1. OBJETIVO

Establecer el procedimiento para reportar, escalar, evaluar, gestionar y brindar respuesta a los incidentes de seguridad de la información, buscando minimizar los impactos en el sistema de seguridad de la información.

2. ALCANCE

Los términos y condiciones descritos aplican a todos los procesos, colaboradores, consultores, contratistas y proveedores, que sean responsables y que tengan acceso a la información que sea de propiedad de Ser Ambiental S.A. ESP

3. NORMAS GENERALES

3.1. Perspectiva ISO

- ISO 9001 de 2015: Sistema de gestión de calidad.
- ISO 45001 2018: Sistema de gestión de la Seguridad y Salud en el trabajo
- ISO 14001 de 2015: Sistema de gestión ambiental.
- ISO 27001 de 2013: Sistema de seguridad de la información.

NOTA: Servicios Ambientales S.A ESP, solo se encuentra certificado en los requisitos de la norma ISO 9001:2015, sin embargo, adopta normas de referencia como son la ISO 14001:2015, 45001:2018 Y 27001:20113, lo cual no implica que se tengan implementadas y certificadas

3.2. Reglamento legal

- Ver matriz legal

4. DEFINICIONES

4.1. Activo: Cualquier cosa que tenga un valor de importancia relevante para la organización. Entre los activos de una organización se encuentra hardware, software, documentos electrónicos o físicos, infraestructura, servidores, personal, entre otros. El término activo es sinónimo de activo de información.

4.2. Amenaza: Es una fuente generadora de eventos o acciones que puede producir o causar un daño representativo al activo de información, generando un factor o escenario de riesgo que originaría a la organización pérdidas por riesgo de seguridad de la información. La amenaza en el contexto de seguridad de la información que se manifiesta a través de actos deliberados, intencionados o impredecibles y provocados por las personas, la tecnología, la infraestructura, acontecimientos externos, entre otros.

4.3. Confidencialidad: Propiedad de salvaguardar el activo de información de personas, procesos o entidades no autorizados.

4.4. Controles: Medidas deprotección o salvaguardas dispuestas para reducir el nivel de riesgo. Pueden ser la política, lineamientos, procedimientos, directrices,

prácticas, estructuras de la organización, soluciones tecnológicas, entre otros.

4.5. Cadena de Custodia: Registro detallado del tratamiento de la evidencia, incluyendo quienes, cómo y cuándo la transportaron, almacenaron y analizaron, a fin de evitar alteraciones o modificaciones que comprometan la misma

4.6. Contención: Evitar que el incidente siga ocasionando daños.

4.7. Disponibilidad: Propiedad de garantizar que el activo de información sea accesible y utilizable en el momento que se requiera, por parte de las personas, procesos o entidades autorizada.

4.8. Evento de seguridad de la información: Es la ocurrencia identificada de un estado del activo de información (sistema, servicio, red, entre otros) que indica un incumplimiento posible del lineamiento de seguridad de la información, una falla de controles existentes, o una situación previamente desconocida que puede ser pertinente para la seguridad.

4.9. Impacto: Consecuencias que produce un incidente de seguridad sobre la organización.

4.10. IDS: Software de detección de intrusos

4.11. Incidente de seguridad de la información: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. [ISO/IEC 27000:2009]

4.12. Integridad: Propiedad de salvaguardar la exactitud y estado completo del activo de información, de acuerdo a los diferentes métodos de proceso a que se exponga.

4.13. Gestión de Incidentes: Es el conjunto de todas las acciones, medidas, mecanismos, recomendaciones, tanto proactivos, como reactivos, tendientes a evitar y eventualmente responder de manera eficaz y eficiente a incidentes de seguridad que afecten activos de una entidad. Minimizando su impacto en el negocio y la probabilidad que se repita.

4.14. Hash: Función computable mediante un algoritmo, que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija**.**

4.15. Log's: Registro de los sistemas de información que permite verificar las tareas o actividades realizadas por determinado usuario o sistema.

