SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

3.1.1.MF0488_3. Capítulo 1
Parte 1
Respuesta ante incidentes de seguridad

JOSÉ PABLO HERNÁNDEZ

1. INTRODUCCIÓN

La prevención y contención de los incidentes de seguridad es vital para evitar intrusiones en los equipos.

A pesar de todas las medidas de prevención y contención implantadas, se puede producir un incidente: Es necesario establecer un plan de respuesta.

1. INTRODUCCIÓN

Fases a seguir:

- **Verificación de la intrusión.**
- **Recolección de información.**
- **Precisar qué ha sucedido con el uso de técnicas y herramientas.**

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN

La seguridad de la información consiste en el establecimiento de una serie de medidas por parte de las organizaciones que permitan proteger la información manteniendo sus propiedades de confidencialidad, disponibilidad e integridad:

- **Medidas preventivas:** establecimiento de contraseñas, políticas de seguridad, cortafuegos, procedimientos de copias de respaldo, 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.

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN

Se destacan los siguientes beneficios de aplicar una gestión de incidentes :

- **Respuesta sistemática a los incidentes de seguridad.**
- **Agiliza y facilita el proceso de recuperación de equipos y sistemas ante el acontecimiento de incidentes de seguridad. Además reduce la pérdida de datos y el tiempo de interrupción de servicios.**
- **A través del aprendizaje se previenen los incidentes reiterados.**
- **Mejora continua de la seguridad de la organización y del proceso de gestión y tratamiento de incidentes.**
- **Facilita la gestión de los aspectos legales referentes a los incidentes de seguridad.**

2.1. EQUIPO DE RESPUESTA DE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT)

La rapidez con la que se detecte, reconozca, analice y responda a una amenaza minimiza los daños y disminuye considerablemente los costes ligados a la recuperación de la información.

2.1. EQUIPO DE RESPUESTA DE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT)

El término de equipo de respuesta a incidentes de seguridad informática CSIRT (Computer Security Incident Response Team) surgió a finales de los 90 en EE.UU ante la necesidad de designar un conjunto de personas especializadas encargadas específicamente de la gestión y tratamiento de incidentes.

2.1. EQUIPO DE RESPUESTA DE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT)

Toda organización, independientemente del tamaño que sea, debe designar a uno o varios responsables que se encarguen de ejecutar con detalle las tareas asignadas en el plan de respuesta a incidentes definido en cada organización.

2.1. EQUIPO DE RESPUESTA DE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT)

El Plan de Gestión de Incidentes está elaborado por el responsable de seguridad informática de la empresa y consiste en un conjunto de tareas y procedimientos encaminados a la correcta y adecuada gestión de incidentes de seguridad junto con las personas designadas para llevar a cabo todas y cada una de estas tareas.

