Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.
CONSEJERÍA DE ECONOMÍA, INNOVACIÓN, CIENCIA Y EMPLEO

AndalucíaCERT
CENTRO DE SEGURIDAD TIC

Informe de divulgación
Respuesta a incidentes de seguridad

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-3967-130520*
Edición:	*0*
Categoría	*Público*
Fecha de elaboración:	*20/05/2013*
N° de Páginas	*1 de 18*

1 TABLA DE CONTENIDOS

1. TABLA DE CONTENIDOS....2
2. OBJETO....3
3. ALCANCE....3
4. INTRODUCCIÓN....3
5. RESPUESTA A INCIDENTES....4
6. PREPARACIÓN....4
7. DETECCIÓN Y ANÁLISIS....7
8. CONTENCIÓN, RESOLUCIÓN Y RECUPERACIÓN....12
9. ACCIONES TRAS LA RECUPERACIÓN DE LOS SISTEMAS....14
10. GLOSARIO....17
11. REFERENCIAS....18

2 OBJETO

En este documento se pretende proporcionar al personal de la Junta de Andalucía una pequeña guía metodológica para la gestión de incidentes de seguridad.

3 ALCANCE

Este documento va destinado al personal técnico de la Junta de Andalucía y al público en general.

4 INTRODUCCIÓN

Un **incidente de seguridad** TI es cualquier suceso que pueda afectar al correcto funcionamiento de los sistemas TI de nuestra organización (en cuanto a su integridad, disponibilidad y/o confidencialidad).

Atendiendo a la creciente dependencia que hoy en día cualquier organización tiene de las tecnologías de la información, un incidente de seguridad puede tener un impacto **muy grave** en la normal actividad de la misma. Un incidente de seguridad puede afectar directamente al funcionamiento de la organización, pudiendo dejarla paralizada hasta su resolución, y afectar como consecuencia a la confianza de los usuarios. Las repercusiones serán económicas, tanto directa o cómo indirectamente.

Planteado el problema, debemos hacernos varias preguntas:

- ¿Existe en su organismo personal dedicado a gestionar incidentes de seguridad en los sistemas de información?

Y en caso de que la respuesta sea NO:

- ¿Qué preparación tiene su departamento de TI para tratar con incidentes de seguridad?

Tenemos que estar preparado para actuar ante cualquier eventualidad que pueda comprometer el buen funcionamiento de todos los sistemas de nuestra organización. La urgencia de los momentos inmediatamente posteriores al incidente nos impedirá responder adecuadamente a no ser que ya tengamos procedimientos y personal formado.

La respuesta apropiada a un incidente debe ser una parte esencial de la directiva de seguridad general y de la estrategia de mitigación de riesgos de toda organización.

5 RESPUESTA A INCIDENTES

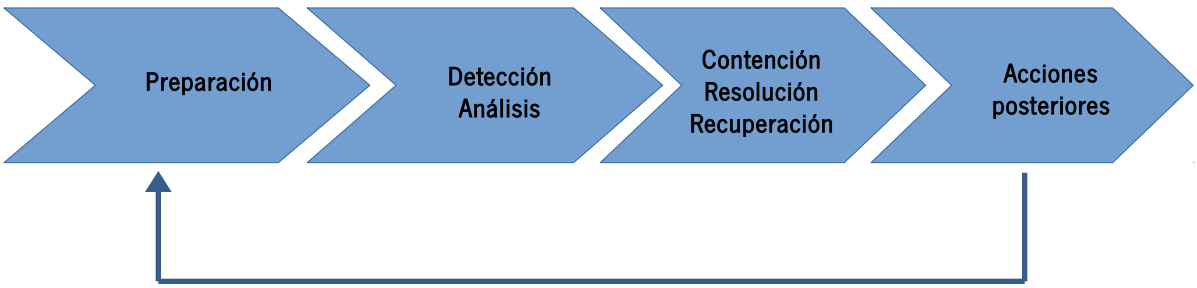
La primera parte de la respuesta a un incidente empieza por la creación de un **equipo de respuesta a incidentes.** En una organización pequeña puede no ser posible o eficiente un equipo dedicado en exclusiva a estas tareas, en ese caso conviene asignar las estas funciones a algunas personas del equipo TI.

El equipo de respuesta a incidentes de una organización, dependiendo de su tamaño y de si tiene las herramientas apropiadas para la detección de incidentes, podrá llegar a detectar una gran cantidad de indicios de incidentes en sus redes y sistemas.