4.16. Procesamiento de Información: Es la capacidad que tiene un sistema de información de efectuar cálculos con base a una secuencia de operaciones preestablecidas y permitiendo la transformación de datos fuentes en información para ser utilizada en la toma de decisiones.

4.17. Propietario: Se refiere al dueño responsable del activo de información utilizado para el desarrollo y cumplimiento de sus funciones. Está encargado de garantizar la seguridad adecuada del mismo, con base a los principios básicos de seguridad a saber: confidencialidad, integridad y disponibilidad.

4.18. Seguridad de la información: Preservación fundamental de la confidencialidad, integridad y disponibilidad del activo de información, además de otros criterios o propiedades tales como la autenticidad, no repudio, confiablidad, propiedad y/o responsabilidad, entre otros.

4.19. Sistema de Información: Es una disposición de personas, actividades o procedimientos y recursos tecnológicos integrados entre sí, para apoyar y mejorar las operaciones diarias de la organización, con la finalidad de satisfacer las necesidades de información en general y facilitar la toma de decisiones por parte

de los directivos de la organización. Ejemplos aplicados: sistemas de automatización de oficina, sistemas de procesamiento de transacciones y sistemas de información de gestión.

4.20. Software malicioso: Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse en o dañar recursos informáticos, sistemas operativos, redes de datos o sistemas de información.

4.21. Tratamiento del riesgo: Proceso de selección e implementación de controles o acciones para ajustar el nivel de riesgo del activo a los niveles aceptables para la Organización.

4.22. Vulnerabilidad: Es la debilidad o incapacidad de resistencia de un activo de información frente a una amenaza.

4.23. Recuperación: Volver el entorno afectado a su estado natural.

4.24. Sniffer: Software que captura los paquetes que viajan por la red para obtener información de la red o del usuario.

4.25. SSI: Subsistema de Seguridad de la Información.

4.26. Validación: Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.

4.27. Vulnerabilidad: Ausencia o debilidad de un control. Condición que podría permitir que una amenaza se materialice con mayor frecuencia, mayor impacto o ambas. Una vulnerabilidad puede ser la ausencia o debilidad en los controles administrativos, técnicos y/o físicos.

5. CONDICIONES

5.1. Generales

- El responsable del presente documento es el gerente de tecnología de la información
- Se deben consolidar las lecciones aprendidas que dejan los incidentes de seguridad de la información y su gestión para aprender rápidamente. Esto tiene como objeto incrementar las oportunidades de prevenir la ocurrencia de futuros incidentes, mejorar la implementación y el uso de las salvaguardas y mejorar el esquema global de la gestión de incidentes de seguridad de la información.

5.2. Calidad

- Este documento se rige bajo la norma ISO 9001: 2015.

5.3. Seguridad y Salud en el trabajo

- Ajustar a su medida los elementos regulables del puesto de trabajo (sillas, pantalla y teclado), la espalda debe de quedar recta y apoyada en la silla y los pies no deben de quedar colgando, deben de quedar apoyados en el suelo, las rodillas deben de hacer un Angulo de 90 grados.
- Usar los archivadores con precaución, evitar colocar objetos pesados en la parte

superior.

- Para desconectar un equipo tire siempre de la clavija, nunca del cable.
- Mantener libre de obstáculos las salidas y zonas de paso.
- Realizar pausas activas
- No hablar por celular ni chatear mientras camina.
- En caso de robo de algún equipo fuera de las instalaciones de Ser Ambiental S.A. ESP, se debe generar denuncio en la fiscalía e iniciaría proceso sancionatoriocon gestión humana.