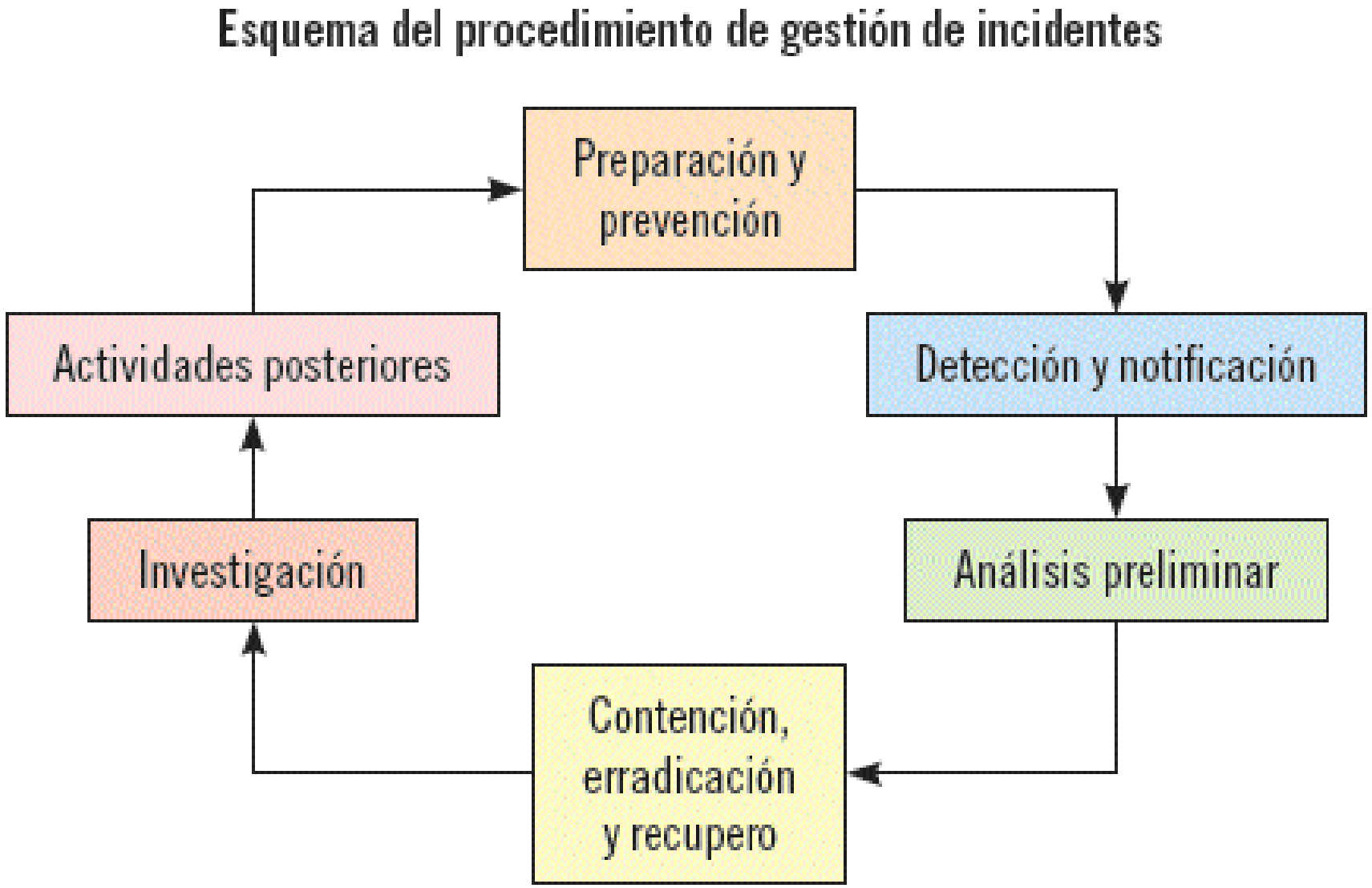
Un buen Plan de Gestión de Incidentes permite a las organizaciones la automatización de numerosos procesos de respuesta ante incidentes y la reducción considerable de los daños ocasionados, a la vez que se facilita la recuperación de los sistemas afectados.

