SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

3.1.2.MF0488_3. Capítulo 1 Parte 2

Respuesta ante incidentes de seguridad

JOSÉ PABLO HERNÁNDEZ

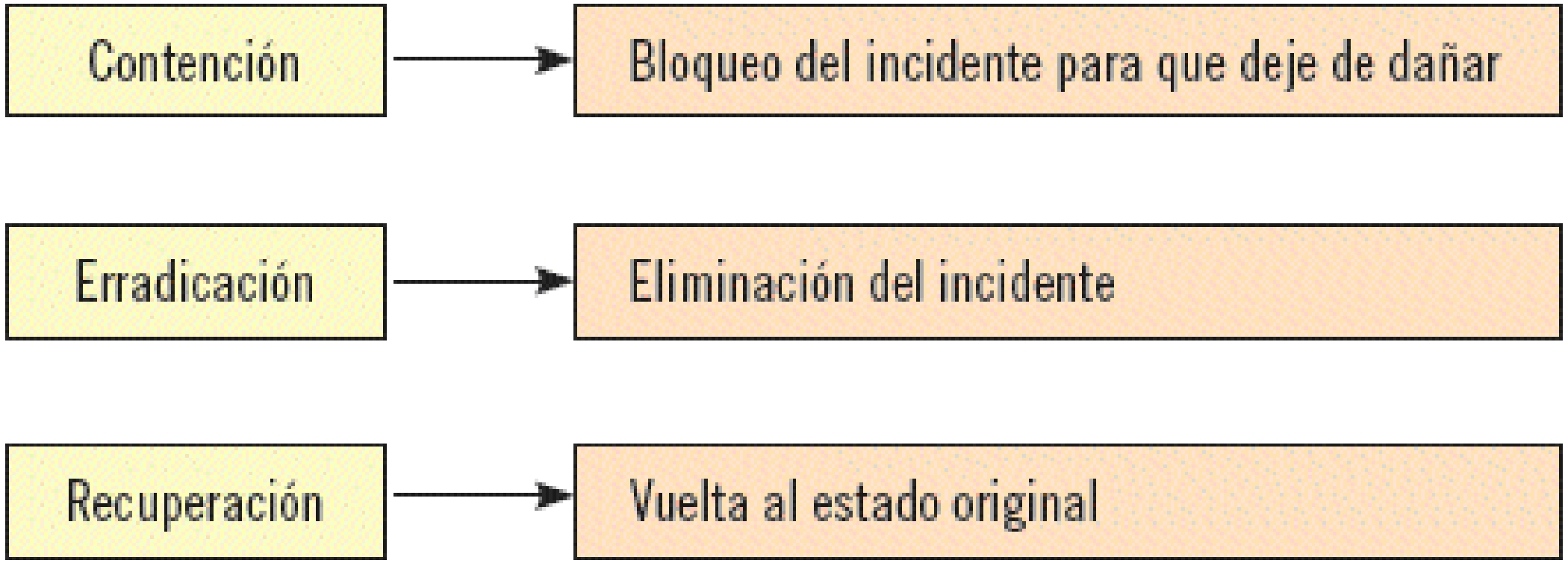
4. PROCESO DE VERIFICACIÓN DE LA INTRUSIÓN

Como ya se sabe, el incidente debe pasar por las fases de prevención y preparación, detección y notificación y análisis preliminar.

A partir de ahí, y una vez verificado que un incidente es real y concluido el proceso de recolección de información, para conocer con más profundidad sus detalles, se prosigue con la fase de contención, erradicación y recuperación.

4.1. CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN ANTE INCIDENTES DE SEGURIDAD

Fases de contención, erradicación y recuperación



4.1. CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN ANTE INCIDENTES DE SEGURIDAD

Por ejemplo, cuando se produce una infección de un virus en el equipo en las fases de contención, erradicación y recuperación debería realizarse lo siguiente:

Contención: desconectar el equipo afectado de la red para impedir que se propague a los demás equipos.

Erradicación: con un antivirus, localizar el virus y eliminarlo del equipo.

Recuperación: restaurar el sistema dañado con la última copia de respaldo realizada con los datos del equipo.