5.4. Ambiental

- Apagar los equipos que no vayan a ser usados durante más de una hora y desconectar aquellos que no tengan uso (fotocopiadoras, impresoras, etc.).
- Configurar el salvapantallas del computador en modo “Suspensión” no mayor a 5 minutos evitando así que funcione mientras no es utilizado.
- Evitar el uso de impresiones siempre que sea posible, por ejemplo, guardando los documentos en formato digital, compartiendo información en lugar de generar copias para cada persona, utilizando la Intranet, correos electrónicos, teléfono, etc.
- Utilizar de forma preferente y en la medida de lo posible papel reciclado.
- Utilizar el papel por las dos caras en el fotocopiado e impresión de documentos en la medida de lo posible.
- Imprimir en calidad de borrador para evitar el derroche de tinta y facilitar la reutilización.
- Realizar la separación en la fuente de los residuos sólidos de acuerdo a sus características en lo puntos verdes identificados.
- Utilice la luz artificial solo en caso de ser necesario.

5.5. Seguridad de la Información

El responsable de la información debe definir los eventos considerados como críticos junto con sus respectivas alertas y registros de seguridad de la información, los cuales deberán ser generados. Éstos deben ser activados, vigilados, almacenados y revisados permanentemente, y las situaciones no esperadas deben ser reportadas de manera inmediata al comité de atención de incidentes. Los registros y los medios que los generan y administran deben ser protegidos por controles que eviten modificaciones o accesos no autorizados, para preservar la integridad de las evidencias.

Los incidentes de seguridad, resultantes del incumplimiento de los lineamientos y normas de seguridad de Ser Ambiental S.A. ESP serán direccionados por el procedimiento de gestión de incidentes de seguridad de la información, con el objetivo de realizar la respectiva investigación y entregar los resultados a los respectivos responsables dentro de la compañía, encargados de tomar las acciones correctivas y preventivas del caso.

Los colaboradores deberán estar informados del proceso disciplinario que se llevará a cabo en caso de incumplimiento de los lineamientos de seguridad de la información o alguno de los elementos que la soportan. En cualquier caso, se hará un seguimiento de acuerdo con los procedimientos establecidos para el manejo de incidentes de seguridad.

5.4.1. Características de un modelo de gestión de incidentes

Se plantea una serie de actividades para dar cumplimiento con el ciclo de vida de la gestión y respuesta a un incidente de seguridad.

Para definir las actividades de esta guía se incorporaron componentes definidos por el NIST alineados con los requerimientos normativos de la NTC–ISO–IEC 27035-2013.

Es recomendable crear un equipo de atención de incidentes de seguridad en cómputo CSIRT o un grupo que haga sus veces, quienes se encargaran de definir los procedimientos a la atención de incidentes, realizar la atención, manejar las relaciones con entes internos y externos, definir la clasificación de incidentes, y además de esto se encargaran de:

- **Detección de Incidentes de Seguridad**: Monitorear y verificar los elementos de control con el fin de detectar un posible incidente de seguridad de la información.
- **Atención de Incidentes de Seguridad:** Recibe y resuelve los incidentes de seguridad de acuerdo con los procedimientos establecidos.
- **Recolección y Análisis de Evidencia Digital:** Toma, preservación, documentación y análisis de evidencia cuando sea requerida.
- **Anuncios de Seguridad:** Deben mantener informados a los Colaboradores, contratistas o terceros sobre las nuevas vulnerabilidades, actualizaciones a las plataformas y recomendaciones de seguridad informática a través de algún medio de comunicación (Web, Intranet, Correo).
- **Auditoria y trazabilidad de Seguridad Informática:** El equipo debe realizar verificaciones periódicas del estado de la plataforma para analizar nuevas vulnerabilidades y brechas de seguridad.
- **Certificación de productos:** El equipo verifica la implementación de las nuevas aplicaciones en producción para que se ajusten a los requerimientos de seguridad informática.
- **Configuración y administración de dispositivos de seguridad Informática:** Se encargarán de la administración adecuada de los

elementos de seguridad informática.

- **Clasificación y priorización de servicios expuestos:** Identificación de servicios sensibles y aplicaciones expuestas para la prevención o remediación de ataques.

