Tratamiento de los incidentes de seguridad de la información

Breve descripción:

La gestión de incidentes de seguridad de la información se consolida como estrategias para atender en un mínimo tiempo cualquier evento que ponga en riesgo la seguridad de la misma, a partir de la aplicación de métodos y técnicas para identificar, evaluar, atender y recuperar, garantizando así la continuidad del negocio.

Mayo 2023

Tabla de contenido

Introducción

Las organizaciones se enfrentan a diario a gran variedad de amenazas que ponen en riesgo sus activos de información más preciados y que son necesarios para dar continuidad al negocio, que en algunas ocasiones se vuelve una actividad de tipo “bombero” en la que se busca atender y dar respuesta sin lineamientos o unas instrucciones claras, que permitan establecer planes para atender otros incidentes que surjan en el futuro, aprovechando las vulnerabilidades presentes o alguna otra que sea nueva. El siguiente video presenta la importancia de la gestión de incidentes y la profundización que se tendrá de esta temática a lo largo del componente:

Video 1. Tratamiento de los incidentes de seguridad de la información

Enlace de reproducción del video

Síntesis del video: tratamiento de los incidentes de seguridad de la información
La gestión de incidentes permite adoptar metodologías que contribuyen a organizar procedimental y sistemáticamente las acciones necesarias para hacer frente a cualquier evento que ponga en riesgo la información. Las acciones para una adecuada atención de los incidentes de seguridad de la información inician con una revisión y evaluación de las vulnerabilidades. A partir de allí, se establecen acciones que otorgan una ruta de implementación, y al final del día una serie de lecciones aprendidas. Es así como en este componente formativo se revisarán algunas de las acciones necesarias para evaluar la seguridad digital de la organización y el establecimiento de un plan de gestión de incidentes, el cual será de gran importancia para garantizar una continuidad del negocio. ¡Bienvenidos!

1. Evaluación de la seguridad digital

A medida que las organizaciones van implementando soluciones y estrategias articuladas para la gestión de la ciberseguridad en las organizaciones, se hace necesario que esta sea evaluada para determinar si está siendo efectiva y si no se están aprovechando otras vulnerabilidades, que no han sido identificadas o se estén generando nuevas brechas a la seguridad de la información.

Las normas como la familia ISO 27000 y "frameworks" técnicos como NIST han incorporado dentro de su metodología las fases que llevan a que las estrategias sean evaluadas de tal manera que permita identificar debilidades y a partir de estas establecer nuevos focos de la estrategia de seguridad, teniendo como premisa, que este ejercicio debe ser permanente y continuo, debido a que las amenazas crecen de manera permanente y cada vez son más complejas.

A continuación, se reconocen algunas técnicas que permiten realizar una evaluación de la seguridad digital en las organizaciones y que son el insumo fundamental para determinar la efectividad y eficiencia de la estrategia propuesta:

1.1. Gestión de vulnerabilidades

Este ejercicio de gestionar las vulnerabilidades, que pueden ser aprovechadas para convertirse en una amenaza para una organización, es un trabajo complejo dependiendo el tamaño de la organización y de la cantidad de sus activos de información (es decir cada uno de los recursos de información útil para la organización, así como los que indirectamente son necesarios para que ese dato o información pueda funcionar) tal como se observa la caracterización de dichos tipos de activos de información en la siguiente figura:

Figura 1. Activos de información

Los ejercicios para la gestión de vulnerabilidades pueden variar de acuerdo al tipo de organización y el enfoque que se le quiera dar a la gestión; pues es muy distinto realizar una gestión de vulnerabilidades en una institución financiera o crítica frente a una pequeña o mediana empresa.

El procedimiento para su desarrollo ha sido basado en siete etapas principales que abordan esta gestión, entre las que se encuentran:

Planeación

- Definición de activos.
- Planeación de la evaluación.

Etapa en donde se define el alcance del procedimiento de gestión de vulnerabilidades y se identifica cuál será el campo de evaluación o cuáles activos serán objetos de la revisión.

a) Descubrimiento

- Recopilación de información.
- Mapeo de elementos.

Aquí se realiza la recolección de información sobre las aplicaciones, sistemas o información y de las vulnerabilidades que se encuentran presentes, a partir de ejercicios de escaneos que permita validar sus debilidades; como resultado de esta etapa, se debe de generar un mapeo de los elementos involucrados.

b) Análisis y evaluación del riesgo

- Identificación de brechas.
- Determinar impacto.

En esta etapa se establecen las brechas a la seguridad, identificando el impacto de estas sobre cada uno de los activos de información y cómo puede afectar la organización; en este ejercicio se deben de identificar y priorizar aquellas vulnerabilidades que se consideren críticas.

c) Definición de planes de acción

- Diseño plan de mitigación.
- Determina controles.

Esta etapa debe consolidar el plan para la adopción de acciones correctivas para el control de las vulnerabilidades; estas acciones se pueden tipificar en:

- **Controles correctivos**: controles aplicados directamente sobre sistemas o aplicaciones vulnerables.
- **Controles compensatorios:** controles aplicados indirectamente sobre los sistemas vulnerables.

d) Ejecución de plan de acción

- Implementa controles y acciones.

En esta etapa se deben de desplegar e implementar las acciones propuestas en el plan de acción, bajo los tiempos y condiciones establecidas.

e) Verificación de la efectividad

- Verifica planes y acciones.

Consiste en realizar la evaluación de las acciones aplicadas para determinar su validez y asertividad en la reducción a las brechas de seguridad; en algunas ocasiones, se requerirá de evaluar nuevamente o aplicar otras técnicas con el fin de garantizar su efectividad.

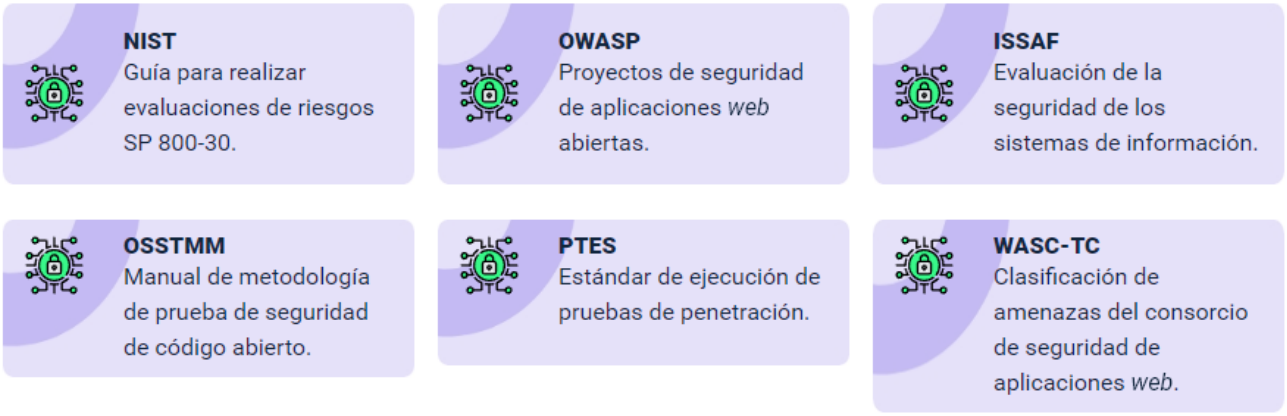
f) Lecciones aprendidas

- Revaluar y mejorar el proceso de gestión de vulnerabilidades.

En esta última etapa, busca que el trabajo realizado sea material de insumo para la mejora del mismo proceso, a partir de los casos acertados como de los que no fueron.

A partir de estas etapas anteriormente descritas, han surgido diferentes alternativas para este ejercicio, como se puede apreciar en la siguiente figura:

Figura 2. Metodologías para la gestión de vulnerabilidades



De las cuales se profundizará en algunas de ellas:

NIST

Este marco de trabajo para la mejora de la seguridad cibernética en infraestructuras críticas, el cual fue generado por el Gobierno de los Estados Unidos a mediados del año 2014, brinda a las organizaciones la metodología para la reducción de riesgos cibernéticos a partir de una adecuada gestión de riesgos.

Este marco de trabajo propone la gestión desde una serie de funciones, las cuales se desarrollan de manera simultánea y continua como son: Identificar, Proteger, Detectar, Responder y Recuperar. Estas funciones del marco de trabajo, conlleva a desarrollar una serie de actividades basadas en categorías, encaminadas a reducir los riesgos que se pueden presentar y afectar la información de una organización.