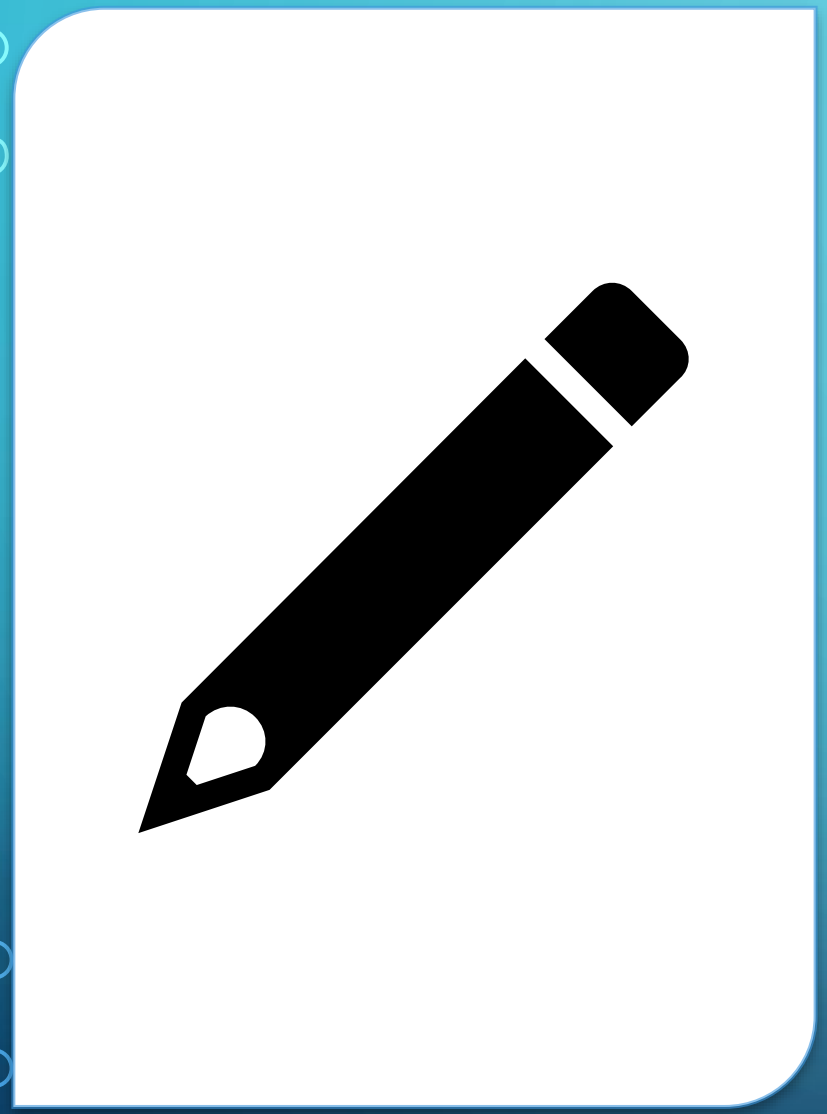
2.1. EQUIPO DE RESPUESTA DE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT)

El equipo de respuesta ante incidentes de seguridad, además de la confección del Plan de Gestión de Incidentes, deberá encargarse de establecer:

- **Una política general de gestión de incidentes en la que se deberá basar el plan de gestión.**
- **Los procedimientos a seguir para la gestión de incidentes basados en la política e incluidos en el plan.**
- **Relaciones entre el equipo de respuesta a incidentes y otros grupos de la organización internos y externos.**
- **Las guías en las que se defina el procedimiento a seguir en la comunicación de la organización con terceros en caso de ocurrencia de incidentes.**
- **Organización de los responsables de la gestión de respuesta a incidentes y definición y asignación de funciones.**

2.1. EQUIPO DE RESPUESTA DE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT)





Ejemplo

EN SU ORGANIZACIÓN SE HA DETECTADO UN INCIDENTE Y HA VERIFICADO QUE ES UN INCIDENTE REAL Y QUE NO SE TRATA DE UNA FALSA ALARMA. EN ESTOS MOMENTOS VA A PROCEDER A RECOGER INFORMACIÓN DEL INCIDENTE QUE SE ESTÁ PRODUCIENDO. ¿CUÁL ES LA INFORMACIÓN QUE DEBE OBTENER SOBRE EL INCIDENTE?

