MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL

SERVICIO PÚBLICO DE EMPLEO ESTATAL
SEPE
SERVEI PÚBLIC D'OCUPACIÓ ESTATAL

MINISTERIO DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y DEPORTES

Generalitat de Catalunya
SOC Servei d'Ocupació de Catalunya

IRON HACK SPAIN

Gestión de incidentes de seguridad informática

IFCT0109 – Seguridad informática

MF0488_3 (90 horas)

Respuesta ante incidentes de seguridad

- Introducción
- Procedimiento de recolección de información relacionada con incidentes de seguridad
- Exposición de las distintas técnicas y herramientas utilizadas para el análisis y correlación de información y eventos de seguridad
- Proceso de verificación de la intrusión
- Naturaleza y funciones de los organismos de gestión de incidentes
- Resumen

Introducción

La prevención y contención de incidentes de seguridad son vitales para evitar intrusiones en los equipos, minimizando así daños y pérdidas de información.

Sin embargo, cuando a pesar de las medidas preventivas se produce un incidente, es crucial establecer un plan de respuesta para su eliminación y reducir al mínimo los daños.

Este capítulo detalla las recomendaciones y fases para manejar estos incidentes.

Primero, se debe recolectar toda la información del incidente para su identificación y restaurar los equipos a su estado original.

Luego, se emplean técnicas y herramientas para analizar los eventos de seguridad y comprender precisamente lo ocurrido durante el incidente, así como obtener pistas sobre su origen.

Es importante verificar la intrusión, ya que podría ser una falsa alarma.

Además, se presentan organizaciones nacionales e internacionales que brindan apoyo e información para la gestión de incidentes, complementando los planes de respuesta y mejorando la eficacia en la lucha contra los riesgos de seguridad.

Procedimiento de recolección de información relacionada con incidentes de seguridad

Introducción

Definición de incidente de seguridad

Un incidente de seguridad es un evento o conjunto de eventos que pueden provocar la interrupción, la degradación o la indisponibilidad de los servicios ofrecidos por un sistema informático, así como la pérdida de información o la afectación a la confidencialidad, integridad o disponibilidad de la misma.

Medidas de seguridad. Se clasifican en:

- Medidas preventivas: establecimiento de contraseñas, políticas de seguridad, cortafuegos, procedimientos de copias de seguridad, concienciación del personal, etc.
- Medidas correctivas: procedimientos de restauración del sistema, establecimiento de esquemas de tolerancia a fallos, etc.
- Medidas de detección: revisiones de seguridad, análisis de registros de auditoría, análisis de logs, etc.

Gestión de incidentes de seguridad. Es la parte de la seguridad de la información encargada de:

- Prevenir: Implementar medidas de seguridad para evitar que ocurran incidentes.
- Detectar: Monitorizar los sistemas y detectar los incidentes de forma temprana.
- Corregir: Responder a los incidentes de forma rápida y eficaz para minimizar el impacto en la organización.

Procedimiento de recolección de información relacionada con incidentes de seguridad

Introducción

Beneficios de la gestión de incidentes

- Respuesta sistemática y eficaz a los incidentes de seguridad.
- Agilización y facilitación del proceso de recuperación de equipos y sistemas.
- Reducción de la pérdida de datos y del tiempo de interrupción de servicios.
- Prevención de incidentes reiterados a través del aprendizaje.
- Mejora continua de la seguridad de la organización.
- Facilitación de la gestión de los aspectos legales.

Recolección de información

Parte fundamental de la gestión de incidentes. La información recopilada debe ser:

- Completa: Debe incluir toda la información relevante sobre el incidente, como la fecha y hora, el tipo de incidente, los sistemas afectados, la causa del incidente y el impacto en la organización.
- Precisa: La información debe ser precisa y veraz para poder tomar decisiones correctas.
- Oportuna: La información debe ser recopilada de forma oportuna para poder responder al incidente de forma rápida y eficaz.

Procedimiento de recolección de información relacionada con incidentes de seguridad

Introducción

Fuentes de información

- Registros del sistema: Los registros del sistema pueden proporcionar información sobre la actividad del sistema, como los inicios de sesión, los accesos a archivos y las ejecuciones de programas.
- Análisis de logs: Los logs son archivos que contienen información sobre eventos del sistema. El análisis de logs puede ayudar a identificar las causas de los incidentes.
- Testimonios de usuarios: Los usuarios que han sido testigos del incidente o que han sido afectados por el mismo pueden proporcionar información valiosa sobre el incidente.
- Informes de expertos: Los expertos en seguridad informática pueden ayudar a analizar el incidente y a determinar la mejor forma de responder al mismo.

Herramientas de recolección de información

- Herramientas de análisis de logs: Estas herramientas pueden ayudar a analizar los logs del sistema para identificar las causas de los incidentes.
- Herramientas de entrevistas: Estas herramientas pueden ayudar a entrevistar a los usuarios que han sido testigos del incidente o que han sido afectados por el mismo.
- Herramientas de análisis de malware: Estas herramientas pueden ayudar a analizar el malware que ha sido utilizado en el incidente.