A continuación, se puede observar un resumen de estas categorías y actividades que se desarrollan para la adecuada gestión de vulnerabilidades:

Identificar (ID)

Función identificador único	Funciones
ID	IDENTIFICAR

Categoría Identificador Único	Categorías
ID.AM	Gestión de activos
ID.BE	Ambiente de negocios
ID.GV	Gobernanza
ID.RA	Evaluación de riesgos
ID.RM	Estrategia de gestión de riesgos
ID.SC	Gestión del riesgo de la cadena de suministro

Proteger (PR)

Función identificador único	Funciones
PR	PROTEGER

Categoría Identificador Único	Categorías
PR.AC	Gestión de identidad, autenticación y control de acceso
PR.AT	Conciencia y capacitación
PR.DS	Seguridad de datos

Categoría Identificador Único	Categorías
PR.IP	Procesos y procedimientos de protección de la información
PR.MA	Mantenimiento
PR.PT	Tecnología de protección

Detectar (DE)

Función identificador único	Funciones
DE	DETECTAR

Categoría Identificador Único	Categorías
DE.AE	Anomalías y eventos
DE.CM	Monitoreo continuo de seguridad
DE.DP	Procesos de detección

Responder (RS)

Función identificador único	Funciones
RS	RESPONDER

Categoría Identificador Único	Categorías
Planificación de respuesta	Planificación de respuesta
Comunicaciones	Comunicaciones
Análisis	Procesos de detección
Mitigación	Mitigación
Mejoras	Mejoras

Recuperar (RC)

Función identificador único	Funciones
RC	RECUPERAR

Categoría Identificador Único	Categorías
RC.RP	Planificación de la recuperación
RC.IM	MEJORAS
RC.CO	Comunicaciones

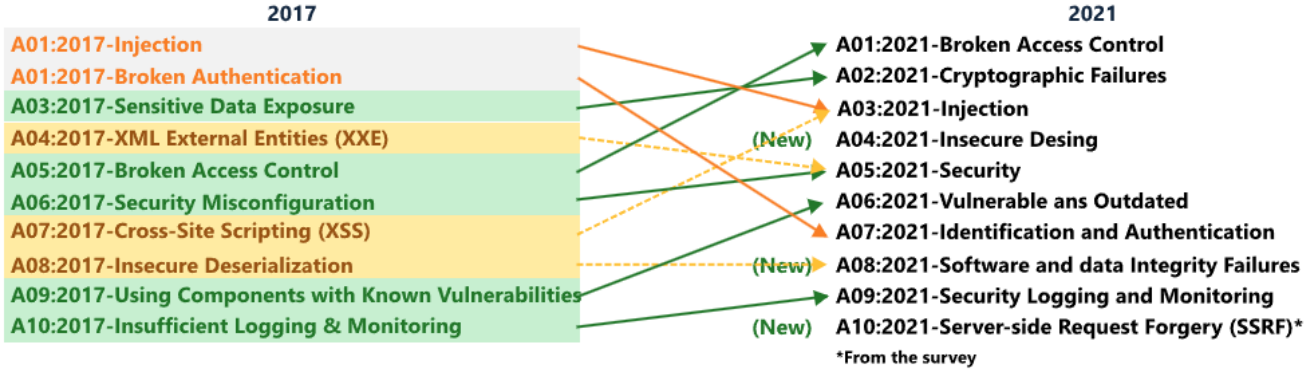
NIST. Aunque este ha sido propuesto para infraestructuras críticas, se puede aplicar a cualquier tipo de organización, lo que lo hace un método muy llamativo para entidades del gobierno. Consulte la versión completa del documento desde su sitio oficial. Este recurso también está en el material complementario. Enlace Página oficial NIST

OWASP

Es una organización sin fines lucrativos, la cual busca ayudar a visibilizar las vulnerabilidades en aplicaciones para su mejoramiento de la seguridad a partir de una adecuada gestión del riesgo, siendo este un pilar fundamental para el desarrollo y aplicación de su metodología.

Owasp provee de un "framework" abierto el cual permite implementar auditorías en aplicaciones principalmente de tipo web, basados esencialmente en pruebas de caja blanca y caja negra. A partir de su ejercicio identifica las vulnerabilidades más representativas y presentes en la actualidad en su Owasp top 10. En su último reporte, el Owasp Top 10 2021 se puede apreciar la siguiente clasificación frente al informe previo del año 2017:

Figura 3. Owasp Top 10 – 2021



Nota. Tomado de OWASP (2021)

Con base en este reporte, se analiza el comportamiento de las vulnerabilidades identificadas, así:

Pérdida del control de acceso (“Broken Access Control”)

El control de acceso permite cumplir una política de permisos y roles. Estas restricciones implican que los usuarios no puedan actuar fuera de los permisos y, además, llevar un control de quien accede a cada recurso. La vulnerabilidad “Broken Access Control” permite que un usuario sin privilegios pueda acceder a un recurso al que no tendría que acceder.

¿Qué impacto puede tener esto en una empresa?

- Un ciberdelincuente podría actuar en el sistema con permisos de usuario o administrador.
- Acceso a registros, directorios o archivos confidenciales para su posterior posible divulgación.

Fallos criptográficos (“Cryptographic Failures”)

Hay ciertos datos que deben estar cifrados, como credenciales de acceso, datos bancarios, información confidencial de la empresa, etc., ya que aparte de que la ley lo exija, el que un ciberdelincuente se pueda hacer con ellos puede ser catastrófico para la empresa. En resumen, para que estos sean vistos únicamente por las personas autorizadas de la empresa hay que aplicarles un cifrado con algoritmos y protocolos estándares y robustos.

¿Qué impacto puede tener esto en una empresa?

- Exposición de datos sensibles a un ciberdelincuente (datos personales, críticos o estratégicos para la empresa; credenciales…).

Inyección (“Injection”)

Esto sucede cuando un ciberdelincuente puede enviar datos dañinos a un intérprete. Como novedad este año, el Cross-site Scripting forma parte de esta categoría. Para ello, hay que tener API seguras y controles de verificación a la hora de introducir los datos.

¿Qué impacto puede tener esto en una empresa?

- Exposición y posible modificación de datos sensibles por parte de un ciberdelincuente.
- Bajo ciertas circunstancias podría permitir al ciberdelincuente tomar el control del servidor.

Diseño inseguro (“Insecure Desing”)

A la hora de desarrollar una aplicación web es primordial incluir la seguridad de la aplicación desde la fase del diseño, ya que este año se ha incluido esta nueva categoría debido a la gran cantidad de aplicaciones que no la cumplen. Muchas aplicaciones cuentan con defectos en el diseño de las mismas.

¿Qué impacto puede tener esto en una empresa?

- Exposición y posible modificación de datos por un ciberdelincuente.
- Acceso al servidor/aplicación por parte de un ciberdelincuente con permisos de administrador o usuario.

Configuración de seguridad defectuosa (“Security Misconfiguration”)

En nuestro entorno de la aplicación web, los ciberdelincuentes intentarán acceder mediante cuentas por defecto, versiones obsoletas con vulnerabilidades sin actualizar, directorios desprotegidos, etc. Por ello, tiene que estar todo bien configurado y evitar usar credenciales por defecto, como puede ser en el caso de nuestro servidor, aplicaciones o dispositivos.

¿Qué impacto puede tener esto en una empresa?

- Acceso no autorizado al sistema por parte del ciberdelincuente

Componentes vulnerables y obsoletos (“Vulnerable and Outdated Components”)

Un ciberdelincuente podrá comprometer un sistema mediante vulnerabilidades ya conocidas en componentes comunes, como por ejemplo la versión del sistema operativo o aplicaciones instaladas en el servidor, entre otras.

¿Qué impacto puede tener esto en mi empresa?

- Algunas de estas vulnerabilidades pueden tener un impacto pequeño, pero las mayores brechas de seguridad se han producido mediante la explotación de este tipo de vulnerabilidades.

Fallos de identificación y autenticación (“Identification and Authentication Failures”)

Esto sucede cuando en las interfaces de acceso no se controla el número de intentos de autenticación, hay una baja complejidad de las contraseñas o no se implanta un sistema multifactor “2FA”. Esto podría permitir a un ciberdelincuente

realizar ataques de fuerza bruta o diccionario para ingresar en él o cuando tu aplicación permite utilizar contraseñas débiles.

¿Qué impacto puede tener esto en una empresa?

- Los ciberdelincuentes tendrán acceso a cuentas administrativas o de empleados en la aplicación.

Fallos en el "software" y en la integridad de los datos ("Software and Data Integrity Failures")

Muchas aplicaciones se actualizan de manera automática. Cuando estas actualizaciones no son verificadas los ciberdelincuentes podrían modificarlas cargando sus propias actualizaciones y distribuyéndolas.

¿Qué impacto puede tener esto en una empresa?

- Inclusión de código no deseado por un ciberdelincuente en mi aplicación.

