Gestión de Incidentes en Seguridad de la Información

Teveandina S.A.S.– Canal Trece

Revisiones y control de cambios

Titulo	**Manual De Gestión De Incidentes En Seguridad De La Información**
Autores	Camilo Beltrán, Wilmar López
Tema	Manual De Gestión De Incidentes En Seguridad De La Información
Fecha de Elaboración	Febrero 2024
Formato	PDF
Versión	2.0
Palabras Relacionadas	Gestión de incidentes en seguridad de la información, Tecnología, Información, Proyecto, proyectos de tecnología de información

Control de Cambios			
Fecha	**Autores**	**Versión**	**Cambio**
Abril 2022	Gonzalo Joya Alexander Trejos Miller Dorado	1.0	Documento Original MA-GTI-M01
Febrero 2024	Wilmar López Camilo Beltrán	2.0	Actualización de Formato y actualización de documento

CONTENIDO

CONTENIDO DE TABLAS

1. INTRODUCCIÓN

Este documento describe la gestión de incidentes de seguridad, en TEVEANDINA S.AS. – CANAL TRECE. En el documento se describen el objetivo, las responsabilidades, los tipos de incidentes, actividades y remediación que se pueden implementar, al momento de un incidente/evento de seguridad.

2. OBJETIVO

Proporcionar los lineamientos y generalidades enmarcados en el Sistema de Seguridad y Privacidad de la Información (SGSI) para la identificación, gestión de incidentes y eventos con el fin de reducir la afectación negativa de los activos de información y la continuidad en las operaciones de TEVEANDINA S.A.S. – CANAL TRECE

3. ALCANCE

Este documento muestra las acciones que deben ser tenías en cuenta para la detección y contención de incidentes de seguridad de la información sobre todos los activos de información, independiente de las herramientas tecnológicas dispuestas para tal efecto.

4. GLOSARIO

ACTIVO DE INFORMACIÓN: Es el elemento de información que se recibe o se genera dentro las labores de la organización que tiene valor para la organización y la cual puede ser producidas en medios impresos, escritos, en papel, en medios digitales y trasmitida por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo software, hardware, recurso humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes.

CONFIDENCIALIDAD: Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado.

CUSTODIO: Responsable de la entidad de administrar y hacer efectivos los controles de seguridad.

DISPONIBILIDAD: Es la propiedad de la información de estar accesible y disponible cuando lo requiera el personal autorizado.

INTEGRIDAD: Es la propiedad de la información que garantiza que la información no fue modificada.

INFORMACIÓN: Datos en formato digital o físico, tratados, creados, procesados, almacenados, archivados o borrados durante la ejecución de procesos los procesos de la entidad.

INFORMACIÓN PÚBLICA CLASIFICADA: Aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica porque su acceso podrá ser negado o exceptuando siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 6 de la ley 1712 de 2014.1

INFORMACIÓN PÚBLICA RESERVADA: Es aquella información que estando en poder custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a interés públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la ley 1712 de 2014.2

PROPIETARIO DEL ACTIVO DE INFORMACIÓN: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene como responsabilidad velar por la protección del activo de información. Tiene responsabilidad de controlar la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos.

USUARIO: Son quienes generan, obtienen, transforman, conservan, eliminan o utilizan la información, en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información

EVENTO DE SEGURIDAD INFORMÁTICA: Un evento de seguridad informática es una ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información o la falla de medidas de seguridad (safeguards), o una situación previamente desconocida que pueda ser relevante para la seguridad. [ISO 18044].

INCIDENTE DE SEGURIDAD INFORMÁTICA: Un incidente de seguridad informática es la violación o amenaza inminente a la violación de una política de seguridad de la información implícita o explícita. También es un incidente de seguridad un evento que compromete la seguridad de un sistema (confidencialidad, integridad y disponibilidad). Un incidente puede ser denunciado por los involucrados, o indicado por un único o una serie de eventos de seguridad informática. [NIST800-61, ISO 18044].

AMENAZA: Factor externo que aprovecha una debilidad en los activos de información y puede impactar en forma negativa en la organización. No existe una única clasificación de las amenazas, lo importante es considerarlas todas a la hora de su identificación.

AUTENTICIDAD: Aseguramiento de la identidad respecto al origen cierto de los datos o información que circula por la Red.

AVISO DE IDS SOBRE BUFFER OVERFLOW: Es un error de software que se produce cuando un programa no controla adecuadamente la cantidad de datos que se copian sobre un área de memoria reservada.

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

CONTENCIÓN: Evitar que el incidente siga ocasionando daños.

ERRADICACIÓN: Eliminar la causa del incidente y todo rastro de los daños.

EVENTO DE SEGURIDAD: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad. [ISO/IEC 27000:2009]

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.

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.

IDS: Software de detección de intrusos

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

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

RECUPERACIÓN: Volver el entorno afectado a su estado natural.

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

SSI: Subsistema de Seguridad de la Información.