Procedimiento de recolección de información relacionada con incidentes de seguridad

Equipo de respuesta de incidentes de seguridad informática

Importancia y funciones del CSIRT

La rapidez en la detección, reconocimiento, análisis y respuesta a una amenaza minimiza los daños y reduce considerablemente los costes de recuperación de la información.

Un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) es un grupo de personas especializadas en la gestión y tratamiento de incidentes. Aunque generalmente solo las grandes organizaciones tienen CSIRT, toda organización debe designar responsables para ejecutar el plan de respuesta a incidentes.

Funciones del CSIRT:

- Confeccionar el Plan de Gestión de Incidentes: conjunto de tareas y procedimientos para la correcta gestión de incidentes de seguridad.
- Establecer:
  - Política general de gestión de incidentes.
  - Procedimientos para la gestión de incidentes.
  - Relaciones con otros grupos de la organización.
  - Guías para la comunicación con terceros.
  - Organización de los responsables de la gestión de respuesta a incidentes.

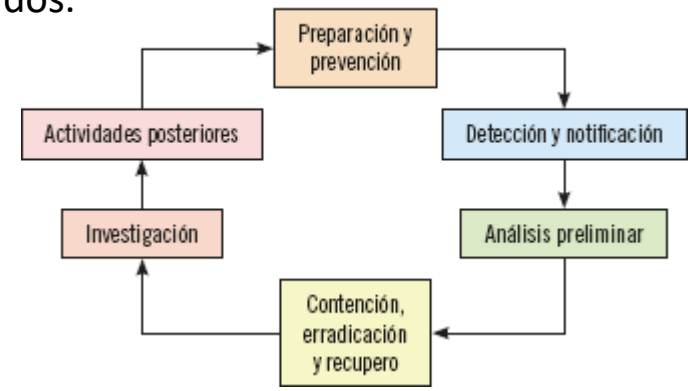
Procedimiento de recolección de información relacionada con incidentes de seguridad

Equipo de respuesta de incidentes de seguridad informática

Fases del Plan de Gestión de Incidentes

1. Preparación y prevención: Establecimiento de medidas preventivas para minimizar el riesgo de aparición de incidentes.
2. Detección y notificación. Establecimiento de medidas para:
    - Detectar la entrada de posibles amenazas.
    - Notificar a los responsables su detección.
3. Análisis preliminar. Análisis de la posible amenaza:
    - Determinar si es real o una falsa alarma.
    - En caso de ser real, analizar la incidencia para conocer los detalles y los daños ocasionados.
4. Contención, erradicación y recuperación. Establecimiento de medidas correctivas para:
    - Minimizar los daños ocasionados.
    - Restaurar el sistema a situaciones anteriores a la aparición de la amenaza.
5. Investigación. Análisis profundo de la incidencia para conocer:
    - Su procedimiento de ataque.
    - Cómo ha podido acceder al sistema.
6. Actividades posteriores. Utilizar la investigación del incidente para Implementar medidas correctivas que impidan que la amenaza vuelva a acceder a los sistemas de la organización.

Esquema del procedimiento de gestión de incidentes



Procedimiento de recolección de información relacionada con incidentes de seguridad

Equipo de respuesta de incidentes de seguridad informática **Fases del Plan de Gestión de Incidentes**

1. Preparación y prevención

Definición y objetivos. La fase de prevención y preparación de incidentes busca:

- Evitar intrusiones al sistema.
- Minimizar la producción de incidentes.

Medidas de preparación

- Políticas, normas y procedimientos: para la gestión de incidentes.
- Criterios de clasificación y priorización: para determinar la gravedad y el orden de respuesta.
- Preparación del equipo de respuesta: entrenamiento y definición de roles.
- Entrenamiento del personal: sobre seguridad informática y respuesta a incidentes.
- Documentación: topología de la red, configuración de equipos, patrones de redes y sistemas.
- Logs: activación, centralización y gestión.
- Sincronización de relojes: para facilitar la investigación.
- Copias de seguridad: definición e implementación de un sistema de backup.

Procedimiento de recolección de información relacionada con incidentes de seguridad

Equipo de respuesta de incidentes de seguridad informática **Fases del Plan de Gestión de Incidentes**

1. Preparación y prevención

INCIDENTE	Efectos negativos producidos o potenciales		
	Grave	Moderado	Leve
Incidente 1			
Incidente 2			
Incidente 3			
Incidente 4			
Incidente 5			

RECURSO	Criticidad de los recursos		
	Alta	Media	Baja
Recurso 1			
Recurso 2			
Recurso 3			
Recurso 4			
Recurso 5			

Atendiendo a estos dos criterios se establecerá el nivel de criticidad del incidente distinguiendo entre muy grave, grave, moderado y leve tal como se muestra en la siguiente tabla:

		Criticidad de los recursos		
		Alta	Media	Baja
Efectos negativos producidos o potenciales	Grave	MUY GRAVE	GRAVE	MODERADO
	Moderado	GRAVE	MODERADO	LEVE
	Leve	MODERADO	LEVE	LEVE

Por ejemplo, un incidente que produzca efectos negativos moderados, pero que la criticidad de los recursos a los que afecta sea alta se clasifica como incidente “grave”.

