efectivo sobre la estrategia de seguridad de la información a la junta directiva y demás partes interesadas.

- Cuando se presente un potencial riesgo o amenaza, inmediatamente se debe comunicar al jefe de la Oficina de Planeación e Informática OPEI, con el fin, de identificar, contener y minimizar el daño a la infraestructura o equipos de la empresa, por otro lado, se debe elaborar el informe administrativo, teniendo en cuenta el nivel del incidente.
- Nivel del incidente: teniendo en cuenta el nivel de protección de los activos y la criticidad de la información contenida en este, la empresa debe contar con capacidad para dar respuesta oportuna a los incidentes de seguridad, y también debe garantizar la detección, evaluación y gestión de las vulnerabilidades de su plataforma tecnológica que soporta la operación, y, de todos los sistemas de información implicados: misionales, gestión y apoyo, principalmente de los medios que alojan los activos de información de EMSERFUSA.

  También debe clasificar el incidente de acuerdo a su severidad, la cual puede ser:

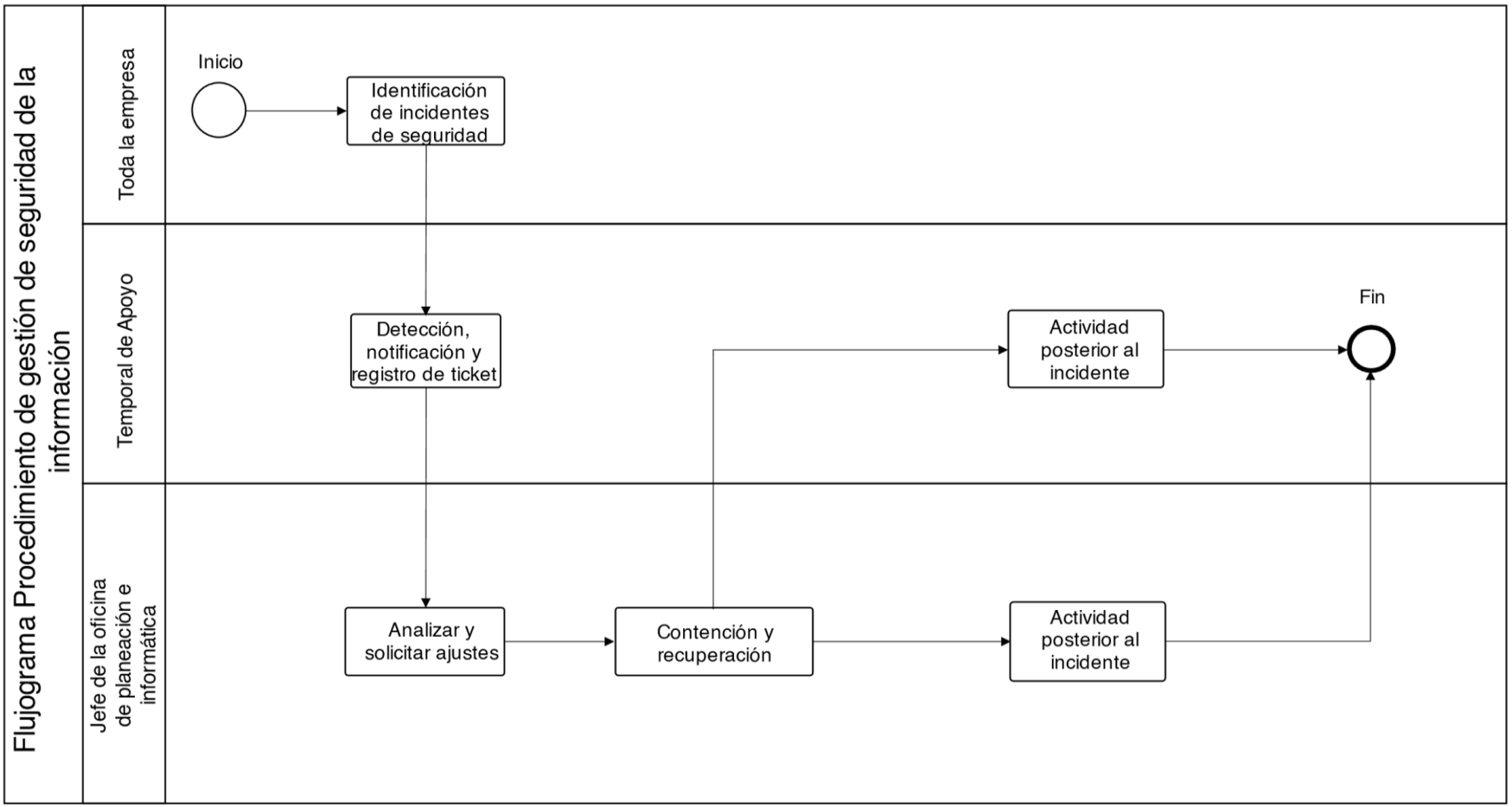
  - **Alto impacto:** el incidente de seguridad afecta a los activos de información considerados de impacto mayor, que influyen directamente a los objetivos misionales de la empresa. Se incluyen en esta categoría aquellos incidentes que afecten la reputación y el buen nombre o involucren aspectos legales, estos incidentes **deben tener respuesta inmediata.**
  - **Medio impacto:** el incidente de seguridad afecta a los activos de información considerados de impacto moderado que influyen directamente a los objetivos de un proceso determinado.
  - **Bajo impacto:** el incidente de seguridad afecta a los activos de información considerados de impacto menor e insignificante, que no influyen en ningún objetivo, estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto.