Fallos en el registro y la supervisión de la seguridad ("Security Logging and Monitoring Failures")

La falta de registros sobre eventos, los denominados logs, en la aplicación o en el sistema, como inicios de sesión (tanto válidos como fallidos). Por ejemplo: que estos registros no se almacenen remotamente impide que se puedan detectar las infracciones.

¿Qué impacto puede tener esto en mi empresa?

- Desconocimiento sobre inicios de sesión no autorizados.
- Desconocimiento sobre los actos de un ciberdelincuente en nuestro sistema.

Falsificación de Solicitud del Lado del Servidor (“Server-side Request Forgery o SSRF”)

Cuando nuestra aplicación web obtiene un recurso externo y este no valida la URL un ciberdelincuente podría modificarla con fines malintencionados y realizar peticiones no autorizadas.

¿Qué impacto puede tener esto en una empresa?

- Robo de datos sensibles de la empresa.
- Acceso a sistemas internos de la empresa

Dado lo anterior, owasp, se ha vuelto una metodología práctica para la identificación de vulnerabilidades en las aplicaciones web más utilizadas por los equipos de desarrollo en los últimos años. Se sugiere explorar y hacer uso de esta metodología, consultando su documento oficial. Este recurso también está en el material complementario. Enlace documentación owasp

ISSAF

Es un marco de trabajo para el testeo e identificación de vulnerabilidades de seguridad estructurado en tres fases. Esta metodología está enfocada en realizar análisis de seguridad a partir de los resultados obtenidos, a continuación, se observa un esquema general de sus fases y su respectiva conceptualización:

a) **Planeación y preparación**

Establece los pasos iniciales para el desarrollo de la auditoría y ejercicios de testeo.

Entre las actividades relacionadas se encuentran: Identificación de interesados, reuniones de apertura, definición de enfoque y metodología, cronograma de tiempo.

b) Evaluación

En esta fase, se desarrollan las validaciones de acuerdo a las siguientes 9 capas:

- Capa 1: Reconocimiento de información
- Capa 2: Mapeo de la red de trabajo
- Capa 3: Identificación de vulnerabilidades
- Capa 4: Penetración
- Capa 5: Obtención de accesos y escalamiento de privilegios
- Capa 6: Enumeración
- Capa 7: Compromiso de usuarios y sitios remotos
- Capa 8: Mantener el acceso
- Capa 9: Cubrir rastros

c) Reportes, limpieza y destrucción de objetos

Fase donde se analizan las pruebas, consolidan resultados y se presenta los reportes a los interesados.

Este proyecto lleva varios años sin mantenimiento, pero se puede consultar el texto completo de la metodología en el enlace. Este recurso también puede ser consultado en el material complementario. Enlace Metodología ISSAF

OSSTMM

Esta metodología para pruebas de seguridad también es muy utilizada y, debido a su aplicación tan extensa, se ha convertido en un estándar de facto para el desarrollo de auditorías de seguridad, ya que proporciona un marco de trabajo que describe las actividades a desarrollar, las cuales están comprendidas como se presentan a continuación:

Sección A -Seguridad de la Información

- Revisión de la Inteligencia Competitiva
- Revisión de Privacidad
- Recolección de Documentos

Sección B - Seguridad de los Procesos

- Testeo de Solicitud
- Testeo de Sugerencia Dirigida
- Testeo de las Personas Confiables

Sección C - Seguridad en las tecnologías de Internet

- Identificación de los Servicios del Sistema de
- Logística y Controles
- Exploración de Red
- Identificación de los Servicios del Sistema
- Búsqueda de Información Competitiva
- Revisión de Privacidad

- Obtención de Documentos
- Búsqueda y Verificación de Vulnerabilidades
- Testeo de Aplicaciones de Internet
- Enrutamiento
- Testeo de Sistemas Confiados
- Testeo de Control de Acceso
- Testeo de Sistema de Detección de Intrusos
- Testeo de Medidas de Contingencia
- Descifrado de Contraseñas
- Testeo de Denegación de Servicios
- Evaluación de Políticas de Seguridad

Sección D - Seguridad en las Comunicaciones

- Testeo de PBX
- Testeo del Correo de Voz
- Revisión del FAX
- Testeo del Modem

Si se desea profundizar detalles de esta metodología, se puede consultar su sitio oficial; el cual también se encuentra ubicado en el material complementario. Enlace sitio web oficial ISECOM

PTES

Se consolida como estándar para pruebas de penetración y "testing", que puede ser aplicado en cualquier organización. Entre sus objetivos se encuentra el de

disponer de un marco de trabajo para la realización de auditorías técnicas de seguridad en sistemas de información. Se desarrolla en las siguientes siete fases:

Lo invitamos a consultar con más detalle esta metodología a través de su sitio oficial, el cual también se encuentra en el material complementario. Enlace sitio web PTES Technical Guidelines

Las metodologías anteriormente descritas permitirán realizar un análisis de vulnerabilidades, establecer planes de acciones y un proceso importante, que es adoptar planes de mejoramiento al interior, dado que el proceso de gestión de vulnerabilidades debe ser un proceso continuo.

1.2. Tipo de pruebas

Cuando se está desarrollando el proceso de evaluación de la seguridad, se debe de garantizar que los resultados presentados estén respaldados en ejercicios de verificación y comprobación que permitan establecer si una condición se está cumplimento o no; para este caso estamos hablando de controles, técnicas, tácticas

para el aseguramiento de la información y en este ejercicio pueden surgir diferentes alternativas para verificar este tipo de cumplimientos, entre las que se pueden apreciar:

- **Pruebas unitarias**. Este tipo de pruebas se enfocan en testear fragmentos de código o aplicaciones para evaluar la lógica bajo la cual se ha programado y si desarrolla adecuadamente las tareas bajo ciertas condiciones.
- **Pruebas de integración**. Estas pruebas, buscan verificar el desarrollo de una actividad que involucra más de un componente, por ejemplo, la lógica de una aplicación web y la de un motor de base de datos.
- **Pruebas de extremo a extremo**. Estas buscan verificar el traslado de información y cómo viajan entre un punto de origen y uno de destino, este tipo de pruebas son comunes cuando se prueban API's o plataformas de envío de mensajes.
- **Prueba de aceptación**. Este tipo de pruebas, busca validar si una solución cumple con lo requerido o solicitado por un cliente.
- **Pruebas de caja blanca**. Este tipo de pruebas validan el comportamiento de la lógica de la solución, para realizar este tipo de pruebas, se asume que conoce los detalles de su arquitectura, métodos, funciones entre otros.
- **Pruebas de caja negra**. Este tipo de pruebas son de funcionalidad y comportamiento de un sistema, por lo general desconociendo la estructura de la solución.
- **Pruebas de caja gris**. Propone una validación, combinando las pruebas de caja blanca y caja negra, permitiendo abordar aspectos más complejos e integrales en las soluciones.

- **Prueba manual**. Son pruebas que se especifican manualmente y sin automatización, para la evaluación de los resultados obtenidos.
- **Prueba estática**. Son aquellas que se realizan sin código real, para determinar si hay defectos en el rendimiento de la solución.
- **Pruebas dinámicas**. Este tipo de pruebas se ejecuta con código real para validar su funcionamiento.
- **Pruebas visuales o de interfaz de usuario**. Son las pruebas que se realizan a interfaces de usuario para la revisión del comportamiento y la integridad de la información.
- **Pruebas de humo**. Tipo de prueba que se realiza a un conjunto pequeño de controles para verificar su funcionalidad.
- **Pruebas de regresión**. Permite validar si una funcionalidad o característica se rompe o no está funcionando como se propuso.
- **Pruebas de carga**. Este tipo de pruebas buscan verificar el comportamiento de una solución de acuerdo a diferentes momentos de demanda del servicio.
- **Pruebas de inserción**. Este tipo de pruebas permite verificar la integridad de la seguridad de la información dentro de la solución.

Existen varios tipos de pruebas que se pueden realizar a las aplicaciones o soluciones con las que cuenta la organización que permite verificar si realmente están realizando las operaciones según lo solicitado y lo establecido en el programa.

Su aplicación dependerá del alcance de la evaluación a realizar, así como también dependerá si las soluciones son construidas “in-house” o son adquiridas a un tercero,

en cualquiera de los casos, debería de validarse la información para garantizar su integridad.

1.3. Hacking ético

Para conocer los fundamentos de hacking ético y seguridad informática, lo invitamos a ver el siguiente video.