5.4.2. Roles que participan en el proceso

5.4.2.1. Coordinador de Tecnología:

- Orientar y dar adecuado tratamiento a los incidentes de seguridad de la información detectados o reportados.
- Debe hacer un seguimiento periódico a los incidentes de seguridad presentados.
- En caso de no presentarse un número significativo de reportes de incidentes, revisara los reportes de las herramientas de seguridad para el análisis pertinente y otras fuentes con el propósito de mejorar la gestiónde incidentes de seguridad.

5.4.2.2. Colaboradores y contratistas

- Deben tomar conciencia de su responsabilidad para reportar eventos y debilidades de seguridad de la información, tan pronto como sea posible a la mesa de servicios y por otros medios disponibles.
- Recibir las capacitaciones y participar en las campañas de sensibilización que se realicen al interior de la entidad.
- Reportar oportunamente los incidentes o eventos de seguridad de la información y cualquier comportamiento anormal que se presente en la entidad o en sus activos de información.

5.4.2.3. Comité de atención de incidentes

- Debe mantener constante capacitación y sensibilización a los colaboradores, contratistas y demás partes interesadas en cuanto al reporte de incidentes de seguridad de la información y vulnerabilidades de los sistemas de información con los que cuenta la entidad, debe hacer énfasis en:

  a. Los riesgos de un control de seguridad ineficaz
  b. Que es la violación de la integridad, confidencialidad o expectativas de disponibilidad de la información.
  c. Los errores humanos.
  d. Las no conformidades con los lineamientos o directrices.
  e. Violaciones en la seguridad física.
  f. El mal funcionamiento en el software o hardware.
  g. Las violaciones de acceso.

  Lo anterior con el propósito de que los colaboradores, contratistas y demás partes interesadas de la compañía estén en capacidad de reconocer y reportar incidentes de seguridad.

- Debe mantener contactos apropiados con las autoridades, grupos de interés o foros externos que manejen las cuestiones relacionadas con incidentes de seguridad de la información.

5.4.3. Tipo de Incidentes de seguridad.

Las partes interesadas de seguridad de la información deben conocer y saber identificar los incidentes aceptados por la compañía, como son:

- Acceso no autorizado a la información.
- Divulgación de información sensible.
- Denegación del servicio.
- Daño de la información.
- Ataques externos o internos.
- Ataques dirigidos y no dirigidos
- Pérdida o robo de la información.
- Modificación no autorizada.
- Información no actualizada.
- Mala gestión del conocimiento.
- Diligenciamiento errado de formatos.
- Perdida o daño de la documentación.
- Daños sobre activos de información
- Uso indebido de activos de información
- Uso indebido de software
- Uso indebido de usuarios
- Suplantación de identidad

El comité de atención de incidentes de seguridad de la información, de acuerdo a los niveles de criticidad del evento/incidente, dará el tratamiento adecuado.

Nivel	Descripción
Alto	Interrumpe seriamente la operación de la entidad, el incidente puede tener velocidad significativa/rápida en su propagación y ocasionar daños de activos. Podría llegar a afectar más de un tipo de activo. **Nota:** Si el incidente pone en riesgo al personal / comunidad / autoridades locales y la continuidad del negocio podría generar una crisis mediática, para este tipo de casos remitirse al documento del proceso de Comunicaciones y Relaciones Institucionales "Protocolo de crisis. Escenario **Fuga y/o filtración de información**".
Medio	Interrumpe en un periodo corto de tiempo los procesos generales de la entidad, el incidente/evento compromete un activo importante.
Bajo	No interrumpe los procesos generales de la entidad, el incidente/evento, se detecta y puede controlar fácilmente con recursos existentes en la entidad.

Tabla 1. Niveles de criticidad del evento/incidente

El comité de atención de incidentes de seguridad de la información, debe conocer la siguiente tabla de escalamiento a fin de darle el tratamiento adecuado.

Relevancia	Escalamiento
Alto	Se escala a los proveedores pertinentes y si es el caso a las autoridades externas competentes
Medio	Se escala al Grupo de Administración y Seguridad de la Información, Oficina de Tecnologías de la Información y a las áreas involucradas
Bajo	Solo se diligencia el caso en la herramienta de gestión de Mesa de Servicios, o se escala al responsable del activo de información involucrado en caso de ser necesario.