Ejemplo. Solución

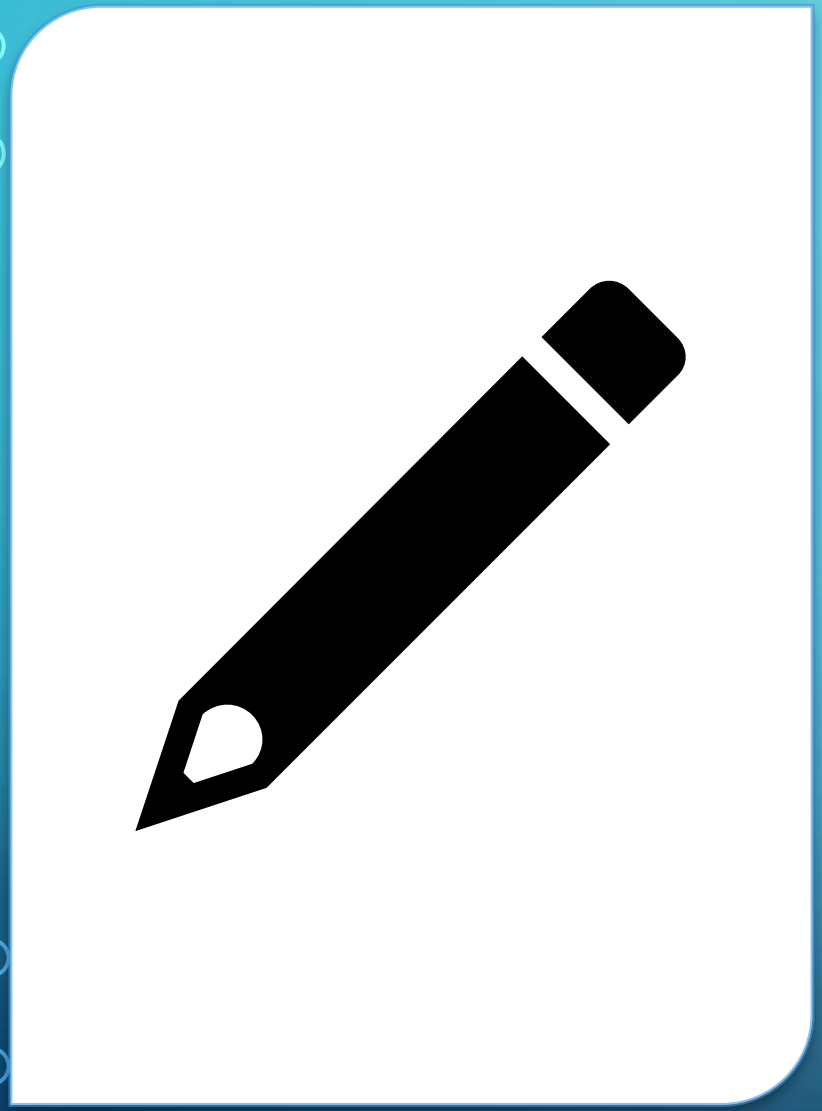
UNA VEZ COMPROBADO QUE EL INCIDENTE PRODUCIDO ES REAL HAY QUE RECOGER INFORMACIÓN SOBRE EL MISMO CONSISTENTE EN:

EL ALCANCE DEL INCIDENTE, A QUÉ HA AFECTADO: REDES, EQUIPOS, SISTEMAS Y APLICACIONES.

QUÉ HA SIDO LO QUE HA ORIGINADO EL INCIDENTE.

IMPACTO DEL INCIDENTE EN LAS ACTIVIDADES, SERVICIOS Y PROCESOS QUE SE LLEVAN A CABO EN LA ORGANIZACIÓN.

CÓMO HA OCURRIDO EL INCIDENTE: HERRAMIENTAS Y MÉTODOS UTILIZADOS Y VULNERABILIDADES DETECTADAS Y EXPLOTADAS.