Fundamentos de “hacking” ético y seguridad informática, lo invitamos a ver el siguiente video:

Video 2. Fundamentos de “hacking” ético y seguridad informática

Enlace de reproducción del video

Síntesis del video: fundamentos del “hacking” ético y seguridad informática
El video presenta la importancia del “hacking” ético y la seguridad informática en el mundo digital. Destaca que la información se ha convertido en un activo crucial y que existen amenazas tanto internas como externas que pueden poner en riesgo los sistemas y los datos almacenados. Se menciona que las empresas y las personas enfrentan constantemente problemas de ciberseguridad, y se resalta el aumento de los datos pirateados y violados. Se destaca la necesidad de tomar conciencia sobre la seguridad cibernética y de implementar prácticas efectivas para proteger los datos. Además, se menciona el aumento de los costos asociados a los delitos cibernéticos y la importancia de invertir en seguridad. Por último, se hace referencia a los diferentes tipos de ataques, como el “phishing”, la ingeniería social, los ataques de denegación de servicio distribuido DDoS, el “malware” y el “ransomware”, entre otros.

El “hacking” ético o también denominado sombrero blanco, es un conjunto de técnicas que se aplican para el descubrimiento de vulnerabilidades dentro de un entorno o un conjunto de aplicaciones.

Esta técnica se desarrolla de manera consentida y aprobada por las organizaciones y los responsables de realizar las validaciones correspondientes, con lo cual buscan identificar las debilidades, anormalidades y falencias en su seguridad.

Los expertos que realizan este tipo de validaciones hacen uso de técnicas especializadas que se denominan “Test” de Penetración o “Pentesting”, y su objetivo es burlar los controles de seguridad y en caso de conseguir una identificación positiva, este deberá reportarlo a la organización. Este tipo de estrategia no debería de causar daño, dado que es concebido y tiene fines de exploración.

Ahora, lo invitamos a ver el video sobre las metodologías del “hacking”.

Video 3. Metodologías del hacking ético

Enlace de reproducción del video

Síntesis del video: metodologías del “hacking” ético
El “hacking” ético es el acto de acceder a los sistemas y redes para descubrir las posibles amenazas en esos sistemas. También es un proceso para quebrantar las vulnerabilidades de la red que un atacante malintencionado pudiera explorar, causando pérdidas de datos, pérdidas financieras y otros daños importantes. En cuanto a su metodología, los “hackers” éticos utilizan los mismos métodos e instrumentos que los “hackers” maliciosos (sombrero negro), tras el permiso de

un usuario autorizado. Mientras que, por otra parte, los piratas informáticos malintencionados utilizan los métodos de una manera deshonrosa e ilegal.

Actualmente, se está realizando un esfuerzo por dotar de una metodología estable y efectiva a las tareas de "testing". Con frecuencia, si no se estandarizan las pruebas a realizar sobre un sistema, resulta complejo evaluar el resultado de las mismas. Hay diversos factores que interfieren de forma significativa, tanto aspectos técnicos como de personalidad de los desarrolladores.

El definir una serie de pautas, procedimientos y metodologías permitirá obtener una información imparcial que pueda ser comprobable y repetible, y que sirva para hacer un seguimiento sobre el alineamiento de las necesidades del cliente. De este modo, quedarán definidas qué pruebas se realizan y de qué forma se ejecutan.

Este ejercicio se desarrolla básicamente en las siguientes 5 fases:

Fase 1 - Reconocimiento

Preparación del escenario, hace uso de diferentes técnicas para el descubrimiento de pistas que le permitan alcanzar su objetivo.

- Ingeniería social.
- "Dumpster diving".
- "Footprinters".

Fase 2 - Escaneo

A partir de la información recolectada, inicia con el escaneo con la ayuda de herramientas para la búsqueda de vulnerabilidades.

- Escáner de puertos.
- Escáner de vulnerabilidades.

Fase 3 - Obtener acceso

Fase en la cual explota las vulnerabilidades encontradas.

- Inyección de código.
- Basado en web.
- Basado en red.
- Ingeniería social.
- Ataque de contraseñas.
- “Network spoofung”.
- “Network sniffers”.

Fase 4 - Mantener acceso

Fase en donde mantiene el sistema vulnerable.

- “Back Doors”.
- Troyanos.
- “Rootkit”.
- “Keyloggers”.
- “Botnets”.

Fase 5 - Cubrir huella

Fase en la cual cubre todas las pistas de las acciones realizadas durante el ejercicio.

- Troyanos.
- 2Rootkit".
- Esteganografía.
- "Tuneling".

Ahora bien, dependiendo de su alcance, se puede determinar el tipo de hacker requerido, tal como se evidencia en el siguiente video e infografía.

Video 4. Tipos de hacker

Enlace de reproducción del video

Síntesis del video: tipos de hacker
En este video se aborda la controvertida definición del término "hacker". Se discute cómo los programadores informáticos diferencian entre los “hackers”, que poseen un conocimiento avanzado de computadoras y redes, y los “crackers”, quienes irrumpen en sistemas informáticos de manera ilegal. Los “hackers” de sombrero negro (“crackers”) buscan obtener acceso no autorizado y causar daño, mientras que los “hackers” de sombrero blanco (“hackers” éticos) realizan pruebas de penetración y evaluaciones de vulnerabilidad para identificar debilidades sin dañar los sistemas. Además, se mencionan los “hackers” de sombrero gris, que explotan vulnerabilidades sin intenciones maliciosas, y los “hacktivistas", quienes utilizan la tecnología para promover mensajes sociales o políticos, a menudo mediante acciones disruptivas en sistemas informáticos seguros.

Figura 4. Tipos de “hacker”

Estos ejercicios son muy comunes cuando las organizaciones quieren identificar vulnerabilidades presentes en sus sistemas, y requieren que una persona externa desarrolle esta actividad, pero siempre mediando algún acuerdo de confidencialidad y naturalmente una autorización de por medio.

1.4. Equipos de seguridad "Red Team & Blue Team"

Los equipos de seguridad "Red Team & Blue Team" se consolidan como estrategias para organizaciones más complejas y de mayor tamaño y como su nombre lo indica, está conformado por equipos de personas quienes, desde cada uno de sus grupos, realizan acciones para la identificación de vulnerabilidades.

Este concepto proviene de elementos relacionados con entrenamiento militar, los cuales fueron adoptados por la disciplina de la ciberseguridad y que incorporaron para establecer estrategias de auditoría desde dos frentes distintos. Veamos:

Comparación entre el Red Team y el Blue Team

"Red team". Busca burlar la seguridad de la organización, y simular ataques para la identificación de vulnerabilidades, haciendo uso de técnicas de "pentesting", herramientas especializadas e incluso de técnicas de recolección de información convencionales, todo esto realizándose desde el exterior de la organización; lo anterior teniendo en cuenta:

- Seguridad ofensiva.
- Hackeo ético.
- Explotación de vulnerabilidades.

- Pruebas de penetración.
- Pruebas de caja negra.
- Ingeniería social.
- Escaneo de aplicaciones web.

Entre sus actividades se encuentran:

- Pruebas de penetración en las que un miembro del equipo rojo intenta acceder al sistema utilizando una variedad de técnicas del mundo real.
- Tácticas de ingeniería social, que tienen como objetivo manipular a los empleados u otros miembros de la red para que compartan, divulguen o creen credenciales de red.
- Interceptar la comunicación para mapear la red u obtener más información sobre el entorno para eludir las técnicas de seguridad más comunes.
- Clonación de tarjetas de acceso de un administrador para obtener acceso a áreas sin restricciones.

"**Blue team**". Hacen frente a los ataques y defienden a la organización de los posibles riesgos de seguridad de la información, convirtiéndose en una primera línea frente a la atención a cualquier incidente de seguridad; teniendo en cuenta:

- Seguridad defensiva.
- Protección de infraestructura.
- Control de daños.
- Respuesta al incidente.
- Seguridad operacional.
- Caza de amenazas.

- Forense digital.

El trabajo desarrollado por este equipo azul está enfocado en la prevención, detección y remediación. Incorporan las siguientes capacidades:

- Comprensión completa de la estrategia de seguridad de la organización.
- Habilidades de análisis para identificar con precisión las amenazas más peligrosas y priorizar las respuestas en consecuencia.
- Técnicas de endurecimiento para reducir la superficie de ataque, particularmente en lo que se refiere al sistema de nombres de dominio (DNS) para prevenir ataques de “phishing” y otras técnicas de violación basadas en la web.
- Gran conocimiento de las herramientas y sistemas de detección de seguridad existentes de la empresa y sus mecanismos de alerta.

Sumado a lo anterior, contar con estos equipos en las organizaciones puede fortalecer a la empresa a través de estos beneficios:

- Identificación de configuraciones erróneas y brechas a la seguridad.
- Fortalecimiento de la seguridad de la red para detectar ataques dirigidos y mejorar el tiempo de ruptura.
- Aumentar la competencia sana entre el personal de seguridad y fomentar la cooperación entre los equipos de TI y seguridad.
- Aumentar la conciencia entre el personal sobre el riesgo de vulnerabilidades humanas que pueden comprometer la seguridad de la organización.