Tabla 2. Niveles de escalamiento de evento/incidentes de seguridad de la información

El comité de atención de incidentes de seguridad de la Información para preservar la integridad, disponibilidad y confidencialidad de los activos de información debe generar las alertas tempranas así:

- Alertas de activos de seguridad
- Alertas de fuga de información
- Alertas de las plataformas de información.

5.4.4. Especificas

- Si un colaborador, contratista y demás partes interesadas, nota que se está presentando un ataque a los activos de la entidad, es conocedor de alguna violación del lineamiento de seguridad de la información o conoce de riesgos asociados a la información, debe reportar al proceso de TI.
- El incidentes o evento de seguridad se reportar en la mesa de ayuda de la entidad enviando un correo a miguel.perozo@serambiental.com, llamando al celular de soporte 3023641410, en la página web de mesa de ayuda (GLPI)o informando directamente al personal de tecnología.
- Al registrar el incidente o evento se debe incluir fecha, hora y descripción de lo ocurrido.
- En la evaluación del incidente se debe identificar los activos afectados, cuál es el alcance del mismo, que pronóstico tiene de expansión, así como los daños potenciales o reales que se generen.
- Para evaluar la severidad de los eventos/incidentes considerará la relevancia de los activos y el nivel del incidente. Cuando exista la posible relación de más de un activo comprometido y/o más de un incidente o evento, todo el conjunto se valorará de acuerdo a los niveles descritos en la Tabla 1 de la presente guía, teniendo en cuenta la relevancia del activo.
- La evaluación del impacto y la relevancia se harán con la matriz de riesgos de los activos de información
- En la identificación de la relevancia se establecerá la afectación del activo de información, incluyendo el valor económico y la cantidad de información relevante para la compañía.
- El coordinador de tecnología o quien haga sus veces, deberá identificar el nivel de afectación del incidente de acuerdo a los niveles de criticidad del evento/incidente descritos en la tabla 1 de la presente guía.
- Para buscar una solución al incidente el coordinador de tecnología o quien haga sus veces debe tener en cuenta los niveles de escalamientos tabla 2 de la presente guía.
- Para saber cómo actuar ante un incidente, conforme al nivel de evento/incidente debe considerar los siguientes tipos de respuesta: Proceder de acuerdo con las instrucciones de la brigada de emergencias y según lineamientos de los cuerpos de socorro, privilegiando la conservación de la vida e integridad de las personas tanto de la compañía como los visitantes.
- En la medida que haya tiempo y recursos, el equipo de gestión de incidentes debe adelantar las actividades que tiendan a proteger la información, solicitando autorización y activando la funcionalidad soportada a través del centro alterno de cómputo cambiando la dirección de producción a la dirección contingente, en caso de no requerirse este tipo de manejo debe seguir con la siguiente actividad de la presente guía.
- Se deben tener en cuenta los siguientes factores para la contención del incidente o evento

  a. Daño potencial de recursos a causa del incidente.
  b. Necesidad de preservación de la evidencia.
  c. Tiempo y recursos necesarios para poner en práctica la estrategia.

d. Efectividad de la estrategia.
e. Duración de las medidas a tomar.
f. Criticidad de los sistemas afectados.
g. Características de los posibles atacantes.
h. Si el incidente es de conocimiento público.
i. Pérdida económica.
j. Posibles implicaciones legales.

- Para hacer una correcta recolección de evidencia se deben tener en cuenta lo siguientes criterios para la recolección de evidencia:

  a. Información basada en la red: Log's de IDSs, logs de monitoreo, información recolectada mediante Sniffers, logs de routers, logs de firewalls, información de servidores de autenticación.
  b. Información Basada en el Equipo: Live data collection: Fecha y hora del sistema, aplicaciones corriendo en el sistema, conexiones de red establecidas, puertos abiertos, aplicaciones escuchando en dichos puertos, estado de la tarjeta de red.
  c. Otra información: Testimonio de funcionario o contratista que reporta el evento o incidente.

- Se debe dar un correcto manejo a los datos y evidencias recolectadas, los cuales deben ser almacenados para futuras investigaciones e implementación de controles preventivos o de mejoramiento.
- La información que debe ser almacenada y custodiada por el coordinador de tecnología incluye:

  a. Cantidad de incidentes presentados y tratados.
  b. Tiempo asignado a los incidentes.
  c. Daños ocasionados.
  d. Vulnerabilidades explotadas.
  e. Cantidad de activos de información involucradas.
  f. Frecuencias de ataques.
  g. Pérdidas.

  Además, debe cumplir con un control de seguridad que garantice la confidencialidad, integridad y disponibilidad de las evidencias retenidas.

- El almacenamiento físico seguro de las evidencias estará custodiado por el coordinador de tecnología y el electrónico se almacena en la herramienta de gestión de TI.
- Al gestionar el incidente de seguridad, debe tener identificadas las posibles fuentes de ataque posteriormente mencionadas:

  a. Empleados descontentos.
  b. Baja concientización.
  c. Crecimiento de redes.
  d. Falta de previsión de contingencias.
  e. Falta de lineamientos.
  f. Desastres naturales.
  g. Inadecuada protección de la infraestructura.

h. Confianza creciente en los sistemas
i. Virus.
j. Caballos de troya.
k. Explotación de vulnerabilidades, tanto a nivel de host, como de arquitectura de red (vulnerabilidades de la seguridad perimetral).
l. Falsificación de identificadores (biométricas, de autenticación o de encabezado de paquetes).
m. Robo de Información confidencial.
n. Violación a la privacidad.
o. Ingeniería social.
p. Denegación de servicios.
q. Hacking.

- Se debe tener en cuenta para definir y decidir las estrategias de erradicación los siguientes factores:

