T4. Respuesta ante incidentes de seguridad

Apartados del BOE

* 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 tipo CERT nacionales e internacionales

Incidentes de seguridad

Un incidente de seguridad es:

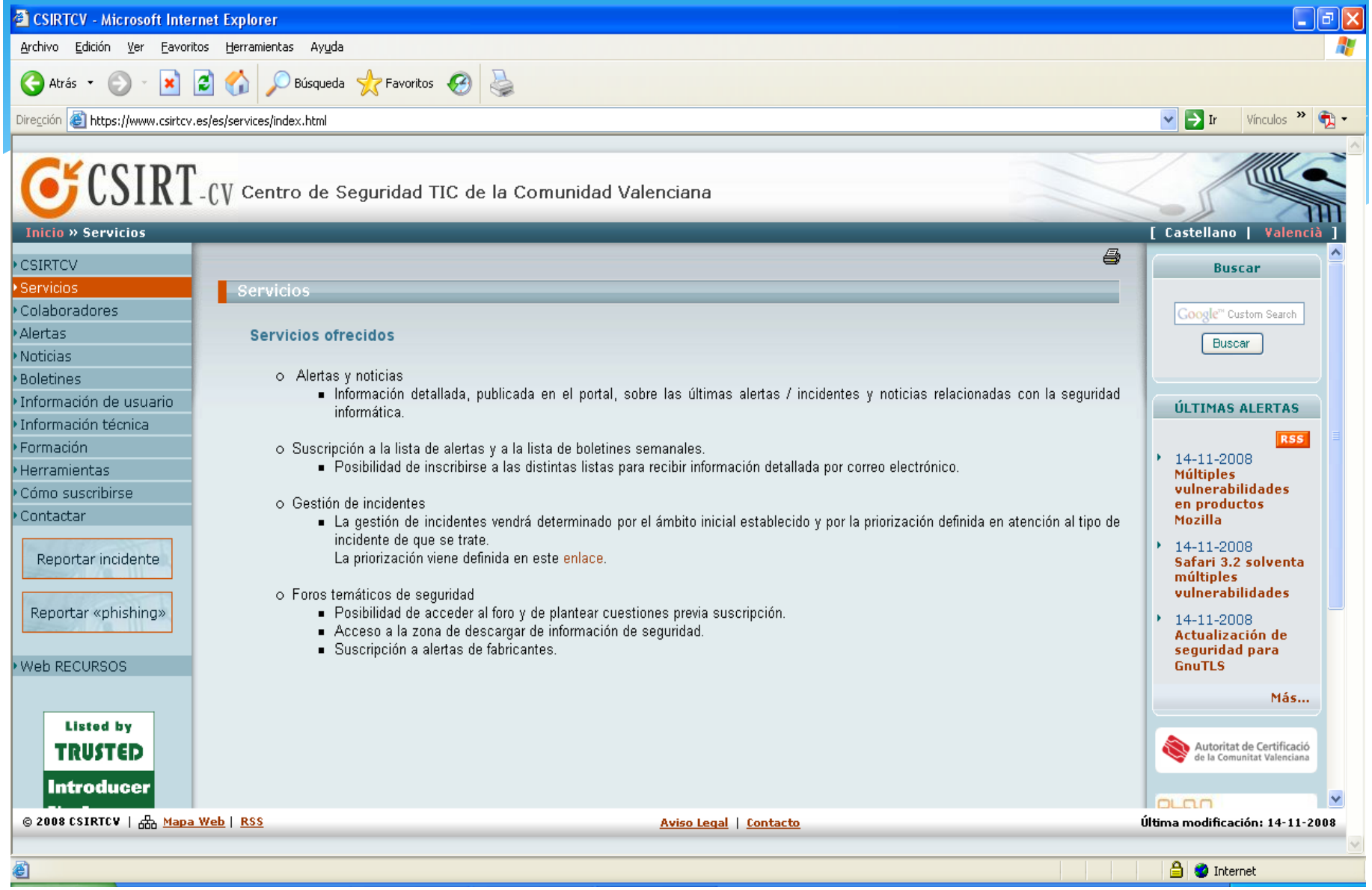
* Cualquier evento adverso real o sospechado en relación a la seguridad de los sistemas o redes informáticas;
* La violación de una política de seguridad implícita o explícita

Para tratar los incidentes debe haber un equipo (CSIRT) formado por personal con experiencia en el trato de incidentes que tendrá por objetivo:

* Recibir, revisar y responder a los incidentes de seguridad.
* Ayudar a las organizaciones a contener y recuperarse de violaciones y amenazas en la seguridad informática.

