UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf

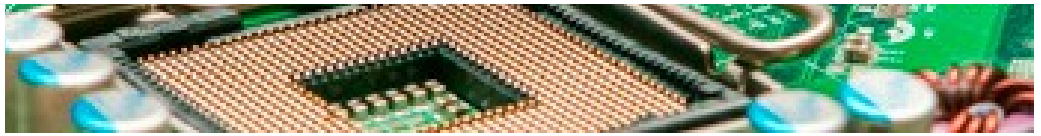
Máster Universitario en Ingeniería Informática

CyberSeguridad
Tema 9: Gestión de Ciber-Incidentes

José Ismael Ripoll Ripoll

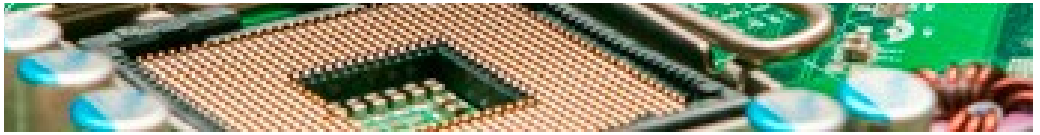
Máster Oficial Universitario en Ingeniería Informática
muiinf.webs.upv.es

MUIInf



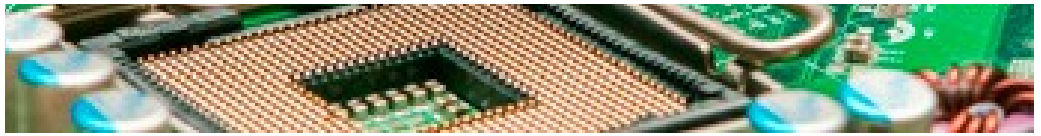
Contenido

- Terminología.
- Introducción.
- Las fases de un incidente.
  - Preparación
  - Identificación
  - Confinamiento
  - Eliminación
  - Recuperación
  - Aprendizaje



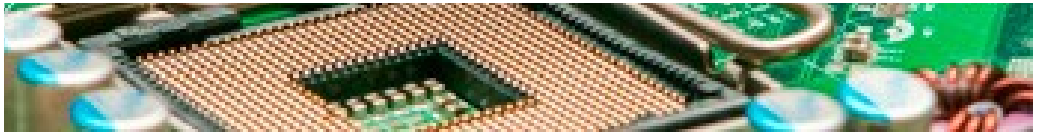
Términos

- **Ciberincidente**: Acción desarrollada a través del uso de redes de ordenadores u otros medios, que se traducen en un efecto real o potencialmente adverso sobre un sistema de información y/o la información que trata o los servicios que presta.
- **CSIRT**: Computer Security Incident Response Team.
- **Plan de Respuesta a Ciberincidentes**: Conjunto predeterminado y ordenado de instrucciones o procedimientos para detectar, responder y limitar las consecuencias de un ciberincidente.

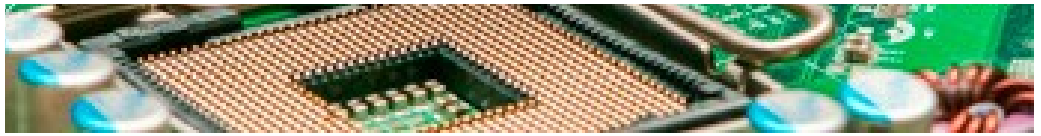


Términos

- **RAT**: Pieza de software que permite a un "operador" controlar a distancia un sistema como si se tuviera acceso físico al mismo. Aunque tiene usos perfectamente legales, el software RAT se asocia habitualmente con ciberataques o actividades criminales o dañinas. En estos casos, el malware suele instalarse sin el conocimiento de la víctima, ocultando frecuentemente un troyano

