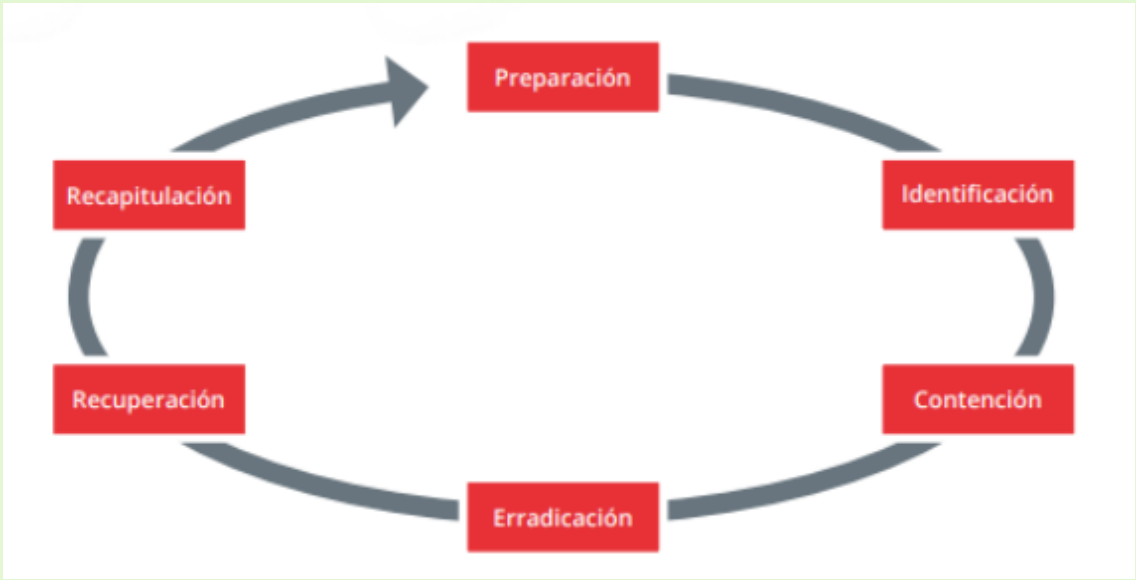
Investigación de los Incidentes de Ciberseguridad.

Gestión de Incidentes de Ciberseguridad



INCIBE. *Gestión de Incidentes* (CC0)

La **gestión de incidentes de seguridad** consiste en la detección, notificación, evaluación, respuesta, tratamiento y aprendizaje de incidentes de seguridad de la información.

La gestión de ciberincidentes de seguridad de la información es 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.

Las **fases** más habituales del **proceso de investigación** son las siguientes:

- **Preparación**: en este estado previo al ciberincidente se busca que toda la entidad esté preparada ante la llegada de cualquier posible suceso, para ello, la anticipación y el entrenamiento previo son claves, siempre teniendo en cuenta tres pilares fundamentales: las personas, los procedimientos y la tecnología.
- **Identificación**: conociendo el estado normal de la operativa diaria, la organización es capaz de identificar anomalías que requieran de análisis en profundidad. Si el evento finalmente se descarta, se vuelve a la fase de preparación.
- **Contención**: el tiempo es determinante cuando ocurre un ciberincidente, ya que la reputación o la continuidad del negocio están en juego. En esta fase se busca contener

el problema, evitando que el atacante cause más daños como, por ejemplo, comprometiendo dispositivos adicionales o divulgando más información. Posteriormente se estudia la situación y se clasifica el ciberincidente. También conviene registrar y documentar lo ocurrido con ayuda de herramientas de gestión y ticketing, además de llevar a cabo procedimientos de toma y preservación de evidencias para su análisis posterior.

- **Mitigación**: se toman las medidas necesarias para la mitigación, las cuales dependerán del tipo de ciberincidente. En algunos casos, puede ser necesario solicitar asistencia de entidades externas, como proveedores de servicios de mitigación de este tipo de ataques o un CSIRT nacional como INCIBE-CERT, que puedan apoyar en el análisis y definición de la estrategia de mitigación.
- **Recuperación**: la finalidad de esta fase consiste en devolver el nivel de operación a su estado normal y que las áreas de negocio afectadas puedan retomar su actividad. También se debe realizar un seguimiento durante la puesta en producción, en busca de posibles actividades sospechosas.
- **Actuaciones post-incidente**: una vez que el ciberincidente está controlado y la actividad ha vuelto a la normalidad llega la hora de las lecciones aprendidas, cuya finalidad es asimilar lo sucedido para que se puedan tomar las medidas preventivas adecuadas y evitar que una situación similar se pueda repetir.

El **procedimiento y los mecanismos para la notificación de ciberincidentes al CSIRT de referencia**, puede realizarse desde la entidad afectada, ciudadanos, PYMEs, entidades de derecho privado o instituciones afiliadas a RedIRIS hacia INCIBE-CERT o viceversa, para beneficiarse del servicio de respuesta, independientemente de que finalmente resuelva el ciberincidente por sus propios medios.