6. DESARROLLO DE LAS ACTIVIDADES PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD

ACTIVIDAD	DESCRIPCIONES	RESPONSABLE	DOCUMENTO DE REFERENCIA
1. Identificación de incidentes de seguridad	Identificar las necesidades de seguridad de la información y de los activos informáticos (servicios y activos críticos), con el fin de definir oportunidades de mejora que brindan a la organización un seguimiento oportuno	Toda la empresa	Herramienta de gestión de solicitudes, Catálogo de servicios, Política de seguridad de la información.
2. Detección, notificación y registro de ticket	Registrar nuevos requerimientos y analizarlos para definir su tratamiento: este proceso se lleva a cabo mediante el uso de herramientas de monitoreo y de registro de incidentes (**registrar ticket**), a través de la mesa de servicio. **Nota:** una vez se identifica el incidente de seguridad, este debe escalar al jefe de la oficina de planeación e informática.	Temporal de Apoyo	Herramienta de gestión de solicitudes
3.Analizar y solicitar ajustes	Una vez recibido el incidente de seguridad, se debe seguir los siguientes pasos: 1. Comprender la naturaleza y la gravedad del incidente 2. Analizar el activo teniendo en cuenta su carácter crítico y el impacto de este, en la empresa; de igual forma realizar recomendaciones. 3. Si se identifica que el activo crítico es de alto nivel para la empresa, se debe registrar y marcar en el inventario de activos de EMSERFUSA, indicando características y ubicación 4. Los activos de información se deben proteger teniendo en cuenta su grado de confidencialidad, integridad y disponibilidad, para lo cual deberá etiquetar (documentación lógica y física) o rotular (equipos), para indicar al personal, el nivel de seguridad con la que el activo debe ser tratado 5. Realiza un análisis de riesgos de seguridad, para identificar las	Jefe de la oficina de planeación e informática	Herramienta de gestión de solicitudes

	amenazas, vulnerabilidades de cada activo. Entre las amenazas, se encuentran: ● Seguridad física, lógica y de datos ● Amenazas (internas, externas) ● Probabilidad de ocurrencia ● Impacto potencial de cada riesgo		
4. Contención y recuperación	Una vez se haya completado el análisis, y teniendo una comprensión técnica de los servicios afectados y sus componentes y su impacto potencial de pérdida para la empresa, se deben definir los posibles controles de seguridad que podrían minimizar el nivel del riesgo e impacto en el negocio, para lo cual, se debe considerar lo siguiente: ● Los controles a implementar o mejorar ● Justificar el costo frente a posibles impactos ● La relación de riesgos a mitigar ● Las personas responsables de su implementación ● Relación de tareas y actividades a ejecutar con sus respectivos responsables ● Cuando sea necesario implementar un plan de capacitación a todos los involucrados en la implementación de controles Una vez realizadas las actividades, el servicio podría ser restaurado utilizando sistemas alternativos. En caso de requerir, se debe borrar el almacenamiento y los sistemas se reconstruyen a partir de fuentes conocidas y confiables (copias de seguridad). Los procesos de negocio se consideran recuperados cuando se puede realizar actividades sin amenazas, incidentes, o daños adicionales del incidente original.	Jefe de la oficina de planeación e informática	Herramienta de gestión de solicitudes

