Plan de respuesta de incidentes y certificación - 4Geeks Academy

1. Plan de respuesta a Incidentes

En este documento presenta un plan de respuesta ante incidentes para la empresa 4Geeks Academy, usando las cinco funciones del Marco de Ciberseguridad del NIST SP 800-61: Preparación, Identificación, Contención, Erradicación y Actividades Post-Incidente. Con este marco detallado para la organización 4Geeks Academy, proporciona una guía práctica para establecer la respuesta ante incidentes, desde prevenir hasta recuperarlo.

1.1. Preparación

La primera fase es la preparación ante cualquier incidente, estableciendo una política de seguridad, una formación de todos los usuarios en el sistema, concienciarlos para el uso seguro de los sistemas y que puedan responder ante cualquier incidente.

- Definir el criterio de la clasificación de los incidentes.
- Herramientas para la detección de intrusiones.
- Formación básica al personal.
- Inventario actualizado de los servicios, como los “backups”, bases de datos y aplicaciones.

1.2. Identificación

En esta fase se necesita detectar la vulnerabilidad que ha amenazado el sistema y analizarlo dependiendo de la criticidad de la amenaza. Con ello se siguen los siguientes pasos:

1. **Detección:** Identificar el incidente es lo más importante de los pasos, si no se localiza la amenaza o vulnerabilidad ocurrida, no se podrá seguir con los siguientes pasos.

En este paso se pueden usar varias herramientas para analizar el sistema vulnerado.

- Monitorear los logs para identificar si se ha entrado en la máquina.
- Detectar el tráfico de la red para localizar anomalías.

- Reportar la vulnerabilidad a los docentes.

2. **Análisis:** Analizar los indicadores de que el sistema ha sido comprometido.

- Inicios de sesión desde sitios desconocidos.
- Procesos desconocidos del sistema.
- Cambios en la configuración.
- Uso indebido en las credenciales.

3. **Clasificación:** Se clasifica todo lo analizado anteriormente para clasificarlos.

- Tipo de incidente.
- Catalogarlo según lo crítica que es la amenaza.
- El impacto que causaría si aún está expuesta la vulnerabilidad.

1.3. Contención

Gracias al paso anterior se ha podido identificar el incidente y por ello se ejecuta las acciones para su contención, siguiendo según su criticidad e impacto hacia el sistema afectado, es decir, primero lo más crítico y con mayor impacto exponencialmente siguiendo de lo menos crítico y con menor impacto. Se necesita seguir los siguientes pasos:

1. **Contención a corto plazo:** Primeramente se necesita aislar de forma inmediata el sistema comprometido hacia los otros sistemas (si es necesario), bloqueando las cuentas y credenciales sospechosas, y se crea una copia para analizarla forensemente.
2. **Contención a largo plazo:** Después de haber contenido todo el sistema y dejado de lado la transmisión de esta. Se realiza una revisión en el firewall o segmentación de la red, restringiendo los accesos a procesos administrativos y aplicando políticas como el mínimo privilegio para la continuación del curso.

1.4. Erradicación

Una vez contenida la amenaza, se debe proceder a suprimirla desde su punto inicial para evitar la reincidencia de ella o incluso la intensificación de la amenaza. Se debe:

- Suprimir todo tipo de malware, proceso o vulnerabilidad detectada.
- Aplicar parches de seguridad para ayudar a la seguridad del sistema.
- Cambiar todas las credenciales existentes para evitar recaídas.
- Verificar que no existan puertas traseras y que los parches estén bien aplicados.

1.5. Recuperación:

Tras la erradicación del sistema se necesita volver a configurar el sistema con los parches pertinentes para evitar recurrencia de las amenazas pasadas, además de restaurar los sistemas afectados de forma segura y controlada.

- Restaurar los sistemas afectados desde “backups” verificados.
- Volver a configurar el sistema para tenerla limpia con los parches pertinentes.
- Monitoreo constante para posibles amenazas no identificadas.

Con este plan de respuesta ante cualquier incidente puede ayudar a 4Geeks Academy a la mitigación de cualquier incidente e incluso mejorar continuamente el sistema.