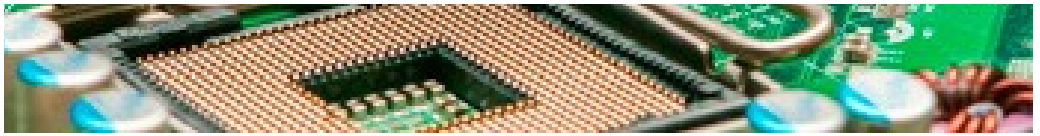


- El artículo 11 del ENS señala la obligación de que las entidades públicas de su ámbito de aplicación dispongan de una **Política de Seguridad** de la Información que articule una serie de Requisitos Mínimos de Seguridad. Entre tales requisitos se contempla la **Gestión de Incidentes de Seguridad,** exigencia que se concreta en el artículo 24 del mismo cuerpo legal, que señala que:
  - Se establecerá un **sistema de detección** y reacción frente a código dañino.
  - Se **registrarán los incidentes de seguridad** que se produzcan y las acciones de tratamiento que se sigan. Estos registros se emplearán para la mejora continua de la seguridad del sistema.



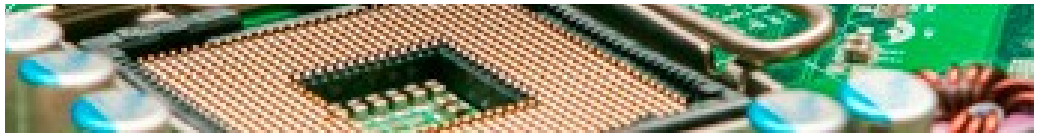
Fases de la gestión

- Las fases de la gestión de un ciberincidente cubren el antes, durante y el después del incidente:
  1) Preparación
  2) Identificación
  3) Confinamiento
  4) Eliminación
  5) Recuperación
  6) Aprendizaje



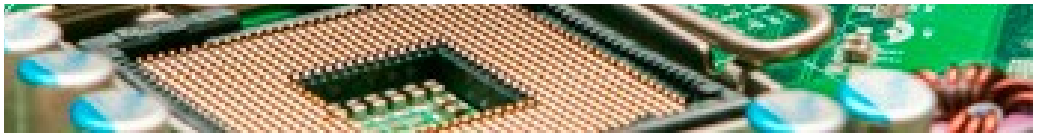
Fase de Preparación I

- Se deben abordar las siguiente tareas:
  - Definir una política con los principios, reglas y prácticas que rigen la organización. Y darla a conocer a los empleados.
  - Elaborar el plan/estrategia de respuesta.
    - Listar los activos y asignar prioridades y protocolos de actuación en función de su criticidad.
  - Decidir la comunicación interna (entre los componentes del ERC) y con el exterior (medios, clientes, CERT, fuerzas de seguridad, etc.)
    - **LUCIA**: Listado Unificado de Coordinación de Incidentes y Amenazas
    - **GPG**: cifrado de mail
  - Preparar la documentación que se utilizará (checklists, manuales, etc) y la que se tendrá que generar durante la respuesta.



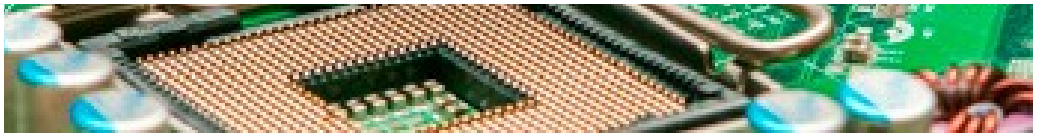
Fase de Preparación (II)

- Se deben abordar las siguiente tareas (cont):
  - Definir el Equipo de Respuesta a Ciberincidentes (ERC). Compuesto por abogados, relaciones públicas, equipo técnico, personal de seguridad, etc.
  - Asegurarse que el equipo ERC dispondrá de los permisos o credenciales especiales (o contraseñas).
  - Herramientas. Es imprescindible disponer tanto del software como del hardware necesario, incluidos destornilladores, sniffers, live-usb, extintores, portatiles, teléfonos, etc. Todo ello debe estar preparado para ser utilizado.
  - Entrenamiento. Es evidente que si el equipo no conoce las herramientas y está familiarizado con la organización, la respuesta será mala. Los integrantes del equipo debe conocerse bien entre ellos y establecer los lazos de "confianza" necesarios para trabajan en equipo con seguridad.