Efectos negativos producidos/potenciales + Criticidad de los recursos afectados = Criticidad del incidente

Criticidad del incidente	Tiempo de reacción
LEVE	4 h
MODERADO	2 h
GRAVE	30 min
MUY GRAVE	10 min

En función de la criticidad del incidente, se deberá establecer un tiempo máximo de respuesta para su tratamiento desde el momento de la detección

Procedimiento de recolección de información relacionada con incidentes de seguridad

Equipo de respuesta de incidentes de seguridad informática **Fases del Plan de Gestión de Incidentes**

1. **Preparación y prevención**

   Medidas de prevención.

   - Análisis de riesgos periódicos.
   - Auditorías periódicas.
   - Gestión eficaz de las actualizaciones.
   - Seguridad en la red.
   - Seguridad de los equipos.
   - Detección y prevención de códigos maliciosos.
   - Concienciación del personal.

Procedimiento de recolección de información relacionada con incidentes de seguridad

Equipo de respuesta de incidentes de seguridad informática **Fases del Plan de Gestión de Incidentes**

2. Detección y notificación

Diferencias entre Advertencias e Indicadores:

- Advertencia: Señal que indica un posible incidente. Ejemplos: (Amenazas de ataques web, alertas de IDS durante un escaneo de red, …
- Indicador: Señal que confirma que un incidente está ocurriendo. Ejemplos (Detección de un virus por el antivirus, ejecución lenta de aplicaciones, ralentización del acceso a internet, bloqueo de una cuenta por exceso de intentos fallidos, cambios de configuración sin permiso del usuario.)

Herramientas y Técnicas de Detección

- Sistemas IDS/IPS.
- Antivirus.
- Monitorización de la red.
- Análisis de logs.
- Control de integridad de archivos y datos.

Notificación de Incidentes

- El Plan de Gestión de Incidentes debe definir un proceso de notificación.
- El proceso debe incluir pautas, procedimientos y métodos de notificación.

Procedimiento de recolección de información relacionada con incidentes de seguridad

Equipo de respuesta de incidentes de seguridad informática **Fases del Plan de Gestión de Incidentes**

2. Detección y notificación

Formulario de notificación

Característica	Detalle
Incidente detectado	1
Fecha y hora	25.03.2013 20:00:23
Identificación del incidente	Troyano
Clasificación	Moderado
Breve descripción	Intento fallido de acceso del código malicioso troyano.
Efectos y daños producidos	Ninguno
Descripción detallada	Intento de acceso de un troyano espía que ha sido interceptado por el sistema de protección del antivirus, impidiendo la producción de cualquier daño en el equipo. Reacción correcta de la seguridad del sistema.
Estado	Resuelto
Fecha de cierre	25.03.2013 20:00:40
Detalles de la solución	No ha sido necesaria más intervención que la propia realizada por el antivirus.

Destinatarios de la Notificación:

- Personal de informática.
- Responsable de seguridad.
- Dueños de la información afectada.
- Altos directivos.
- ….

Procedimiento de recolección de información relacionada con incidentes de seguridad

Equipo de respuesta de incidentes de seguridad informática **Fases del Plan de Gestión de Incidentes**

3.- Análisis preliminar

Consiste en realizar un análisis de los indicadores y advertencias disponibles para determinar si se trata de un incidente real o una falsa alarma.

En caso de confirmarse un incidente real, se debe seguir un proceso de recolección de información para analizar:

- Alcance del incidente: redes, equipos, sistemas y aplicaciones afectados.
- Origen del incidente: causa y responsables.
- Impacto del incidente: actividades, servicios y procesos de la organización afectados.
- Metodología del incidente: métodos y herramientas utilizadas, vulnerabilidades explotadas, etc.

La fase de análisis preliminar es crucial en la gestión de incidentes de seguridad: una información previa errónea puede ocasionar errores en el tratamiento del incidente, con consecuencias negativas mayores.

Para determinar el alcance del incidente se consideran:

- Cantidad de equipos y redes afectadas.
- Nivel de privilegio alcanzado por la intrusión.
- Nivel de riesgo de las aplicaciones críticas y de los equipos y la red.
- Conocimiento de la vulnerabilidad explotada y análisis de otros equipos con la misma vulnerabilidad.

Procedimiento de recolección de información relacionada con incidentes de seguridad

Equipo de respuesta de incidentes de seguridad informática **Fases del Plan de Gestión de Incidentes**

3.- Análisis preliminar

Para obtener un conocimiento más profundo del incidente y su alcance se recolecta información mediante:

- Indagación a administradores y personal de la organización.
- Revisión de reportes de sistemas y herramientas IDS.
- Revisión de logs de comunicaciones y sistemas.
- Análisis de la topología y arquitectura de la red y de las listas de acceso.

El proceso de recolección de información permite:

- Conocer el origen específico del incidente y detectar a su causante.
- Emprender medidas legales contra el causante (si procede).
- Establecer medidas de contención y erradicación del incidente.
- Proponer medidas correctivas para impedir futuras ocurrencias.

Algunos datos recolectados en la fase de análisis preliminar son:

- Información sobre sucesos anormales en los sistemas y actividades.
- Detección de actividades anormales.
- Conocimiento de los detalles concretos del incidente.
- Detección de cambios no autorizados.