2. Plan de respuesta ante el mismo incidente

Para actuar en contra el mismo incidente se necesita crear un plan para contrarrestarlos, por ello con el siguiente plan de respuesta a este incidente se reduce el impacto de este, prever que ocurra el incidente e incluso poder notificarlo a los docentes para mitigar lo antes posible.

1. Identificación

Primero de todo se debe hacer un breve reconocimiento del entorno, los activos afectados y el alcance de este incidente. Los activos que fueron vulnerados de 4Geeks Academy fueron:

- La máquina por la cual entraron y vulneraron el puerto, además de los sistemas almacenados en este sistema tanto la información sensible como archivos de configuración o credenciales.
- Podría haber escalado la amenaza hacia la máquina física, escalando hacia otros sistemas en la red.

2. Protección

El objetivo de esta fase es implementar controles preventivos para reducir la probabilidad de que ocurra el mismo incidente.

- Se debe proteger el acceso del puerto como “root”.
- Implementar un firewall bastante fuerte para evitar direcciones “IP” desconocidas o no autorizadas.
- Aplicar el acceso al mínimo privilegio controlando la escalada de privilegios.
- Administrar respaldos automáticos y verificados para ayudar con la recuperación del sistema.

3. Detección

Con esta fase, se identifica de forma temprana la actividad maliciosa.

- Monitorear constantemente los “logs”, así se puede detectar los accesos, intentos fallidos e incluso las “IPs” desconocidas.
- Usar alertas automáticas.
- Incluso hay que verificar los procesos desconocidos, puertos abiertos no autorizados y usuarios nuevos sospechosos.

4. Respuesta

Se debe contener, analizar y erradicar el incidente de forma controlada.

1. **Contener:** Para contener la amenaza se necesita aislar la máquina a la red, bloquear las “IPs” en un firewall, deshabilitar el servicio “SSH” para corregirlo y usar parches de seguridad, y capturar evidencias para ayudar a mejorar continuamente.

2. **Analizar:** En el análisis se determina cómo se entró en la máquina, acciones realizadas del atacante y que datos han sido modificados o eliminados.
3. **Erradicar:** Eliminar completamente la amenaza con todo lo relacionado al ataque, aplicar parches y reconfigurar los servicios.

5. Recuperación

Se debe restaurar el sistema a uno más seguro y normal para poder seguir la normalidad de las lecciones.

- Restaurar el sistema, verificando que el respaldo esté completamente limpio.
- Reactivar todos los servicios para reanudar la continuidad.
- Documentar lo ocurrido para ayudar a la prevención de esta amenaza.
- Actualizar los procedimientos ante la respuesta de este incidente y la política de seguridad.

3. Mecanismo de protección de datos

Sabiendo que la información es un aspecto fundamental, se garantiza un entorno seguro, eficiente y confiable hacia unas bases para un manejo seguro de la información, permitiendo que se proteja la confianza de la Academia de 4Geeks, para que se mantengan a salvo de accesos no autorizados, amenazas a la academia e incluso la pérdida de datos. Ayudándonos en las siguientes secciones:

1. **Confidencialidad**

Se compromete a que la información esté única y exclusivamente accesible a personas, procesos o sistemas que tengan autorización a ella. Para ello, se establecen unos mecanismos de control de acceso, clasificando la información y concienciando a los usuarios. Adoptando medidas para prevenir el acceso a esta información, como uso de autenticación multifactor o incluso el principio de mínimo privilegio.

2. **Integridad**

Debe mantener la información completa, exactamente como ha sido recibida, protegida ante cualquier modificación o accidente, introduciendo controles de seguridad que permitan la fiabilidad de los datos proporcionados y detectar posibles alteraciones indebidas o pérdida de ellas.

3. **Disponibilidad**

Hay que garantizar a los usuarios que la información y servicios estén disponibles cuando sea necesario, adoptando medidas preventivas para el minimizar las interrupciones y garantizar la continuidad de estos.