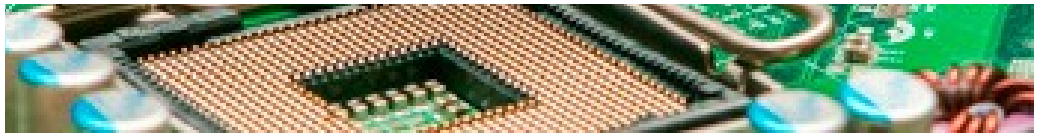
Fase de Preparación(III)

- Material de campaña preparado:
  - Libreta para anotar los eventos durante el incidente: quién, qué, dónde, porqué y cómo de cada decisión, acción indicio.
  - Lista de contactos: miembros del ECR, policía, bomberos, hospitales, etc.
  - Discos extraíbles: HD o USB.
  - USB-live. Con una instalación para hacer análisis forense.
  - Equipo portátil "**confiable**" con software instalado. Que no estuviera conectado a la red.
  - Juego de destornilladores para poder acceder físicamente a los equipos.
  - Bolsa para transportar todo.
- Estaremos trabajando con pruebas de "**delitos**".



Fase de Identificación

- Determinar si una anomalía de funcionamiento es causada por un incidente se seguridad.
  - También hay que determinar el ámbito del incidente.
- Se recogen y analizan "eventos" de varias fuentes:
  - Log files, firewalls, IDS, operarios, etc.
- Los trabajadores deben ser elementos activos en la identificación de incidentes, y deben notificarlos al responsable de seguridad
- **Documentar** las primeras fases del incidente es fundamental, para evitar problemas legales.
  - Todas las anotaciones deben estar fechadas.



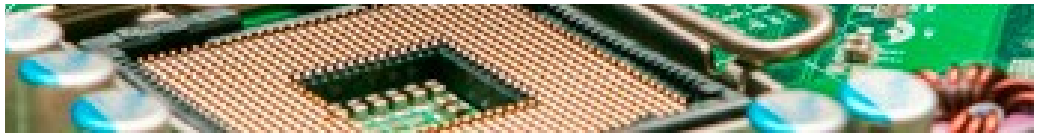
Fase de Contención

- Tratar de limitar el daño que se pueda causar. Lo que se consigue con un confinamiento a corto plazo:
  - Aislar el equipo o segmento de red afectado.
  - Realizar una copia del sistema afectado cuanto antes para poder hacer un estudio forense a posteriori.
  - Buscar y liminar las puertas de acceso (backdoors)
  - Instalar parches de seguridad en el equipo afectado y adyacentes.
  - **Documentar** lo que se hace.

En esta fase los nervios y las prisas pueden ser un problema.

Calma.

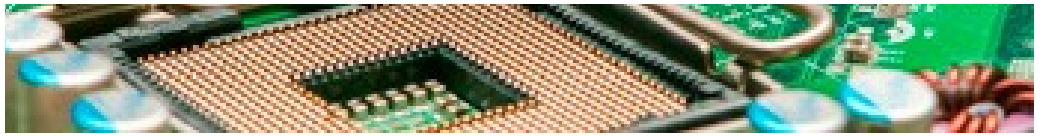
Escribir relaja.



Fase de Eliminación

- Substitución de los los sistemas afectados.
- Un sistema afectado debe ser reinstalado por completo a partir de un estado seguro y confiable.
  - Un sistema que ha sido hackeado… no es confiable.
- Reinstalar tanto el sistema operativo como las aplicaciones.
  - Actualizando los parches de seguridad.

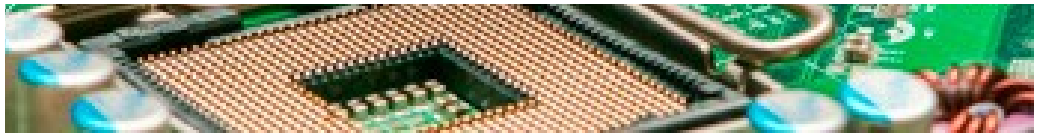
- Revisar que el incidente no haya afectado a las copias de backup.
  - Para ello es necesario determinar el inicio del mismo.
- Asegurarse que el atacante no puede volver a entrar.