Exposición de las distintas técnicas y herramientas utilizadas para el análisis y correlación de información y eventos de seguridad

Introducción

Análisis y correlación de eventos de seguridad

El análisis y la gestión de logs y la correlación de eventos de seguridad son fundamentales para la gestión de riesgos de seguridad de la información. Una gestión adecuada permite:

- Conocer en tiempo real todo lo que está ocurriendo en términos de seguridad en los equipos de la red.
- Reducir el tiempo de reacción y de toma de medidas correctivas ante incidentes.
- Disminuir considerablemente los daños que pueda ocasionar algún incidente de seguridad.

Las herramientas de correlación de eventos permiten:

- Llevar a cabo una gestión más eficiente de todos los sistemas, herramientas y aplicaciones críticas mediante su monitorización.
- Detectar posibles vulnerabilidades y amenazas con el fin de minimizar los riesgos de intrusiones.

Las herramientas de gestión de información y eventos de seguridad (SIEM):

- Recogen, cotejan y elaboran informes con los datos facilitados por los logs.
- Permiten llevar a cabo un tratamiento organizado de los incidentes para resolverlos en el menor tiempo posible.

Exposición de las distintas técnicas y herramientas utilizadas para el análisis y correlación de información y eventos de seguridad

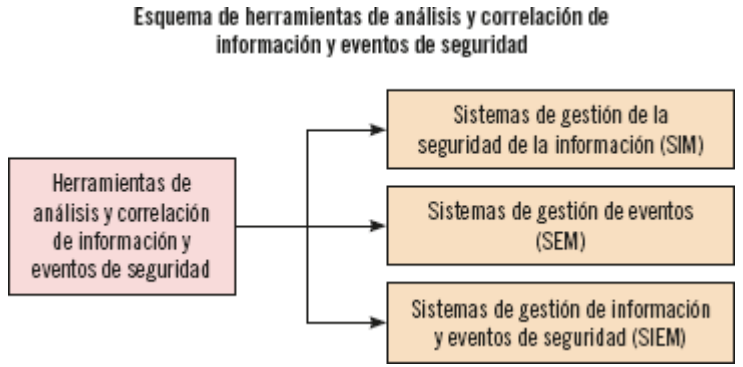
Introducción

Un sistema de análisis y correlación de eventos adecuado debe permitir:

- Determinar en tiempo real la probabilidad de materializarse una amenaza.
- Detectar a tiempo real el inicio de un ataque, emitiendo alertas con la menor demora posible.
- Conocer el éxito o fracaso de un ataque y de su impacto real sobre el sistema.
- Determinar los patrones de materialización de las amenazas para ser utilizados en la implantación de nuevas medidas de seguridad.

Tipos de sistemas:

- Sistemas de gestión de la seguridad de la información o SIM (Security Information Management).
- Sistemas de gestión de eventos o SEM (Security Event Management).
- Sistemas de gestión de información y eventos de seguridad o SIEM (Security Information and Event Management).



Exposición de las distintas técnicas y herramientas utilizadas para el análisis y correlación de información y eventos de seguridad

Sistemas de gestión de la seguridad de la información (SIM)

Las herramientas de gestión de seguridad de la información o SIM son sistemas de supervisión que recopilan, correlacionan y analizan información de seguridad en diferido, no en tiempo real. Crean una base de datos indexada con los datos obtenidos de la supervisión de equipos y dispositivos.

Funciones principales:

- Recogida, ordenación y correlación de información de la red.
- Automatización y monitorización de eventos de sistemas y dispositivos de seguridad.

Centralización, correlación y priorización de eventos para:

- Estandarizar los eventos.
- Reducir el tiempo de detección de ataques y vulnerabilidades.
- Minimizar la información a procesar para mejorar el rendimiento.

Las herramientas SIM ayudan a:

- Centralizar y administrar la información de eventos de seguridad.
- Crear reportes de análisis de archivos de registro y reportes de cumplimiento.

Exposición de las distintas técnicas y herramientas utilizadas para el análisis y correlación de información y eventos de seguridad

Sistemas de gestión de la seguridad de la información (SIM)

Usos principales:

- Administrar la infraestructura de la red y los activos de la organización.
- Centralizar y monitorizar los componentes de la infraestructura de seguridad.
- Analizar la información de los componentes de seguridad.
- Predecir y pronosticar amenazas.
- Correlacionar eventos de seguridad.
- Detectar, identificar y emitir reportes de eventos de seguridad.
- Realizar análisis forense de los eventos.
- Establecer políticas de seguridad más adecuadas.

Las herramientas SIM se basan en el análisis de información de seguridad en diferido, lo que significa que no son ideales para la detección de amenazas en tiempo real.

Exposición de las distintas técnicas y herramientas utilizadas para el análisis y correlación de información y eventos de seguridad

Sistemas de gestión de eventos (SEM)

Los sistemas de gestión de eventos o SEM son herramientas que monitorizan y gestionan eventos de seguridad en tiempo real o casi real. Su función principal es recopilar datos de eventos de seguridad de diferentes equipos, sistemas y dispositivos para realizar análisis en tiempo real y responder lo más rápido posible.

Beneficios principales:

- Acceso a registros a través de una interfaz central.
- Almacenamiento seguro de registros con integridad garantizada.
- Representación gráfica de la actividad para informes más sencillos y visuales.
- Activación de alertas programables.
- Gestión de eventos de varios sistemas operativos.
- Recuperación de registros ante bloqueos del sistema o eliminación inesperada.