- Desarrollar las habilidades y la madurez de las capacidades de seguridad de la organización dentro de un entorno de capacitación seguro y de bajo riesgo.

Estas son algunas de las estrategias para la evaluación de la seguridad de la información en las organizaciones. Su elección dependerá del tipo, complejidad, tamaño y alcance de la evaluación que se quiera realizar.

2. Gestión de incidentes de seguridad digital

Actualmente, la gestión de incidentes se establece en las organizaciones como una capacidad para hacer frente a los diferentes requerimientos e incidentes que se presentan cada día, desarrollando actividades enmarcadas en buenas prácticas buscando regresar las operaciones de la organización a su estado normal en un tiempo mínimo.

Esta tendencia de apropiar los procedimientos para la gestión de incidentes busca que las organizaciones cuenten cada día con estrategias para afrontar de una manera muy rápida y casi que sistemática a su estado normal de operaciones, reduciendo el tiempo fuera de línea o reduciendo pérdida de activos de información.

Antes de dar paso a las temáticas asociadas, es importante tener clara la definición del término incidente y es que de acuerdo a la Norma ISO-IEC 27035:2012. Un incidente de seguridad de la información se define como:

“Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazas la seguridad informática” (ICONTEC, 2012)

Con este concepto claro, vamos ahora a revisar algunos aspectos importantes para la adopción de un modelo de gestión de incidentes:

2.1. Normatividad relacionada

Como todo procedimiento tecnológico que está regulado, la gestión de incidentes se fundamenta en estándares para la atención y remediación de los

incidentes que se pueden presentar en una organización; es así como se encuentran los siguientes referentes interesantes:

- GTC-ISO-IEC 27035:2012 - Gestión de incidentes de seguridad de la información.
- NIST SP 800-61 Rev. 2- Guía de manejo de incidentes de seguridad informática.

A continuación, se explica cada uno de estos:

GTC-ISO-IEC 27035:2012 - Gestión de incidentes de seguridad de la información

Esta norma técnica es una de las principales que existe actualmente y sirve como base para el establecimiento de otras normas y marcos de trabajo para la gestión de incidentes de seguridad informática. Proporciona los lineamientos necesarios para la adopción en una organización y prepararse para atender cualquier tipo de incidente.

Además, se vincula con las estrategias de seguridad de las organizaciones para la implementación de controles y procedimientos que posibiliten la continuidad del negocio reduciendo el impacto por alguna amenaza materializada. Sugiere cinco fases establecidas para la gestión de los incidentes de seguridad, como se enumeran a continuación:

Fases Gestión de incidentes ISO – IEC 27035:2012

Planificación y recuperación

- Establece la política para la gestión de incidentes de seguridad.
- Establece políticas para la gestión de riesgos y seguridad de la información.

- Define esquema de gestión de incidentes de seguridad de la información.
- Establece el ISIRT (Equipo de respuesta a incidentes de seguridad de la información):
    - Establecimiento del esquema de soportes
    - Instrucción y formación para la toma de conciencia relacionada con la gestión de incidentes de seguridad de la información.
    - Pruebas del esquema de gestión de incidentes de seguridad de la información.

Detección y reporte

Detecta y reporta los eventos de seguridad de la información.

Evaluación y decisiones

Evaluación de los eventos de seguridad de la información, para la determinación si corresponde a un incidente de seguridad de la información.

Respuestas

- Respuestas a los incidentes presentados, incluyendo análisis forense
- Recuperación del incidente de seguridad de la información.

Lecciones aprendidas

- Análisis forense complementario.
- Identificación de lecciones aprendidas.
- Identificación y establecimiento de las mejoras a la seguridad.
- Identificación y establecimiento de las mejoras a la evaluación de riesgos de la seguridad de la información.

- Identificación y establecimiento de mejoras al esquema de gestión de incidentes de seguridad de la información.

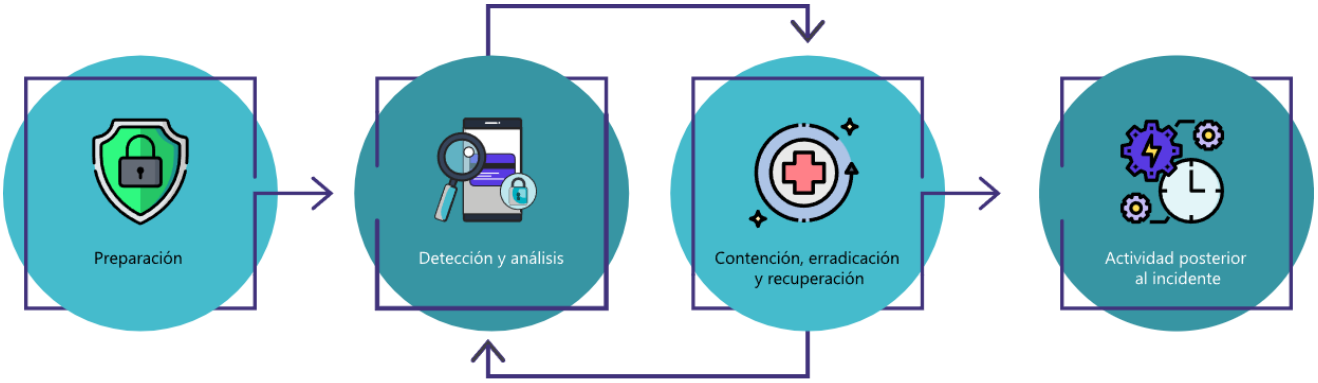
Esta norma es de las más adoptadas por las organizaciones, ya que su modelo permite su fácil adopción y alineación con sistemas de gestión como los SGSI.

NIST SP 800-61 Rev. 2- Guía de manejo de incidentes de seguridad informática

El Instituto Nacional de Normas y Tecnología NIST nos hace entrega de la guía de incidentes para seguridad informática, la cual dicta los lineamientos para la gestión de la seguridad de la información de acuerdo a su correspondiente análisis y metodología de evaluación.

Esta guía en su metodología también propone unas fases para la atención de incidentes de seguridad, como se puede apreciar en su esquema de ciclo de vida:

Figura 5. Ciclo de vida de la atención de incidentes según NIST SP 800-61 Rev. 2



Preparación

Busca reducir el número de incidentes de seguridad de la información, a partir de la selección e implementación de controles de seguridad seleccionados a partir de un

análisis de riesgos previo, además, es necesario el establecimiento de contactos y los planes de comunicación con terceros con el fin de establecer medios de comunicación.

Detección y análisis

En esta fase se identifican las brechas a la seguridad de la información e iniciar el alertamiento a los responsables del proceso de acuerdo a la ruta de atención establecidas y los patrones que represente el incidente.

Esta fase considera tres pasos para la gestión de riesgos de terceros, como son:

- Investigar indicadores de incidentes pasados e indicios de posibles incidentes futuros.
- Implementar un sistema de seguimiento de problemas para registrar toda la información pertinente sobre cada incidente.
- Priorizar los incidentes en función de su impacto funcional, el impacto de la información y la capacidad de recuperación.

Contención, erradicación y recuperación

A partir del establecimiento de la gravedad del incidente, la organización puede mitigar su impacto conteniéndolo y recuperándose de él. En esta fase, se vuelve a la detección y el análisis, por ejemplo, para ver si hay hosts adicionales infectados por "malware" mientras se erradica el incidente.

La contención varía de acuerdo al tipo de incidente y para establecer una acción de respuesta se evalúan diferentes criterios, incluida la necesidad de preservación de evidencia para cualquier procedimiento legal posterior, el daño potencial, la disponibilidad del servicio o los recursos disponibles. La guía indica algunas formas de identificar hosts atacantes como la validación de las direcciones IP, usar bases de datos

de incidentes y monitorear los canales de comunicación del atacante. El monitoreo de riesgos cibernéticos de terceros puede ayudar con estos esfuerzos.

Finalmente, en la erradicación se busca eliminar el "malware", desactivar las cuentas comprometidas y mitigar vulnerabilidades, y en la recuperación se intenta restaurar los sistemas. Las plataformas de gestión de riesgos de terceros ayudan a la corrección a fin de evitar futuras exposiciones de seguridad.

Actividad posterior al incidente

Una vez que el incidente sea controlado y gestionado, la organización genera los reportes que presentan la causa, el costo del incidente y las acciones que se deben de realizar para prevenir futuros incidentes. Los datos como el tiempo dedicado a manejar incidentes y las evaluaciones objetivas y subjetivas de incidentes se pueden utilizar para identificar debilidades de seguridad sistémica.

