¿Estáis preparados?

Cuestionario inicial de respuesta a incidentes

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL

Índice

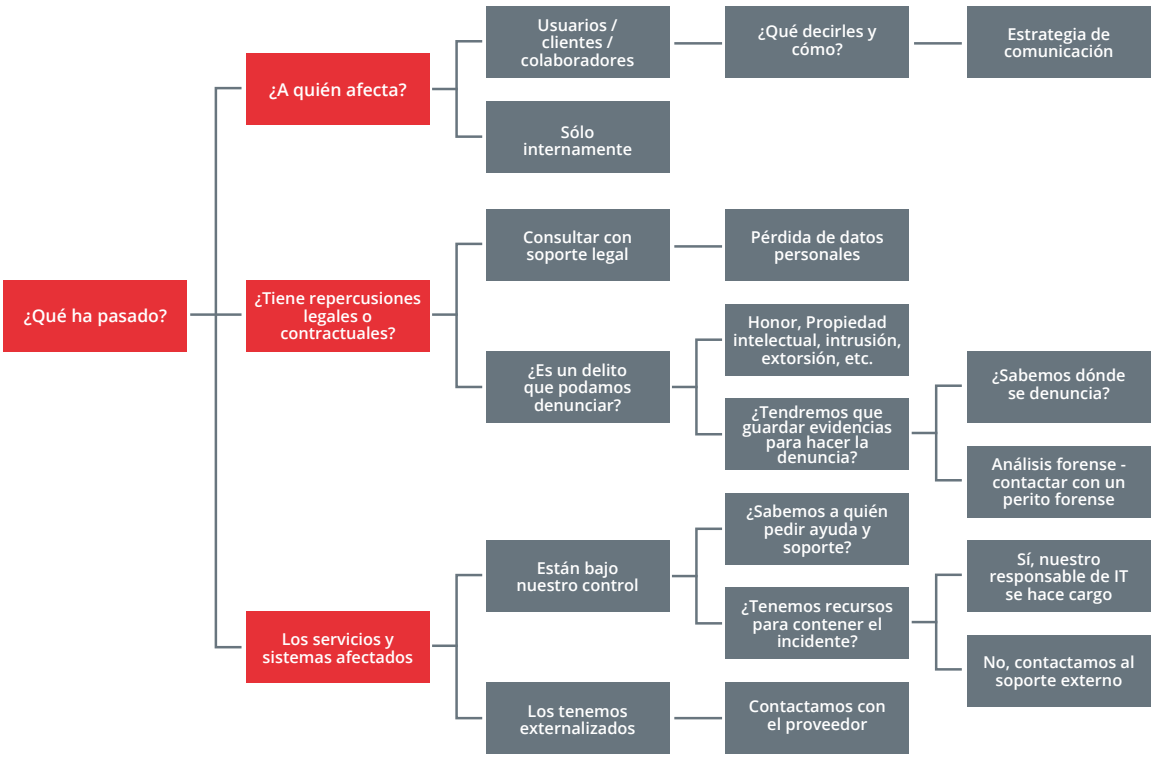
Índice de figuras

Índice de tablas

1 ¿Respuesta a incidentes?

Ante un incidente de seguridad podemos hacernos las siguientes preguntas:

Figura 1: Análisis inicial, ¿qué ha pasado?



En caso de que tengamos un responsable de IT que pueda hacerse cargo del incidente, incluimos aquí un cuestionario de respuesta a incidentes, que puede servir de base para establecer e iniciar la gestión de incidentes en su organización. Está adaptado de *Initial Security Incident questionnaire for responders* **(1).**

(1) *De Lenny Zeltser, que lidera el equipo de consultoría de seguridad en SAVVIS, y enseña análisis de malware en el instituto SANS. Reconocimiento especial por su feedback a Jack McCarthy y Patrick Nolan.*

1 ¿Respuesta a incidentes?

1.1 Antecedentes

- Con los datos que tienes, ¿cómo definirías el problema?

  - Valora la gravedad o criticidad del incidente (bajo, medio, alto, muy alto y crítico) según la prioridad con la que deba resolverse
  - ¿Es un incidente de origen externo o interno?
  - ¿Podrías clasificar *(2)* el incidente? (a modo orientativo se incluye la siguiente tabla).