Diferencias con las herramientas SIM:

Las herramientas SEM trabajan en tiempo real, mientras que las SIM lo hacen en diferido.

En resumen, las herramientas SEM permiten:

- Visualizar, monitorizar y gestionar eventos.
- Detectar situaciones anómalas.
- Automatizar respuestas y medidas correctivas ante incidentes de seguridad.

Exposición de las distintas técnicas y herramientas utilizadas para el análisis y correlación de información y eventos de seguridad

Sistemas de información y eventos de seguridad (SIEM)

Las herramientas de información y eventos de seguridad o herramientas SIEM son una mezcla de las herramientas SIM y SEM, englobando las funcionalidades de ambas:

- Recopilan los logs de los equipos, sistemas y dispositivos monitorizados.
- Los almacenan a largo plazo.
- Agregan y correlacionan en tiempo real la información recibida.

Todo ello para lograr una detección y establecimiento de medidas más eficaz, minimizando los daños ocasionados.

Son herramientas que permiten una gestión de incidentes de seguridad más global y entre sus funciones principales destacan:

- Detección de anomalías y amenazas
- Análisis de todas las fases del incidente
- Captura total de los paquetes de la red
- Conocimiento del comportamiento del usuario y su contexto
- Cumplimiento de nuevas normativas
- Administración más efectiva del riesgo a través de la recopilación de información obtenida, como:
  - Topología y arquitectura de la red
  - Vulnerabilidades detectadas
  - Parámetros de configuración del equipo y de los dispositivos
  - Análisis de fallos
  - Priorización de vulnerabilidades
  - Correlación avanzada y profunda de los eventos

Exposición de las distintas técnicas y herramientas utilizadas para el análisis y correlación de información y eventos de seguridad

Sistemas de información y eventos de seguridad (SIEM)

Las herramientas SIM, SEM y SIEM disponibles en el mercado son de lo más variadas. Las organizaciones deben realizar un análisis previo de necesidades y prioridades para elegir la herramienta más adecuada y pertinente.

Actualmente, este tipo de herramientas destacan por combinar también funciones de IDS/IPS, creando soluciones de seguridad muy completas, y que suelen ser de gran utilidad en organizaciones de un tamaño considerable. Una de estas herramientas es AlienVault, y proporciona principalmente las siguientes opciones:

- Detección e identificación de los activos de la red
- Identificación de las vulnerabilidades de los sistemas
- Detección de tráfico malicioso en la red, así como violaciones de seguridad
- Relaciona y analiza los datos generados por los distintos eventos de seguridad ocurridos
- Monitorización y comportamientos sospechosos

Las ventajas de utilizar herramientas SIEM son:

- Mejoran la visibilidad de la red y los sistemas.
- Permiten una detección más rápida de las amenazas.
- Ayudan a reducir el tiempo de respuesta a los incidentes.
- Proporcionan una mejor comprensión del comportamiento del usuario.
- Ayudan a cumplir con las normativas de seguridad.
- Permiten una mejor administración del riesgo.

Exposición de las distintas técnicas y herramientas utilizadas para el análisis y correlación de información y eventos de seguridad

Sistemas de información y eventos de seguridad (SIEM)

Las herramientas SIM, SEM y SIEM disponibles en el mercado son de lo más variadas. Las organizaciones deben realizar un análisis previo de necesidades y prioridades para elegir la herramienta más adecuada y pertinente.

Actualmente, este tipo de herramientas destacan por combinar también funciones de IDS/IPS, creando soluciones de seguridad muy completas, y que suelen ser de gran utilidad en organizaciones de un tamaño considerable. Una de estas herramientas es AlienVault, y proporciona principalmente las siguientes opciones:

- Detección e identificación de los activos de la red
- Identificación de las vulnerabilidades de los sistemas
- Detección de tráfico malicioso en la red, así como violaciones de seguridad
- Relaciona y analiza los datos generados por los distintos eventos de seguridad ocurridos
- Monitorización y comportamientos sospechosos

Las ventajas de utilizar herramientas SIEM son:

- Mejoran la visibilidad de la red y los sistemas.
- Permiten una detección más rápida de las amenazas.
- Ayudan a reducir el tiempo de respuesta a los incidentes.
- Proporcionan una mejor comprensión del comportamiento del usuario.
- Ayudan a cumplir con las normativas de seguridad.
- Permiten una mejor administración del riesgo.

Proceso de verificación de la intrusión

Contención, Erradicación y Recuperación ante Incidentes de Seguridad

Un incidente debe pasar por las fases de prevención y preparación, detección y notificación, y análisis preliminar.

Una vez que se ha verificado que un incidente es real y se ha completado el proceso de recolección de información, se procede con la fase de contención, erradicación y recuperación para conocer en profundidad los detalles del incidente.

- La contención tiene como objetivo evitar que el incidente cause más daño.
- La erradicación implica eliminar la causa del incidente y cualquier rastro del daño causado.
- La recuperación implica restaurar los sistemas, dispositivos y equipos a su estado original antes del incidente.