4.2. ELABORACIÓN DEL INFORME FINAL DEL INCIDENTE

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 en cuanto a daño en equipos, aplicaciones afectadas, información perdida, personal técnico especializado contratado, etc.**
- **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.**

4.2. ELABORACIÓN DEL INFORME FINAL DEL INCIDENTE

Evaluación de la toma de decisiones y de las actuaciones llevadas a cabo por el equipo de respuesta a incidentes:

- **Rapidez de respuesta en decisiones y medidas tomadas por el equipo de respuesta a incidentes.**
- **Personal integrante, formación recibida, organización y papeles 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:**
  - **Los procedimientos que no hayan funcionado deben rediseñarse.**
  - **Se deben adoptar medidas correctivas que mejoren la respuesta ante futuras incidencias.**

4.2. ELABORACIÓN DEL INFORME FINAL DEL INCIDENTE

Análisis de las políticas de seguridad:

- **Revisión de las políticas de seguridad de la información para detectar fallos y redefinir aquellas pautas ineficientes.**

4.2. ELABORACIÓN DEL INFORME FINAL DEL INCIDENTE

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.**

4.2. ELABORACIÓN DEL INFORME FINAL DEL INCIDENTE

Se puede obtener una imagen global de:

- **Por qué sucedió la intrusión.**
- **Qué es lo que ha quedado afectado.**
- **Cómo se ha actuado al respecto.**
- **Qué hay que modificar para que no vuelva a ocurrir.**

4.3. DOCUMENTACIÓN DEL INCIDENTE

- Reporte del incidente en el que se debe especificar:
  - Tipo de incidente.
  - Hechos ocurridos.
  - Daños ocasionados.
- Estado actual del incidente (fechando las distintas etapas por las que ha ido pasando el incidente).
- Conclusiones del análisis.
- Acciones y medidas tomadas para erradicar el incidente y restaurar los equipos afectados.
- Evidencias obtenidas en el proceso de análisis posterior.
- Personas involucradas, tanto a nivel interno de la empresa como a nivel externo (terceros).
- Acciones futuras y recomendaciones para aumentar el nivel de seguridad y evitar incidencias similares en próximas ocasiones.

5. FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES

CERT (Computer Emergency Response Team) o equipo de respuesta ante emergencias informáticas:

Centros de respuesta a incidentes de seguridad en tecnologías de información formados por un grupo de expertos encargados de diseñar medidas preventivas y reactivas ante incidentes de seguridad.

5. FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES

También surgieron los CSIRT (Computer Security Incident Response Team) o equipo de respuesta a incidentes de seguridad informática:

Organizaciones encargadas de recibir, revisar y responder a actividades y reportes de incidentes de seguridad informática ya vista anteriormente.

5. FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES

De los CERT/CSIRT hay que destacar tres tipos de servicios distintos:

Servicios reactivos: elaboración de informes de equipos, sistemas y dispositivos afectados por amenazas, códigos maliciosos, vulnerabilidades y otros eventos de seguridad detectados en los registros. Estas actividades son las funciones principales de los CERT y CSIRT. Los servicios principales son:

- Análisis de la situación.
- Elaboración de recomendaciones para controlar la situación ante incidentes.
- Diseño de contramedidas de seguridad para reducir el riesgo de futuras amenazas.

5. FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES

De los CERT/CSIRT hay que destacar tres tipos de servicios distintos:

Servicios proactivos: servicios de asistencia e información para ayudar a prevenir, preparar y proteger los sistemas, equipos y dispositivos de los usuarios para reducir el riesgo de producción de amenazas e incidentes en un futuro.

5. FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES

De los CERT/CSIRT hay que destacar tres tipos de servicios distintos:

Servicios de gestión de calidad de la seguridad: servicios independientes de la gestión de incidentes encargados de buscar herramientas y medidas que mejoren la calidad de la seguridad informática. Se basan sobre todo en actividades de concienciación y educación de los usuarios.

5. FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES

En cuanto a funciones de estos organismos cabe destacar las siguientes:

- Ayudar al público objetivo a prevenir y atenuar incidentes graves de seguridad.
- Ayudar a proteger informaciones y datos de gran valor.
- Coordinar centralizadamente la seguridad de la información.
- Apoyar y asistir a los usuarios para que el proceso de recuperación ante incidentes de seguridad sea lo más leve posible.
- Dirigir centralizadamente la respuesta ante incidentes de seguridad.

5. FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES

Para desempeñar sus funciones los CSIRT/CERT las llevan a cabo mediante:

- El mantenimiento de una base de datos de vulnerabilidades de seguridad para consulta, seguimiento y registro histórico.
- El mantenimiento de una base de datos de incidentes de seguridad de las organizaciones integrantes.
- Provisión de un servicio de asesoramiento especializado en seguridad de la información.
- Mantenimiento de contactos con otros CSIRT/CERT del mundo y sus organizaciones para intercambiar información.

5.1. ORGANISMOS DE GESTIÓN DE INCIDENTES

CERT/CC (Computer Emergency Response Team/Coordination Center)

El CERT/CC o equipo de respuesta a emergencias informáticas fue el primer equipo de respuesta y el más conocido. Su creación se produjo en 1.988 por la agencia DARPA de EE.UU con la finalidad de gestionar aquellos incidentes de seguridad relacionados con los servicios de internet.

Se puede consultar información del CERT/CC en: <http://www.cert.org>.

5.1. ORGANISMOS DE GESTIÓN DE INCIDENTES

Cert Inteco

Cert Inteco es el Centro de Respuesta a Incidentes de Seguridad en España. Fue creado en 2.006 dentro del Instituto Nacional de Tecnologías de la Comunicación y sus funciones se clasifican en tres pilares fundamentales:

Servicios: Inteco ofrece servicios de seguridad para proteger la privacidad de los usuarios y desarrollar herramientas que mejoren la efectividad de las medidas de prevención y reacción ante incidentes de seguridad.

Investigación: además de los servicios, también desarrolla funciones de investigación para analizar proyectos complejos de ciberseguridad y aplicar tecnologías y mecanismos emergentes en el combate de incidentes de seguridad.

Coordinación: Inteco también se coordina y colabora con otras entidades (públicas y privadas, nacionales e internacionales) para intercambiar información y facilitar la inmediatez, globalidad y efectividad de las medidas a tomar ante incidentes de seguridad.

Se puede encontrar más información de los servicios y funciones de Inteco en <http://www.inteco.es>.

5.1. ORGANISMOS DE GESTIÓN DE INCIDENTES

Cert Inteco

Cert Inteco	
Funciones	Servicios
	Investigación
	Coordinación
Público objetivo	Empresas y profesionales
	Expertos en ciberseguridad
	Ciudadanos

5.1. ORGANISMOS DE GESTIÓN DE INCIDENTES

Agencia Europea de Seguridad de las Redes de la Información

La Agencia Europea de Seguridad de las Redes y de la Información (European Network and Information Security Agency) se creó por decisión del Consejo y Parlamento Europeo para elevar los niveles de seguridad de las redes y del tratamiento de la información dentro de la Unión Europea. Se creó en 2.005 y fijó su sede en Grecia, en la isla de Creta.

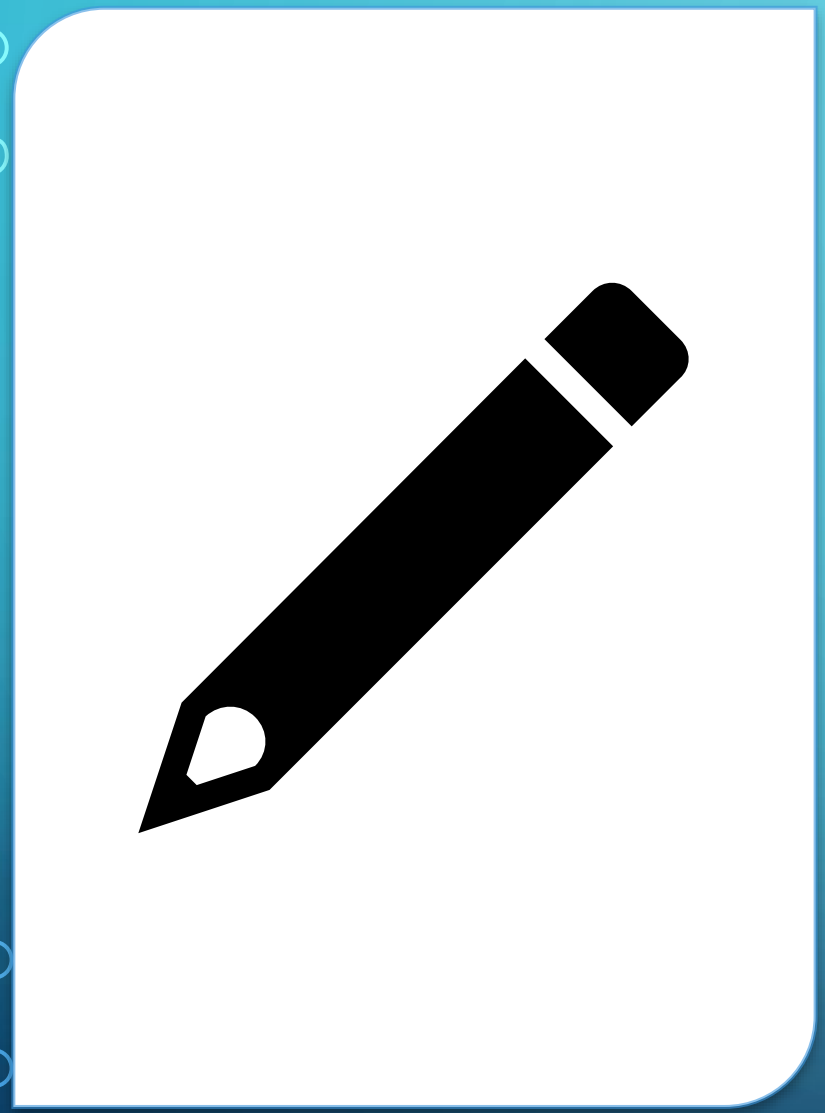
Su web oficial es <http://www.enisa.europa.eu>

5.1. ORGANISMOS DE GESTIÓN DE INCIDENTES

Forum of Incident Response and Security Teams (FIRST)

El Forum of Incident Response and Security Teams se creó en 1.990 con la finalidad de agilizar los procesos de intercambio de información sobre los incidentes de los centros de respuesta a incidentes de seguridad que integran la organización.

Se considera la asociación global de los CSIRT/CERT y su web oficial es <http://www.first.org>.