Tabla 1: Clasificación de incidentes

Clase de incidente	Tipo de incidente
Ataque	Ataque dirigido (incluido ataque de ingeniería social)
	Modificación de sitio web
Código malicioso	Infección extendida
	Infección única
Denegación de servicio (DoS)	Con éxito
	Sin éxito (intento de)
Acceso no autorizado, robo o pérdida de datos	Acceso no autorizado
	Robo o pérdida de equipos
	Pérdida de datos
Pruebas y reconocimientos	Pruebas no autorizadas
	Alarmas de sistemas de monitorización
Daños físicos	Daños o cambios físicos no autorizados a los sistemas
Abuso de privilegios y usos inadecuados	Abuso de privilegios o de políticas de seguridad
	Infracciones de derechos de autor o piratería
	Uso indebido de la marca

(2) Para una clasificación de las amenazas consultar: ENISA Threat Taxonomy: A tool for structuring threat information v 1.0 (2016) disponible en https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information

1 ¿Respuesta a incidentes?

- ¿Cuándo lo detectasteis por primera vez?, ¿quién lo detectó? ¿Qué dispositivos de seguridad tenéis en el entorno afectado por el incidente? (cortafuegos, antivirus, ...)
- Estos dispositivos de seguridad, ¿estaban activados?, ¿están actualizados?, ¿se ha revisado recientemente si tienen fallos o vulnerabilidades?
- ¿Quién(es) ha(n) resultado afectados por el incidente (externos e internos)?, ¿cómo se han dado cuenta?
- ¿Se han detectado otros incidentes en ese mismo entorno?

1.2 Comunicación

- ¿Qué personas en la empresa deben tener conocimiento del incidente?
- ¿Tenemos los contactos de personal de apoyo en caso de incidente? Por ejemplo:

  - soporte técnico
  - proveedores de servicios
  - asesor legal
  - perito forense
  - policía o Guardia civil (en caso de que haya que hacer denuncia)
  - el CERT de Incibe: CERTSI u otro CIRST o CERT

- ¿Quién es el responsable de coordinar la respuesta al incidente?
- ¿Quién está autorizado a tomar decisiones de negocio sobre las operaciones o servicios afectados?
- ¿Qué medio(s) se ha(n) de utilizar (email, teléfono,...) para transmitir mensajes sobre el desarrollo o avance del incidente? ¿Deben utilizarse mecanismos de cifrado en estas comunicaciones?
- ¿Cada cuánto tiempo tendremos que informar sobre el avance del incidente?, ¿a quién?
- ¿Quién va a realizar el análisis de la infraestructura afectada (anotar los datos del contacto)?
- Si fuera necesario, ¿quién(es) debe(n) comunicárselo a entidades externas: medios de comunicación, redes sociales, asistencia legal, partners, etc.?

1 ¿Respuesta a incidentes?

1.3 Valora el alcance del incidente

- ¿Qué elementos de infraestructura: dispositivos, equipos, servidores, redes, etc. están directamente afectados por el incidente?
- ¿Qué aplicaciones, procesos o servicios hacen uso de la infraestructura afectada?
- ¿Somos conscientes de las obligaciones legales o contractuales asociadas al incidente? (LOPD, PCI, etc.)
- ¿Cuáles son los posibles puntos de entrada/salida (contagio, fuga de información,...) del entorno afectado?
- ¿Cómo creemos que se inició el incidente?
- La infraestructura afectada, ¿supone algún riesgo para terceros?,
- Si constituye un delito contra nuestra empresa, ¿vamos a denunciarlo a las autoridades?
- ¿Está cubierto por alguno de los seguros que tenemos contratados?

1.4 Revisa qué acciones se tomaron nada más detectar el incidente

- ¿Qué hizo la persona que detectó el incidente nada más detectarlo?
- ¿Qué comandos o herramientas se ejecutaron en los sistemas?
- ¿Se actuó de alguna forma para valorar el alcance del incidente?
- ¿Se tomaron algunas medidas para contener el alcance del incidente? (por ej. desconectar el equipo de la red de datos, etc.)
- ¿Generó el incidente alguna alerta (antivirus, IDS, etc.)?
- ¿Se revisaron los logs de los sistemas para localizar entradas sospechosas?, ¿se encontraron?
- ¿Se observó algún otro suceso o información que haga sospechar?

