Curso Fundamentos de Ciberseguridad
Módulo 3
Relator: José Morales Antúnez

¿Qué es la respuesta ante incidentes?
La respuesta ante incidentes es el conjunto de actividades y medidas que se llevan a cabo para abordar y solucionar un incidente de seguridad de la información. La respuesta ante incidentes incluye los siguientes pasos:

1. Detección del incidente: El primer paso en la respuesta ante incidentes es detectar que ha ocurrido un incidente. Esto puede hacerse de varias maneras, como a través de alertas de seguridad, informes de personal o análisis de logs.
2. Evaluación del incidente: Una vez detectado el incidente, es necesario evaluar su impacto y gravedad. Esto incluye determinar la magnitud del incidente y el daño potencial que puede causar.
3. Contención del incidente: El siguiente paso es contener el incidente para evitar que cause más daño. Esto puede incluir desconectar equipos, cortar accesos o tomar otras medidas de contención apropiadas.
4. Investigación del incidente: Es necesario investigar el incidente para determinar su causa y cómo se produjo. Esto puede incluir la revisión de logs, la realización de entrevistas y el análisis de la evidencia.
5. Resolución del incidente: Una vez investigado el incidente, es necesario tomar medidas para solucionarlo y evitar que vuelva a ocurrir. Esto puede incluir la aplicación de parches o actualizaciones de software, la modificación de configuraciones o la implementación de nuevas medidas de seguridad.
6. Comunicación del incidente: Es necesario comunicar el incidente a las personas afectadas y a las autoridades apropiadas. También es importante informar sobre las medidas tomadas para solucionar el incidente y prevenir futuros incidentes.

La respuesta ante incidentes es importante porque permite abordar y solucionar los problemas de seguridad de la información de manera eficiente y minimizar el daño potencial.
Otra definición que podríamos tener de que es una respuesta a incidentes es la siguiente:
La respuesta a incidentes es el proceso de identificar, analizar y responder a un incidente o violación de seguridad cibernética. Implica un conjunto de actividades que están diseñadas para evitar que el incidente se intensifique, minimizar el impacto del incidente y restaurar las operaciones normales lo más rápido posible.

La respuesta a incidentes normalmente sigue un proceso específico, que incluye:

1. Planificación y preparación: desarrollar un plan de respuesta a incidentes y establecer un equipo de respuesta a incidentes para garantizar que la organización esté preparada para responder a incidentes de manera efectiva.
2. Detección y análisis: Identificar y analizar el incidente para determinar su alcance e impacto.
3. Contención, erradicación y recuperación: Tomar medidas para contener el incidente y eliminar la causa, y luego recuperarse del incidente.
4. Actividades posteriores al incidente: realizar una revisión posterior al incidente, actualizar el plan de respuesta al incidente y comunicarse con las partes interesadas.

La respuesta efectiva a incidentes requiere una combinación de experiencia técnica, sólidas habilidades de comunicación y la capacidad de tomar decisiones rápidas e informadas bajo presión. Es una parte esencial de la estrategia de ciberseguridad de cualquier organización.

La importancia de la respuesta a incidentes

La respuesta a incidentes es importante porque ayuda a las organizaciones a proteger sus activos, minimizar el impacto de los incidentes de ciberseguridad y restaurar las operaciones normales lo más rápido posible.

Un incidente o infracción de ciberseguridad puede tener graves consecuencias para una organización, incluidas pérdidas financieras, daños a la reputación y responsabilidades legales. Al responder a los incidentes de manera efectiva, las organizaciones pueden minimizar estos impactos negativos y proteger a sus partes interesadas.

La respuesta efectiva a incidentes también ayuda a las organizaciones a mantener la confianza de los clientes y las partes interesadas, ya que demuestra que la organización está tomando medidas proactivas para protegerse contra las amenazas cibernéticas y puede responder de manera efectiva cuando ocurren incidentes.

Además, la respuesta a incidentes es una parte esencial del cumplimiento de una organización con diversas leyes y reglamentos, como el Reglamento general de protección de datos (GDPR) en la Unión Europea y la Ley de portabilidad y responsabilidad de seguros médicos (HIPAA) en los Estados Unidos.