Ejemplo

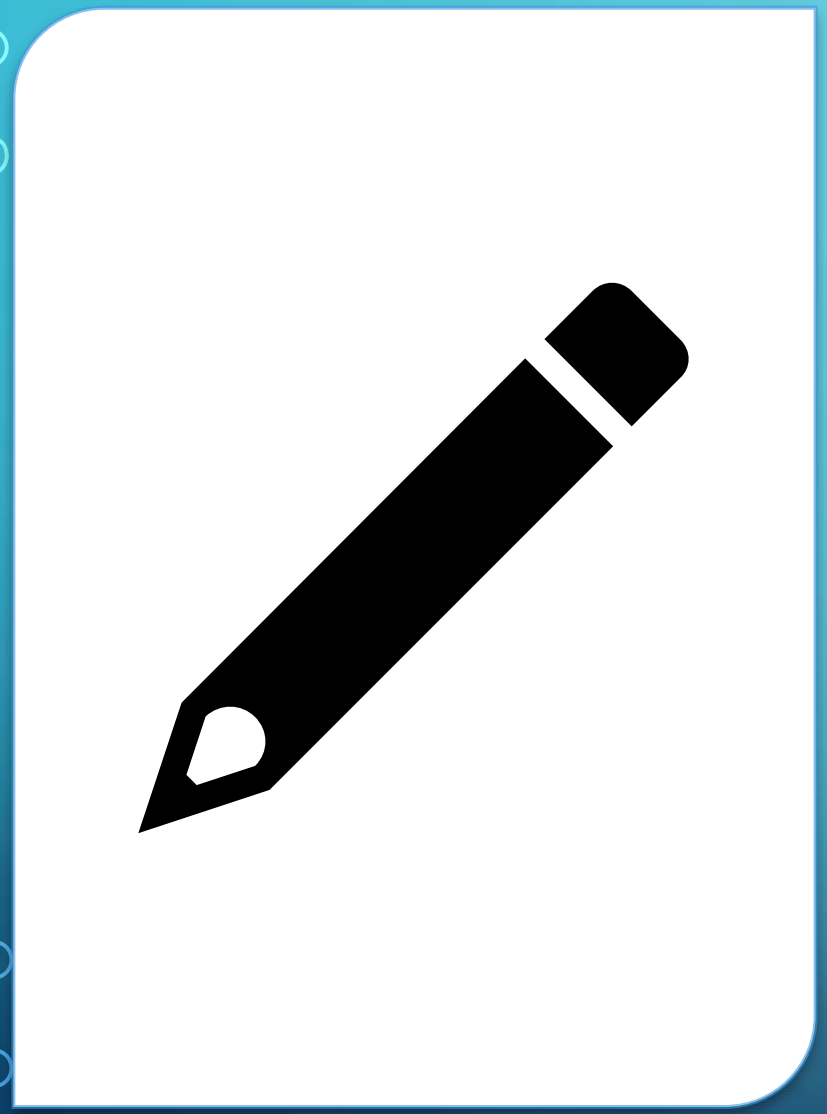
USTED Y SUS COMPAÑEROS DEL DEPARTAMENTO DE SEGURIDAD DE SU EMPRESA SON LOS ENCARGADOS DE IMPLEMENTAR UN PLAN DE GESTIÓN DE INCIDENTES DE SEGURIDAD QUE LES AYUDE A PREVENIR, CONTENER Y ELIMINAR LOS POSIBLES INCIDENTES QUE PUEDEN SUCEDER EN LOS EQUIPOS Y SISTEMAS DE LA ORGANIZACIÓN. COMO NO SON MUY EXPERTOS EN LA MATERIA QUIEREN RECURRIR A UN ORGANISMO NACIONAL QUE LES AYUDE EN LA IMPLEMENTACIÓN DE ESTAS MEDIDAS.

¿A QUÉ ORGANIZACIÓN DEBEN RECURRIR PARA RECIBIR MÁS INFORMACIÓN Y APOYO EN EL DISEÑO E IMPLANTACIÓN DEL PLAN? ¿QUÉ OTROS SERVICIOS OFRECE ESTA ORGANIZACIÓN?

Ejemplo. Solución

A NIVEL INTERNACIONAL HAY NUMEROSAS ORGANIZACIONES DE APOYO ANTE LA GESTIÓN DE INCIDENTES DE SEGURIDAD. A NIVEL NACIONAL, LA ORGANIZACIÓN ENCARGADA DE ESTOS ASUNTOS Y DE APOYAR A LAS EMPRESAS EN LA IMPLANTACIÓN DE SUS SISTEMAS DE GESTIÓN DE INCIDENTES ES LA LLAMADA CERT INTECO.

APARTE DE SERVICIOS DE APOYO Y AYUDA EN LA IMPLANTACIÓN DE ESTOS SISTEMAS, CERT INTECO TAMBIÉN OFRECE SERVICIOS DE INVESTIGACIÓN (ANALIZAN PROYECTOS COMPLEJOS DE CIBERSEGURIDAD CON LA APLICACIÓN DE NUEVAS TECNOLOGÍAS Y SISTEMAS EMERGENTES) Y DE COORDINACIÓN CON OTROS ORGANISMOS (TANTO PÚBLICOS COMO PRIVADOS) CON EL FIN DE CONSEGUIR LA IMPLANTACIÓN DE MEDIDAS MÁS EFECTIVAS Y RÁPIDAS ANTE INCIDENTES DE SEGURIDAD.



Ejercicios

3.1.100.1.MF0488_3_EJERCICIOSCAPITULO_1.DOCX