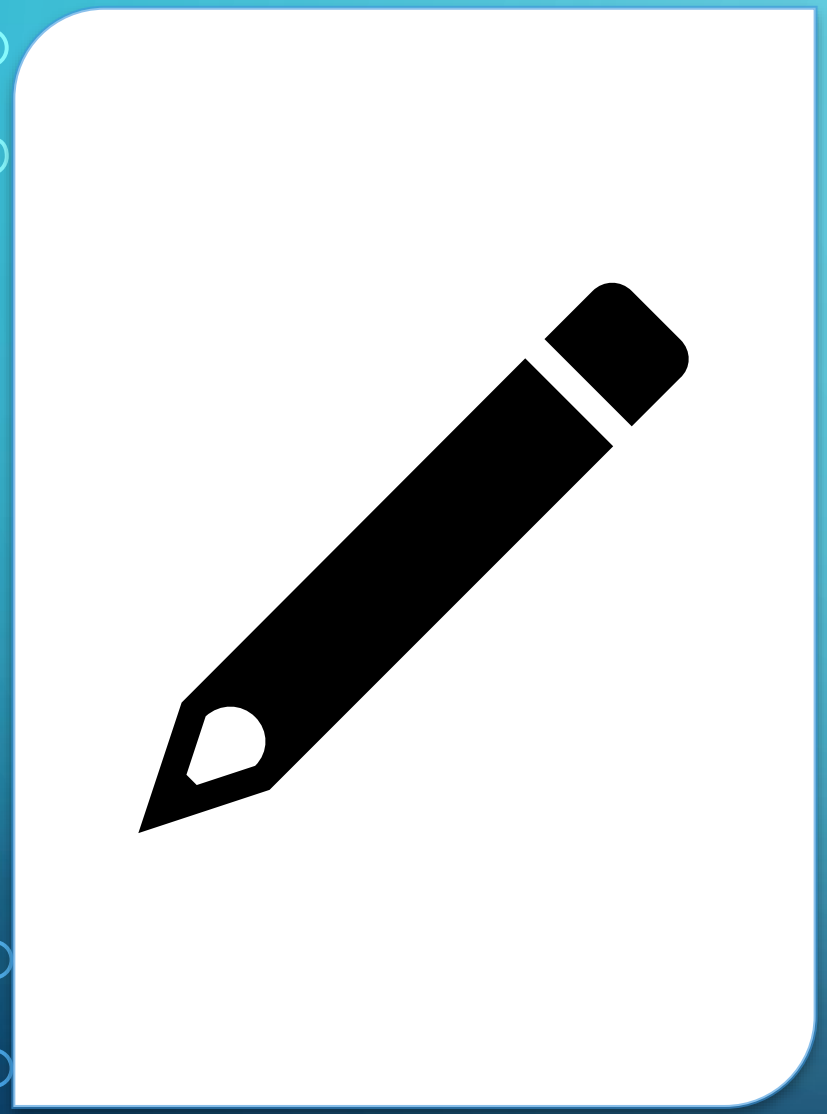


Ejemplo

USTED, COMO RESPONSABLE DE SEGURIDAD DE SU EMPRESA, ESTÁ LLEVANDO A CABO UN PROCESO DE CATEGORIZACIÓN DE LOS POSIBLES INCIDENTES QUE PUEDEN OCURRIR.

ENTRE ELLOS HA PROPUESTO DOS INCIDENTES DISTINTOS: UNO CUYA CRITICIDAD DE LOS RECURSOS ES ALTA Y LOS EFECTOS QUE PUEDE PRODUCIR SON MODERADOS Y OTRO CUYOS EFECTOS NEGATIVOS SON GRAVES Y CUYA CRITICIDAD DE LOS RECURSOS IMPLICADOS ES TAMBIÉN ELEVADA.

INDIQUE LA CRITICIDAD DE CADA INCIDENTE Y EL TIEMPO DE REACCIÓN MÁXIMO ANTE CADA UNO DE ELLOS.



Ejemplo. Solución

EN CUANTO AL PRIMER INCIDENTE, AL TENER UNA CRITICIDAD DE RECURSOS ALTA Y UNOS EFECTOS NEGATIVOS MODERADOS, SU NIVEL DE CRITICIDAD GENERAL ES “GRAVE”. SU TIEMPO MÁXIMO DE REACCIÓN DEBE SER DE 30 MINUTOS.