5.Actividad posterior al incidente	Se debe garantizar la eliminación de la amenaza, por lo tanto, se supervisan los sistemas y servicios, es necesario: ● Validar si las oportunidades de mejora implementadas agregan valor a las operaciones ● Crear informe de incidentes y socializar ● Resolver y cerrar los incidentes de seguridad, siguiendo el Anexo 2.1 Procedimiento de gestión de incidentes y problemas de EMSERFUSA	Temporal de Apoyo, jefe de la oficina de planeación e informática	Herramienta de gestión de solicitudes


Flujograma Procedimiento de gestión de seguridad de la información
Toda la empresa
Temporal de Apoyo
Jefe de la oficina de planeación e informática
Inicio
Identificación de incidentes de seguridad
Detección, notificación y registro de ticket
Analizar y solicitar ajustes
Contención y recuperación
Actividad posterior al incidente
Actividad posterior al incidente
Fin

7. DESARROLLO DE LAS ACTIVIDADES DE GESTIÓN DE AUDITORÍA Y DE REVISIÓN

A continuación, se describen las actividades que deben llevarse a cabo, para garantizar que el proceso de seguridad de la información sea monitoreado, y en caso de ser necesario se implemente, cambie o mejore los controles de seguridad.

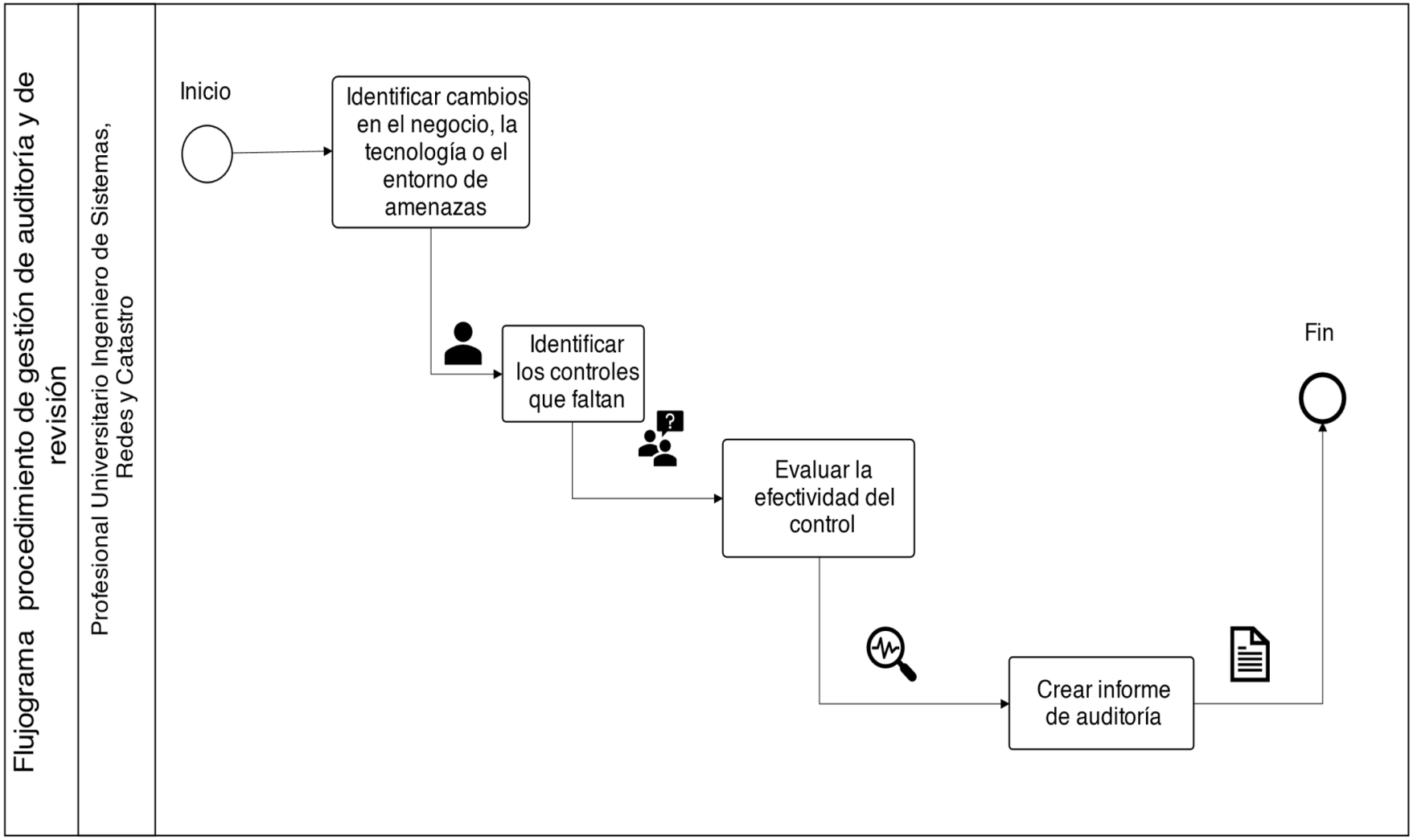
Esta auditoría puede ser realizada por un agente interno o externo, siguiendo un cronograma con los tiempos establecidos, estas auditorías, también deben realizarse luego de la identificación de un incidente importante o debido a los resultados de la evaluación de amenazas y vulnerabilidades.