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

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. GENERALIDADES

Este documento es orientado a los lineamientos y registro dados por el Ministerio de Tecnologías de la Información y Comunicaciones - MinTIC a través de sus decretos y normativa reglamentaria, específicamente en los siguientes componentes:

- Modelo de Seguridad y Privacidad de la Información – MSPI. se apoya en las buenas prácticas establecidas en la norma ISO 27001 de 2022

- Ley 1712 de 2014, por medio de la cual se crea la Ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.

- Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales. Por medio del registro de activos de información se puede determinar la información que debe ser protegida en la Entidad, las características de esta, los responsables de su creación o custodia y el nivel de clasificación que a cada activo de información debe tener. Establecer un inventario de activos de información hace parte de la debida diligencia que a nivel estratégico se ha definido en el Modelo de Seguridad y Privacidad de la Información MSPI y cuyo objetivo es apoyar en la implementación de los siguientes controles de la Guía 8 - Controles de Seguridad de la Información de dicho modelo.

6. ROLES Y RESPONSABILIDADES

Equipo de Respuesta a Incidentes en Seguridad de la Información. (ERISI)

Equipo que tiene como fin la detección y prevención de incidentes en seguridad de la información. Deben contar con la experiencia necesaria para atender las solicitudes de los usuarios en los tiempos establecidos para asegurar los sistemas de información, servicios tecnológicos e infraestructura. Conformado por los siguientes integrantes en orden de prioridad: (ver roles en documento de gobierno TI)

- Especialista en Seguridad de Información.
- Administrador de Servicios Tecnológicos e Infraestructura.
- Ingeniero de Operaciones Gestor de Proyectos.
- Ingeniero de Soporte TI.
- Líder TI.

7. PRINCIPALES FUNCIONES

- Definir un procedimiento para la atención de incidentes en seguridad de la información.
- Clasificar los incidentes en seguridad de la información.
- Monitorear, realizar seguimiento y control sobre los elementos que permitan detectar posibles incidentes de seguridad de la información.
- Recibir y resolver los incidentes de seguridad con base en el procedimiento establecido.
- Realizar toma de muestras digitales, preservación, documentación y análisis de evidencia cuando sea requerida.
- Mantener informados a los colaboradores de la Entidad sobre nuevas vulnerabilidades, actualizaciones en sistemas operativos, herramientas, sistemas de información, sistemas de seguridad de la información entre otros. Así mismo, realizar recomendaciones de seguridad informática a través de los medios de comunicación interna disponibles.
- Realizar verificaciones periódicas del estado de la infraestructura tecnológica, servidores y redes, con el fin de analizar vulnerabilidades y brechas de seguridad.
- Verificar que la implementación de las nuevas aplicaciones y servicios en producción, se ajusten a los requerimientos de seguridad informática definidos por el equipo.
- Administrar de forma adecuada los elementos de seguridad informática tales como consola antivirus, firewall, agentes, entre otros.
- Identificar y priorizar servicios sensibles y aplicaciones expuestas a vulnerabilidades para la prevención y mitigación de ataques.
- Realizar una búsqueda constante de nuevos productos en el mercado o implementar nuevas herramientas para la protección ante brechas de seguridad, proponer iniciativas en seguridad de la información para llevarlas a proyectos de inversión.

8. COLABORADORES (FUNCIONARIOS, CONTRATISTAS, PRACTICANTES)

Encargados de reportar eventos ante vulnerabilidades a la seguridad de los activos de información a través de la herramienta de soporte a usuarios (Osticket). Dispuestos a recibir capacitaciones y participar en las campañas de sensibilización que se programen en la Entidad. Responsables del manejo adecuado de los activos de información y del cumplimiento de las políticas en seguridad de la información.

9. RECURSOS FISICOS

En caso de llegar a ser necesario, el equipo de recursos físicos deberá realizar una valoración económica del activo de información de tipo hardware que llegue a estar involucrado en un incidente de seguridad de la información.

10. TIPOS DE INCIDENTE DE SEGURIDAD

Las partes que conforman el ERISI, los colaboradores y demás miembros activos deben identificar incidentes reconocidos por la Entidad. Los siguientes son incidentes base que serán tenidos en cuenta al realizar su identificación.

- 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

11. CRITERIOS DE CLASIFICACIÓN

11.1. NIVEL DE CRITICIDAD

NIVEL	DESCRIPCIÓN
ALTO	Se compromete seriamente la operación de la Entidad, el incidente puede tener una velocidad significativa de propagación y generar daños sobre los activos de información, la infraestructura, los sistemas de información y servicios tecnológicos.
MEDIO	Se interrumpen de forma temporal las tareas diarias de la Entidad, el incidente compromete activos de información de información, la infraestructura, los sistemas de información y servicios tecnológicos de alta importancia.
BAJO	No interrumpe procesos o tareas generales de la Entidad, el incidente es detectado y controlado fácilmente con los propios recursos de la Entidad.

Tabla 1: Nivel de Criticidad

La tabla muestra los niveles de criticidad de los incidentes y su impacto sobre los activos de información, la infraestructura, los sistemas de información y servicios tecnológicos.