En general, no se puede exagerar la importancia de la respuesta a incidentes. Es un componente crítico de la estrategia de ciberseguridad de cualquier organización y ayuda a garantizar la seguridad y la resiliencia continuas de la organización.

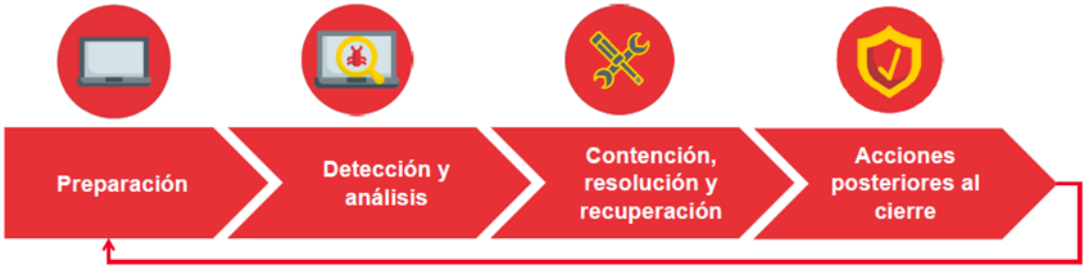
El proceso de respuesta incidentes

El proceso de respuesta a incidentes es un enfoque estructurado para identificar, analizar y responder a un incidente o violación de seguridad cibernética. Por lo general, sigue un conjunto de pasos que están diseñados para evitar que el incidente se intensifique, minimizar el impacto del incidente y restaurar las operaciones normales lo más rápido posible.

Aquí hay un esquema general del proceso de respuesta a incidentes:

1. Planificación y preparación: desarrollar un plan de respuesta a incidentes y establecer un equipo de respuesta a incidentes para garantizar que la organización esté preparada para responder a incidentes de manera efectiva. Esto también puede implicar la capacitación y evaluación del equipo de respuesta a incidentes y otro personal relevante.
2. Detección y análisis: Identificar y analizar el incidente para determinar su impacto. Esto puede implicar la recopilación y el análisis de pruebas, como archivos de registro, tráfico de red y otras fuentes de datos.
3. Contención, erradicación y recuperación: Tomar medidas para contener el incidente y eliminar la causa, y luego recuperarse del incidente. Esto puede implicar la desconexión de los sistemas afectados de la red, la restauración de copias de seguridad y la implementación de otras medidas de reparación.
4. Actividades posteriores al incidente: realizar una revisión posterior al incidente, actualizar el plan de respuesta al incidente y comunicarse con las partes interesadas. Esto puede implicar analizar la causa raíz del incidente e identificar formas de prevenir incidentes similares en el futuro.

El proceso de respuesta a incidentes puede variar según las necesidades y los recursos específicos de la organización, así como la naturaleza y la gravedad del incidente. Es importante contar con un proceso de respuesta a incidentes bien definido y probado para garantizar que la organización esté preparada para responder de manera efectiva a los incidentes.



Un incidente de seguridad va a afectar a uno o más aspectos relacionados de ciberseguridad o de seguridad de la información en este caso hablamos de Confidencialidad, Integridad y Disponibilidad

¿Cómo podrían ocurrir estos incidentes?

Existen muchas causas probables por nombrar algunas:

- Un incendio en el centro de datos o sala de servidores, factor externo que afecta a la Disponibilidad como ejemplo.
- Un ataque de Phishing que contiene un Ransomware, esto afectaría la Integridad en el caso de un usuario y si se propaga a servidor la Disponibilidad de ellos.
- Una acción mal intencionada de un usuario enviando información al exterior, esto afectaría la confidencialidad de la información.
- Existen muchos casos posibles más, pero se nombraron los 3 anteriores como ejemplos.