Este guía para la gestión de incidentes también ha cobrado fuerza entre las organizaciones, por su fácil aplicabilidad y por la aplicabilidad incluso de terceros de la organización.

2.2. Aplicación

Desde el punto de vista metodológico y para las organizaciones colombianas, el MinTIC, ha generado una guía para la adopción de estos planes en las organizaciones tanto públicas principalmente pero no excluye las entidades privadas. Esta guía se denomina "Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información" y establece los lineamientos para su adopción de acuerdo como se presenta a continuación.

Procesos de la gestión de incidentes de seguridad de la información

Prevención

La entidad debe prepararse antes de la materialización de una amenaza; el equipo de Csirt Gobierno establece recomendaciones referentes a la configuración de últimas actualizaciones en sistemas operativos, servicios y aplicaciones. Es necesario que se cuente con campañas de concienciación y sensibilización hacia los funcionarios en materia de ciberseguridad.

Protección y detección

El equipo de especialistas de Csirt Gobierno dispone de aptitudes como investigación, servicios proactivos, así como reactivos frente a eventos e incidentes presentados en portales web y servicios de las entidades gubernamentales. Las anormalidades observadas en el monitoreo constante, se informan a las organizaciones afectadas. Adicional, se debe contar con herramientas como es el caso del SIEM, que permitan correlacionar eventos asociados a amenazas.

En esta fase se remiten análisis de la amenaza, directorios en donde se establece persistencia de la misma e indicadores de compromiso que deben ser incluidos en los dispositivos perimetrales con el fin de proteger la infraestructura tecnológica de la entidad.

Respuesta y comunicación

En esta etapa se recomienda a la entidad dependiendo de la criticidad del evento y de sus consecuencias, aislar equipos, detener servicios y deshabilitar cuentas de

usuarios entre otros; alterno, se realiza un análisis más profundo de la amenaza para indicar ubicaciones en la infraestructura tecnológica donde puede existir una copia del "malware" o de artefactos asociados a este. La evidencia se conserva para entender el comportamiento de la campaña.

Es sumamente importante el establecimiento constante y desde un primer instante con la entidad, desde la evidencia del incidente hasta la mitigación y seguimiento; remitiendo procedimientos de respuesta a incidentes y de seguridad de la información; adicional a esto, se actúa de manera colaborativa reportando cuando sea pertinente al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT).

Recuperación y aprendizaje

Mediante recomendaciones emitidas por Csirt Gobierno, es necesario concienciar a la entidad y a sus funcionarios acerca de los vectores de infección y propagación de la amenaza, adoptando mecanismos necesarios para restablecer la infraestructura o servicio afectado antes de la materialización de la amenaza.

Las lecciones aprendidas siempre se deben tomar en cuenta en el plan de mejoramiento de la entidad, una vez se identifican las brechas de seguridad y vulnerabilidades en el entorno tecnológico; también, se realiza un seguimiento periódico establecido en las políticas de la entidad para observar los factores que aún se deben mejorar.

La guía brinda así mismo, las indicaciones para su adopción en la organización, definiendo los recursos humanos, económicos y de procedimiento, necesarios para su

implementación y operación, en donde se ha involucrado el Csirt Gobierno, como entidad que acompaña dicho proceso a las entidades gubernamentales.

Se sugiere consultar este documento base desde el sitio oficial del MinTIC para conocer los detalles y guía de implementación. Este recurso se encuentra también en el material complementario. Enlace Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.

2.3. Características

La gestión de incidentes desde lo establecido por la guía del MinTIC, se aborda desde cada una de sus fases, estableciendo las características y condiciones para su adopción y desarrollo de las actividades enmarcadas en el plan. En este orden de ideas, se recorrerá cada una de las fases sugeridas, para reconocer sus características, funciones y actividades:

- Preparación
- Detección, evaluación y análisis
- Contención, erradicación y recuperación
- Actividades post-incidentes

Veamos una explicación de cada una:

Preparación

Esta fase conlleva a que las entidades establezcan el plan para afrontar un incidente de seguridad. Esto involucra fortalecer las capacidades de detección, evaluación, contención y/o recuperación. Esta fase debe estar directamente apoyada

por las áreas responsables de tecnología, dado que deben de reconocer las capacidades actuales y las necesarias para realizar una adecuada gestión.

Dentro de las actividades que deben adelantar para la preparación, se recomiendan:

a) **Gestión de parches de seguridad**. Se debe considerar contar con un plan para la aplicación de parches en sus sistemas operativos, aplicaciones, servicios entre otros.
b) **Aseguramiento de plataforma**. Las organizaciones deben de realizar ejercicios de endurecimiento de las plataformas de servicios, tomando como referencia marcos de buenas prácticas.
c) **Seguridad en redes**. Mantener un control y monitoreo permanente de los elementos que conforman las redes de datos, aplicar actualizaciones a dispositivos, realizar segmentación de redes y considerar la implementación de sistemas, que permitan la identificación de patrones anormales en el tráfico. Aquí hay que considerar la implementación de IDS, IPS, “Firewalls”, “Waf”, entre otros.
d) **Prevención de código malicioso**. Todos los dispositivos de la red deberán contar con sistemas antivirus, antimalware y mantener sus bases de datos al día.
e) **Sensibilización y entrenamiento de usuarios**. Mantener capacitados a todo el personal de la organización sobre buenas prácticas de seguridad, políticas y procedimientos establecidos desde la organización, así como los lineamientos de orden superior y que se deban aplicar por su naturaleza.

Detección, evaluación y análisis

Esta fase requiere que la organización fortalezca las capacidades para detectar, evaluar y analizar cualquier comportamiento por fuera de lo común; para ello, se recomienda:

Detección

Revisar los indicadores o eventos que conlleven a sospechar que algún elemento no está funcionando o respondiendo como se espera, puede apoyarse en: alertas de sistemas de seguridad, reportes de caída de servidores, reportes de usuarios, reportes de antivirus, logs de servidores, de aplicaciones, de herramientas de seguridad como los SIEM, entre otros.

Análisis

Aquí se busca que se desarrollen actividades que permitan determinar si un comportamiento no es el adecuado; para lo cual, se requiere fortalecer el conocimiento en:

- Conocimiento sobre comportamientos sobre la red y los sistemas.
- Conocimiento sobre comportamiento de infraestructura.
- Conocimiento sobre análisis de logs.
- Dominar la correlación de eventos.
- Mantener relojes sincronizados.
- Establecer matrices de diagnóstico.

Evaluación

Esta actividad requiere tener en cuenta los niveles de impacto a partir del análisis de riesgos realizado sobre los activos de información, teniendo presente que la severidad se puede clasificar de la siguiente manera:

- **Alto impacto:** cuando un incidente afecta los activos de información de manera catastrófica, afectando el desarrollo de los objetivos de la organización.
- **Medio impacto:** el incidente afecta activos de información de manera moderada, y su impacto es medio.
- **Bajo impacto:** cuando el incidente afecta activos de información con bajo impacto o insignificante o no afecta el desarrollo de los objetivos de la organización.

Clasificación de incidentes de seguridad de la información

En esta fase se requiere de capacidades para clasificar un incidente, teniendo como referente clasificaciones establecidas previamente por cada una de las organizaciones y las cuales dependerán de la infraestructura, riesgo y criticidad de cada activo en particular.

Priorización de los incidentes y tiempos de respuesta

Se requiere de contar con una escala de prioridad, definida previamente que permita clasificar los incidentes, estas escalas pueden ser: prioridad, criticidad de impacto, impacto actual e impacto futuro.

Una vez se hayan establecido las variables y las escalas, se puede obtener la prioridad, con la ayuda de la siguiente fórmula:

Nivel Prioridad = (Impacto actual * 2,5) + (Impacto futuro * 2,5) + (Criticidad del Sistema * 5)

Obteniendo como resultado la tabla para la determinación de la prioridad de atención:

Tabla 1. Determinación de la prioridad de atención

Nivel de prioridad del incidente	Valor
Inferior	00.00 – 02.49
Bajo	02.50 – 03.74
Medio	03.75 – 04.99
Alto	05.00 – 07.49
Superior	07.50 – 10.00

Tiempo de respuesta

Se establece el tiempo de atención máximo en los cuales se debe de brindar atención a los incidentes dependiendo del nivel de prioridad, de acuerdo a la siguiente tabla; aunque cada organización puede definir los tiempos de acuerdo a sus capacidades y mejor lo considere pertinente.