Dicho **procedimiento** se divide en **tres fases**:

- **Apertura**: cuando se recibe una notificación, el equipo técnico de INCIBE-CERT realiza un análisis inicial para determinar el ámbito de actuación.
- **Priorización**: a cada ciberincidente se le asignará una prioridad en función de la peligrosidad y del impacto potencial del mismo.
- **Resolución**: una vez que se ha alcanzado una solución que implique el cierre del incidente, tanto por parte del afectado como por parte de INCIBE-CERT, ésta será comunicada a los actores implicados en el ciberincidente.

1.- Recopilación de Evidencias.

Los Pilares de la Recopilación de Evidencias

INCIBE. *Recopilación de Evidencias* (CC0)

Una evidencia es una información que, por sí misma, o en combinación con otra información, se utiliza para probar algo.

La **recopilación de incidencias** es una fase inicial en la que **toda entidad debe estar preparada para cualquier suceso que pudiera ocurrir.** Una buena anticipación y entrenamiento previo es clave para realizar una gestión eficaz de un incidente, para lo que hace falta tener en cuenta **tres pilares fundamentales:**

- Las **personas**
- Los **procedimientos**
- La **tecnología**

Para saber más

El estándar *de facto* para la recopilación de información de incidentes de seguridad es la RFC3227: Directrices para la recolección de evidencias y su almacenamiento.

Los detalles de esta documentación se pueden consultar en el siguiente enlace:

https://www.incibe-cert.es/blog/rfc3227

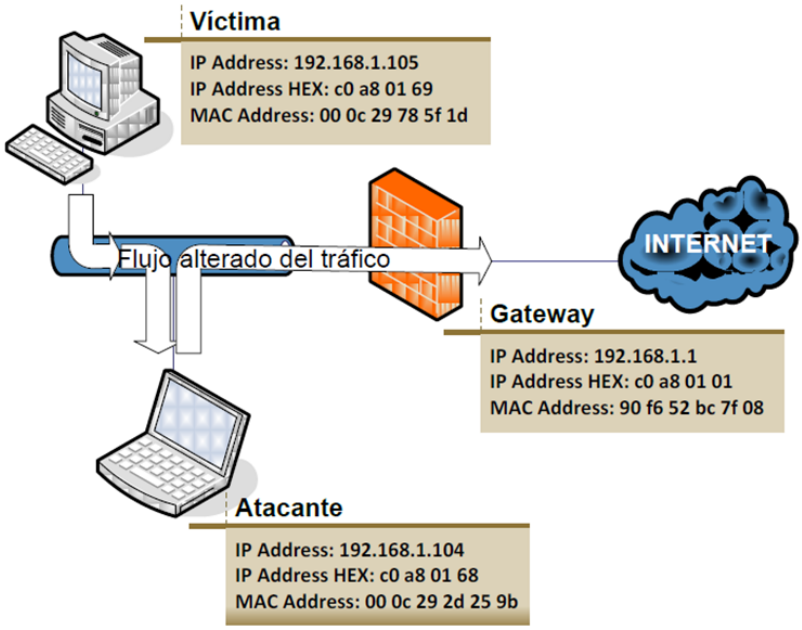
1.1.- Principios durante la recolección de evidencias.

INCIBE. *Recolección de Evidencias* (CC0)

Durante el **proceso de recolección de evidencias** relativas a incidentes de ciberseguridad, se deberán tener en cuenta los siguientes **Principios**:

- Capturar una **imagen del sistema** tan precisa como sea posible.
- Realizar **notas detalladas**, incluyendo fechas y horas e indicando si se utiliza horario local o UTC.
- **Minimizar los cambios en la información** que se está recolectando y eliminar los agentes externos que puedan hacerlos.
- En el caso de enfrentarse a un dilema entre recolección y análisis, se deberá elegir **primero recolección y después análisis**, para evitar así el potencial deterioro de información valiosa.
- Recoger la información según el **orden de volatilidad** (de mayor a menor).
- Tener en cuenta que **para cada dispositivo** la recogida de información puede realizarse **de distinta manera**.

1.1.1.- Orden de volatilidad.



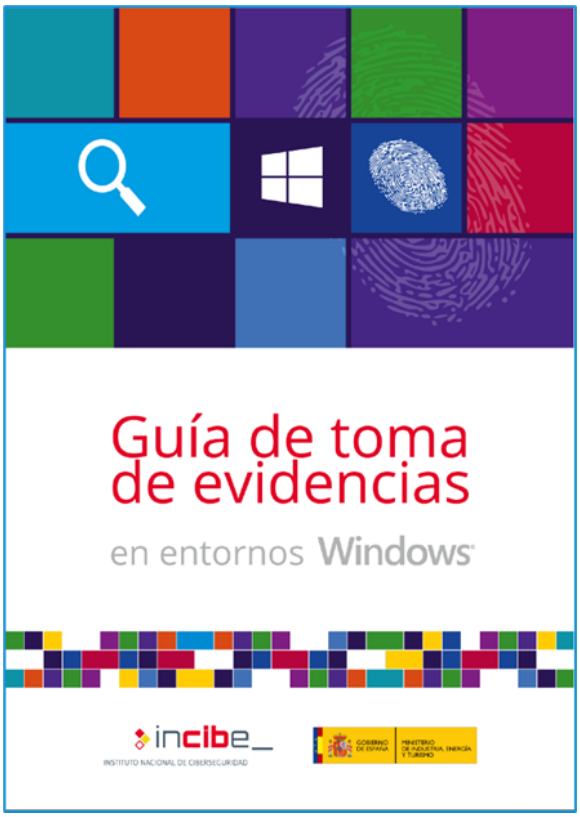
INCIBE. *ARP Spoofing* (CC0)

El orden de volatilidad hace referencia al **período de tiempo durante el cual está accesible cierta información**. Por esta razón se debe recolectar en primer lugar aquella información que vaya a estar disponible durante el menor período de tiempo, es decir, aquella cuya volatilidad sea mayor.

De acuerdo con esta escala se puede crear la siguiente **lista en orden de mayor a menor volatilidad**:

- Registros y contenido de la caché.
- Tabla de enrutamiento, caché ARP, tabla de procesos, estadísticas del kernel, memoria.
- Información temporal del sistema.
- Disco.
- Logs del sistema.
- Configuración física y topología de la red.
- Documentos.

1.1.2.- Acciones que deben evitarse.

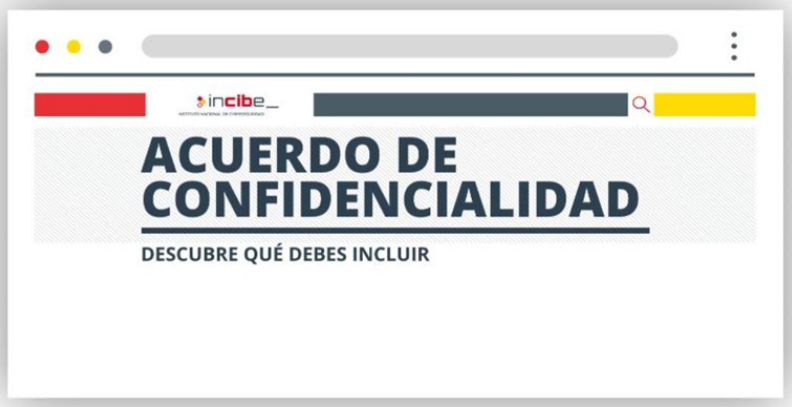


INCIBE. *Guía de Toma de Evidencias* (CC0)

Se deben evitar ciertas acciones para no invalidar el proceso de recolección de información, ya que debe preservarse su integridad con el fin de que los resultados obtenidos puedan utilizarse en un juicio en el caso de que sea necesario:

- No apagar el ordenador hasta que se haya recopilado toda la información.
- No confiar en la información proporcionada por los programas del sistema, ya que pueden haberse visto comprometidos. Se deberá recopilar la información mediante programas desde un medio protegido.
- No ejecutar programas que modifiquen la fecha y hora de acceso de todos los ficheros del sistema.

1.1.3.- Consideraciones sobre la Privacidad.



INCIBE. *Acuerdo de Confidencialidad* (CC0)

- **Es muy importante tener en consideración las pautas de la empresa en lo que a privacidad se refiere**. Es habitual solicitar una autorización por escrito a quien corresponda para poder llevar a cabo la recolección de evidencias. Este es un aspecto fundamental, ya que puede darse el caso de que se trabaje con información confidencial o de vital importancia para la empresa, o que la disponibilidad de los servicios se vea afectada. En este ámbito de trabajo, el documento más habitual es el **Acuerdo de No Divulgación** o NDA, puesto que generalmente la información comprometida por el incidente puede ser información industrial secreta, o datos protegidos de clientes.
- **No hay que entrometerse en la privacidad de las personas sin una justificación.** No se debe recopilar datos de lugares a los que normalmente no hay razón para acceder, como ficheros personales, a menos que se disponga de suficientes indicios. En el mundo de la Ciberseguridad, a aquellas personas o empresas que recopilan datos personales de forma indiscriminada, con o sin justificación, se los denomina coloquialmente "Diógenes del Dato".

Autoevaluación

¿Qué es ser un "Diógenes del Dato"?

- ○ No tener en cuenta la volatilidad a la hora de recopilar la información de un incidente
- ○ Ignorar las pautas de la empresa en lo que a privacidad de la información se refiere

- ○ No confiar en la información proporcionada por los programas del sistema
- ○ Recopilar datos personales de forma indiscriminada, con o sin justificación

INCORRECTO

Es recopilar datos personales de forma indiscriminada, con o sin justificación

INCORRECTO

Es recopilar datos personales de forma indiscriminada, con o sin justificación

INCORRECTO

Es recopilar datos personales de forma indiscriminada, con o sin justificación

¡ CORRECTO !

Solución

1. Incorrecto
2. Incorrecto
3. Incorrecto
4. Opción correcta

1.2.- Procedimiento de Recolección.

INCIBE. *Procedimiento de Recolección* (CC0)

El procedimiento de recolección debe de ser lo más detallado posible, procurando que no sea ambiguo y reduciendo al mínimo la toma de decisiones durante el mismo.

No todos los eventos y alertas que se manifiestan en un entorno o sistema constituyen incidentes de seguridad. En un primer momento no se puede saber si lo ocurrido es un incidente de seguridad o no, por lo que no se discriminará la información a recolectar y se acopiará toda aquella que sea sospechosa, teniendo en cuenta las siguientes **líneas de trabajo**:

- Explorar todos los dispositivos potencialmente afectados.
- Capturar todas las evidencias posibles de cada uno de dichos dispositivos.
- No descartar ninguna información aparentemente inútil, puesto que el análisis posterior se efectuará con varios niveles de detalle y profundidad, y cualquier dato puede resultar útil para el estudio manual o para el automático.
- Detallar al máximo las tareas efectuadas durante la captura de evidencias, puesto que algunas de ellas pueden ser interferentes con los datos a analizar y esto resultará también muy importante para el posterior proceso de análisis.
- Anotar la secuencia de acciones en el tiempo, pues la sucesión de las mismas estará muy relacionada con el apilamiento ordenado de evidencias, que resulta clave asimismo para el análisis.
- Por si más tarde estas evidencias tuvieran que utilizarse durante un proceso legal, será muy importante garantizar que se mantiene la denominada Cadena de Custodia, que se extiende desde el momento en el que se recopila la evidencia, hasta el instante en que se entrega para el propósito que corresponda.
- Documentar las conclusiones del proceso de recolección de evidencias, que constituirán la base de partida para el análisis posterior.
- Y finalmente, tras el análisis y una vez constatada la necesidad o no de guardar la información, descartar todos aquellos datos que se consideren inútiles.

1.2.1.- Transparencia.

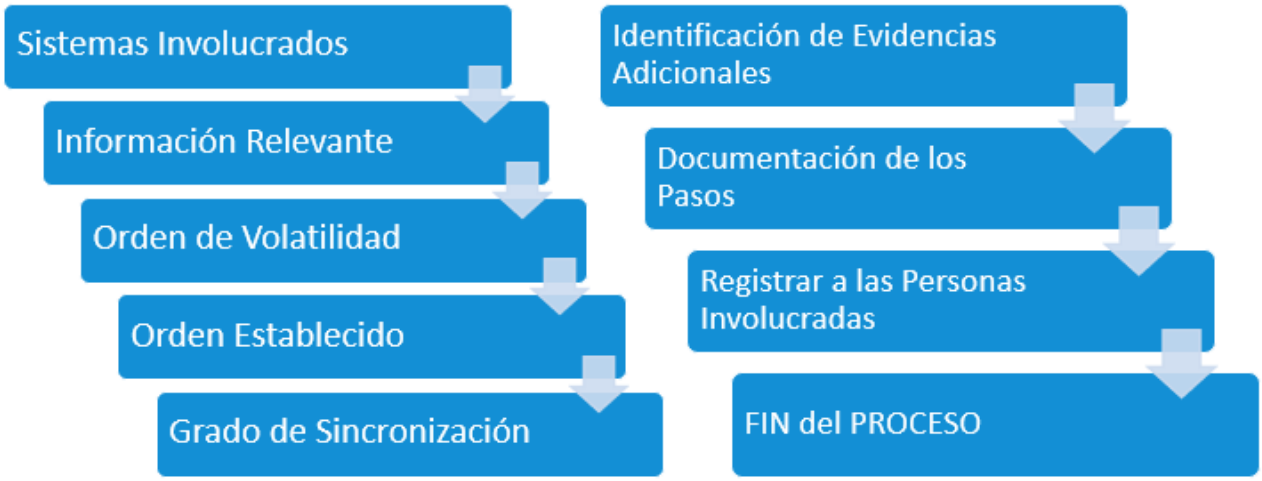
INCIBE. *Transparencia en la Recolección de Evidencias* (CC0)

Los métodos utilizados para recolectar evidencias deben ser transparentes y reproducibles. Se debe estar preparado para reproducir con precisión los métodos usados, y que dichos métodos hayan sido probados por expertos independientes.

La mayor parte de las labores que se efectúan durante la investigación de incidentes tienen por objeto **obtener información con valor legal**. Precisamente por esta razón, el método que se utilice para recopilar los datos debe ser legalmente válido, porque en caso contrario las evidencias pueden quedar invalidadas, como ocurre con cualquier otra prueba de cargo en un proceso judicial.

Esto atañe, por una parte, a que los **procedimientos** sean **conocidos y replicables** y, por otra parte, a que se considere suficientemente contrastado que **no alteran la información al recogerla.**

1.2.2.- Pasos.



Francisco Artés. *Pasos Recopilación Evidencias* (CC0)

Durante el proceso de **recopilación de evidencias**, se seguirán los siguientes **Pasos**:

- ¿Dónde está la evidencia? Listar qué sistemas están involucrados en el incidente y de cuáles de ellos se deben tomar evidencias.
- Establecer qué es relevante y qué no lo es. En caso de duda es mejor recopilar mucha información que poca.
- Fijar el orden de volatilidad para cada sistema.
- Obtener la información de acuerdo con el orden establecido.
- Comprobar el grado de sincronización del reloj del sistema.
- Según se vayan realizando los pasos de recolección preguntarse qué más puede ser una evidencia.
- Documentar cada paso.
- No olvidar a las personas involucradas. Anotar en detalle las personas que estaban presentes, qué estaban haciendo, qué observaron y cómo reaccionaron.

Autoevaluación

Señalar la afirmación correcta:

- ○ Todos los eventos que se manifiestan en un entorno o sistema constituyen incidentes de seguridad
- ○ Todas las alertas que se manifiestan en un entorno o sistema constituyen incidentes de seguridad
- ○ No todos los eventos y alertas que se manifiestan en un entorno o sistema constituyen incidentes de seguridad

INCORRECTO

No todos los eventos y alertas que se manifiestan en un entorno o sistema constituyen incidentes de seguridad

INCORRECTO

No todos los eventos y alertas que se manifiestan en un entorno o sistema constituyen incidentes de seguridad

¡ CORRECTO !

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta

1.3.- El procedimiento de almacenamiento.

INCIBE. *Almacenamiento Seguro de la Información* (CC0)

El procedimiento de almacenamiento de evidencias tiene dos claves:

- La **Cadena de Custodia** de la información. Este concepto tiene su origen en el ámbito legal, cuando se establece una sucesión de controles sólidos para evitar el deterioro, modificación o pérdida de una prueba de un delito. Está relacionado con todas las cuestiones contextuales de vigilancia de un objeto de cualquier tipo, y se implementa mediante un procedimiento de control que afecta a ubicaciones, personal técnico o no, condiciones de conservación, embalaje, climatología, contaminación y posible sustracción. Si el incidente es susceptible de desencadenar posteriores acciones judiciales, un fallo en la Cadena de Custodia puede tener como consecuencia la impugnación de la prueba, que en este caso será una evidencia técnico-informática. Por el contrario, si se han respetado todos los puntos y principios de la Cadena de Custodia establecida, la evidencia tendrá un valor legal indiscutible.
- El **almacén lógico/físico** de la misma. Adicionalmente a lo expresado en el punto anterior en relación con la Cadena de Custodia, en el caso particular de las incidencias de naturaleza técnica y/o informática es necesario poner énfasis en la cuestión de su almacenamiento, dado el carácter tecnológico del mismo. Suponiendo que se cumplen puntualmente las cuestiones de seguridad relativas al almacenamiento físico (dependencias, temperatura, humedad, vigilancia, accidentes, incendios), el punto clave será la solidez del almacenamiento informático. Para gestionar el almacenamiento informático de forma consistente, se deberá poner atención en los dos puntos siguientes:
  - A la hora de **almacenar los datos**, habrá que asegurar que no se está almacenando también el malware que ocasionó el problema, sino sólamente sus consecuencias. Para hacer esto, es conveniente sacar una copia de las evidencias recolectadas, analizarla a fondo una vez que se disponga de la firma del malware, extraer dicho malware y respaldar sólo datos pasivos. Este procedimiento será necesariamente de prueba y error, para lo cual habrá que recurrir repetidamente al respaldo de la información efectuado en un principio.
  - A la hora de **acceder a los datos**, habrá que garantizar que sólo pueden leerlos las personas autorizadas, o bien, capacitadas para analizarlos, pues en muchas ocasiones se pierden o alteran las evidencias debido a acciones voluntaristas pero toscas y sin base técnica, efectuadas por personas de la organización que están analizando el problema sin saber realmente cómo hacerlo (acciones voluntaristas o *fuego amigo*).

1.3.1.- Cadena de custodia.

INCIBE. *Cadena de Custodia* (CC0)

La Cadena de Custodia debe estar claramente documentada y se deben detallar los siguientes puntos:

- Dónde, cuándo y quién descubrió y recolectó la evidencia.
- Dónde, cuándo y quién manejó la evidencia.
- Quién ha custodiado la evidencia, cuánto tiempo y cómo la ha almacenado.
- En el caso de que la evidencia cambie de condiciones de custodia, indicar cuándo y cómo se realizó el intercambio, detallando número de albarán, etc. (seguimiento o *tracking*).

1.3.2.- Dónde y cómo almacenar las evidencias.

INCIBE. *Almacenamiento Seguro* (CC0)

Se debe **almacenar la información en dispositivos cuya seguridad haya sido demostrada** y que permitan detectar intentos de acceso no autorizados.
Además, es crucial que dichos dispositivos dispongan de un **cifrado potente que impida la modificación de la información.**

Ejercicio Resuelto

En este ejercicio implementaremos de forma consistente un almacén de información con múltiples niveles de cifrado.

Para ello, cifraremos un medio de almacenamiento extraible conectado a un servidor Linux, utilizando diferentes técnicas para proteger la información almacenada.

Mostrar retroalimentación

Ejercicio Resuelto (pdf - 807399 B)

Autoevaluación

¿Qué es el Fuego Amigo en el almacenamiento de información de un incidente?

- ○ Ataques auto-infligidos a los medios de almacenamiento, como parte de una estrategia de Hacking Ético
- ○ Pérdida o alteración de evidencias debido a acciones voluntaristas pero toscas y sin base técnica
- ○ Impugnación de una evidencia debido a la ruptura de la Cadena de Custodia

INCORRECTO

Es la pérdida o alteración de evidencias debido a acciones voluntaristas pero toscas y sin base técnica

¡ CORRECTO !

INCORRECTO

Es la pérdida o alteración de evidencias debido a acciones voluntaristas pero toscas y sin base técnica

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto

1.4.- Herramientas Necesarias.

INCIBE. *Herramientas Recolección Incidencias* (CC0)

Existen una serie de **pautas que deben seguirse a la hora de seleccionar las herramientas** con las que se va a llevar a cabo el proceso de recolección:

- Se deben utilizar **herramientas ajenas al sistema** ya que éstas pueden haberse visto comprometidas, principalmente en los casos de malware.
- Se debe procurar utilizar **herramientas que alteren lo menos posible el escenario**, evitando el uso de herramientas de interfaz gráfica y aquellas cuyo uso de memoria sea grande. Lo más recomendable es utilizar herramientas que se puedan ejecutar desde un terminal simple.
- Los programas que se vayan a utilizar para recolectar las evidencias deben estar ubicados en un **dispositivo de sólo lectura** (CD-ROM, USB-ROM, etc.).
- Se debe preparar un **conjunto de utilidades adecuadas a los sistemas operativos** con los que se trabaje.

Para saber más

El **Kit de Análisis** debe incluir los siguientes tipos de herramientas:

- Programas para listar y examinar procesos.
- Programas para examinar el estado del sistema.
- Programas para realizar copias bit a bit.

1.5.- Conclusiones de la Recopilación.

INCIBE. *Conclusiones de la Recopilación de Evidencias* (CC0)

A la hora de enfrentarse a un incidente de seguridad hay que tener muy claras las acciones que se deben realizar, siendo muy meticuloso y detallando en todo momento dicho proceso de manera minuciosa. Asimismo, se debe realizar el proceso procurando ser lo menos intrusivo posible, con el fin de preservar el sistema en su estado original, y siguiendo las pautas indicadas en las diversas metodologías y/o guías existentes.

Finalmente, se debe tener presente que **los requisitos o pautas** a seguir a la hora de realizar un análisis forense digital que vaya a derivar en un proceso legal **varían dependiendo del país**, ya que no existe una legislación común. De todas formas, se debe tender a seguir las indicaciones establecidas en alguna metodología como la RFC3227, con el fin de que dicho proceso se realice de una manera rigurosa.

Para saber más

"Si te mido, te interfiero"

En el ámbito de la mecánica cuántica, **Werner Heisenberg** enunció su famoso **"Principio de Incertidumbre".**

En él, Heisenberg postuló que **no se pueden determinar, simultáneamente y con precisión arbitraria, ciertos pares de variables físicas,** como son, por ejemplo, la posición y el momento lineal de un objeto dado.

Este principio aplica en el mundo **microscópico** y también en el **macroscópico**.

Si se desea conocer la velocidad de una partícula que viaja por el espacio, la única forma de obtener esta información es golpeándola con otra partícula y midiendo la radiación emitida. Esto permitirá conocer la velocidad hasta el momento de la colisión, pero tras la misma la partícula estudiada ya tendrá otra velocidad y otra trayectoria diferentes.

A nivel macroscópico también se ocasiona una interferencia cuando se molesta a una persona que está estudiando, o cuando se ejecuta una aplicación informática sobre un ordenador que ha resultado afectado previamente por un incidente. En ambos casos, la información del contexto cambiará y pasaremos a tener un contexto distinto, lo cual puede que no sirva a nuestros propósitos iniciales.

Autoevaluación

¿Qué programas debe contener un Kit de Análisis?

- ○ Programas para examen de procesos y estado del sistema
- ○ Programas de respaldo selectivo de información
- ○ Programas de registro seguro de la información para asegurar la Cadena de Custodia

¡ CORRECTO !

INCORRECTO

Debe contener programas para examen de procesos y estado del sistema

INCORRECTO

Debe contener programas para examen de procesos y estado del sistema

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto

2.- Análisis de Evidencias.

La Identificación de Ciberincidentes Reales

INCIBE. *Análisis de Evidencias* (CC0)

Los incidentes son cualquier evento que no sea parte de la operación estándar de un servicio, que ocasione o pueda ocasionar una interrupción o una reducción de la calidad de ese servicio.

El objetivo de esta fase es identificar o detectar un ciberincidente real, para lo cual es importante realizar una **monitorización** lo más completa posible. Teniendo en cuenta la máxima de que no todos los eventos o alertas de ciberseguridad son ciberincidentes.

Una vez recopiladas todas las evidencias necesarias en relación con un potencial incidente y asegurada su integridad física y lógica por todos los medios, **se da paso al análisis preliminar de evidencias**.

Este análisis es el paso previo a la investigación del incidente, que es el paso inmediatamente posterior, y tiene por objeto filtrar y completar la información con base en las siguientes consideraciones:

- **Identificar o detectar el incidente**, discriminando entre lo que se considere como tal en la empresa. Cada organización tiene sus usos y costumbres, y en ocasiones algo que puede disparar una alerta en una empresa, puede que sólo sea la situación habitual en otra (por ejemplo, el número de tentativas de acceso erróneas por segundo en un determinado servidor). Los patrones que permiten efectuar este filtrado no se pueden normalizar, pues dependen fuertemente del contexto informático y empresarial, por lo que le corresponderá establecerlos al equipo técnico habitual.
- **Eliminar la información sobrante o confusa**. Una vez que se haya determinado si se trata efectivamente de un incidente, se dispondrá de una mejor base de análisis para discriminar lo qué es útil y lo que no lo es, con el conocimiento añadido de la naturaleza

de los procesos de investigación que se efectuarán después. En la mayoría de las ocasiones, un exceso de información enturbia y alarga la investigación, eliminando la mejor ventaja posible que proporciona la detección temprana de incidentes: el factor tiempo.

- **Complementar la información filtrada con información adicional que resulte valiosa o imprescindible**. Generalmente, los equipos técnicos que recopilan la información y la analizan preliminarmente tienen una visión más amplia que los equipos de investigación, sobre todo porque tienen muy presente el histórico de incidentes acaecidos en el entorno en cuestión. Así pues, se encuentran en una posición propicia para añadir a la información filtrada otros datos que pueden resultar clave para la posterior investigación del incidente.
- **Correlacionar la información con otra información análoga**, semejante, similar o parecida que pueda facilitar la extracción de conclusiones durante el proceso de análisis. Adicionalmente al paso anterior, que sólo trata de enriquecer la información, en este paso se persigue otro objetivo, que es localizar lotes de incidentes aparentemente relacionados que faciliten al investigador la identificación de la causa raíz del incidente.

Autoevaluación

¿Qué es correlacionar la información de un incidente?

- ○ Identificar el incidente y recoger la información asociada al mismo
- ○ Eliminar la información confusa
- ○ Localizar lotes de incidentes aparentemente relacionados
- ○ Enriquecer un incidente con información adicional

INCORRECTO

Es localizar lotes de incidentes aparentemente relacionados

INCORRECTO

Es localizar lotes de incidentes aparentemente relacionados

¡ CORRECTO !

INCORRECTO

Es localizar lotes de incidentes aparentemente relacionados

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

3.- Investigación del Incidente.

La Evolución Constante de la Investigación de Incidentes

INCIBE. *Investigación del Incidente* (CC0)

La investigación de incidentes es una ciencia amplia, compleja y dinámica, que no deja de evolucionar en ningún momento para estar siempre alineada con la aparición de nuevos casos, trabajando intensamente para prevenirlos en la medida de lo posible.

El propósito de este apartado es sólo reflejar las **técnicas empleadas hasta el momento para la investigación de incidentes**, pues el estudio detallado de cada una de ellas supondría el desarrollo de un programa de formación monográfico en cada caso.

Las **técnicas** de investigación de incidentes **están asociadas al momento en el que se efectúa la investigación del incidente**, a saber:

Antes de la aparición del incidente en el entorno. Se trata de técnicas de prevención de incidentes a través del conocimiento profundo de los sistemas de la empresa. Las más habituales son las siguientes:

- **Inventario de los activos clave que soportan los procesos empresariales**. Es recomendable que se efectúe mediante herramientas automáticas de autodescubrimiento y automantenimiento.
- **Evaluación técnica de Vulnerabilidades**. En primera instancia, se identificarán las vulnerabilidades técnicas para los sistemas de información, interfiriendo lo menos posible con los procesos informáticos. En segunda instancia, se asignará severidad y

riesgo a cada una de ellas y se propondrán contramedidas factibles y realistas para la empresa.

- **Tests de Intrusión**. Se desarrollarán pruebas de intrusión contra los sistemas informáticos empresariales, con objeto de identificar vulnerabilidades conocidas y posibles carencias en términos de seguridad software. Hecho esto, se efectuarán pruebas de ataque hardware (canal lateral, inyección de faltas, ingeniería inversa, etc.), de conformidad de protocolos y de servicios de comunicaciones.
- **Análisis de brecha y plan de acción de ciberseguridad**. Este análisis se efectuará desde el punto de vista de las personas, los procesos y la tecnología. Se estudiará el nivel de madurez de los procedimientos asociados y se desarrollará un plan de ciberseguridad en consecuencia.
- **Análisis de riesgos y plan director de ciberseguridad**. Al análisis de brecha anterior se añadirá un análisis de riesgos, del que derivará un plan director de ciberseguridad y un conjunto de proyectos priorizados en función de los riesgos detectados.
- **Despliegue de soluciones de respaldo y restauración** automatizados para la información relevante del negocio.
- **DFIR** ***a priori*** (Digital Forensics & Incident Response). Análisis y preparación ante los incidentes y desarrollo del plan de respuesta a los mismos.
- **Despliegue de soluciones de detección de incidentes basadas en tráfico**: DPI, detección de IoC, identificación de vulnerabilidades, etc.
- **Despliegue de soluciones SIEM** con cuadros de mando preconfigurados y casos de uso para eventos provenientes de sistemas y de soluciones de seguridad empresarial.
- **SOC .** Centro de monitorización de eventos de seguridad y salud de los sistemas empresariales, desde el que se efectuarán labores de contención, prevención y asesoramiento sobre resolución de incidentes de seguridad.
- **Red Team**. Equipo Rojo. Emulación de atacantes que den lugar a los incidentes habituales.

Durante la manifestación del incidente. Técnicas de monitorización, alerta temprana y respuesta rápida.