EN REFERENCIA AL SEGUNDO INCIDENTE, ESTE TIENE ALTA CRITICIDAD DE RECURSOS Y EFECTOS NEGATIVOS GRAVES, POR LO QUE SU NIVEL DE CRITICIDAD GENERAL SE ESTABLECE EN “MUY GRAVE”. EL TIEMPO DE RESPUESTA MÁXIMO ANTE ESTE TIPO DE INCIDENTES DEBE SER DE 10 MINUTOS.

3. TÉCNICAS Y HERRAMIENTAS

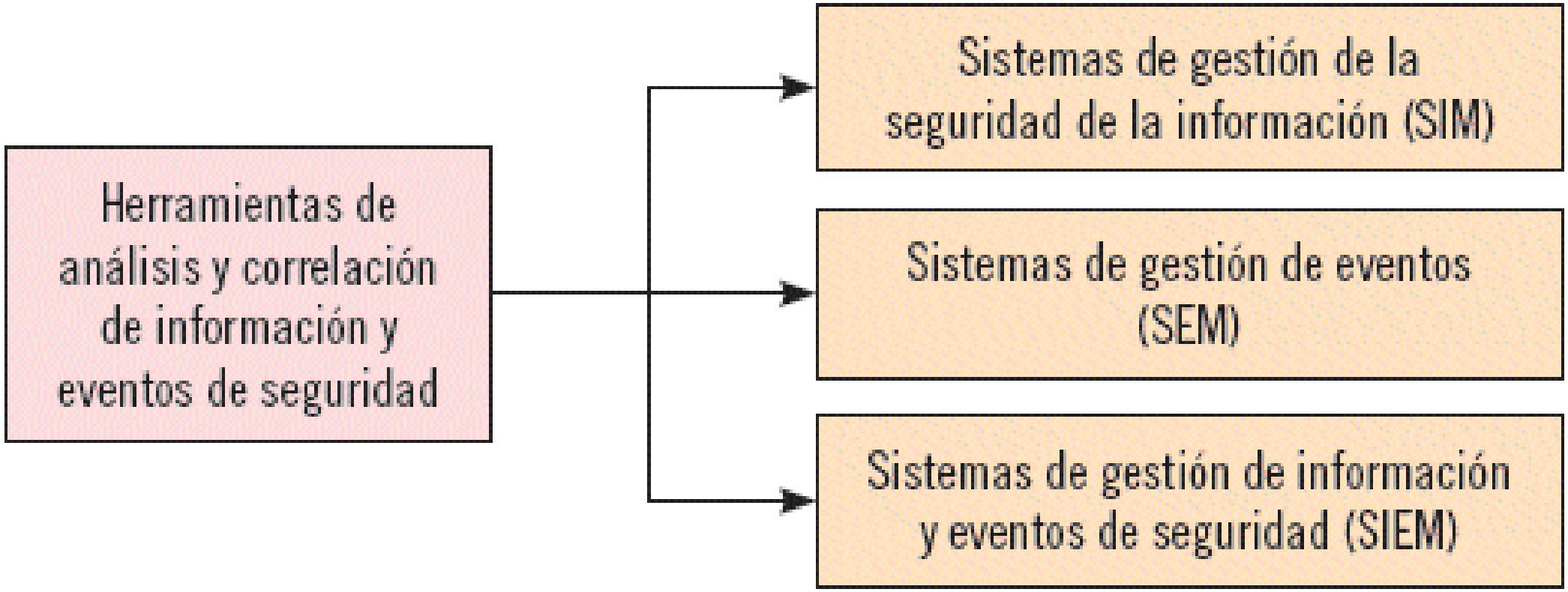
Las herramientas de gestión de información y eventos de seguridad son un conjunto de productos cuya función es la gestión de eventos o incidentes de seguridad en cualquiera de sus fases, tanto antes, como durante o después de la ocurrencia del incidente. Se encargan de recoger, cotejar y elaborar informes con los datos facilitados por los logs.