A la hora de que un equipo de respuesta a incidentes trate todos estos indicios deberá pasar por las fases que se definen en la siguiente metodología.

Metodología de gestión de incidentes:

- Preparación.
- Detección y análisis del incidente.
- Contención, resolución y recuperación.
- Acciones posteriores al incidente.



6 PREPARACIÓN

Siempre se ha dicho que es mejor prevenir que curar, la seguridad TI no es una excepción. Siempre que sea posible, se deseará evitar que, en primer lugar, se produzcan incidentes de seguridad. No obstante, resulta bastante complicado (o más bien imposible) evitar todos los incidentes de seguridad. Así pues, cuando se produzca un incidente de seguridad debemos ser capaces de garantizar que su impacto sea el mínimo.

En esta fase debemos por tanto contemplar 2 tipos de actividades:

- Orientadas a establecer la capacidad de respuesta a incidentes.

- Orientadas a la prevención de incidentes.

6.1 Preparar la capacidad de respuesta a incidentes

Para poder ser capaces de proporcionar una respuesta respuesta rápida y eficaz a los posibles incidentes de seguridad que surjan deberemos prever la disponibilidad de:

- **Política y procedimientos de gestión de incidentes :** Imprescindible para llevar a cabo la respuesta a incidentes. Si no se sabe cómo actuar a la hora de que un incidente ocurra, qué pasos dar y en qué orden, la gestión de un incidente puede convertirse en toda una odisea.

- **Personal** (equipo, personas individuales) dedicado a la gestión de incidentes: gestores, técnicos, etc.

- **Contactos y responsabilidades**: Debemos contar con un listado de datos sobre personas y organizaciones que puedan necesitarse para la resolución de un incidente de seguridad en la organización.

- **Canales de comunicación**. Necesario para que usuarios y otras organizaciones puedan comunicarse con nuestro equipo de respuesta, alertarnos de cualquier incidente y viceversa. Por ejemplo, teléfono, e-mail, sitio web, etc.

- **Documentación de infraestructura TI**: inventario de activos, sistemas, redes, diagramas, procedimientos y ficheros de configuración. En definitiva, una base de datos completa y actualizada de la infraestructura TI por la que velamos.

- **Informes de actividad considerada normal** ("baseline") en nuestra infraestructura TI que nos permitan detectar actividades anómalas.

- **Herramientas para seguimiento de incidentes** de seguridad. Por ejemplo, un sistema de ticketing.

- Una **sala de reuniones** para comunicar, coordinar información y esfuerzos en la respuesta a incidentes.

- Sistemas para el **almacenamiento seguro** de la información.

- **CERTs** en los que pueda apoyarse la organización y su capacidad de respuesta.

- Otras herramientas

- Programas de análisis de red.
- Sistemas de virtualización que permitan desplegar un laboratorio para análisis de amenazas.
- Sistemas de almacenamiento portátil.
- Ordenadores portátiles para acudir al lugar del incidentes de forma física si es necesario.
- Sistemas para registro de evidencias (cámaras de fotografía, sistemas de cadena de custodia...).
- Imágenes de recuperación de los sistemas que intentamos proteger.
- Etc...

Una gran idea para un equipo de respuesta a incidentes, acomodándose a los puntos antes expuestos, es tener un **kit o equipamiento de respuesta rápida** que incluya los programas, bases de conocimiento, datos de contacto y herramientas necesarias para la resolución de un incidente.

6.2 Prevención de incidentes

Más importante que estar preparados para la resolución de un incidente, es prevenir que éstos ocurran. Si no se **aseguran los sistemas adecuadamente**, el número de incidentes puede llegar a sobrepasarnos. Aunque el equipo de respuesta a incidentes normalmente no tiene la potestad para bastionar los sistemas que no están a su cargo, sí deben mantener informados a los responsables de éstos sobre las posibles debilidades de sus sistemas.

Aunque sólo para cubrir este punto podríamos necesitar un documento bastante extenso, a continuación se citan, a modo de recordatorio, algunos puntos claves:

- **Evaluación de riesgos:** La evaluación periódica del nivel de riesgo al que está expuesto cada uno de los activos de nuestra organización es fundamental para poder definir qué urgencia aplicamos a la gestión de cada problema.