- **Ejecución del Plan de Respuesta** a los Incidentes diseñado en la fase anterior.
- **Combate Activo frente al Incidente**. Defensa proactiva de los sistemas frente a los incidentes (**blue team,** equipo azul) y gestión de la seguridad de los activos empresariales (**purple team,** equipo morado).

Tras la finalización del incidente. Técnicas de análisis forense.

- **DFIR** ***a posteriori*****.** Análisis forense de los sistemas, recopilación de tráfico y eventos, búsqueda activa de IoC (indicadores de compromiso) e IoA (indicadores de ataque) en los sistemas, correlación y análisis de eventos.

Autoevaluación

¿Qué labores principales se efectúan desde un SOC?

- ○ Inventariado de los activos clave que soportan los procesos empresariales
- ○ Pruebas de intrusión contra los sistemas informáticos empresariales
- ○

Labores de contención, prevención y asesoramiento sobre resolución de incidentes de seguridad

○ Evaluación técnica de Vulnerabilidades

INCORRECTO

Se efectúan labores de contención, prevención y asesoramiento sobre resolución de incidentes de seguridad

INCORRECTO

Se efectúan labores de contención, prevención y asesoramiento sobre resolución de incidentes de seguridad

¡ CORRECTO !

INCORRECTO

Se efectúan labores de contención, prevención y asesoramiento sobre resolución de incidentes de seguridad

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

4.- Intercambio de Información del Incidente con Proveedores u Organismos Competentes.

La Notificación de Incidentes

INCIBE. *Intercambio de Información del Incidente* (CC0)

Una de las claves de la prevención de incidentes es la adecuada notificación de los mismos.

En la Unidad 5 del módulo de "Incidentes de Ciberseguridad" se detalla el mecanismo de Notificación de Incidentes a los **organismos públicos,** mediante el sistema de **Ventanilla Única**, si bien es igualmente relevante la notificación al **resto de interesados que pudieran resultar potencialmente afectados.**

De forma simultánea con el cumplimiento de la obligación legal de notificación del incidente a las Administraciones Públicas, **se debe informar puntualmente a proveedores, partners y otras empresas relacionadas** que pudieran resultar potencialmente afectados por el incidente. Este mecanismo de notificación privada deberá estar recogido en detalle en los planes de actuación ante incidentes.

Autoevaluación

¿Qué debe recoger un Plan de Actuación ante incidentes?

- ○ Los Mecanismos de Notificación de Incidentes a los Organismos Públicos
- ○ Los Mecanismos de Notificación a proveedores, partners y otras empresas relacionadas
- ○ Los Mecanismos de Notificación, sin distinción de destinatarios

INCORRECTO

El plan debe incluir a todos los destinatarios involucrados, sean públicos, privados, internos o externos

INCORRECTO

El plan debe incluir a todos los destinatarios involucrados, sean públicos, privados, internos o externos

¡ CORRECTO !

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta

5.- Medidas de Contención de Incidentes.

El Triaje de Incidentes

INCIBE. *Contención de Incidentes* (CC0)

En el momento que se ha identificado un ciberincidente la máxima prioridad es contener su impacto en la organización, de forma que se pueda evitar lo antes posible la propagación a otros sistemas o redes evitando un impacto mayor, así como la extracción de información fuera de la organización.

Ésta suele ser la fase en la que se realiza el triaje, que consiste en evaluar toda la información disponible en ese momento y realizar una clasificación y priorización preliminar del ciberincidente en función del tipo y de la criticidad de la información y los sistemas afectados. Adicionalmente se identifican **posibles impactos en el negocio** y en función de los procedimientos se trabaja en la **toma de decisiones con las unidades de negocio apropiadas** y/o los responsables de los servicios potencialmente afectados.

Durante la **fase de contención del incidente** se debe:

- Registrar y monitorizar los eventos de las redes, sistemas y aplicaciones.
- Recolectar información situacional que permita detectar anomalías.
- Disponer de capacidades para descubrir ciberincidentes y comunicarlos a los contactos apropiados.
- Recopilar y almacenar de forma segura todas las evidencias.
- Compartir información con otros equipos internos y externos de forma bidireccional para **mejorar las capacidades de detección**.

Las medidas de mitigación dependerán del tipo de ciberincidente, ya que en algunos casos será necesario contar con apoyo de proveedores de servicios, como en el caso de un ataque de denegación de servicio distribuido (DDoS), y en otros ciberincidentes puede suponer incluso el borrado completo de los sistemas afectados y recuperación desde una copia de seguridad.

Autoevaluación

¿Para qué sirve el Triaje de Incidentes?

- ○ Para evaluar toda la información disponible en un momento dado
- ○ Para realizar una clasificación del incidente
- ○ Para priorizar preliminarmente el incidente
- ○ Para todas las cuestiones anteriores

INCORRECTO

Esta es sólo una de las partes del Triaje

INCORRECTO

Esta es sólo una de las partes del Triaje

INCORRECTO

Esta es sólo una de las partes del Triaje

¡ CORRECTO !

Solución

1. Incorrecto
2. Incorrecto
3. Incorrecto
4. Opción correcta

6.- Bibliografía

Bibliografía (pdf - 36635 B)