Tabla 2. Atención a los incidentes dependiendo del nivel de prioridad

Nivel de prioridad del incidente	Valor
Inferior	3 horas
Bajo	1 hora
Medio	30 minutos
Alto	15 minutos
Superior	5 minutos

Declaración y notificación de incidentes

Indica que se debe de contar con la ruta para el reconocimiento y reporte de un incidente de seguridad de la información junto con el responsable de su gestión.

A continuación, se presenta un ejemplo de una escala de prioridad en la actividad de priorización de los incidentes y tiempos de respuesta:

Tabla 3. Ejemplo de niveles de criticidad de impacto

Nivel prioridad del incidente	Valor	Definición
Inferior	0.10	Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas.
Bajo	0.25	Sistemas que apoyan a una sola dependencia o proceso de una entidad.
Medio	0.5	Sistemas que apoyan más de una dependencia o proceso de la entidad.

Nivel prioridad del incidente	Valor	Definición
Alto	0.75	Sistemas pertenecientes al área de Tecnología y estaciones de trabajo de usuarios con funciones críticas.
Superior	1.00	Sistemas Críticos

Ahora bien, de acuerdo con el impacto futuro, este dependerá del daño que pueda causar si no es contenido y se representa a continuación:

Tabla 4. Ejemplo de niveles de impacto actual y futuro

Nivel prioridad del incidente	Valor	Definición
Inferior	0.10	Impacto leve en uno de los componentes de cualquier sistema de información o estación de trabajo.
Bajo	0.25	Impacto moderado en uno de los componentes de cualquier sistema de información o estación de trabajo.
Medio	0.5	Impacto alto en uno de los componentes de cualquier sistema de información o estación de trabajo.
Alto	0.75	Impacto moderado en uno o más componentes de más de un sistema de información.
Superior	1.00	Impacto alto en uno o más componentes de más de un sistema de información.

Contención, erradicación y recuperación

Esta fase es de gran importancia, ya que incorpora la estrategia propuesta para tomar decisiones en caso de presentarse un incidente y evitar que este se propague o tenga una mayor afectación. Consta de los siguientes componentes:

- **Contención**. Con la cual se busca detectar y contener el incidente a partir de la estrategia identificada y del mapa de ruta establecido; por ejemplo: apagar sistema, deshabilitar red, apagar servicios
- **Erradicación y recuperación**. Busca restaurar el servicio, posterior a la identificación y contención, borrando los rastros del incidente.

Actividades post-incidentes

Esta fase se desarrolla posterior a la recuperación tras un incidente y busca consolidar los informes que con los detalles más precisos que informen la situación presentada. Entre ellas se encuentran las lecciones aprendidas, las cuales hacen parte del plan de mejoramiento continuo, buscando conocer en detalle lo sucedido, sus vectores de ataque, soluciones dadas y plan de erradicación y recuperación para ocasiones futuras.

2.4. Documentación

Lo invitamos a ver el siguiente video para conocer la documentación y reporte de procesos.

Video 5. Documentación y reporte de procesos

Enlace de reproducción del video

Síntesis del video: documentación y reporte de procesos
En la era de la cuarta Revolución Industrial, las organizaciones han adoptado el teletrabajo y el home office, dando lugar a conceptos como los nómadas digitales. Esto ha creado la necesidad de proteger los datos e información de posibles fugas y ataques cibernéticos. La ciberseguridad desempeña un papel fundamental en la identificación de riesgos, el establecimiento de controles y la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Mediante este sistema, las empresas pueden gestionar los riesgos y mejorar continuamente su seguridad. El reporte de procesos es un documento importante que describe el progreso de una

investigación o labor realizada, brindando información precisa y suficiente para evaluar y proponer soluciones. El documento debe seguir una estructura que incluya partes iniciales, cuerpo, anexos y parte final. Los documentos son esenciales para documentar y registrar análisis de resultados, y son la base para generar estrategias de prevención y soluciones en seguridad digital. Es así como en este componente formativo se revisarán algunas de las acciones necesarias para evaluar la seguridad digital de la organización y el establecimiento de un plan de gestión de incidentes, el cual será de gran importancia para garantizar una continuidad del negocio.

La gestión de incidentes, como parte primordial de las estrategias de seguridad de la información en las organizaciones, se fundamenta en la información recolectada, la cual es fundamental para la toma de decisiones, informes, lecciones aprendidas e incluso para el mejoramiento continuo del plan de gestión.

En este orden de ideas, se debe mantener un registro detallado de los incidentes de seguridad que son identificados, para poder dar tratamiento y una gestión adecuada. Se empieza estableciendo los mecanismos de captura de estos incidentes, para lo cual puede ser útil documentos de captura, o formularios que recolectan la información relevante, la norma GTC-ISO-IEC 27035:2012 en su anexo D, presenta algunos modelos de formularios que pueden ser adaptados a nuestras necesidades. Algunos de ellos son:

Instrumentos de registro de información

Estos instrumentos deben almacenar la información relevante al incidente, en pocas palabras, que permita identificar el cómo, cuándo, dónde y por qué ocurrió un

incidente. A continuación, se propone la siguiente información básica como mínima para registrar y almacenarse por cada incidente identificado en la organización.

Información básica

- Fecha del evento
- Número del evento
- Evento relacionado y/o número de incidentes, si aplica.

Detalles de la persona que reporta

- Nombre
- Información de contacto
  - Dirección
  - Organización
  - Departamento
  - Teléfono
  - Correo electrónico

Descripción del evento

- Qué ocurrió
- Cómo ocurrió
- Por qué ocurrió
- Consideraciones sobre componentes/activos afectados
- Cualquier vulnerabilidad identificada

Detalle del evento

- Fecha y hora en la que ocurrió el evento.
- Fecha y hora en la que se descubrió el evento
- Fecha y hora en la que se reportó el evento

Instrumentos de captura de información

Tomando como referencia la información que se requiere almacenar, la norma GTC-ISO-IEC 27035:2021 en su anexo D, nos presenta algunos modelos de formularios para la captura de datos relacionados con incidentes.

Estos formatos pueden distribuirse como impresos o realizar implementaciones electrónicas para su distribución.

En la norma anteriormente citada, se pueden encontrar múltiples modelos de formularios, los cuales pueden ser adaptados a las necesidades de la organización. Por otra parte, a continuación, se puede observar un modelo de formulario básico para la captura de información de un incidente. Esta información, dado que almacenará datos personales, estará obligada a contar con los procesos necesarios para la protección adecuada de datos y garantizar así su privacidad.

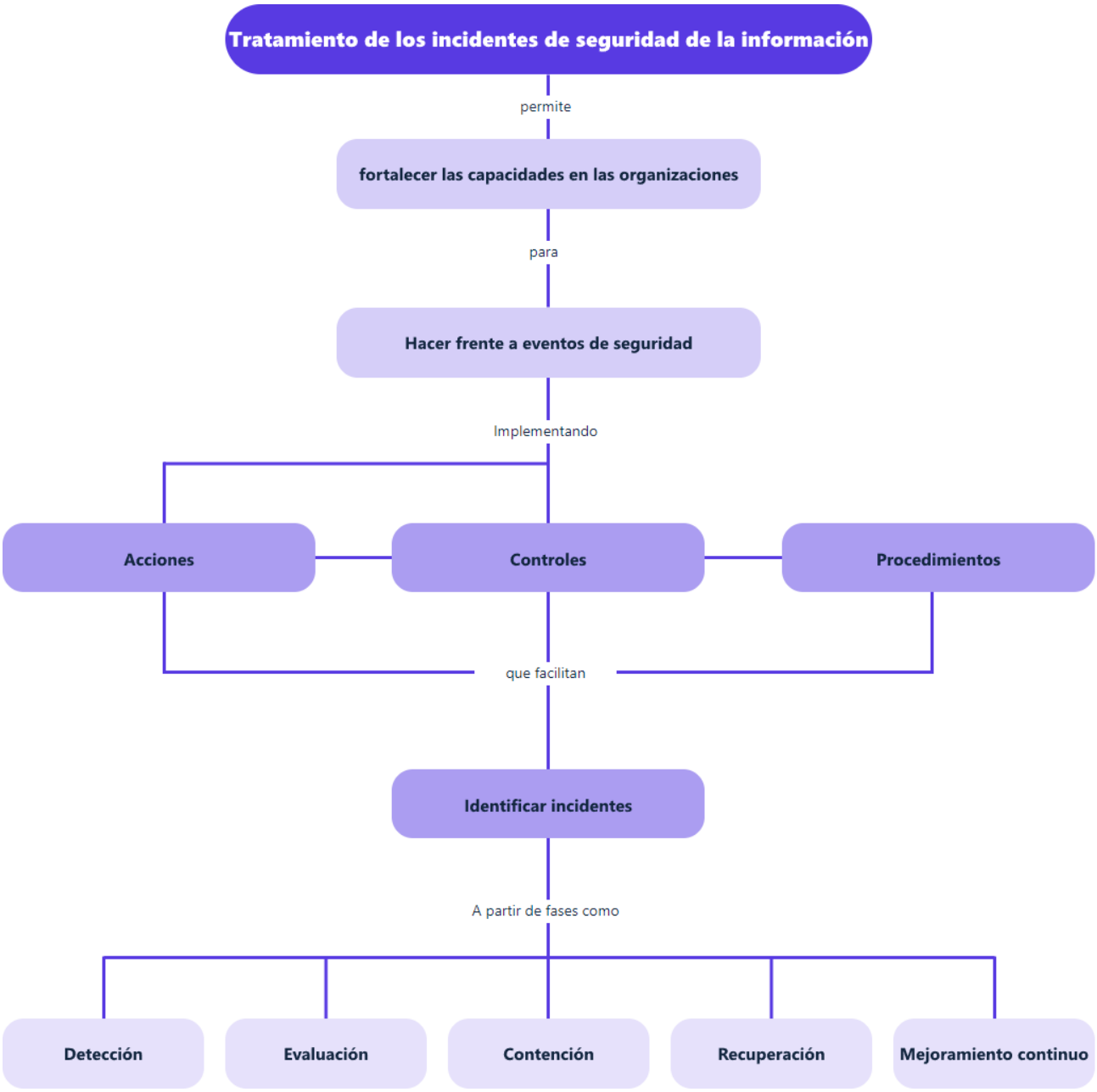
Figura 6. Modelo de formato básico para la captura de información de un incidente