- **Asegurar todas las máquinas, ¡TODAS!:** Cada máquina debería implementar sus propias medidas de seguridad, estar actualizadas, establecer los privilegios adecuados, contraseñas seguras, comprobar que exista un antivirus analizándolas periódicamente (o constantemente). También es importante asegurar los dispositivos móviles y, en general, cualquier máquina que se conecten a nuestra red (incluyendo las de invitados).

- **Securizar la red:** Nuestra red es una fortaleza y debemos asegurarnos que nada traspasa sus muros si no está permitido. Establecer las políticas de control adecuadas para conseguirlo.

- **Prevención de malware:** El malware es posiblemente el peligro más habitual y extendido al que se enfrentará un equipo de incidentes. Es básico usar programas anti-malware y mantener unas buenas practicas en la navegación y en el tratamiento de unidades de almacenamiento extraíbles.

- **Concienciación del personal:** Hagamos lo que hagamos, el usuario accederá a nuestros sistemas con privilegios y desde dentro de nuestra red. Concienciar de los peligros y explicar la importancia de buenas practicas a los usuarios de nuestros sistemas los convertirán en un apoyo en lugar de un riesgo.

7 DETECCIÓN Y ANÁLISIS

Las actividades de detección y análisis incluyen la clasificación de incidentes que pueden afectar a la organización, detección de signos indicadores y precursores de incidentes, análisis, priorización, notificación y documentación de los incidentes.

7.1 Signos de incidentes

Comprenden la base de la detección y análisis de los incidentes de seguridad. Los signos de un incidente pueden ser de dos tipos:

- **Signos indicadores:** Signos de que un incidente ha ocurrido o puede estar ocurriendo. Por ejemplo, alerta de un sensor avisando de desbordamiento de buffer en un servicio, antivirus informando de sistema infectado, caída total de un servidor, accesos lentos y generalizados a servicios o sistemas, etc .

  Éstos deberían poner en marcha acciones reactivas previstas por la empresa. Algunos signos indicadores pueden ser los siguientes:

  - Sistemas de detección de intrusos que alertan de intentos de explotar vulnerabilidades.
  - Alertas de antivirus.
  - Archivos modificados.
  - Cambios no registrado de configuraciones.
  - Logs que alertan de muchos fallos de autenticación.
  - Desvíos de los flujos de red a protocolos poco comunes.

- **Signos precursores:** Signos de que un incidente puede ocurrir en el futuro. Por ejemplo, barrido de puertos, anuncio de códigos que pueden aprovechar vulnerabilidades existentes en la empresa, amenazas de ataque dirigidas a la empresa anunciadas por delincuentes, etc.

  Éstos deberían ser tratados con acciones preventivas. Ejemplos de precursores:

- Logs que indican que se están utilizando un escáner de vulnerabilidades.
- La publicación de un nuevo exploit para una vulnerabilidad de sistemas de nuestra organización.
- Noticias de campañas de ataque por parte de algún grupo reconocido.

7.2 Vector de ataque

A fin de tener capacidad de detección, debemos conocer las posibles métodos o vías para vulnerar nuestros sistemas. Hay una cantidad innumerable de formas de vulnerar un sistema y es bastante complicado cubrirlas todas, por lo que resulta necesaria la formación continuada de las personas dedicadas a la respuesta a incidentes en las nuevas amenazas que vayan surgiendo.

Algunos vectores de ataque habituales:

- Uso de un sistema de almacenamiento externos malintencionado o corruptos.
- Ataques de fuerza bruta que intentan comprometer o degradar los sistemas.
- Ataques hacia nuestros sistemas expuestos en internet como los portales WEB.
- Ataques de phishing mediante correo electrónico.
- Ataques de suplantación, spoofing, puntos wifi falsos...
- Violaciones de las políticas de la empresa como la revelación de documentación sensible o descarga de contenido ilegal de Internet.
- Perdida o robo de equipo informático.
- Malware.

Se conscientes de los posibles ataques que podemos sufrir es fundamental. Por un lado nos sirve para fijar una hoja de ruta de pruebas en nuestros sistemas TI con el fin de verificar si seríamos vulnerables ante una situación real de ataque.

Por otro lado, conocer las amenazas nos permitirá monitorizarlas. No todas pueden ser bloqueadas por lo que resulta necesaria su monitorización.