Fase 1 de Preparación:

- El primer paso consiste en estimar las necesidades para la gestión de incidentes.
- Personal que va a realizar la gestión de incidentes.
- Documentación de los sistemas y redes que se usan en la empresa:
- Definir cuál es la actividad «normal» para permitir detectar actividades sospechosas que sean indicios de incidentes.
- Registrar los contactos de terceras partes. Por ejemplo, si tenemos una web que la mantiene un proveedor, en caso de incidencia hay que tener identificado al responsable en el proveedor.
- Centros de respuesta a incidentes de organismos externos en los que apoyarnos para la gestión de incidentes:
- CERT (de sus siglas en inglés Computer Emergency Response Team) y CSIRT (Computer Security Incident Response Team). Más adelante hablaremos sobre estos centros.

Establecimiento de procedimientos de gestión

- Las buenas prácticas señalan la necesidad de definir una política de gestión de incidentes, así como el procedimiento a seguir en caso de que ocurran.
- También es recomendable tener un catálogo con las incidencias que más probabilidad tengan de suceder o mayor impacto puedan tener en la empresa. De esta forma, se podrán predefinir pautas de actuación en caso de producirse dichas incidencias.

Fase 2 de Detección y Análisis

Los signos de un incidente pueden ser de dos tipos:

Signos indicadores: aquellos que evidencian que un incidente ha sucedido o puede estar ocurriendo, por ejemplo:

- Alertas de sensores de un servidor.
- Una alerta del antivirus.

- La caída de un servidor o sistema.
- Accesos lentos.

Signos precursores: aquellos que tienen capacidad para predecir la probabilidad de que un incidente ocurra en el futuro, por ejemplo:

- La detección de un escáner de puertos.
- El resultado del análisis de vulnerabilidades.
- Las amenazas de ataque por parte de ciberdelincuentes.

Clasificación y priorización de incidentes

Una vez detectado un incidente, hay que clasificarlo. Se pueden usar los siguientes atributos para la tarea de clasificación:

- Tipo de amenaza: código dañino, intrusiones, fraude, etc.
- Origen de la amenaza: interna o externa.
- La categoría de seguridad o criticidad de los sistemas afectados.
- El perfil de los usuarios afectados, su posición en la estructura organizativa de la entidad y, en su consecuencia, sus privilegios de acceso a información sensible o confidencial.
- El número y tipología de los sistemas afectados.

En el caso de manifestarse más de un incidente de forma paralela, el orden de prioridad en el uso, los atributos del incidente, tipo de recursos perjudicados y criticidad de estos definirán el impacto potencial sobre el negocio de la compañía.

Notificación del incidente, el procedimiento de comunicación de incidentes de seguridad está compuesto por las siguientes fases: reportar, notificar y registrar el incidente e iniciar el seguimiento en un evento de gestión En función del tipo de incidente, este se asignará y escalará a las personas convenientes para asegurar su estudio, resolución y cierre.

Fase 3 Contención, Resolución y Recuperación

- Las estrategias de contención de incidentes varían dependiendo del tipo de incidente, así como el posible impacto sobre la empresa.
- En función de la gravedad de los incidentes, podría llegar a ser imprescindible emplear medidas como la deshabilitación de servicios, el apagado de sistemas o la desconexión de estos de la Red. De esta forma, se intentará impedir que el incidente se disperse por la empresa.
- Estas soluciones podrán facilitarse y agilizarse en el caso de haberse definido previamente estrategias y procedimientos para la contención de los diferentes tipos de posibles incidentes.
- Una vez detenido el incidente, habría que valorar la necesidad de suprimir o limpiar elementos asociados al incidente, además de comenzar con el rescate de todos los sistemas afectados. De esta forma, los sistemas intentarán ser devueltos a la situación de operación habitual de la compañía.
- En las actividades de recuperación se realiza la eliminación de los componentes asociados al incidente y otras actividades que se consideren adecuadas de cara a resolver el incidente o prevenir que vuelva a ocurrir en el futuro.

Actividades de resolución:

- Instalación de parches de seguridad.
- Cambios en el cortafuegos (firewall).
- Cambios en las listas de acceso.

Actividades de recuperación:

- Restaurar información desde las copias de seguridad (backups).
- Reemplazar componentes afectados con otros limpios de infección.
- Instalar actualizaciones de software.
- Reforzar la seguridad actualizando las reglas del cortafuegos.