Fase de Recuperación

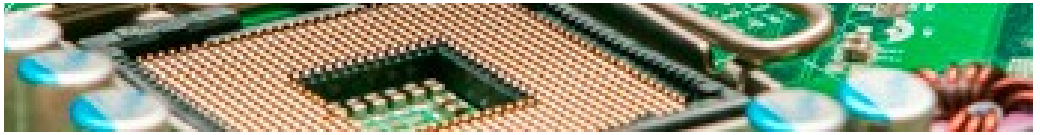
- Restaurar los datos y aplicaciones del equipo para poder ponerlo en producción.
- Las copias de seguridad son aquí un fundamentales.
- Se tiene que monitorizar de cerca el equipo para verificar que el fallo utilizado en el ataque no está presente.
- Se tiene que decidir:
  - Cuándo se repone el servicio.
  - Cómo determinar que el sistema está limpio.
  - Cuánto tiempo se mantendrá en supervisión el sistema.
  - Qué herramientas se emplearan para monitorizarlo.

Hay que evitar que se produzca otro incidente similar.
¡Sería un gran desprestigio!



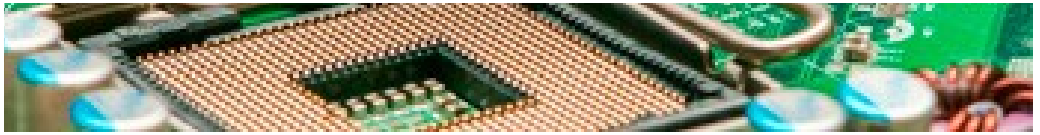
Fase de Aprendizaje (I)

- El objetivo es completar y organizar la información recogida durante el incidente para:
  - Aprender de los posibles errores.
  - Mejorar el sistema prevención de incidentes y la seguridad en su conjunto.
  - Disponer de evidencias de los hechos en caso de tener que emprender acciones legales.
  - Se puede utilizar como material explicativo para nuevos miembros del equipo.
- El equipo debería reunirse transcurridos unos días del incidente (~2 semanas) para analizar con calma.



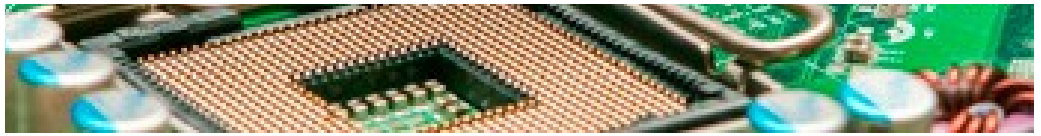
Fase de Aprendizaje (II)

- Los incidentes de cierta importancia deben concluir con un informe breve donde se exponga:
  - Cómo se inicio el incidente.
  - Ámbito y repercusión.
  - Cómo se contuvo en los primeros momentos.
  - Detalles de las actividades realizadas en la recuperación.
  - Aspectos positivos y elementos a mejorar del equipo y los protocolos de seguridad.



Checklist para recopilar info

- Preparase una lista de ordenes y acciones a realizar.
- Existen muchas lista públicas que podemos utilizar como base:
  - https://zeltser.com/security-incident-survey-cheat-sheet/
  - https://www.sans.org/score/checklists
  - https://www.cst.ucf.edu/wp-content/uploads/infosec/Procedure_for_Unix_Incident_Response.pdf
  - https://wikihead.wordpress.com/incident-handling/



Referencias

- https://www.us-cert.gov/sites/default/files/publications/data_backup_options.pdf
- SANS Incident Response Whitepaper:
  - http://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
- Incluso en The Hacker News:
  - http://thehackernews.com/2015/11/how-to-incident-response-plan.html
- GUÍA DE SEGURIDAD DE LAS TIC CCN-STIC-817 ESQUEMA NACIONAL DE SEGURIDAD GESTIÓN DE CIBERINCIDENTES:
  - https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html