A nivel nacional suele haber un CSIRT para dar repuesta coordinada a los incidentes. Ejemplo para las administraciones publicas españolas https://www.ccn-cert.cni.es/

https://www.ccn-cert.cni.es/index.php?option=com_content&view=article&id=12&Itemid=32&lang=es


CSIRTCV - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos
Dirección https://www.csirtcv.es/es/services/index.html
Ir Vínculos
CSIRT-CV Centro de Seguridad TIC de la Comunidad Valenciana
Inicio » Servicios
[Castellano | Valencià]
CSIRTCV
Servicios
Colaboradores
Alertas
Noticias
Boletines
Información de usuario
Información técnica
Formación
Herramientas
Cómo suscribirse
Contactar
Reportar incidente
Reportar «phishing»
Web RECURSOS
Listed by TRUSTED Introducer
Servicios
Servicios ofrecidos
Alertas y noticias
Información detallada, publicada en el portal, sobre las últimas alertas / incidentes y noticias relacionadas con la seguridad informática.
Suscripción a la lista de alertas y a la lista de boletines semanales.
Posibilidad de inscribirse a las distintas listas para recibir información detallada por correo electrónico.
Gestión de incidentes
La gestión de incidentes vendrá determinado por el ámbito inicial establecido y por la priorización definida en atención al tipo de incidente de que se trate.
La priorización viene definida en este enlace.
Foros temáticos de seguridad
Posibilidad de acceder al foro y de plantear cuestiones previa suscripción.
Acceso a la zona de descargar de información de seguridad.
Suscripción a alertas de fabricantes.
Buscar
Google Custom Search
Buscar
ÚLTIMAS ALERTAS
RSS
14-11-2008 Múltiples vulnerabilidades en productos Mozilla
14-11-2008 Safari 3.2 solventa múltiples vulnerabilidades
14-11-2008 Actualización de seguridad para GnuTLS
Más...
Autoritat de Certificació de la Comunitat Valenciana
© 2008 CSIRTCV | Mapa Web | RSS
Aviso Legal | Contacto
Última modificación: 14-11-2008
Internet

En una empresa es fundamental identificar las necesidades de seguridad de una organización para establecer las medidas que permitirán a dicha organización actuar adecuadamente frente a un incidente.

No obstante, es imposible evitar por completo todo tipo de riesgos, por lo que todas las empresas deben estar preparadas para experimentar algún día un incidente. resulta fundamental una reacción rápida y coordinada. Esta reacción suele dirigirse por un grupo especializado en incidentes CSIRT.

Es **fundamental** detectar el incidente a tiempo. Identificar y analizar el incidente lo debe hacer este grupo, suelen darse falsos positivos.

Ejemplos reales de incidentes

Infección masiva de virus

- Un virus enviado en un anexo de e-mail infectó el PC de un usuario.
- En pocas horas, la infección se propagó a diferentes redes en distintos países, provocando la saturación de diversos enlaces y la no disponibilidad de diversos servicios de la empresa.
- Se diseñó un plan de aislamiento y remediación, para evitar en primer instancia que la infección se siga propagando, y avanzar luego en la eliminación de la infección y reparación de los equipos.
- En 24 horas se recuperó la mayor parte de la operatoria normal, se comenzó a trabajar en un **plan de prevención para evitar nuevas ocurrencias**.

Fuga de información (wikileaks)

Un mail interno enviado entre directivos, en el que se mencionaba la estrategia de negociación de la compañía frente a la compra de otra compañía llego a manos de la otra empresa.

Se efectuaron revisiones sobre diversos equipos, archivos de auditoria, bases de datos y BackUps del servicio de e-mail, no encontrándose evidencia de robo de información.

Se analizó el documento impreso y se determinó que el mismo había sido enviado por fax

Borrado de equipos

Se detectaron algunos equipos Unix con la mayor parte de sus archivos eliminados. Esto afecto a la producción de la empresa por lo que se restauraron rápidamente pero volvieron a borrarse.

Se analizaron en detalle los servidores involucrados, y se determinó que el borrado lo producía un script automático de mantenimiento

¿Pero como? Si el script funcionó sin problemas durante años y no había sido modificado…

Finalmente se determinó que el script tenía un error, pero era "tolerado" por las versiones anteriores del intérprete. En los servidores involucrados, se había actualizado el intérprete.

Sabotaje corporativo

Un empleado descontento colocó una “bomba lógica” en el servidor que controla la línea de cajas de una de las sucursales de la empresa, provocando la salida de producción de las mismas un sábado en hora punta.

Una vez reportado el incidente, se comenzó por identificar la naturaleza y las causas del mismo. Dado que era urgente volver a la operatoria normal, se realizaron imágenes forenses de diferentes equipos y servidores, así como de archivos de log para su análisis posterior.

El análisis forense y la correlación de eventos permitieron identificar el equipo desde donde se realizó el ataque, y mas tarde al responsable del mismo.

¿Por qué suceden los Incidentes de Seguridad?

* Falta de conciencia sobre seguridad de la información.
* Falta de controles adecuados.
* Exceso de “confianza”.
* Amplia disponibilidad de herramientas.
* Sensación de “anonimato” en las redes.
* Crecimiento de la dependencia tecnológica de la información.
* Disponibilidad de datos sensibles.
* Oferta y demanda de información confidencial más abierta.

¿Cómo detectar un incidente?

Hay varias vías por las que una organización detecta un incidente:

* Mediante revisiones operativas
* Revisión y correlación de eventos
* Revisión de alarmas
* Por reporte de un usuario a una mesa de ayuda o a Seguridad de la Información
* Reporte del usuario a su superior
* Mediante terceras partes
* Extorsión, amenaza
* Acción de público conocimiento
* Siempre es preferible detectar el incidente internamente, y lo antes posible, para minimizar sus efectos

Se detectó un incidente, ¿y ahora qué hacemos?

Antes que nada, es imprescindible determinar si REALMENTE se trata de un incidente:

* Confirmar la naturaleza del evento reportado
* Descartar errores, malos entendidos o falsas alarmas

Una vez confirmado el incidente, se debe seguir la política de la empresa, la cual debería contemplar los siguientes pasos:

* Recepción y Análisis del Incidente
* Neutralización del ataque
* Búsqueda de información y rastreo del intruso
* Secuestro y preservación de evidencia
* Recuperación de datos o sistemas afectados
* Cierre y documentación del proceso de manejo de incidentes

Generalmente, la etapa de reacción es la que menos se toma en cuenta en los proyectos de seguridad informática. Esta etapa consiste en prever incidentes y planificar las medidas que deben tomarse si surge un problema.

* La implementación de un plan de recuperación de desastres permite a la organización evitar que el desastre empeore y tener la certeza de que todas las medidas tomadas para establecer pruebas se aplicarán correctamente.
* Asimismo, un plan contra desastres desarrollado correctamente define las responsabilidades de cada individuo y evita que se emitan órdenes y contraórdenes, que impliquen una pérdida de tiempo.

Es importante establecer pruebas en caso de que se realice una investigación judicial. De lo contrario, si la máquina comprometida se ha usado para realizar otro ataque, la compañía corre el riesgo de ser considerada responsable.

* **Restauración:** en el plan de recuperación, se debe especificar en detalle cómo hacer que el sistema comprometido vuelva a funcionar correctamente. Es necesario tomar en cuenta los siguientes elementos:
  * **Anotar la fecha de intrusión**: conocer la fecha aproximada en la que se ha comprometido la máquina permite a la organización evaluar el nivel de riesgo de intrusión para el resto de la red y el grado de compromiso de la maquina.
  * **Restringir el compromiso**: tomar las medidas necesarias para que el compromiso no se expanda
  * **Establecer pruebas**: por razones legales, es necesario guardar los archivos de registro diario del sistema corrompido para poder restituirlos en caso de una investigación judicial
  * Cómo configurar un sitio de **reemplazo**: en lugar de reinstalar el sistema comprometido, es preferible desarrollar y activar a tiempo un sitio de reemplazo que permita que el servicio continúe activo cuando sea necesario.

Realizar test periódicos de los planes

Práctica del plan contra desastres: De la misma forma en que los simulacros de incendio son fundamentales para repasar un plan de escape en caso de incendio, la práctica del plan contra desastres permite a una organización confirmar que el plan funciona y garantizar que todas las personas involucradas sepan qué hacer.

Realizar Plan de Contingencia y Plan de Continuidad

Dentro del Plan de respuesta deben contemplarse el momento de activar el Plan de Contingencia o el Plan de Continuidad para afectar lo menos posible al negocio.

Plan de Contingencia.- Define los procedimientos de resolución y métodos de recuperación de las aplicaciones vitales del negocio (implica corte de las operaciones, es un plan reactivo.

Plan de Continuidad.- Define los procedimientos que garantizan la disponibilidad de servicios críticos ante situaciones de emergencia sin que se produzcan interrupciones en los mismos (intenta evitar el corte de las operaciones, plan proactivo)

El plan de continuidad debe contener por debajo un plan de contingencia de las infraestructura y además debe tener en cuenta la logística, las comunicaciones,