Fase 4 Acciones posteriores al cierre

- El cierre de un incidente de seguridad y el fin de su gestión debe incluir un conjunto de evidencias que acrediten las acciones que se han llevado a cabo, los procesos que se han realizado y todas las personas que han estado involucradas o han sido consultadas para su gestión.
- Se aconseja disponer de un registro común para todos los incidentes. En él se describirán aquellos datos indicados anteriormente. Se incluirá la procedencia y la persona que detecta el incidente, los servicios y los sistemas infectados, fechas/horas más relevantes, responsables de la gestión y acciones tomadas.
- De forma periódica, deben analizarse las acciones tomadas estudiando posibles mejoras o cambios a realizar ante futuros incidentes.
- Además, es recomendable recoger y analizar métricas sobre los tipos y frecuencia de incidentes, impactos (financieros, obligaciones legales, imagen frente a terceros y operativos), métodos de resolución, coste de la resolución de incidentes y acciones correctivas o preventivas.
- De esta forma, si es necesario, se pueden detectar mejoras en los procedimientos de gestión, escalamiento, etc.

Es importante que estos pasos o metodología expuesta no es la única. Existen otras mas detalladas con otras fases y actividades, también dependeré del tamaño de la empresa y servicios asociados o rubro, ya que de ello dependen también normativas o leyes que deba cumplir en este aspecto.

Consejos básicos que aplican a cualquier empresa:

1. Mantener un registro de los incidentes sufridos en tu negocio.
2. Hacer un seguimiento de las acciones realizadas y las personas que hayan intervenido en la gestión del incidente.
3. Mantener un registro de los documentos que sirvan como evidencia de las acciones realizadas para solucionar o cerrar el incidente de seguridad.
4. Mantener esta información como inventario de los incidentes de seguridad sufridos por mi negocio para intentar mejorar la gestión sobre mis activos, implementando medidas que contribuyan a impedir que los incidentes de seguridad se repitan

Conceptos:

Qué es CERT: corresponde por sus siglas en inglés a (Computer Emergency Response Team) o equipo de respuesta a emergencias informáticas es el personal que se encarga de dar respuesta a incidentes de seguridad en tecnologías de la información.

Qué es CSIRT: corresponde por sus siglas en inglés (Computer Security Incident Response Team) y este se traduce como centro de respuesta a incidentes de seguridad.

Ambos tienen la misión de contribuir a la mejora de la ciberseguridad, además de prevenir y gestionar el riesgo de organizaciones y personas, para el caso de Chile se dispone de CSIRT de Gobierno que también mediante guías y comunicados no solo es para entidades de gobierno, sino que también para los ciudadanos.

Lo pueden visitar acá: https://csirt.gob.cl/

¿Qué es la informática Forense Digital?

La informática forense digital es una disciplina que se ocupa de la recopilación, análisis e interpretación de datos digitales de manera forense, es decir, de manera rigurosa y científica, con el objetivo de utilizar esa información como prueba en un proceso judicial. Los profesionales de la informática forense digital, conocidos como peritos forenses digitales, utilizan técnicas y herramientas especializadas para recopilar, analizar y preservar de manera adecuada la evidencia digital en una amplia variedad de casos, como investigaciones criminales, disputas civiles o violaciones de seguridad.

Otra descripción podría ser el análisis forense digital se define como un conjunto de técnicas de recopilación y exhaustivo peritaje de datos, la cual sin modificación alguna podría ser utilizada para responder en algún tipo de incidente en un marco legal. Un incidente es un evento en donde las políticas de seguridad de un sistema se ven corrompidas, siendo entonces el objetivo entender la naturaleza del ataque

Este tipo de técnica está creciendo mucho en los últimos años y normalmente se encuentra relacionada a casos de estudio en donde ocurrió un delito financiero, evasión de impuestos, investigación sobre seguros, acoso o pedofilia, robo de propiedad intelectual, fuga de información y ciberterrorismo o ciberdefensa, entre muchos otros campos.