Por ejemplo, cuando un equipo se infecta con un virus, las fases de contención, erradicación y recuperación deberían ser las siguientes:

- Contención: Desconectar el equipo afectado de la red para evitar que el virus se propague a otros equipos.
- Erradicación: Ya sea utilizando un antivirus, de forma manual u otras técnicas, se debe localizar el malware y eliminarlo del equipo.
- Recuperación: Restaurar el sistema dañado utilizando la última copia de seguridad realizada con los datos del equipo.

La rapidez con la que se implementan las medidas de contención, erradicación y recuperación es de suma importancia para evitar la expansión de los posibles daños causados por el incidente de seguridad. Además, cuanto antes se recupere la normalidad, antes se podrá reanudar la actividad habitual y prestar servicio al cliente, minimizando así las pérdidas de calidad ocasionadas por la interrupción del servicio.

Proceso de verificación de la intrusión

Elaboración del informe final del incidente

Una vez eliminado el incidente y restaurada la situación original, el siguiente paso es la investigación del incidente y la realización de actividades posteriores, como la definición de nuevas medidas de seguridad, utilizando la información obtenida en el proceso de investigación.

La verificación de la intrusión se realiza mediante la elaboración de un informe final. Este informe debe contener, al menos, los aspectos que se reflejan en la tabla de la diapositiva siguiente.

Con la evaluación y análisis de todos los aspectos reflejados en el informe de verificación del incidente, se puede obtener una imagen global de por qué sucedió la intrusión, qué se ha visto afectado, cómo se ha actuado y qué se debe modificar para prevenir futuras intrusiones.

De este modo, se realiza un proceso de aprendizaje del incidente para que en futuras intrusiones la respuesta sea más rápida y efectiva y los daños ocasionados sean lo más reducidos posible.

Proceso de verificación de la intrusión

Elaboración del informe final del incidente

Contenido mínimo del informe:

Aspectos a Reflejar en el Informe	Actividades a Realizar
Análisis de las causas y consecuencias del incidente	- Revisión exhaustiva de los logs de los equipos, sistemas y dispositivos afectados por el incidente - Análisis de las consecuencias que hayan podido afectar a terceros - Análisis de la información del incidente compartida con terceros - Cuantificación del coste de los daños provocados por la intrusión en la organización - Estudio de la documentación elaborada por el equipo de respuesta a incidentes de seguridad - Evaluación y control de las posibles acciones legales que se hayan podido emprender por el incidente.
Evaluación de la toma de decisiones y de las actuaciones llevadas a cabo por el equipo de respuesta a incidentes	- Evaluación de la rapidez de respuesta en decisiones y medidas tomadas por el equipo de respuesta a incidentes - Análisis del personal integrante, formación recibida, organización y roles asignados en el equipo de respuesta a incidentes - Implementación de nuevas herramientas necesarias para evitar futuros incidentes.
Evaluación de los procedimientos y de las herramientas técnicas utilizadas en la respuesta al incidente	- Rediseño de los procedimientos que no hayan funcionado - Adopción de medidas correctivas que mejoren la respuesta ante futuras incidencias.
Análisis de las políticas de seguridad	- Revisión de las políticas de seguridad de la información para detectar fallos y redefinir aquellas pautas ineficientes.
Análisis de directrices de la organización	- Revisión de las directrices actuales de la organización e implantación de nuevas directrices para reforzar su nivel de seguridad.

Proceso de verificación de la intrusión

Documentación del incidente

Objetivo:

- Registrar el proceso de aprendizaje del incidente para evitar la pérdida de detalles y facilitar su análisis e investigación posterior.
- Asegurar que la información clave sobre el incidente se documente de manera precisa y completa.

¿Qué documentar?

Información básica:

- Tipo de incidente: Categoría del incidente (p. ej., malware, phishing, intrusión).
- Fecha y hora de detección: Momento en que se identificó el incidente por primera vez.
- Personas involucradas: Personal interno y externo que participó en la gestión del incidente.

Detalles del incidente:

- Hechos ocurridos: Descripción cronológica de los eventos que se desarrollaron durante el incidente.
- Daños ocasionados: Impacto del incidente en los sistemas, datos y operaciones de la organización.
- Evidencias obtenidas: Pruebas y capturas de pantalla relacionadas con el incidente.

Análisis y respuesta:

- Conclusiones del análisis: Causa raíz del incidente y su posible impacto en la organización.
- Acciones y medidas tomadas: Pasos específicos para contener, erradicar y remediar el incidente.
- Estado actual del incidente: Fase actual en la que se encuentra el proceso de gestión del incidente.

Naturaleza y funciones de los organismos de gestión de incidentes

Organismos CERT/CSIRT

Los CERT (Computer Emergency Response Team) o CSIRT (Computer Security Incident Response Team) son equipos de expertos en seguridad informática que se encargan de:

- Responder a incidentes de seguridad: analizar la situación, elaborar recomendaciones y diseñar contramedidas.
- Prevenir incidentes: ofrecer asistencia e información para ayudar a proteger los sistemas y equipos de los usuarios.
- Mejorar la calidad de la seguridad informática: realizar actividades de concienciación y educación de los usuarios.