3.1. Respaldos periódicos

Los respaldos (backups) son copias seguras de los datos y sistemas que no han sido comprometidas, ayudando así a la recuperación de la información. Con esto debemos tener en cuenta cuatro componentes clave para un buen respaldo:

- **Tipos de respaldo:** Se debe tener en cuenta el tipo de respaldo necesario para tener los mismos datos seguros y realizarlos de forma que el sistema no esté colapsado por mucho tiempo, se divide en: Completo (Copia completamente toda la información), Incremental (Solo afecta cambios desde el último respaldo automático) y Diferencial (Cambios realizados desde el último respaldo completo).
- **Automatización y frecuencia:** Un buen sistema debe estar bien programado para ejecutarse sin ninguna intervención, además deben realizarse de forma según la criticidad de la información.
- **Almacenamiento:** Los respaldos deben estar guardados en ubicaciones seguras y en diferentes sistemas, se puede usar la regla “3-2-1”, esta regla consiste en 3 copias de seguridad, 2 medios diferentes (una copia en la nube y otra física) y 1 copia fuera del sitio.
- **Verificación:** Antes de realizar cualquier restauración, se debe tener en cuenta que el respaldo que se va a utilizar no

está corrupto y está íntegro para poder realizar la restauración.

- **Seguridad y control de acceso:** Se debe tener en cuenta que los respaldos deben estar bien cifrados, con una buena protección para evitar restaurar las máquinas con un respaldo malicioso y que las copias no pueden ser modificadas ni borradas sin autorización.

3.2. Cifrado de datos sensibles

El cifrado es importante porque protege la información frente a accesos no autorizados, incluso si los datos son robados, interceptados o extraviados. Convierte la información legible en datos incomprensibles que sólo pueden interpretarse con una clave de cifrado.

- **Tipos de cifrados:** Se debe proteger los datos sensibles durante su ciclo de vida, clasificándolos en: En reposo (los datos están protegidos y almacenados en discos, servidores o en respaldos), En tránsito (la información está pasando de un remitente a un receptor, por ende se debe proteger mientras se transmite, como el uso de “VPN” o protocolos seguros como “HTTPS”) y En uso (se debe proteger los datos mientras están siendo procesados por el sistema o el ordenador, por ello se usa claves o el uso del cifrado homomórfico).
- **Gestión de claves:** Con el uso de claves, se necesita una rotación de estas para retrasar aún más la vulnerabilidad a estas, como el cambio de claves cada mes y el almacenamiento protegido de estas claves en software o hardware autorizados como KMS (software) o HSM (hardware).
- **Políticas de Acceso:** El cifrado tiene que estar vinculado a la identidad del usuario para evitar accesos no autorizados, garantizando que sólo los usuarios puedan acceder, por ello se usaría el principio de mínimo privilegio (los usuarios solo

tienen acceso a lo necesario) y una autenticación multifactor (sólo se permite el acceso tras una verificación).
- **Cumplimiento normativo:** Se debe cumplir con los estándares permitidos por las leyes o documentadas en políticas de seguridad.

3.3. Implementación de Controles de Acceso

Se limita el acceso a los datos, basándonos en el mínimo privilegio, el usuario solo tiene permitido el uso necesario a los datos en concreto.

- **Autenticación:** Es obligatorio para todos los sistemas críticos, una buena autenticación verificar que realmente eres el que dice ser, por ello se aplica una autenticación multifactor, combinando algo que sabes (la contraseña), con algo que tienes (tarjeta o app de autenticación) y algo que eres (biometría o reconocimiento facial).
- **Revisión periódica:** Se monitorea constantemente los roles y permisos para revocar los permisos de los usuarios, los cambios de rol de ellos o incluso añadir permisos si es necesario.
- **Registro:** Se documenta todas las acciones realizadas como acceso a claves, descifrado de datos y cambios de permisos para ayudar a la revisión periódica de accesos anómalos o no autorizados.
- **Autorización:** Se establecen los permisos claros para cada función o responsabilidades que se establezcan, asignando los permisos mínimos necesarios para poder realizar el trabajo.

4. Organizar la documentación del SGSI

4.1. Alcance

Se crea un inventario sobre todos los activos de la información que son los más relevantes, hacia 4Geeks Academy tanto en los límites físicos, como límites virtuales.

Activos de Información	Importancia
Servidores	Alto
Base de datos	Crítico
Información financiera	Alto
Plataforma web	Medio
Credenciales de usuarios	Medio
Datos de estudiantes y docentes	Alto
Datos y resultados de proyectos	Medio
Copias de seguridad	Alto

En la tabla anterior, se puede divisar los activos de la información con su valor clave en la 4Geeks Academy, clasificados por la importancia de estos dentro de la organización.