1 ¿Respuesta a incidentes?

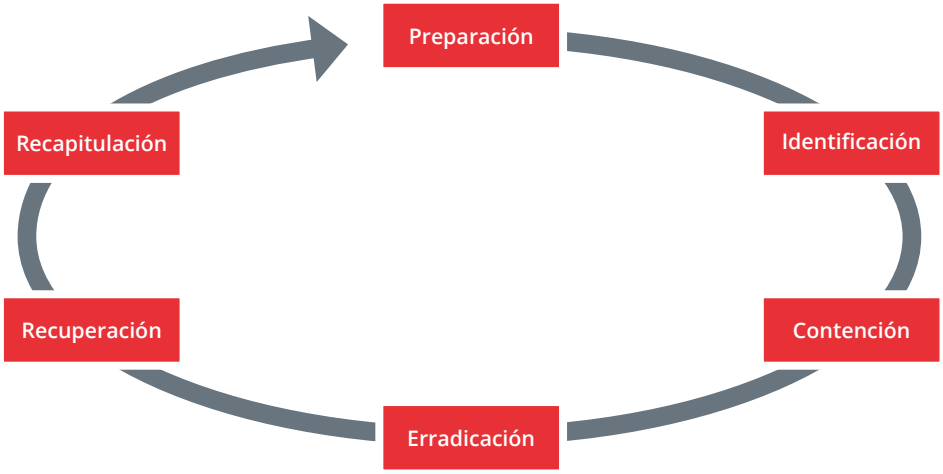
1.5 Prepara la respuesta al incidente

- ¿Disponéis de instrucciones o una guía para la gestión de incidentes?
- ¿Qué herramientas tenéis a vuestro alcance para monitorizar la red o la actividad de los sistemas en el entorno afectado?
- ¿Con qué medios contáis (por ejemplo: la red, USB, CD-ROM, etc.) para transferir ficheros de o hacia los elementos de la infraestructura afectados?
- ¿Dónde están ubicados físicamente los elementos afectados de la infraestructura?
- ¿Qué mecanismos de backup y restauración están implantados para apoyo a la recuperación de los sistemas afectados por el incidente?
- ¿Cuáles son los siguientes pasos para responder a este incidente? ¿Quién ha de realizarlos y cuándo?
- ¿Hay que contener inmediatamente el incidente (si los daños son elevados o hay peligro de que se propague) o podemos esperar para capturar al delincuente?
- ¿Es necesario realizar un análisis en vivo (esperar a ver qué pasa para tener más datos) o un análisis forense?, ¿tenemos que obtener evidencias (llamar al perito forense) para aportarlas junto a una denuncia?

2 Fases para la respuesta incidentes

La respuesta a incidentes es un ciclo con las siguientes fases:

Figura 2: Ciclo de vida de la respuesta a incidentes



1 Preparación

Reúne las herramientas necesarias y aprende su funcionamiento, familiarizándote con ellas.

- Antimalware y comprobadores de integridad de ficheros/dispositivos.
- Escáneres de vulnerabilidades, análisis de logs, detectores de intrusiones y otras herramientas de auditoría.
- Recuperación de backups.
- Herramientas de análisis forense (las traerá el perito forense).

2 Identificación

Detecta el incidente, determina su alcance y forma de solución e involucra a los responsables del negocio, las operaciones y la comunicación.

- Contacta con el soporte técnico, con el CIRST o CERT, o con un perito forense si fuera necesario.
- Contacta la policía si fuera necesario.
- Contacta con el asesor legal si fuera necesario.

2 Fases para la respuesta incidentes

3 Contención

Impide que el incidente se extienda a otros recursos, minimizando su impacto.

- Separa el/los equipos de la red cableada o wifi.
- Deshabilita cuentas de usuario comprometidas.
- Cambia las contraseñas de las cuentas de usuario comprometidas.

5 Erradicación

Elimina si fuera necesario los elementos comprometidos antes de iniciar la recuperación.

- Reinstala los sistemas afectados.
- Restaura desde un backup.

6 Recapitulación

Documenta los detalles del incidente, archiva los datos recogidos y establece un debate constructivo sobre las lecciones aprendidas.

- Informa a los empleados del incidente y dales instrucciones para evitarlo en el futuro.
- Informa a los medios y a los clientes si fuera necesario.

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL