sedian

Seguridad Digital
de Andalucía

Medidas de contención, mitigación y recuperación, así como protocolo para recolección y custodia de evidencias una vez que hemos detectado un ciberincidente

Sesión 3: 23 de marzo de 2021

Junta de Andalucía

INDICE

Medidas de recuperación

Medidas de recuperación

- **¿Qué es una medida de recuperación?**

Las medidas de recuperación permitirán la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales.

Aunque anteriormente en las medidas de mitigación hemos visto los planes de continuidad de negocio y por lo tanto hemos introducido el concepto de plan de recuperación de desastres, que pertenece en su conjunto a medidas de mitigación y de manera individual a medidas de recuperación.

Es decir una vez que hemos contenido la amenaza y mitigado sus efectos, tenemos que iniciar el proceso de recuperación de los sistemas.

Medidas de recuperación

- **¿Cómo iniciamos las medidas de recuperación?**

En este caso, su fase de análisis es menos profunda y se enfoca más al ámbito más técnico, de modo que es un plan reactivo ante una posible catástrofe. Por ejemplo, si tenemos un plan de desastres para nuestra página web de comercio electrónico, el contendrá todos los pasos para la recuperación de la aplicación.

Para poder hablar de las medidas de recuperación, primero tenemos que plantearnos el tipo de estrategia que vamos a seguir, se puede seguir una estrategia distinta para cada tipo de sistema pero para ello necesitaremos cierto tipo de información que obtendremos de un análisis de impacto en el negocio (BIA).

El propósito final es garantizar que la estrategia de continuidad en su conjunto respalda de forma adecuada la entrega de los productos y servicios de la organización, evitando momentos de incertidumbre en la supervivencia mientras se recupera de una actividad interrumpida.

Para lograr cierto grado de previsión y certeza en las actuaciones de recuperación es necesario tener en cuenta unos requisitos

Medidas de recuperación

- **Requisitos de recuperación**

Umbrales de recuperación

Los umbrales de recuperación proporcionan la información necesaria para identificar las necesidades de recursos de recuperación dentro de los plazos especificados. Por tanto, las estrategias de recuperación vienen definidas por:

Punto Objetivo de Recuperación (RPO, Recovery Point Objective):	• Básicamente, RPO significa lo que la organización está dispuesta a perder en cantidad de datos. Para reducir un RPO es necesario aumentar el sincronismo de réplica de datos.
Tiempo Objetivo de Recuperación (RTO, Recovery Time Objective):	• es el tiempo que pasará antes de que una infraestructura está disponible. Para reducir el RTO, se requiere que la Infraestructura (Tecnológica, Logística, Física) esté disponible en el menor tiempo posible.

Medidas de recuperación

- **Requisitos de recuperación**

Coste de la recuperación

La elección de las estrategias y soluciones de recuperación está dictada por dos factores:

La capacidad de cumplir con los umbrales de recuperación anteriormente definidos.

El coste correspondiente a la adopción de la solución que haga cumplir con los umbrales de recuperación.

Medidas de recuperación

- **Requisitos de recuperación**

Requisitos mínimos aceptables para la recuperación

Este requisito nos permite delimitar la estrategia de recuperación de un sistema de información, es el concepto de Objetivos Mínimos de Continuidad de Negocio (MBCO), que establece niveles mínimos de servicio o producto aceptables por la organización para alcanzar sus objetivos durante la disrupción.

Como no es objeto de este tema centrarnos en todas las posibles soluciones, vamos a ir directamente al punto que nos interesa: Copias de Seguridad y Recuperación.

Medidas de recuperación

- **Requisitos de recuperación**

Back & Recuperación

A pesar de que la prioridad para todos los servicios es levantar el servicio cuanto antes y cumpliendo con los RTO´s establecidos, los datos son un activo a tener en cuenta y que han de estar disponibles para estos servicios. En caso de que estos datos se perdieran o no estuvieran disponibles durante un periodo de tiempo (superior al RPO establecido), los procesos de negocio podrían detenerse y ocasionar cuantiosas pérdidas. Por tanto, los sistemas de Backup & Recovery deben garantizar esta disponibilidad a lo largo del tiempo y permitir una recuperación que se adapte al RPO previamente fijado.

Las herramientas de Backup & Recovery deben optimizar el uso de recursos (ancho de banda, dispositivos de cinta, etc.) y minimizar el impacto de las copias en los sistemas de producción.

Otro factor a tener en cuenta es que la infraestructura tecnológica en la Organización es muy heterogénea y distribuida. En este contexto, las soluciones de Backup & Recovery deben ser adecuadas para el amplio abanico de entornos y dispositivos que actualmente existen en la Organización.

Medidas de recuperación

- **Requisitos de recuperación**

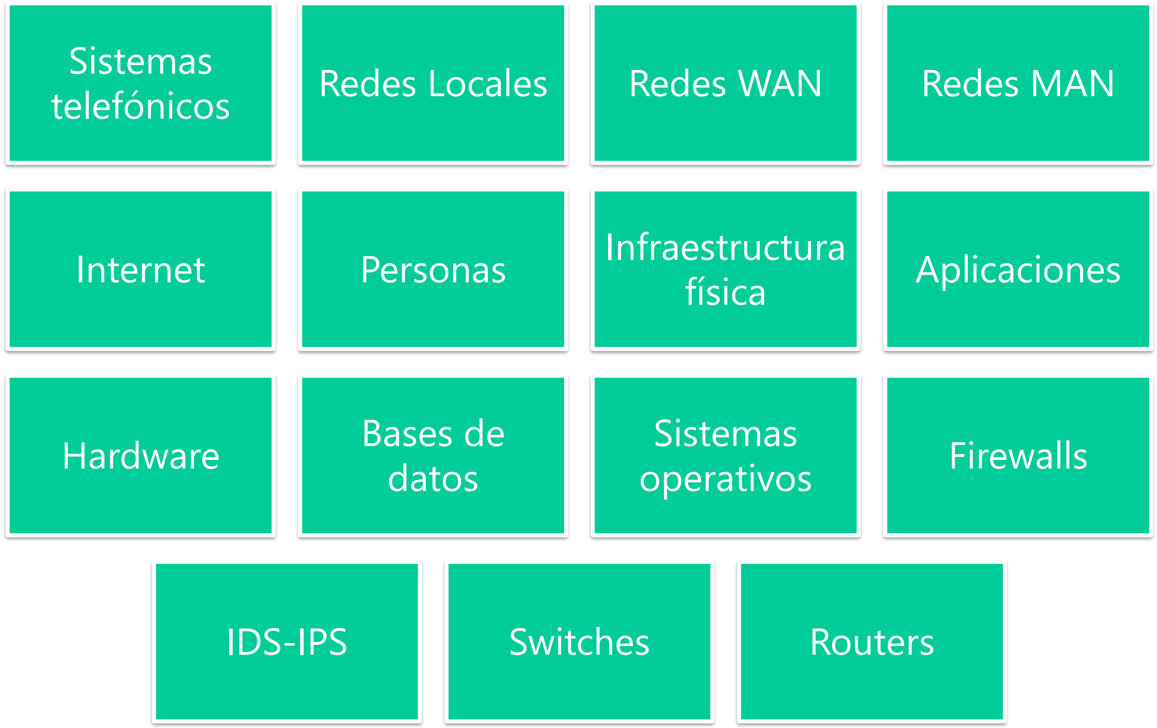
Back & Recuperación

Es necesario tener en cuenta ciertos elementos clave, que son:

Servidor de backup centralizado:	• Habitualmente, la soluciones de Backup & Recovery se basan en un servidor central. Desde este servidor se realiza la gestión del sistema de Backup & Recovery (definición de políticas, definición y monitorización de planificaciones, etc.) y la gestión de los dispositivos de almacenamiento. En ocasiones, por razones de capacidad, distribución geográfica o alta disponibilidad, se implantan varios servidores de backup los cuales gestionan un subconjunto del entorno y sus propios dispositivos de almacenamiento.
Clientes de backup:	• En los servidores donde se van a realizar las copias de los datos "relevantes" se instala un cliente de backup que permite ejecutar las planificaciones definidas en el servidor central y realizar de forma eficiente la copia y recuperación de datos a través de la red. Estos clientes de backup están disponibles para múltiples plataformas, de forma que se simplifica la implantación y gestión del Backup & Recovery en entornos heterogéneos como el existente en la Organización. También es posible acceder a los clientes de backup de forma remota, por ejemplo vía Web, pudiendo realizar copias y recuperaciones sin necesidad de abrir una sesión en el servidor. Con soluciones de este tipo se simplifica la gestión del Backup & Recovery y reduce el gasto derivado del mantenimiento y soporte de los sistemas de Backup & Recovery empresarial. También facilitan el crecimiento en el número de servidores y en el volumen de datos.
Journal Based backup:	• Cuando se realizan copias incrementales en grandes servidores de ficheros, una parte muy importante del tiempo de copia se invierte en inspeccionar los ficheros para ver cuáles han cambiado desde la última copia. Mediante los agentes de journal based backup de algunas herramientas de Backup & Recovery, la detección de los ficheros que han cambiado se va construyendo durante el tiempo de ejecución del servidor. De esta forma, cuando se inicia la copia incremental ya se dispone de la lista de ficheros candidatos a ser copiados. Gracias a esta técnica, en grandes servidores de ficheros puede conseguirse un reducción del 50% del tiempo de copia incremental. El impacto del agente de journal backup es inapreciable.
Instant Archives & Rapid Recovery:	• Resulta difícil realizar copias totales de ciertos servidores y sin embargo es factible la realización de copias incrementales. Esto suele ocurrir en grandes servidores de ficheros o en servidores en delegaciones remotas (las estaciones de la Organización). Una solución a este problema consiste en utilizar la función de "Instant Archive" de algunas herramientas de Backup & Recovery. Gracias a ella es posible generar la copia total de un servidor a partir de los backups incrementales y asignarle una retención diferente

Medidas de recuperación

- **Elementos a considerar:**



Medidas de recuperación

- **Requisitos para considerar un plan de recuperación:**

Requisitos para la recuperación:	• Desarrollar procedimientos de recuperación para identificar la mejor manera de recuperarse en caso de desastre, para llevar acabo estos procedimientos se deben tener en cuento unos requisitos mínimos
Equipo de recuperación de desastres:	• Para lograr una adecuada respuesta a un desastre, se debe establecer un Equipo de Recuperación de Desastres, integrado por personas relacionadas con la infraestructura, sistemas de información y con los procesos de la organización
Recursos necesarios para la recuperación:	• Debe establecerse un tiempo de recuperación objetivo (RTO, Recovery Time Objective), un tiempo máximo tolerable de interrupción o MTPoD (Maximum Tolerable Period of Disruption) y una cantidad de datos objetiva dispuesta a ser perdida (RPO, Recovery Point Objective) para cada uno de sus procesos críticos de la organización, así como los recursos necesarios para que puedan desarrollar sus funciones y las estrategias para la recuperación de dichos recursos.
Pruebas y revisión de todos los procedimientos:	• La efectividad del DRP se puede valorar si existe un plan de pruebas que se lleve a cabo en condiciones reales. La fase de prueba debe contener las actividades más importantes que requieran comprobación y certeza en su funcionamiento futuro. • Se debe probar dentro de un ambiente que simule las condiciones que serían aplicables a una situación real. Es importante que las pruebas se lleven a cabo por las personas que serían responsables en condiciones reales

Ciclo de vida de un incidente de ciberseguridad

Ciclo de vida de un incidente de ciberseguridad

- **¿Qué es un ciberincidente?**

Definición (ENS, NIS, INCIBE, AEPD)

Aquel suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información (ENS), es decir todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información (NIS).

Se conoce como gestión de incidentes de seguridad de la información a un conjunto ordenado de acciones enfocadas a prevenir, en la medida de lo posible, la ocurrencia de ciberincidentes y, en caso de que ocurran, restaurar los niveles de operación lo antes posible. El proceso de gestión de incidentes consta de diferentes fases y, aunque todas son necesarias, algunas pueden estar incluidas como parte de otras o tratarse de manera simultánea (INCIBE).

Una brecha de seguridad es un incidente de seguridad que afecta a datos de carácter personal. Este incidente puede tener un origen accidental o intencionado y además puede afectar a datos tratados digitalmente o en formato papel. En general, se trata de un suceso que ocasione destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos personales.

Una brecha de seguridad puede tener una serie de efectos adversos considerables en las personas, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales; por lo que hay que intentar evitarlas y en caso de que sucedan gestionarlas adecuadamente.

Las entradas en el blog proporcionan una introducción sencilla para iniciarse en la gestión de brechas de seguridad. La Guía para la Gestión y Notificación de Brechas de Seguridad y las Directrices del Comité Europeo de Protección de Datos proporcionan información más completa (AEPD).

Ciclo de vida de un incidente de ciberseguridad

- **¿Porque tantas definiciones?**

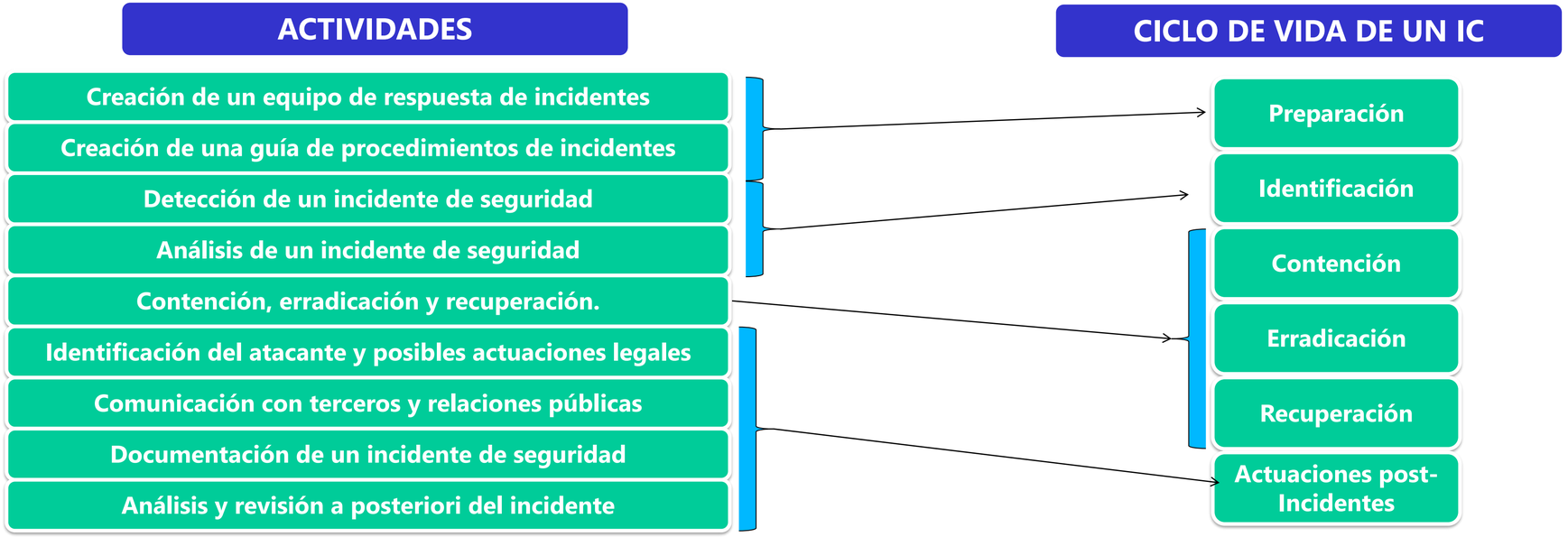
Obligaciones

El Reglamento (UE) 2016/679, General de Protección de Datos (RGPD)	Establece la obligación para las organizaciones (públicas y privadas) que actúen como responsables de tratamiento de notificar a la Autoridad de Control competente las brechas de seguridad que puedan ocasionar daños y perjuicios sobre las personas y, si esos daños son graves, comunicar la brecha a las personas cuyos datos se hayan visto afectados para que puedan tomar sus propias medidas.
Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.	Establece la obligación de disponer de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información. Estos procedimientos cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.
Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.	Los operadores de servicios esenciales y los proveedores de servicios digitales deberán gestionar y resolver los incidentes de seguridad que afecten a las redes y sistemas de información utilizados para la prestación de sus servicios. En el caso de redes y sistemas que no sean propios los operadores deberán tomar las medidas necesarias para garantizar que dichas acciones se lleven a cabo por los proveedores externos. Esta obligación alcanza tanto a los incidentes detectados por el propio operador o proveedor como a los que les señalen el CSIRT de referencia o la autoridad competente, cuando tengan conocimiento de alguna circunstancia que haga sospechar de la existencia de un incidente.

Ciclo de vida de un incidente de ciberseguridad

- **Plan de respuesta a incidentes de ciberseguridad**

La definición e implantación de un plan de respuesta de incidentes de seguridad debe tener en cuenta un conjunto de actividades y tareas, entre las cuales podríamos destacar:



Ciclo de vida de un incidente de ciberseguridad

- **Plan de respuesta a incidentes de ciberseguridad**

Preparación

Durante el estado previo a la declaración de un ciberincidente es necesario que toda entidad esté preparada para cualquier suceso que pudiera ocurrir. Una buena anticipación y entrenamiento previo pueden ser la diferencia entre una gestión eficaz de un incidente o un desastre absoluto, para lo que hace falta tener en cuenta tres pilares fundamentales: las personas, los procedimientos y la tecnología. El momento de declararse un incidente ya será tarde para comenzar a planificar.

Creación de un equipo de respuesta de incidentes:	• Debe esta constituido por personal con formación y experiencia necesaria para poder actuar ante las incidencias que puedan afectar a la organización y sus sistemas. Este punto dependerá en gran parte del tamaño de la organización. • Se deberá tener un listado de contactos (teléfono, correo electrónico) de emergencia para localizar rápidamente a los responsables y personas claves.
Creación de una guía de procedimientos de incidentes:	• La organización debe definir una guía con los procedimientos y acciones necesarias para la detección, contención, erradicación y recuperación de los sistemas. El objetivo de esta guía es conseguir dar una respuesta rápida, sistemática y eficaz ante cualquier tipo de incidente, permitiendo así minimizar el impacto del mismo al mínimo

Ciclo de vida de un incidente de ciberseguridad

- **Plan de respuesta a incidentes de ciberseguridad**

Identificación

Cualquier organización debe conocer cuál es su estado normal de operación y qué sucesos forman parte de la operativa diaria, ya que solamente así será posible identificar aquellos casos que pueden ser considerados anormales y requieren un análisis en profundidad. Resulta imposible disponer de procedimientos para gestionar todos los ciberincidentes que pueden llegar a materializarse, sin embargo, existen unos vectores de ataque comunes que ayudan a identificar un incidente de seguridad, determinar su alcance y los sistemas afectados.

Detección de un incidente de seguridad:	Las organizaciones debe tener definido un proceso de que detecte actividades anómalas en el sistema, ya sea a través de indicadores o comportamientos anómalos no definidos.
Análisis de un incidente de ciberseguridad:	El plan de respuesta de incidentes de seguridad debe tener definido como debe actuar el equipo de respuesta ante un incidente. Se debe determinar el alcance (¿Qué equipos?¿Cuantos equipos?¿Que procesos?¿Cuantos procesos?¿Que información se ha visto comprometida?), el origen (el correo electrónico, un accidente, un error, una vulnerabilidad conocida, etc.), Responsables (¿A quien vas a llamar?) y asignar una prioridad (¿Es importante?¿Puede esperar?)

Ciclo de vida de un incidente de ciberseguridad

- **Plan de respuesta a incidentes de ciberseguridad**

Identificación

Detección de un incidente de seguridad

Fuentes de información

- Registros
- Cuentas de usuario
- Ficheros ocultos
- Ficheros con permisos inusuales.
- Sistemas de prevención de fugas (DLP)
- Procesos y servicios inusuales
- Una carga excesiva de disco o memoria.
- Sesiones abiertas en la máquina desde otros equipos
- Tareas programadas o actividad sospechosa.
- Etc.

Vectores de ataque

- Correo electrónico
- Vulnerabilidades conocidas
- Dispositivos de almacenamiento externo
- Uso inapropiado de los activos
- Pérdida o robo de activos
- Vectores externos
- Etc.

Análisis de un incidente

- ¿Qué?
- ¿Cuántos?
- ¿Quien?
- ¿De donde?
- ¿Responsables?
- ¿Prioridad?
- ¿Cómo solucionarlo?

Ciclo de vida de un incidente de ciberseguridad

- **Plan de respuesta a incidentes de ciberseguridad**

Contención, erradicación y recuperación

Contención:

Dentro del plan de respuestas a incidentes de ciberseguridad, se debe definir una estrategia de contención dependiendo del tipo de incidente.

•**Una rápida actuación:** Evita que el incidente se propague y pueda tener consecuencias mayores. Entre las posibles acciones que se pueden tomar:

- Desconexión de los equipos.
- Desactivación de procesos.
- Desconexión de las comunicaciones.
- Etc.

•**Una segunda opción** es retrasar la contención para poder estudiar con detalle el tipo de incidente, averiguar quien es el responsable, reunir evidencias, etc. Esta actuación se puede llevar a cabo siempre que sea posible monitorizar y controlar la actuación de los atacantes

Erradicación:

Esta fase es la encargada de llevar a cabo la eliminación de todos los factores y agentes que han ayudado a generar el incidente. Entre las posibles acciones que se pueden tomar:

- Eliminar puertas traseras
- Eliminar contenido malicioso.
- Material inadecuado.
- Cuentas de usuario fraudulentas.
- Etc.

Recuperación:

Es la etapa en la que se trata de recuperar toda la información y todos los sistemas afectados para que puedan volver a la normalidad. Entre las posibles acciones que se pueden tomar:

- Reinstalación de Sistemas operativos
- Recuperación de copias de seguridad del sistema.
- Mejora de la configuración de seguridad.
- Actualización de los sistema (parches y actualizaciones).
- Cambio de contraseñas.
- Desactivación de cuentas usadas para y por el incidente, revisión de medidas de seguridad, etc.

Ciclo de vida de un incidente de ciberseguridad

- **Plan de respuesta a incidentes de ciberseguridad**

Actuaciones post-Incidentes

Una vez que el ciberincidente está controlado y la actividad ha vuelto a la normalidad, es momento de llevar a cabo un proceso al que no se le suele dar toda la importancia que merece. En esta fase podemos encontrar las siguientes actividades:

Identificación del atacante y posibles actuaciones legales
Este punto es necesario para poder tomar acciones legales contra el atacante. Antiguamente (hasta hace unos 5 años aproximadamente, esta acción no tenía mucho sentido, ya fuese por desconocimiento, falta de tecnología, incluso diferencias legales entre distintos países, etc. Pero últimamente con el avance de las tecnologías, la actualización de las normativas legales, el impacto económico de los incidentes de seguridad, etc. Este punto está adquiriendo una gran importancia.
No obstante a día de hoy aún existen obstáculos para llevar a cabo la identificación:

- IP SPOOFING: Enmascara la dirección de algunos tipos de ataque.
- Los ataques pueden haber secuestrado un equipo de terceos.
- Uso de IPS dinámicas
- Servidores Proxy con el servicio NAT activo (En resumen compartir direcciones públicas)

Ciclo de vida de un incidente de ciberseguridad

- **Plan de respuesta a incidentes de ciberseguridad**

Actuaciones post-Incidentes

Comunicación con terceros y relaciones públicas

PLAN DE EMERGENCIA	OBLIGACIÓN LEGAL	AYUDA Y COLABORACIÓN	OTROS
• Agentes y fuerzas del orden • Bomberos • Servicios médicos • Etc.	• CCN-CERT • AEPD • CNPIC. • Etc.	• ISP´S • Proveedores • Contratación rápida de servicios de ayuda.	• Periodistas. • Etc.

Ciclo de vida de un incidente de ciberseguridad

- **Plan de respuesta a incidentes de ciberseguridad**

Actuaciones post-Incidentes

Documentación de un incidente de seguridad

El plan de recuperación de incidentes debe establecer como se tiene que documentar. Una correcta y completa documentación del incidente facilitará el posterior estudio de cuales han sido las posibles causas y sus consecuencias. Entre otra información se recomienda recopilar:

- La descripción del incidente
- Todos los registros (logs)
- Daños producidos
- Decisiones y actuaciones del equipo de respuesta
- Comunicaciones que se han realizado con terceros y con los medios
- Todas las evidencias obtenidas durante el análisis
- Comentarios e impresiones del incidente y la manera de proceder.
- Posibles actuaciones y recomendaciones para reforzar la seguridad

Ciclo de vida de un incidente de ciberseguridad

- **Plan de respuesta a incidentes de ciberseguridad**

Actuaciones post-Incidentes

Análisis y revisión a posteriori del incidente

Más conocido como lecciones aprendidas. Una vez que el ciberincidente está controlado y la actividad ha vuelto a la normalidad, es momento de llevar a cabo un proceso al que no se le suele dar toda la importancia que merece: las lecciones aprendidas.

Conviene pararse a reflexionar sobre lo sucedido, analizando las causas del problema, cómo se ha desarrollado la actividad durante la gestión del ciberincidente y todos los problemas asociados a la misma. La utilización de una herramienta de gestión de incidentes o una bitácora en la que se registre toda la información a medida que se ha ido recopilando ayudará en la elaboración de un informe post-incidente y evitará obviar información importante.

La finalidad de este proceso es aprender de lo sucedido y que se puedan tomar las medidas adecuadas para evitar que una situación similar se pueda volver a repetir. Esto ayudará también a evaluar los procedimientos de actuación, la cadena de mando, las políticas de seguridad y entrenará a los implicados para futuras situaciones de crisis.

Cada miembro del equipo implicado en la gestión del ciberincidente debe aportar sus anotaciones y todas deben ser recogidas en un informe general que puede ser revisado en una reunión. El informe post-incidente debe incluir un breve resumen ejecutivo y anexos técnicos para ser distribuido tanto a altos cargos de la organización como a personal técnico que desee ahondar en lo sucedido y analizar el proceso completo.

Ciclo de vida de un incidente de ciberseguridad

- **Plan de respuesta a incidentes de ciberseguridad**

Informática forense

Es una herramienta fundamental que nos ayudará a adquirir, preservar, obtener y presentar toda la información relacionada con un incidente de seguridad.

A continuación pasaremos a estudiar las distintas etapas de un análisis forense de un incidente de ciberseguridad:

Recolección de información

Custodia de información

Análisis de información

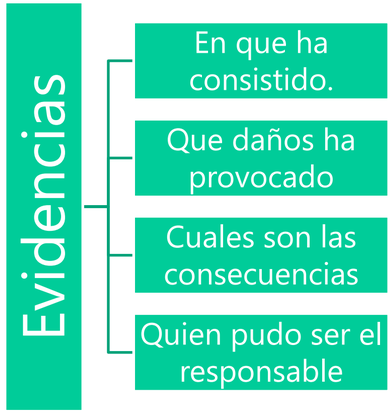
Ciclo de vida de un incidente de ciberseguridad

- **Plan de respuesta a incidentes de ciberseguridad**

Informática forense

Recolección de información

Esta fase también conocida como captura de evidencias, y tiene por objeto recopilar toda aquella información que podrá ser capturada y analizada posteriormente para interpretar la forma más clara y posible un incidente de seguridad:



Ciclo de vida de un incidente de ciberseguridad

- **Plan de respuesta a incidentes de ciberseguridad**

Informática forense

Recolección de información

Las evidencias “digitales”, a pesar de ser intangibles, pueden ser presentadas como prueba ante un juicio, siempre que se ofrezcan suficientes garantías en las distintas etapas del proceso de análisis forense. Por ejemplo mediante el proceso de aislamiento de la escena del crimen, una adecuada cadena de custodia, etc.

La captura de las evidencias puede llegar a ser un proceso tremendamente complicado debido a la volatilidad de las misma, si estas se encuentra en la memoria RAM o en la ROM, ya que se perderá casi seguro cuando se apague el sistema.

Entre estas evidencias podemos encontrar:

- Memoria global del sistema y de cada proceso
- Procesos y servicios en ejecución dentro del sistema
- Controladores (Drivers)
- Información de configuración de servicios, hardware, software.
- Usuarios y grupos de usuarios

Ciclo de vida de un incidente de ciberseguridad

- **Plan de respuesta a incidentes de ciberseguridad**

Informática forense

Custodia de información
También conocido como preservación de evidencias o cadena de custodia, es un proceso compuesto de un conjunto de medidas técnicas y organizativas.

En un primer lugar se debe utilizar un adecuado método de identificación, precinto, etiquetado y almacenamiento de evidencias considerando la incorporación de una firma temporal (digital timestamp) en cada evidencia, para dejar registrado en que momento se obtuvo la evidencia.

Estas evidencias deben ser preservadas en lugares libres de ser afectadas por condiciones ambientales, como la humedad, el agua, el exceso de calor, campos magnéticos, radiaciones, etc.

Se debe garantizar que los datos obtenidos no van a ser alterados, por lo que se deberían utilizar herramientas de verificación de datos.

Otro punto importante es la documentación de todo el proceso. En dicha documentación se debe reflejar toda la información posible del proceso de recolección de información, desde los responsables que llevan a cabo el proceso, el momento, y lugar, etc. En algunos casos se recomienda la grabación en video de todo el proceso.

Ciclo de vida de un incidente de ciberseguridad

- **Plan de respuesta a incidentes de ciberseguridad**

Informática forense

Análisis de la Información
La labor del análisis de riesgos puede comenzar con la búsqueda de información en los volcados de memoria en las copias de los discos afectados para localizar ficheros.
Continua con la ejecución de los ficheros fraudulentos localizados en un entorno de pruebas controlado (por ejemplo en un máquina virtual), para estudiar el comportamiento del mismo, como interacción con el sistema, que aplicaciones llama, a que webs se intenta conectar, etc.

Asimismo, se deberá realizar una comprobación de los ficheros que han sido modificados para detectar posibles manipulaciones.

El análisis de evidencias también deberá contemplar la revisión de todos los ficheros de configuración donde se establezcan parámetros bases del sistema como el arranque del mismo, servicios que se ejecutan al iniciar el SSOO y otras directivas.

Además también se deben obtener información de elementos externos como pueden ser los IPS, Firewall, SIEM, etc.

Ciclo de vida de un incidente de ciberseguridad

- **Plan de respuesta a incidentes de ciberseguridad**

Informática forense

Análisis de la Información

En relación con toda la información comentada hasta el momento conviene realizar un conjunto de tareas:

- Identificación de las extensiones de todos los ficheros o a través de su número mágica (la información contenida en la cabecera de cada fichero).
- Visualización de todo el contenido gráfico.
- Estudio de las fechas de creación, modificación y acceso a los ficheros con el objeto de detectar que ficheros han sufrido cambios desde su creación y para comparar las fechas con las fechas del incidente.
- Revisión de los permisos de acceso y ejecución
- Revisión de todos los ficheros temporales obtenidos (memorias caché)

Ciclo de vida de un incidente de ciberseguridad

- **Plan de respuesta a incidentes de ciberseguridad**

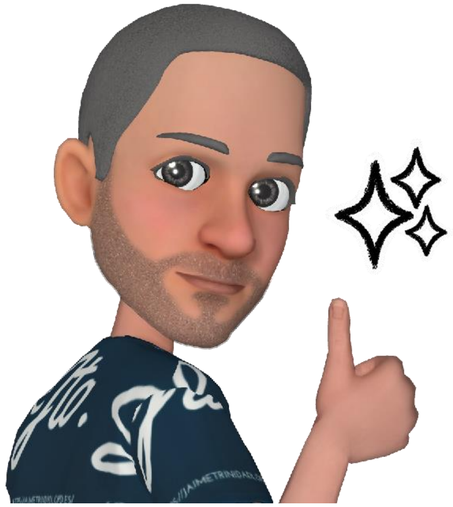
Informática forense

Análisis de la Información

En relación con toda la información comentada hasta el momento conviene realizar un conjunto de tareas:

- Identificación de las extensiones de todos los ficheros o a través de su número mágica (la información contenida en la cabecera de cada fichero).
- Visualización de todo el contenido gráfico.
- Estudio de las fechas de creación, modificación y acceso a los ficheros con el objeto de detectar que ficheros han sufrido cambios desde su creación y para comparar las fechas con las fechas del incidente.
- Revisión de los permisos de acceso y ejecución
- Revisión de todos los ficheros temporales obtenidos (memorias caché)

CON ESTO ACABAMOS EL CURSO,
ESPERAMOS VEREMOS EN OTRO CURSO



https://jaimetrinidadlopd.es/

Jaime T. Ortiz

CONSULTOR DE SEGURIDAD DE LA INFORMACION

HTTPS://JAIMETRINIDADLOPD.ES/

sedian Seguridad Digital de Andalucía