3. TÉCNICAS Y HERRAMIENTAS

Un sistema de análisis y correlación de eventos permite:

- **La determinación en tiempo real de la probabilidad de materializarse una amenaza en un momento concreto.**
- **La detección a tiempo real del inicio de un ataque, emitiendo alertas con la menor demora posible.**
- **El conocimiento del éxito o fracaso de un ataque y de su impacto real sobre el sistema.**
- **La determinación de los patrones de materialización de las amenazas para ser utilizados en la implantación de nuevas medidas de seguridad.**

3. TÉCNICAS Y HERRAMIENTAS



3.1. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SIM)

- Recogida, ordenación y correlación de información de la red.
- Automatización y monitorización de los eventos de sistemas y dispositivos de seguridad.
- Centralización, correlación y priorización de eventos con el fin de:
  - Estandarizar los eventos.
  - Reducir lo máximo posible el tiempo de detección de ataques y vulnerabilidades en la red.
  - Minimizar la información a procesar para obtener mejoras de rendimiento.

3.2. SISTEMAS DE GESTIÓN DE EVENTOS (SEM)

- Acceso a los registros a través de una interfaz central consistente.
- Almacenamiento seguro de los registros, manteniendo su integridad.
- Representación gráfica de la actividad para una elaboración de informes más sencilla, visual y práctica.
- Activación de alertas programadas.
- Gestión de eventos de varios sistemas operativos.
- Recuperación de registros ante bloqueos del sistema o eliminación inesperada de registros

3.2. SISTEMAS DE GESTIÓN DE EVENTOS (SEM)

A parte de las distintas funciones de las herramientas SIM y SEM hay que remarcar que las herramientas SIM trabajan en diferido (análisis del incidente una vez ya ha sucedido) mientras que las herramientas SEM trabajan a tiempo real (análisis del incidente cuando está ocurriendo).

3.3. 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: recogen los logs de los equipos, sistemas y dispositivos monitorizados, los almacenan a largo plazo y, además, 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.

3.3. SISTEMAS DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIEM)

- 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 gracias a 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.

Ejemplo.

LE HAN ENCARGADO LA IMPLANTACIÓN DE HERRAMIENTAS PARA ANALIZAR Y CORRELACIONAR LA INFORMACIÓN Y LOS EVENTOS DE SEGURIDAD PARA PODER OBTENER MÁS INFORMACIÓN DE LOS INCIDENTES DE SEGURIDAD QUE PUEDAN SUCEDER EN LOS EQUIPOS DE SU EMPRESA. LE HAN INDICADO QUE QUIEREN HERRAMIENTAS QUE ANALICEN Y GESTIONEN LOS EVENTOS A TIEMPO REAL PARA PODER REACCIONAR DE INMEDIATO ANTE INDICIOS DE INCIDENTES.

¿QUÉ TIPO DE HERRAMIENTA O HERRAMIENTAS DEBE IMPLANTAR?

Ejemplo. Solución.

PARA GESTIONAR LOS EVENTOS DE SEGURIDAD A TIEMPO REAL SE PUEDEN UTILIZAR DOS TIPOS DE HERRAMIENTAS. LAS HERRAMIENTAS SEM O SISTEMAS DE GESTIÓN DE EVENTOS Y LAS HERRAMIENTAS SIEM O SISTEMAS DE INFORMACIÓN Y EVENTOS DE SEGURIDAD FACILITAN INFORMACIÓN A TIEMPO REAL DE TODOS LOS EVENTOS QUE ESTÁN SUCEDIENDO EN EL SISTEMA. LAS HERRAMIENTAS SIM O SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN NO SE ADAPTAN A ESTOS REQUISITOS, YA QUE NO GESTIONAN LOS EVENTOS A TIEMPO REAL. ESTAS FACILITAN INFORMACIÓN SOBRE LOS EVENTOS EN DIFERIDO PARA PODER ELABORAR INFORMES UNA VEZ SUCEDIDOS LOS INCIDENTES.