4.2. Análisis de riesgos

Se evalúa los activos que se puede encontrar en la 4Geeks Academy, además de sus vulnerabilidades, la probabilidad de que la amenaza suceda y su impacto hacia la organización, y por último la priorización de ciertas amenazas, tanto el tiempo de respuesta como al tiempo requerido para mitigarla.

- Se crea un inventario de la información para saber los activos necesarios a asegurar, haciendo una lista de los archivos que nos encontramos en la organización, dividiéndola en cuatro diferentes tipos de activos:

Inventarios de activos	
Activos hardware	Servidores físicos, equipos conectados a la red, copias de seguridad y sitios de trabajo

Activos software	Plataforma web, sistemas de autenticación, almacenamiento en la nube y recursos humanos
Activos de Información	Datos personales de los estudiantes y del personal, información financiera, datos de los proyectos
Activos Personales	Los docentes y estudiantes, el equipo de ciberseguridad, colaboradores externos y personal de administración

Riesgo	Probabilidad	Impacto
Pérdida de datos	Alta	Daño a la reputación y compromiso de datos sensibles
Acceso no autorizado	Media	Daño reputacional y pérdida financiera
Indisponibilidad de servicios	Media	Interrupción de las actividades
Malware / ransomware	Media	Pérdida de datos y costes elevados de recuperación
Uso indebido de privilegios	Alta	Manipulación de información
Incumplimiento normativo	Media	Pérdida financiera

Sistemas no actualizados	Media	Acceso no autorizado y compromiso de datos

Con estos activos identificados, se ha analizado los riesgos con la probabilidad de ocurrencia y el impacto que se sufriría si ocurriesen los siguientes.

4.3. Políticas y procedimientos de seguridad

Se establecen las bases del Sistema de Gestión de Seguridad de la Información (SGSI) definiendo los principios, compromisos y directrices generales que rigen la seguridad de la información, asegurando que los activos de la información estén protegidos y gestionados por buenas prácticas de seguridad.
Con los principios de la seguridad de la información mencionados anteriormente, se necesita un buen uso hacia los activos de la información asegurando la Confidencialidad, Integridad y la Disponibilidad, siguiendo los siguientes pasos:

1. Control de Acceso de Usuarios

Fundamental para garantizar la protección de la información y de los sistemas, con estos controles los usuarios autorizados accedan a la información necesaria para el desempeño de sus funciones. Para ello se necesitará seguir los siguientes cuatro pasos.

1. **Concesión y modificación de accesos**

Cada usuario tendrá los permisos imprescindibles para su desarrollo académico como su asignación en diferentes tareas. Cada acceso estará vinculado a la identidad del usuario, dejándolo responsable por pérdidas o modificación a estas y incentivando el cuidado del material.

- La concesión de permisos se realizará de forma controlada y documentada.
- Los permisos concedidos se revisarán siempre cuando se produzcan cambios en las funciones, responsabilidades o dependiendo de la situación de cada usuario.

- Supervisión periódica garantiza los privilegios y permisos adecuados al usuario, minimizando errores, pérdida de datos y sistemas no actualizados.
- Con los pasos anteriores, se añadirá una revocación de accesos de manera inmediata cuando se produzcan cesiones o destituciones, cambios de funciones, incumplimiento de las normas establecidas y las bajas temporales.

2. **Mínimo privilegio y autenticación**

En toda organización se necesita un buen sistema de autenticación, para asegurar una segunda capa de seguridad, por el cual la autenticación podría ser por un mensaje SMS o incluso un código en una app de autorización.

- Agregar un método de autenticación para prevenir acceso a personas sin credenciales, confirmando que verdaderamente es la persona que ha intentado acceder al sistema.
- Con el factor anterior, debemos aplicarle un sistema de mínimo privilegio, incorporando otra capa de seguridad más, con este sistema

3. **Control y cumplimiento**

Sin revisión diaria de accesos o de los sistemas, el cumplimiento de las normas anteriores no funcionan, ya que si necesitan actualización, si el sistema tiene fallas o incluso si el sistema está obsoleto y necesita un reemplazo, con las revisiones periódicas lo solucionan. El cumplimiento de las normas es igual de importante que la revisión, por ello si nadie respeta las normas vigentes, conlleva a casos desastrosos, como multas económicas, pérdida de prestigio y el filtrado de datos de los estudiantes y docentes.