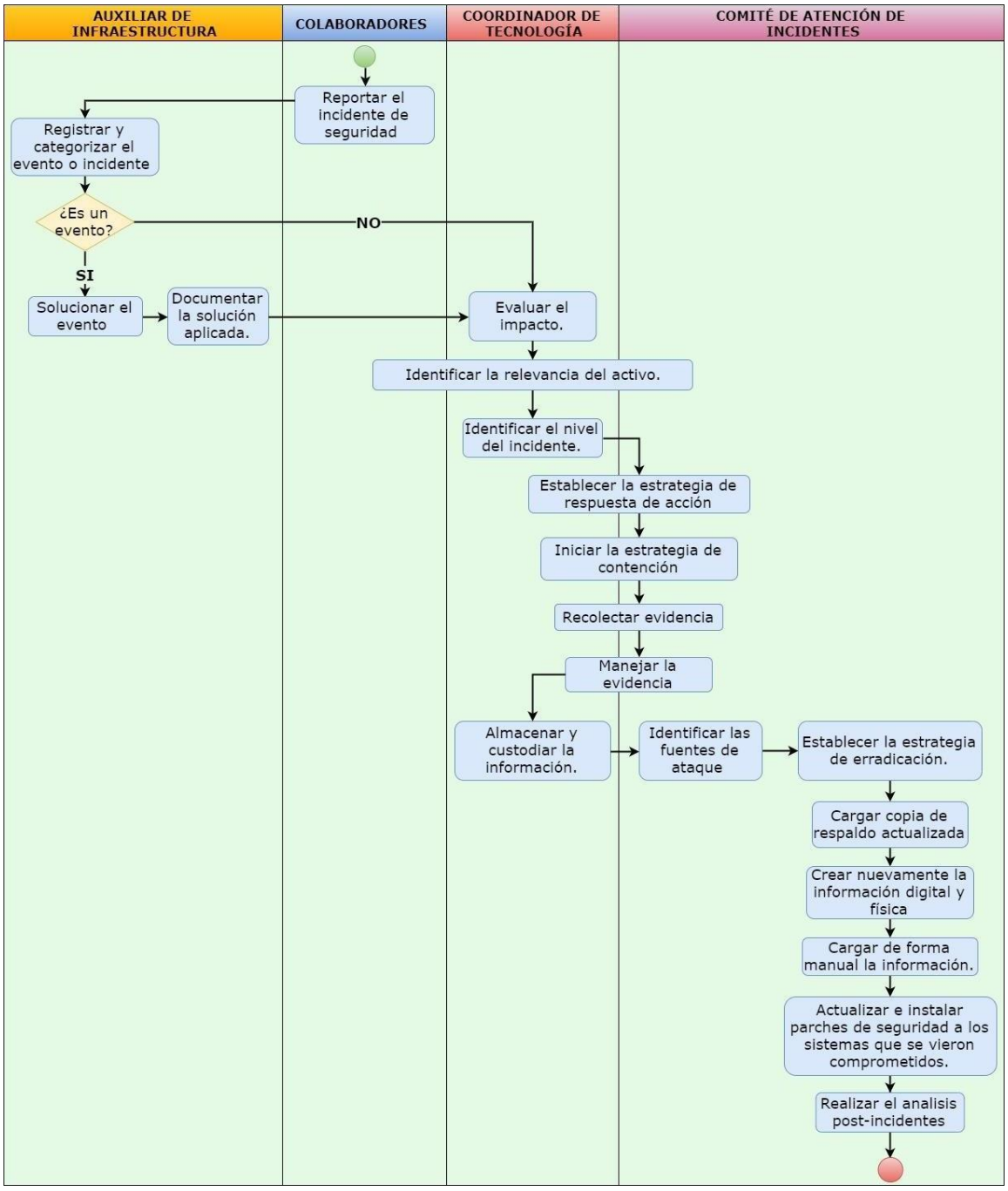
a. Tiempo y recursos necesarios para poner en práctica la estrategia.
b. Efectividad de la estrategia.
c. Pérdida económica.
d. Posibles implicaciones legales.
e. Relación costo-beneficio de la estrategia.
f. Experiencias anteriores.
g. Identificación de los procedimientos de cada sistema operativo comprometido
h. Identificación de usuarios o servicios comprometidos para proceder a desactivarlos.

- Al realizar el análisis post-incidente se debe garantizar el correcto manejo de las lecciones aprendidas, de la siguiente manera:

a. Periódicamente el coordinador de tecnología o quien haga sus veces se reunirá con el comité de atención de incidentes para verificar la mesa de ayuda a fin de analizar los eventos e incidentes presentados durante el periodo.
b. Buscar definir esquemas más efectivos para responder ante situaciones que afecten la seguridad de la información en la entidad.
c. Entre las actividades que se realizan está:
d. Mantener la documentación de los eventos e incidentes de seguridad de la información.
e. Mantener actualizada la bases de datos de conocimientos.
f. Integrar los eventos e incidentes a la matriz de riesgos de los activos de información SGSI.
g. Revisión de la matriz de riesgos de los activos de información SGSI
h. Realización de capacitaciones a los colaboradores de la entidad en lo relacionado a eventos e incidentes de seguridad de la información.
i. Analizar los hechos y tomar decisiones.

La información generada de los incidentes se almacenara en la mesa de ayuda.

6. DESCRIPCIÓN



7. DOCUMENTOS RELACIONADOS

Ítem	Proceso	Documento
1	Proceso de TI	Matriz de riesgos de los Activos de información

8. CONTROL DE CAMBIOS

Versión N°	Fecha	Elaborado/Modificado por	Descripción del cambio
01	27/08/2021	Coordinador de TI	Versión Original

9. RESPONSABLES

Elaboró: Coordinador de TI	**Revisó:** Director de TI
Aprobó: Gerente de TI	

COPIA CONTROLADA:	**SI:**	**NO**