1. Fecha del evento		Página 1 de 1	
2. Número del evento[3]	3. (Si es aplicable) Número de identificación de eventos y/o incidentes relacionados		
4. DETALLES DE LA PERSONA QUE REPORTA			
4.1 Nombre	4.2 Dirección		
4.3 Organización	4.4 Departamento		
4.5 Teléfono	4.6 Correo electrónico		
5. DESCRIPCIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN			
5.1 Descripción del evento: • Qué ocurrió • Cómo ocurrió • Por qué ocurrió • Consideraciones iniciales sobre componentes/activos afectados • Impactos adversos para el negocio • Cualquier vulnerabilidad identificada			
6. DETALLES DEL EVENTO DE SEGURIDAD DE LA INFORMACIÓN			
6.1 Fecha y hora en la que ocurrió el evento			
6.2 Fecha y hora en la que se descubrió el evento			
6.3 Fecha y hora en la que se reportó el evento			
6.4 ¿La respuesta a este evento ya ha finalizado? *(Marque la respuesta adecuada).*		SÍ	NO
6.5 En caso afirmativo, especifique cuánto duró el evento en días/horas/minutos			

Síntesis

Contar con una estrategia de seguridad digital que permita hacer frente a cualquier evento que ponga en riesgo la seguridad de la información y reduzca el riesgo de no continuar con el desarrollo de las actividades propias del negocio, hoy en día, es de gran importancia. Las normas técnicas y guías de implementación permitirán establecer las estrategias, condiciones y procedimientos necesarios para hacer frente a eventos que afecten el normal desarrollo de las actividades de la organización.

Es así como se estudió que entre las normas que más se ajusta a las necesidades actuales están la GTC-ISO-IEC 27035:2012, la cual, además de ser una de las más usadas en las grandes organizaciones, ha servido como referente para otros marcos, validando así su aplicabilidad a cualquier industria.


Tratamiento de los incidentes de seguridad de la información
permite
fortalecer las capacidades en las organizaciones
para
Hacer frente a eventos de seguridad
Implementando
Acciones
Controles
Procedimientos
que facilitan
Identificar incidentes
A partir de fases como
Detección
Evaluación
Contención
Recuperación
Mejoramiento continuo

Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
1. Evaluación de la seguridad digital	Chifla-Villón, M., Puma-Aucapiña, L. & Villacís-Real, K. (2020). Elaboración de un instrumento de auditoría que evalúa la seguridad lógica aplicable en servidores en Instituciones Públicas de Educación Superior de la Zona 5 del Ecuador. Revista CIENCIA UNEMI, 13(34), 127–143.	Artículo	https://search-ebscohost-com.bdigital.sena.edu.co/login.aspx?direct=true&db=fap&AN=146126581&lang=es&site=ehost-live
1.1. Gestión de vulnerabilidades	Nist. (2022). Framework Documents.	Sitio web	https://www.nist.gov/cyberframework/framework
1.1. Gestión de vulnerabilidades	OWASP. (2022). WSTG – Stable	Sitio web	https://owasp.org/www-project-web-security-testing-guide/stable/
1.1. Gestión de vulnerabilidades	OISGG. (2006). Penetration Testing Framework (PTF).	Libro	http://cuchillac.net/archivos/pre_seguridad_pymes/2_hakeo_etico/lects/metodologia_oissg.pdf
1.1. Gestión de vulnerabilidades	Pentest-standard.org. (s.f.). PTES Technical Guidelines.	Sitio web	http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines
1.1. Gestión de vulnerabilidades	ISECOM. (2021). OSSTMM.	Sitio web	https://www.isecom.org/research.html#content5-9d
1.3 Hacking ético	Rodríguez Llerena, A. E. (2020). Herramientas fundamentales para el hacking ético. Revista Cubana de Informatica Medica, 12(1), 116–131.	Artículo	https://search-ebscohost-com.bdigital.sena.edu.co/login.aspx?direct=true&db=fap&AN=144392670&lang=es&site=ehost-live

Tema	Referencia	Tipo de material	Enlace del recurso
2. Gestión de incidentes de seguridad digital	ICONTEC. (2012). Gtc-iso-iec 27035:2012 tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información.	Norma técnica	https://e-collection-icontec-org.bdigital.sena.edu.co/normavw.aspx?ID=311
2.1. Normatividad relacionada	MinTIC. (2021). Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.	Guía	https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237908_maestro_mspi.pdf

Glosario

Contención: proceso mediante el cual se busca evitar que un incidente se propague o genere una mayor afectación.

Detección: fase en la cual se identifican eventos que posiblemente pueden afectar la seguridad de la información

Incidente: “evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazas la seguridad informática” (ICONTEC, 2012)

ISIRT: equipo de respuesta a incidentes de seguridad de la información.

Recuperación: proceso que busca restablecer los servicios o activos a su estado normal.

Referencias bibliográficas

ISECOM. (2021). OSSTMM. https://www.isecom.org/research.html#content5-9d

MinTIC. (2021). Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-237908_maestro_mspi.pdf

OISGG. (2006). Penetration Testing Framework (PTF). http://cuchillac.net/archivos/pre_seguridad_pymes/2_hakeo_etico/lects/metodologia_oissg.pdf

OWASP. (2021). Welcome to the OWASP Top 10 – 2021. https://owasp.org/Top10/

Créditos

Nombre	Cargo	Regional y Centro de Formación
Claudia Patricia Aristizábal	Responsable del Ecosistema	Dirección General
Rafael Neftalí Lizcano Reyes	Responsable de Línea de Producción	Centro Industrial del Diseño y la Manufactura - Regional Santander
Hernando José Peña Hidalgo	Experto Temático	Centro de la Industria, la Empresa y los Servicios - Regional Norte de Santander
Diego E. Acevedo Guevara	Diseñador Instruccional	Centro de la Industria, la Empresa y los Servicios - Regional Norte de Santander
Andrés Felipe Velandia Espitia	Asesor Metodológico	Centro de Diseño y Metrología - Regional Distrito Capital
Darío González	Corrector de Estilo	Centro de Diseño y Metrología - Regional Distrito Capital
Juan Daniel Polánco Muñoz	Diseñador de Contenidos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Emilsen Alfonso Bautista	Desarrollador Full-Stack	Centro Industrial del Diseño y la Manufactura - Regional Santander
Camilo Andrés Bolaño Rey	Locución	Centro Industrial del Diseño y la Manufactura - Regional Santander
Wilson Andrés Arenales Cáceres	Storyboard e Ilustración	Centro Industrial del Diseño y la Manufactura - Regional Santander
Mary Jeans Palacio Camacho	Animador y Productor Audiovisual	Centro Industrial del Diseño y la Manufactura - Regional Santander
Zuleidy María Ruíz Torres	Validación de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander

Nombre	Cargo	Regional y Centro de Formación
Luis Gabriel Urueta Álvarez	Validador de Recursos Educativos Digitales	Centro Industrial del Diseño y la Manufactura - Regional Santander
Daniel Ricardo Mutis	Evaluador para Contenidos Inclusivos y Accesibles	Centro - Regional