Nota: se recomienda ejecutar las actividades de gestión de auditorías por lo menos una vez al año.

Para observar los flujogramas con un mayor detalle, consultar el Anexo 3.5 Flujograma Procedimiento de gestión de seguridad de la información.

ACTIVIDAD	DESCRIPCIONES	RESPONSABLE	DOCUMENTO DE REFERENCIA
1. Identificar cambios en el negocio, la tecnología o el entorno de amenazas	Todos los problemas de seguridad de la empresa, deben haber sido investigados, identificados y gestionados para comprender su(s) causa(s), igualmente los procesos del negocio deben ser evaluados para identificar los posibles cambios que pueden afectar la seguridad de la información. También, se debe evaluar la tecnología que usa la empresa con el fin de identificar tecnologías nuevas, cambiadas o que se hayan vuelto obsoletas, además de identificar los cambios en el entorno con respecto a las amenazas y vulnerabilidades que se identifican mediante una evaluación de las mismas.	Profesional Universitario Ingeniero de Sistemas, Redes y Catastro	Evaluación de amenazas y vulnerabilidades
2. Identificar los controles que faltan	Una vez analizado e investigado las tecnologías, amenazas y la identificación de los controles recomendados, es necesario evaluar: ● Si la lista incluye todos los controles ● Si es necesario adicionar o recomendar nuevos controles ● Sugerir mejoras sobre los mismos Para el desarrollo de esta actividad, es necesario que se cuente con una compresión de la norma de seguridad aplicable (NTC-ISO/IEC Colombiana 27001:2013)	Profesional Universitario Ingeniero de Sistemas, Redes y Catastro	Listado de controles, Anexo 1.6 Política de seguridad de la información, ISO/IEC 27001:2013
3. Evaluar la efectividad del control	En la evaluación de los controles implementados, es necesario identificar posibles vulnerabilidades, las cuales podrían estar relacionadas con su alcance, es decir, evaluar si el control es aplicable en todas las partes en donde fue ubicado (hardware) o configurado (software) y si su nivel de protección es adecuado. En la evaluación de los controles técnicos podría considerarse: ● Revisar los registros y realizar entrevistas al personal ● Revisar los controles de accesos vs la información del directorio activo, con los registros de las solicitudes de acceso concedidas ● Identificar controles ineficientes	Profesional Universitario Ingeniero de Sistemas, Redes y Catastro	Evaluación de amenazas y vulnerabilidades, listado de controles

4. Crear informe de auditoría	Finalmente, la persona encargada de evaluar, revisar los controles e identificar las vulnerabilidades, crea un informe de auditoría con los hallazgos de las etapas anteriores. Dicho informe debe mostrar: ● Información de alto nivel ● Evaluación y priorización de las oportunidades de mejora ● Controles nuevos y mejorados ● Recomendaciones	Profesional Universitario Ingeniero de Sistemas, Redes y Catastro	Informe de auditoría


Flujograma procedimiento de gestión de auditoría y de revisión
Profesional Universitario Ingeniero de Sistemas, Redes y Catastro
Inicio
Identificar cambios en el negocio, la tecnología o el entorno de amenazas
Identificar los controles que faltan
Evaluar la efectividad del control
Crear informe de auditoría
Fin