7.3 Clasificación

Tras la detección de un posible incidente de seguridad, se debe clasificar dentro de una de las categorías contempladas en los procedimientos de gestión de incidentes. Es fundamental que todo incidente pueda ser clasificado para determinar el tipo de tratamiento que requiere.

Para todos aquellos casos que no se puedan clasificar, se deberá contar con un procedimiento genérico de gestión de incidentes.

7.4 Priorización

Los incidentes no deben ser tratados por orden de llegada ya que esto nos llevaría a gastar recursos en incidentes que quizás no tenga tanta importancia por no afectar al funcionamiento de la organización, en detrimento de otros incidente si pudieran ocasionar daños muy graves de no ser tratados con agilidad. Necesitaremos realizar una buena priorización en base de la criticidad de los incidentes que se detecten. Esta criticidad puede determinarse por tres puntos a tener en cuenta:

- **Impacto del incidente en la funcionalidad:** Un incidente de seguridad tiene una repercusión directa o indirecta en los servicios ofrecidos por nuestra organización. Una primera valoración se realizará en base a cuanto afecta a la funcionalidad de los servicios que la empresa provee.

- **Impacto del incidente sobre la información:** Este punto evaluará el valor, impacto y riesgo de la información afectada en un incidente.

- **La dificultad de recuperación del incidente:** Cada incidente necesitará unos recursos y un tiempo para su resolución. Unos incidentes pueden ser solventado con una simple llamada de teléfono o un rápido cambio de una configuración que no llega a afectar a otros servicios. Otros por contra, pueden llegar a ser irrecuperable como el caso de la fuga de información crítica.

Combinando el **impacto sobre los servicios y el impacto sobre la información obtendremos una valoración inicial**. Evidentemente cuanto más afecte a nuestros servicios o a información más critica, mas urgente será atajar el incidente.

Tras esta primera valoración obtendremos otro indicador que se verá afectado por existencia o no de solución. Entendamos que aunque el incidente fuera extremadamente critico, si éste no tiene solución, su prioridad se verá menguada.

7.5 Análisis de incidentes

La complejidad en el análisis de un incidente dependerá en gran medida de la cantidad de signos precursores e indicadores con los que contemos y de su fiabilidad.

Uno de los primeros trabajos que debemos realizar es catalogar y determinar la fiabilidad de los indicios sobre el incidente que se han recopilado. Esta tarea puede necesitar de la colaboración de los administradores de los sistemas de la organización con el fin de determinar si ciertos comportamientos son normales o admitidos en sus sistemas.

Por otro lado, tendremos que valorar la fiabilidad de la fuente que nos ha proporcionado cada indicio (IDS, antivirus, logs, usuarios,...). No todas las fuentes son igual de fiables. Muchos de ellos, aunque sean muy útiles, tendrán una tasa más alta de falsos positivos que otros.

Por último, un factor fundamental será la experiencia de nuestro equipo de respuesta a incidentes de seguridad y la base de conocimientos adquirida de nuestro entorno de trabajo en base a incidentes pasados.

Para la resolución del incidente, el equipo de respuesta debe reaccionar rápidamente y acorde con los pasos que de antemano deben estar dispuestos para determinar el alcance del incidente, su gravedad, su posible contingencia inmediata y que herramientas se ha de usar para su resolución y análisis.

A continuación proponemos algunas recomendaciones que pueden facilitar el análisis de un incidente de seguridad:

- Mantener una base de datos y sumas tipo hash de los sistemas críticos, cualquier modificación será factiblemente reconocible.
- Tener muy claro cuales son los comportamientos "normales" de nuestra red. Es muy sencillo detectar flujos anómalos si conocemos el día a día del uso que se hace de nuestros sistemas.
- Recolección y estudio de los logs de los sistemas críticos ya que son una fuente increiblemente rica de información de todo lo que ocurre en nuestro entorno.
- Mantener todas las máquinas con una hora común será indispensable para cualquier tipo de correlación entre eventos.
- La experiencia. Con un poco de trabajo de documentación podemos mantener una base de conocimiento sobre las situaciones más y menos fiables.
- Las herramientas de monitorización de redes pueden ayudarnos a verificar si un incidente está ocurriendo realmente.

En muchos casos, nada de lo anterior nos dará comprensión absoluta sobre un incidente. De forma habitual habrá que hacer uso de Internet e incluso de los conocimientos de otros grupos de respuesta a incidentes o CERTs.

7.6 Documentación del incidente

En cuanto se establece el inicio de un incidente, se debería empezar a registrar cada paso y detalle del incidente. El inicio, el final y cada punto en el transcurso debe ser documentado guardando con la fecha y hora en que se produjo cada hito en el camino de la gestión del incidente. Este punto es especialmente importante ya que en un futuro, cada paso y descubrimiento de la investigación, podría ser necesitada como evidencia en posibles procedimientos legales.

Para esto será muy útil **usar una herramienta de registro de incidentes** que a ser posible registre los siguientes puntos:

- El estado en cada momento de cada incidente (en curso, resuelto, cerrado...)
- Un sumario de cada hito que va sucediéndose a lo largo de la resolución del incidente.
- Los signos con los que se han detectado el incidente.
- Una evaluación del impacto de incidente.
- Cada acción y modificación en los sistemas que se ha llevado a cabo durante la resolución del incidente.
- Los datos de contactos de todos los involucrados en el incidente.
- Comentarios aclaratorios de cada paso que se da en la resolución del incidente.
- Registrar cual va a ser el siguiente paso en la línea de actuación a fin de que otros puedan seguir el trabajo.

Toda esta información habrá que guardarla segura ya que contendrá información crítica de nuestros sistemas y recursos, tanto humanos como de la infraestructura de nuestra organización.

7.7 Notificación del incidente

Una vez que el incidente ha sido analizado y se ha determinado que no es un falso positivo, el equipo de respuesta deberá notificarlo a las personas involucradas en el incidente, a afectados y equipos de respuesta que puedan actuar. Para este fin es muy importante tener disponibles todos los medios de comunicación necesarios y apropiados para cada caso.

- Email
- Portales web internos o externos
- Teléfonos
- Notificación en persona
- Buzones de voz

Es importante comprender que no todos los medios son adecuados según la información que se va a enviar a través de ellos. No usaremos un portal WEB para notificar las credenciales robadas de un usuario, ni tiene mucho sentido notificar por teléfono a cada usuario, la nueva vulnerabilidad publicada.

8 CONTENCIÓN, RESOLUCIÓN Y RECUPERACIÓN

8.1 Elegir una estrategia de contención

Una vez detectado el incidente, comprendido, categorizado, priorizado, analizado, documentado y notificado, el siguiente paso es la **contención**. Su objetivo es que el incidente no provoque más daño a nuestra organización.

Además **la contención alargará el tiempo del que dispondrá el equipo de respuesta a incidentes** para estudiar las soluciones a implementar definitivamente.

Las estrategias de contención de incidentes varían dependiendo del tipo de incidente y del impacto previsible en la organización. Puede ser necesario tomar decisiones como deshabilitar servicios, apagar sistemas o desconectar equipos de la red antes de que el impacto pueda extenderse a la empresa.

Decidir decisiones a tomar puede resultar más o menos sencillo dependiendo de si las estrategias y procedimientos para contener los distintos tipos de incidentes han sido determinadas previamente. La empresa tiene que analizar los impactos previsibles para cada tipo de incidente y definir estrategias de contención en función del nivel de riesgo considerado como aceptable.

Algunos criterios a tener en cuenta para realizar dicho análisis pueden ser:

- Posible daño a recursos o robo de los mismos.
- Necesidad de preservación de evidencias.
- Si los servicios pueden ser detenidos.
- Tiempo y recursos necesarios para la resolución del incidente.
- Efectividad de la contención (completa o parcial).
- Si la contención es una solución para siempre o temporal.

8.2 Resolución y recuperación

Tras la contención del incidente el siguiente paso es resolverlo de forma definitiva y volver al estado de operación normal de la organización.

En las actividades de **resolución** se realiza la eliminación de los componentes asociados al incidente y otras actividades que se consideren adecuadas para resolver el incidente o prevenir futuras ocurrencias. Desinfectar los equipos del malware, cerrar brechas de seguridad, deshabilitar cuentas comprometidas, parchear los sistemas, cambios en las reglas del cortafuegos, etc.

Las actividades de **recuperación** pueden incluir acciones tales como el restauración de sistemas completos o de copias de seguridad previas al incidente, parcheo de vulnerabilidades, remplazar software vulnerable, cambio de contraseñas, ajustes de los sistemas de protección perimetral (proxys, firewal...).

La resolución y recuperación se debe afrontar por pasos y prioridades. En casos que la restauración de un servicio pueda ser muy costosa y se prevea que puede alargarse demasiado en el tiempo, se podrán acometer los trabajos de prevención de incidentes similares antes que la de la recuperación del sistema afectado.

8.3 Recogida y manejo de evidencias

Durante todo el incidente manejaremos evidencias. Las evidencia cumplen como función principal ayudarnos a la resolución del incidente pero en ocasiones será necesario guardarlas para futuras investigaciones legales por si éstas son reclamadas. Así que para un correcto tratamiento y para asegurar su posible utilidad en una investigación legal debemos asegurar ciertos puntos, datos y cadenas de custodia a la hora de tratarlas y almacenarlas. Ejemplos:

- Información de identificación como localización, numero de serie, nombre de la máquina, IP, MAC...
- Nombre, puesto y número de teléfono de cada persona que ha tratado o aportado una evidencia.
- Fecha y hora del momento de detectarse o producirse la evidencia.
- Lugar donde la evidencia ha sido almacenada.

Aunque en una investigación lo mejor sería poder recoger las evidencias “in situ”, muchas veces esto no es posible. Una buena práctica es realizar imágenes de los sistemas afectados para poder analizarlos en el estado que se encontraban durante el incidente. Esta practica también nos puede ayudar a minimizar el hecho de que en el transcurso de una investigación se modifiquen sin querer las pruebas del incidente.

8.4 Almacenamiento de evidencias

Es importante contar con una política de almacenamiento de las evidencias recolectadas durante la investigación del incidente para decidir cuanto tiempo será necesario mantener las evidencias. Podemos estimar los siguientes puntos:

- Si el incidente ha producido una investigación legal será necesario mantener la información recopilada mientras dure el procedimiento legal y posiblemente sean custodiadas por las FF y CC de Seguridad.

- Las políticas propias de la empresa referente al almacenamiento de información.
- El posible coste que pueda representar en forma de dispositivos de almacenamiento. Aunque el almacenamiento es relativamente barato si tenemos una política de retención de evidencias durante muchos años, puede que necesitemos una cantidad de espacio de almacenamiento que suponga un gasto considerable.

9 ACCIONES TRAS LA RECUPERACIÓN DE LOS SISTEMAS

Tras todo el trabajo realizado y las dificultades superadas es vital recopilar, juzgar e interiorizar el aprendizaje derivado de la resolución del incidente. Esta información será extremadamente útil en futuros incidentes. Para compartir esta información y estudiar los pasos que se han seguido en la resolución de un incidente juzgando su efectividad, se celebrarán reuniones. En estas reuniones al menos deberíamos poder responder a los siguientes puntos:

- Definir de forma exacta en qué ha consistido el incidente.
- ¿Se clasificó el incidente adecuadamente en base a la documentación de procedimiento? ¿Esta documentación ha sido eficaz o no se ajustaba al caso?
- ¿Cual ha sido la información que ha sido necesaria para iniciar la resolución del incidente?
- ¿Alguna de las acciones tomadas ha podido causar un incidente por si misma?
- ¿Que cosas haríamos de distinta forma si tuviéramos que volver a resolver el incidente?
- ¿Ha sido útil el intercambio de información con otras organizaciones?¿Hay que mejorar los canales de comunicación con éstas?
- ¿Que acciones se deberán tomar para la prevención de incidentes similares?
- ¿Que precursores e indicadores nos darán la certeza de que se ha reproducido el incidente u otro similar en el futuro?
- ¿Que herramientas o recursos se han utilizado?

Aunque estas pocas cuestiones puedan parecer fácil de responder, puede llevar mucho tiempo y trabajo resolverlas y documentar las conclusiones de estas reuniones. Posiblemente para incidentes relativamente sencillos no compense el trabajo requerido para coordinar al personal y de documentación necesaria en relación con el aprendizaje que se obtendrá en retorno. Lo más recomendable es sólo concretar reuniones para el estudio de incidentes relevantes, bien por su criticidad o por la posibilidad de aprendizaje que aporte al equipo.

9.1 Métricas y coste

Se recomienda recoger y analizar métricas sobre los tipos y frecuencia de incidentes, impactos (financieros, obligaciones legales, imagen frente a terceros, operativos), métodos de resolución, coste de la resolución de incidentes y acciones correctivas o preventivas.