2. Plan de Respuesta a Incidentes

Este plan de respuesta de seguridad es la misma que los anteriores respuestas, aunque este estará más enfocado en la información crítica de la empresa, con este plan reduce el riesgo de forma exponencial, además de restablecer las amenazas o vulnerabilidades ocurridas lo antes posible. Se deben seguir los siguientes pasos:

1. **Prever**

La primera defensa hacia cualquier incidente es la prevención, reduce en gran cantidad los ataques hacia cualquier organización.

- Identificar de forma concurrente las amenazas que pueden llegar a afectar al sistema, pudiendo aprender de sus fallos y apoyar para que no vuelva a ocurrir el mismo incidente.
- Para prevenir cualquier incidente, lo mejor es la concienciación y la formación de los usuarios en la red, importando más si el puesto tiene mayor privilegio.

2. **Informar**

En cualquier plan de respuesta, se necesita una rapidez ante cualquier sospecha o detección de ella, comunicando el incidente lo antes posible para identificarlo y transmitirlo a los compañeros para poder mitigar la amenaza. Tiene dos fases:

- **Comunicación:** De forma controlada describe el incidente, identificando los sistemas o datos afectados, el impacto del incidente y las medidas o las acciones requeridas para la mitigación de la amenaza.
- **Información:** Transmite el reporte de la amenaza a todos los afectados como clientes o proveedores, informando a los directores o al personal de la Seguridad de la Información (TI) y a las autoridades por si la amenaza escala.

3. **Responder**

Es el procedimiento que se necesita para resolver el incidente, analizando la información, coordinando los equipos y contestando de manera definitiva la brecha de seguridad detectada.

- **Coordinación:** Convoca a todos los equipos para la ayudar a responder a esa amenaza, asignando los roles y respecto a esto la neutralizan.
- **Análisis:** Hacen un diagnóstico rápido de la situación, identificando el tipo de ataque, el alcance inicial, el impacto de ella y prioriza según lo crítica que es la amenaza entre otras.

4. **Mitigar**

Frenan el daño del ataque realizado, intentando reducirlo de manera que el impacto sea el mínimo. Siguiendo los siguientes pasos:

- **Contención:** Lo primero, aíslan los sistemas afectados para que no se extiendan por los sistemas no afectados, bloqueando cuentas, desconectando servicios y suspendiendo procesos. Mientras se clasifican por criticidad, como de corto plazo o de largo plazo.
- **Mitigación:** Eliminan completamente todo tipo de amenaza, corrigiendo configuraciones, actualizando los sistemas, renovando credenciales y eliminando todo rastro de accesos no autorizados.

5. **Aprendizaje**

Aprender de los errores ayuda mucho a retroalimentar, capacitando aún más al personal, mejorar los sistemas técnicos, apoyando a futuras amenazas iguales, corrigiendo comunicaciones innecesarias y evaluar la efectividad de la detección de la brecha del sistema.

- **Mejora:** Tras el análisis de la brecha, se puede llegar a aprender a fortalecer la información digital, suavizando los riesgos futuros y refinando los firewalls o antivirus instalados.
- **Documentación:** Registra de forma contundente todo lo pasado para ayudar a la detección, coordinar mejor la comunicación, la asignación de roles, ajustando mejor el plan de incidentes y mejorar la mitigación hacia amenazas pasadas o incluso a evaluar mejor la criticidad de las amenazas.

5. Conclusión

Este documento está elaborado para garantizar la protección adecuada de la información gestionada para la organización 4Geeks Academy, definiendo de manera estructurada las políticas, procedimientos, los planes de respuestas a todas las amenazas y para la amenaza ocurrida, las evaluaciones de seguridad y los controles de seguridad.

Con todo esto se aborda una seguridad de la información y una protección a los sistemas por el cual apoya y refuerza para reducir la probabilidad de ocurrencia del mismo incidente anteriormente indicado y además de minimizar los impactos de las demás vulnerabilidades.