El área encargada de atender el incidente de Seguridad de la información debe conocer la siguiente tabla de escalamiento a fin de darle el tratamiento adecuado

11.2. NIVELES DE ESCALAMIENTO

RELEVANCIA	DESCRIPCIÓN
ALTO	A proveedores pertinentes si aplica y de ser el caso a autoridades judiciales competentes
MEDIO	Al Equipo de Respuesta a Incidentes en Seguridad de la Información. (ERISI) y áreas involucradas
BAJO	De acuerdo con el registro en la herramienta de soporte a usuarios (osticket), realizando escalamiento al administrador de servicios tecnológicos, ingeniero de operaciones TI o técnico de soporte según corresponda

Tabla 2: Niéveles de Escalamiento

La siguiente tabla muestra los niveles de escalamiento y las actividades a desarrollar ante el registro de los incidentes relacionados con seguridad de la información.

11.3. TIEMPOS DE ATENCION

La atención del incidente será definida bajo la escala de tiempo de horas y días relacionada directamente con el nivel de criticidad definido anteriormente. La escala se determina de acuerdo con el tiempo máximo que puede tomarse para atender y poner en marcha la gestión de atención de incidentes en seguridad de la información, entregando un diagnóstico previo a la respuesta final.

CALIFICACIÓN INCIDEDENTE	TIEMPO DE ATENCIÓN
ALTO	2 HORAS
MEDIO	12 HORAS
BAJO	5 DÍAS

Tabla 3: Tiempo de Atención

La siguiente tabla muestra los niveles de escalamiento y las actividades a desarrollar ante el registro de los incidentes relacionados con seguridad de la información.

11.4. DETECCIÓN

La detección de un incidente involucra su detección, verificación para considerar si es un incidente de seguridad de la información, clasificación y reporte a las personas y autoridades que correspondan, de tal forma que los incidentes pueden ser detectados de acuerdo a las siguientes fuentes:

- Sistemas de detección automáticas de intrusiones (IDS/IPS), sistemas de antivirus.
- Sistemas de logs de sistemas de información, firewalls, Proxy, y auditorias
- Reportes de los usuarios de la entidad, de acuerdo a los procedimientos relacionados con la gestión de incidentes en seguridad de la información

11.5. CONTENCIÓN

La contención hace referencia a la forma como será detenido el impacto de un incidente que pueda llegar a tener sobre la infraestructura, los sistemas de información y servicios tecnológicos. Se presentan las acciones de acuerdo a las siguientes clasificaciones:

a. **Criticidad de incidente bajo**: De acuerdo a la verificación del incidente, se pueden realizar acciones tales como reiniciar el servicio o herramienta tecnológico, debe quedar registro con el fin de realizar seguimiento, control y con el fin de poder anticipar incidentes futuros.

b. Criticidad de incidente medio: Acciones administradas por los gestores de los servicios tecnológicos, sistemas de información e infraestructura. A través de una solicitud enviada por los propietarios, se identifica el incidente, donde se pueden realizar acciones como:

- Reiniciar un servicio de información.
- Realizar cambios en las configuraciones
- Desconectar por un periodo corto de tiempo la red
- Destruir la información con previa autorización del propietario.
- Reconstruir y recuperar la información en ambientes de prueba
- Remover privilegios de los usuarios.

c. Criticidad De Incidente Alto: Acciones de mitigación inmediatas, las cuales deben ser ejecutadas por el Equipo De Respuesta a Incidentes en Seguridad de la Información. (ERISI) a través de:

- Reiniciar completamente un sistema de información.
- Deshabilitar por un prolongado periodo de tiempo un servicio tecnológico para determinar la falla.
- Remover privilegios de los usuarios de ser necesario.
- Reconstrucción en ambientes de producción.
- Solicitar contacto con entes externos.

12. ERRADICACIÓN

Pretende la remoción total de la causa del incidente, teniendo en cuenta lo siguiente:

- Identificar las causas del incidente con el fin de ser eliminadas.
- Realizar pruebas después de garantizar la erradicación completa del incidente.
- Evaluar y realizar las restauraciones necesarias después de la erradicación del incidente.
- Revisar procesos, procedimientos, lineamientos, entre otros, con el fin de determinar modificaciones para prevenir futuros incidentes.

13. RECUPERACIÓN

- Las partes interesadas de la gestión de incidentes deben garantizar:
- Recuperar datos y configuraciones de los servicios, sistemas e infraestructura afectadas.
- Recuperar datos y configuraciones.
- Realizar el restablecimiento de los servicios, sistemas e infraestructura afectada.

14. SEGUIMIENTO

Para verificar la normalización de todos los elementos tecnológicos, el equipo de gestión de incidentes deberá:

a. **Documentar El Incidente.** Registrar los datos completos del incidente de acuerdo con un formato diseñado por el equipo de gestión de incidentes. Incluir un estado del incidente (Abierto, Cerrado).
b. **Reporte De Incidente:** El Equipo de Respuesta a Incidentes en Seguridad de la Información. (ERISI) deberá entregar al líder de tecnología un informe semestral con los incidentes y el trato dado.

c. **Lecciones aprendidas:** El Equipo de Respuesta a Incidentes en Seguridad de la Información. (ERISI) deberá presentar un informe semestral con los incidentes, su tratamiento y acciones, con el fin de determinar las acciones necesarias para que no vuelvan a suceder.