Funciones principales:

- Ayudar al público objetivo a prevenir y atenuar incidentes graves de seguridad.
- Proteger información y datos de gran valor.
- Coordinar centralizadamente la seguridad de la información.
- Apoyar y asistir a los usuarios en la recuperación ante incidentes de seguridad.
- Dirigir centralizadamente la respuesta ante incidentes de seguridad.

Para llevar a cabo sus funciones, los CSIRT/CERT utilizan:

- Bases de datos de vulnerabilidades y de incidentes de seguridad.
- Servicios de asesoramiento especializado en seguridad de la información.
- Contactos con otros CSIRT/CERT del mundo para intercambiar información.

Naturaleza y funciones de los organismos de gestión de incidentes

Organismos CERT/CSIRT

Tipos de servicios que realizan:

- Servicios reactivos: análisis de la situación, elaboración de recomendaciones y diseño de contramedidas.
- Servicios proactivos: asistencia e información para ayudar a prevenir y proteger los sistemas y equipos.
- Servicios de gestión de calidad de la seguridad: búsqueda de herramientas y medidas para mejorar la calidad de la seguridad informática.

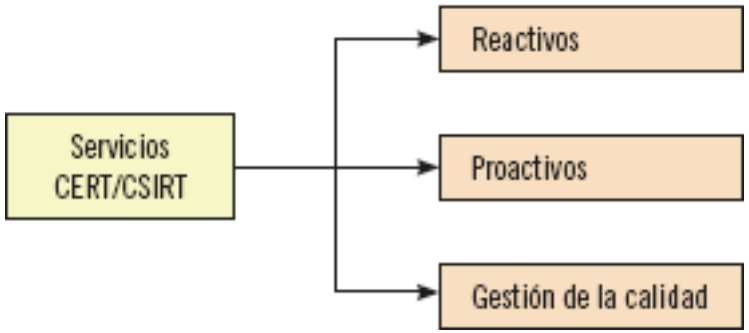
El término CSIRT se suele utilizar en Europa en lugar de CERT.

Los CERT/CSIRT son una herramienta fundamental para la protección de la seguridad informática en la actualidad.

Ejemplos de organismos CERT/CSIRT

Estados Unidos: CERT/CC.
España: INCIBE-CERT.
Europa: ENISA.

Esquema de las funcionalidades de los servicios (CERT/CSIRT)



Naturaleza y funciones de los organismos de gestión de incidentes

Organismos CERT/CSIRT

El CERT/CC, o Centro de Coordinación del Equipo de Respuesta ante Emergencias Informáticas

Fue el primer equipo de respuesta a incidentes de seguridad informática y es el más conocido a nivel mundial. Se creó en 1988 por la agencia DARPA de Estados Unidos para gestionar los incidentes de seguridad relacionados con los servicios de internet

Sus funciones principales son:

- Analizar y responder a incidentes de seguridad informática.
- Desarrollar e implementar herramientas y técnicas de seguridad.
- Proporcionar información y asistencia a las organizaciones sobre seguridad informática.

Naturaleza y funciones de los organismos de gestión de incidentes

Organismos CERT/CSIRT

El CCN-CERT (Centro Criptológico Nacional-Computer Emergency Response Team) es el equipo de respuesta a incidentes de ciberseguridad de España, dependiente del Centro Criptológico Nacional (CCN).

Su función principal es actuar como punto de referencia para la ciberseguridad en España.

Trabaja para:

- Gestionar incidentes de ciberseguridad que afecten a organismos públicos, empresas estratégicas y sistemas clasificados
- Reducir el impacto de los ciberataques
- Desarrollar acciones para fortalecer la ciberseguridad española

El CCN-CERT España ofrece además información y recursos de interés sobre ciberseguridad

Naturaleza y funciones de los organismos de gestión de incidentes

Organismos CERT/CSIRT

INCIBE-CERT es el Centro de Respuesta a Incidentes de Seguridad de referencia para ciudadanos y entidades de derecho privado en España. Creado en 2014, depende del Instituto Nacional de Ciberseguridad (INCIBE) y ofrece una amplia gama de servicios gratuitos para prevenir, detectar y responder a los incidentes de ciberseguridad.

Funciones:

- Respuesta a incidentes: Asiste a ciudadanos y entidades en la gestión de incidentes de seguridad, proporcionando análisis forenses, recomendaciones y apoyo técnico.
- Investigación: Desarrolla proyectos de investigación para analizar las últimas amenazas y tendencias en ciberseguridad, y para mejorar las capacidades de detección y respuesta a incidentes.
- Coordinación: Colabora con otros organismos nacionales e internacionales para compartir información y buenas prácticas, y para fortalecer la respuesta global a las ciberamenazas.
- Prevención: Difunde información y consejos de seguridad a través de la Oficina de Seguridad del Internauta (OSI) y otras iniciativas.

Público objetivo:

- Ciudadanos: La OSI ofrece información y servicios gratuitos para ayudar a los usuarios a navegar por internet de forma segura.
- Empresas y profesionales: INCIBE-CERT pone a disposición de las empresas una serie de herramientas y recursos para mejorar su seguridad informática.
- Expertos en ciberseguridad: INCIBE colabora con la comunidad de expertos en ciberseguridad para compartir conocimientos y desarrollar soluciones innovadoras.