Etapas generales de informática forense digital

1. Identificación y preservación de la evidencia: Los peritos forenses digitales identifican y recopilan la evidencia digital relevante de manera adecuada para garantizar su integridad y autenticidad. Esto puede incluir el uso de medidas de seguridad para proteger la evidencia de la contaminación o la manipulación.
2. Análisis forense: Los peritos forenses digitales analizan la evidencia digital utilizando herramientas y técnicas especializadas para buscar información relevante y examinarla de manera detallada.
3. Presentación de resultados: Los peritos forenses digitales documentan sus hallazgos y los presentan de manera clara y concisa, utilizando informes y, en algunos casos, testimonio en el tribunal.
4. Mantenimiento de registros: Los peritos forenses digitales deben mantener registros detallados de todo el proceso de informática forense digital, incluyendo todas las actividades realizadas y las decisiones tomadas. Estos registros pueden ser utilizados como prueba en caso de que se cuestione la integridad del proceso.

Fases de la informática forense

Usualmente es divido en cinco fases que nos ayudan a mantener un estudio estructurado, facilitando la verificabilidad, la reproducibilidad del análisis. Profundizaremos estas etapas del análisis forense:

1. Adquisición

En esta fase se obtienen copias de la información que se sospecha que puede estar vinculada con algún incidente. De este modo, hay que evitar modificar cualquier tipo de dato utilizando siempre copias bite a bite con las herramientas y dispositivos adecuados. Cabe aclarar este tipo de copia es imprescindible, debido a que nos dejara recuperar archivos borrados o particiones ocultas, arrojando como resultado una imagen de igual tamaño al disco estudiado.

Rotulando con fecha y hora acompañado del uso horario, las muestras deberán ser aisladas en recipientes que no permitan el deterioro ni el contacto con el medio. En muchos casos, esta etapa

es complementada con el uso de fotografías con el objetivo de plasmar el estado de los equipos y sus componentes electrónicos.
Recomendamos la utilización de guantes, bolsas antiestáticas y jaulas de Faraday para depositar dispositivos que puedan interaccionar con ondas electromagnéticas como son los celulares.
La adquisición de muestras debe respetar una regla fundamental que está ligada a la volatilidad de las muestras, por lo que se deberán recolectar en el orden de la más volátil en primera instancia a la menos, sobre el final. A modo de ejemplo, podríamos indicar que primero deberíamos recolectar datos relevantes a la memoria, contenidos del caché y como último paso recolectar el contenido de documentos o información que esté disponible en el soporte de almacenamiento.
Como ya sabemos las RFC son un conjunto de documentos que sirven de referencia para estandarizaciones, normalizaciones en comunicaciones y tecnología. De esta forma consultando la RFC 3227, podremos relevar con mayor profundidad todo lo que compete a esta etapa.

2. Preservación
En esta etapa se debe garantizar la información recopilada con el fin de que no se destruya o sea transformada. Es decir que nunca debe realizarse un análisis sobre la muestra incautada, sino que deberá ser copiada y sobre la copia se deberá realizar la pericia.
De este modo, aparece el concepto de cadena de custodia, la cual es un acta en donde se registra el lugar, fecha, analista y demás actores que manipularon la muestra.
En muchos casos deberemos utilizar las técnicas de Hashes para identificar de forma unívoca determinados archivos que podrían ser de gran utilidad para la investigación.

3. Análisis
Finalmente, una vez obtenida la información y preservada, se pasa a la parte más compleja. Sin duda, es la fase más técnica, donde se utilizan tanto hardware como softwares específicamente diseñados para el análisis forense. Si bien existen métricas y metodologías que ayudan a estructurar el trabajo de campo, se podrán obtener grandes diferencias dependiendo de las herramientas que se utilicen, las capacidades y experiencia del analista.
Además, es muy importante tener en claro qué es lo que estamos buscando, debido a que esto dará un enfoque más preciso a la hora de ir a buscar pruebas. Sin embargo, el estudio de la línea de tiempo (timeline), logs de accesos y una descarga de la memora RAM será muy útil para la mayoría de las pericias.
Es muy importante en esta instancia la evaluación de criticidad del incidente encontrado y los actores involucrados en él.