A continuación indicamos algunos de los indicadores que pueden ser útil:

- **Número y tipos de incidentes tratados:** Nos da una idea de problemas de seguridad que tienen más lugar en nuestra infraestructura.

- **Tiempo por incidente:** Este indicador puede estar basado en varios puntos:
  - Total de tiempo necesitado para la resolución de un incidente.
  - Tiempo transcurrido desde que se produjo el incidente y el momento en que fue detectado.
  - Que tiempo se tardó entre la detección y la notificación del incidente.

- **Valoración objetiva de cada incidente:** Valoración de cuan efectiva ha sido la respuesta y resolución de un incidente. Algunos indicadores que nos ayudarán a realizar esta medida son:
  - Revisar si la actuación del equipo de respuesta se a realizado conforme a los manuales de actuación.
  - Identificar los precursores e indicadores para comprobar si las herramientas de detección son lo suficientemente efectivas o si generan demasiados falsos positivos.
  - Determinar si el incidente ha causado daño antes de su detección.
  - Comprobar si se ha identificado el vector de ataque del incidente.
  - Comprobar si se trata de un incidente recurrente o persistente.
  - Calcular en términos monetarios el daño que ha podido ocasionar el incidente.
  - Identificar qué medida habría evitado el incidente.

- **Una posible valoración subjetiva de los técnicos** implicados en la resolución del problema.

A continuación mostramos una posible tabla de chequeo de puntos que nos pueden indicar si se ha tratado correctamente el incidente.

ID	Acción	Completada
Detección y Análisis		
1	Clasificar el incidente	
2	Priorizar el incidente	
3	Análisis	
3.1	Analizar signos precursores e indicadores	
3.2	Buscar correlación entre los indicios recolectados	
3.3	Determinar la fiabilidad de los indicios	
3.4	Búsqueda de información en base de conocimiento e Internet	
4	Adquisición, preservación y documentación del incidente	
5	Notificar	

Contención, erradicación y recuperación.		
6	Contención del incidente	
7	Resolución del incidente	
7.1	Identificación de la vía de entrada del incidente	
7.2	Eliminación de componentes asociados al incidente	
7.3	¿Se ha conseguido acotar los equipos afectados?	
8	Recuperación	
8.1	¿Los sistemas afectados vuelven a funcionar correctamente?	
8.2	¿Es necesario aplicar parches y/o actualizaciones?	
8.3	¿Es necesario ajustar los sistemas de control y monitorización para impedir que se vuelva a reproducir el incidente?	
Acciones tras el incidente.		
9	Informe de seguimiento	
10	¿Se han compartido lo conocimientos adquiridos?	

10 GLOSARIO

- **TI (Tecnología Informática)** Este termino resume muchos aspectos referidos a la computadora y la tecnología informática. En el contexto de este informe podemos aplicarlo al conjunto de máquinas que forman una red y sus servicios.
- **Virtualización** Se entiende en el contexto a la capacidad de emular distintos sistemas de computación sobre un mismo harware.
- **HASH** Un HASH es una función matemática que consigue un resumen inequívoco de un archivo. De tal manera que si se modifica el archivo original, el resumen no coincidirá con el resumen de este anterior.
- **Vulnerabilidad** Funcionalidad no esperada de un programa que permite llevar a cavo acciones fuera de lo esperado para este programa.
- **Firewall** Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.
- **Proxy** Su finalidad más habitual es la de consiste en interceptar las conexiones de red que un cliente hace a un servidor de destino, por varios motivos posibles como seguridad, rendimiento, anonimato, etc.
- **Malware** Es un programa destinado a acciones malintencionadas.
- **Spoofing** En términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.
- **IDS Sistema de detección de intrusos** es un programa usado para detectar accesos no autorizados a un computador o a una red.
- **Antivirus** En informática los antivirus son programas cuyo objetivo es detectar y/o eliminar virus informáticos.
- **LOG** Un log es un registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.
- **Exploit** Es una pieza de software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.
- **Sniffer** En informática, un analizador de paquetes es un programa de captura de las tramas de una red de computadoras.
- **DDOS** Es un ataque que normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.
- **Parche informático** En informática, un parche consta de cambios que se aplican a un programa, para corregir errores, agregarle funcionalidad, actualizarlo, etc.

11 REFERENCIAS

- Guías del National Institute of Standards and Technology (NIST)