Naturaleza y funciones de los organismos de gestión de incidentes

Organismos CERT/CSIRT

ENISA es una agencia de la Unión Europea encargada de velar por la ciberseguridad en Europa. Su objetivo principal es garantizar un nivel alto y común de ciberseguridad en todos los países miembros de la UE. Se creó por decisión del Consejo y del Parlamento Europeo y su sede está en Grecia, en la isla de Creta.

Algunas de sus funciones son:

- Desarrollar e implementar estrategias de ciberseguridad para la Unión Europea.
- Ayudar a los Estados miembros a mejorar sus capacidades de ciberseguridad.
- Proporcionar asesoramiento y recomendaciones sobre buenas prácticas en ciberseguridad.
- Prevenir, detectar y responder a los ciberataques.
- Cooperar con organismos internacionales en materia de ciberseguridad.

La ENISA es un recurso importante para empresas, organizaciones y ciudadanos de la Unión Europea que buscan información y asesoramiento sobre ciberseguridad.

Naturaleza y funciones de los organismos de gestión de incidentes

Organismos CERT/CSIRT

El Forum of Incident Response and Security Teams (FIRST) es una organización internacional sin ánimo de lucro reconocida como el principal foro mundial de equipos de respuesta a incidentes de seguridad.

Su objetivo principal es fomentar la colaboración entre los equipos de seguridad informática para mejorar la respuesta ante incidentes cibernéticos

Algunas de sus funciones son:

- Facilitar el intercambio de información entre los equipos de respuesta a incidentes.
- Desarrollar mejores prácticas para la gestión de incidentes de seguridad.
- Promover la formación y la educación en materia de ciberseguridad.
- Ayudar a los equipos de respuesta a incidentes a coordinarse entre sí para responder a incidentes globales.

FIRST está integrado por más de 600 equipos de respuesta a incidentes de seguridad de todo el mundo, incluidos equipos gubernamentales, empresariales, académicos y militares.

Algunas organizaciones españolas que son miembros de FIRST incluyen INCIBE-CERT (España) y CCN-CERT (España).

Resumen

Gestión de incidentes de seguridad informática:

Definición:

La gestión de incidentes de seguridad informática es un proceso integral que abarca la prevención, detección, análisis, contención, erradicación, recuperación y aprendizaje posterior a un incidente que afecta la confidencialidad, integridad o disponibilidad de la información.

Objetivos:

- Minimizar el impacto del incidente en la organización.
- Preservar la evidencia para facilitar la investigación.
- Aprender del incidente para mejorar las medidas de seguridad.

Herramientas:

- Herramientas SIM (Security Information Management): centralizan la información de seguridad de diferentes fuentes.
- Herramientas SEM (Security Event Management): correlacionan eventos de seguridad para identificar posibles incidentes.
- Herramientas SIEM (Security Information and Event Management): integran las funcionalidades de SIM y SEM.

Resumen

Gestión de incidentes de seguridad informática: (Fases)

1. Preparación y prevención:

- Implementar medidas de seguridad proactivas como firewalls, antivirus y sistemas de detección de intrusos (IDS).
- Desarrollar un plan de respuesta a incidentes que defina roles, responsabilidades y procedimientos.
- Capacitar al personal en materia de seguridad informática.

2. Detección y notificación:

- Monitorizar los sistemas y redes para identificar posibles intrusiones o anomalías.
- Implementar un sistema de alerta temprana para notificar a los responsables de seguridad de forma inmediata.
- Definir un protocolo de comunicación para informar a las partes interesadas sobre el incidente.

3. Análisis preliminar:

- Recopilar información sobre el incidente, como la fecha, hora, origen, tipo de ataque, sistemas afectados y datos comprometidos.
- Evaluar el impacto del incidente en la organización.
- Priorizar la respuesta al incidente.

4. Contención:

- Aislar los sistemas afectados para evitar la propagación del ataque.
- Desactivar cuentas de usuario comprometidas.
- Implementar medidas de mitigación para minimizar el impacto del incidente.

Resumen

Gestión de incidentes de seguridad informática: (Fases)

5. Erradicación:

- Eliminar el malware o la vulnerabilidad que causó el incidente.
- Restaurar los sistemas y datos a un estado seguro.
- Documentar el proceso de erradicación.

6. Recuperación:

- Restablecer los sistemas y servicios a su estado normal.
- Implementar medidas para evitar que el incidente vuelva a ocurrir.

7. Investigación y actividades posteriores:

- Investigar la causa del incidente para identificar las debilidades de seguridad.
- Documentar las lecciones aprendidas para mejorar las medidas de seguridad.
- Implementar medidas correctivas para prevenir futuros incidentes.

Resumen

Gestión de incidentes de seguridad informática:

Organizaciones de apoyo:

- CERT (Computer Emergency Response Team): equipos de respuesta a incidentes de seguridad informática a nivel nacional e internacional.
- INCIBE-CERT: CERT español que ofrece apoyo y asesoramiento a empresas y ciudadanos.

Beneficios de una buena gestión de incidentes:

- Reduce el tiempo de respuesta a los incidentes.
- Minimiza el impacto del incidente en la organización.
- Mejora la capacidad de recuperación ante un incidente.
- Permite aprender de los incidentes para mejorar las medidas de seguridad.