4. Documentación
Si bien esta es una etapa final, recomendamos ir documentando todas las acciones, en lo posible, a medida que vayan ocurriendo. Aquí ya debemos tener claro por nuestro análisis qué fue lo sucedido, e intentar poner énfasis en cuestiones críticas y relevantes a la causa. Debemos citar y adjuntar toda la información obtenida, estableciendo una relación lógica entre las pruebas obtenidas y las tareas realizadas, asegurando la repetibilidad de la investigación.

5. Presentación
Normalmente se suelen usar varios modelos para la presentación de esta documentación. Por un lado, se entrega un informe ejecutivo mostrando los rasgos más importantes de forma resumida y ponderando por criticidad en la investigación sin entrar en detalles técnicos. Este informe debe ser muy claro, certero y conciso, dejando afuera cualquier cuestión que genere algún tipo de duda.

Un segundo informe llamado “Informe Técnico” es una exposición que nos detalla en mayor grado y precisión todo el análisis realizado, resaltando técnicas y resultados encontrados, poniendo énfasis en modo de observación y dejando de lado las opiniones.

Guía NIST de respuesta incidentes

NIST 800-61 es una guía de la National Institute of Standards and Technology (NIST) de los Estados Unidos que proporciona recomendaciones sobre cómo llevar a cabo la investigación de incidentes de seguridad cibernética. Esta guía se centra en la recopilación y análisis de evidencia digital, y proporciona un marco general para el proceso de investigación de incidentes de seguridad cibernética, incluyendo la identificación de la evidencia relevante, la preservación de la integridad de la evidencia y la presentación de los resultados de la investigación. NIST 800-61 es una guía ampliamente utilizada y respetada en la industria de la seguridad cibernética y se considera un estándar de facto para la investigación de incidentes de seguridad cibernética.

NIST 800-61 divide el proceso de investigación de incidentes de seguridad cibernética en seis etapas:

- Preparación: Esta etapa incluye la planificación y el establecimiento de un equipo de investigación y la definición de los objetivos y alcances de la investigación.
- Identificación: En esta etapa, se busca determinar si se ha producido un incidente de seguridad cibernética y, de ser así, se identifica el alcance del incidente y se establece un plan de respuesta.
- Contención, erradicación y recuperación: En esta etapa, se toman medidas para contener el incidente y evitar que se propague, se eliminan las causas del incidente y se llevan a cabo las actividades necesarias para recuperar el sistema.
- Análisis: En esta etapa, se recopila y analiza la evidencia para determinar cómo ocurrió el incidente y quién puede ser responsable.
- Presentación de resultados: En esta etapa, se documentan los resultados de la investigación y se presentan de manera clara y concisa a las partes interesadas.
- Mejora: En esta última etapa, se examinan los resultados de la investigación y se toman medidas para evitar incidentes similares en el futuro.

Guía para Análisis Forense Digital

El estándar ISO/IEC 27037:2012 puede ser utilizado en el campo de la ciencia forense de la informática como una guía para la gestión de la seguridad de la información durante la realización de trabajos forenses en ordenadores y otros dispositivos electrónicos. En este contexto, el estándar puede ayudar a garantizar que los trabajos forenses se lleven a cabo de manera eficiente y segura, y que se tomen las medidas necesarias para proteger la integridad de la evidencia digital durante el proceso de investigación. Además, el estándar puede ser utilizado para ayudar a asegurar la conformidad con las regulaciones y los requisitos legales aplicables en materia de gestión de la seguridad de la información y ciencia forense de la informática.

Proporciona pautas para el manejo de la evidencia digital; sistematizando la identificación, recolección, adquisición y preservación de esta; con procesos diseñados para respetar la integridad de la evidencia y con una metodología aceptable para asegurar a su admisibilidad en procesos legales.

De acuerdo con la ISO/IEC 27037:2012 la evidencia digital es gobernada por tres principios fundamentales:

- relevancia,
- confiabilidad y
- suficiencia