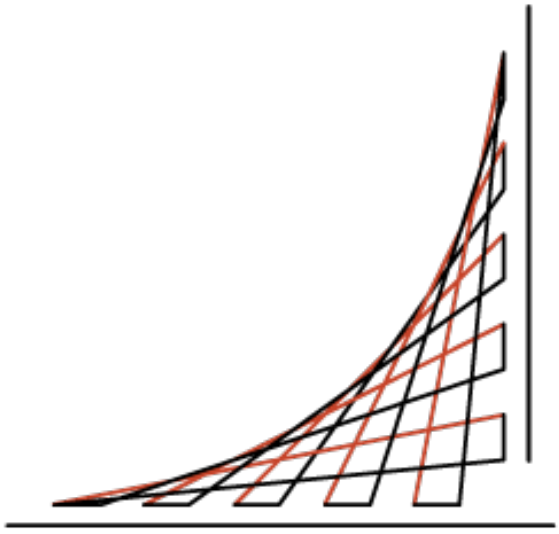

Gestión de Incidentes y Forensia Digital

ECI-CSIRT

Plan de Respuesta a Incidentes de Seguridad Informática

Profesor:
Gerson David Quintero Rodríguez

Autores:

Angie Daniela Ruiz Alfonso

Jorge Enrique Rodríguez Valderrama

Contents

1 Motivación

En los últimos años el concepto de Tecnología de la Información y Comunicación (TIC) ha tomado fuerza, este se refiere al conjunto de recursos, herramientas, equipos informáticos, aplicaciones, redes y medios que permiten la compilación, el procesamiento, almacenamiento, trasmisión de información como voz, datos, texto, video e imágenes.[1]

Como resultado de este acelerado avance los Incidentes de Seguridad Informática han aumentado considerablemente, por lo cual se generan riesgos para las organizaciones, que al materializarse impactan la triada de la CID y, no obstante, ocasionan pérdidas económicas y operacionales.

Es allí donde toma un papel importante y beneficioso el Plan de Respuesta a Incidentes de Seguridad Informática, que hace referencia a una guía de aplicación de medidas estratégicas en caso de que ocurra un Incidente de Seguridad Informática, con el fin de minimizar la gravedad del impacto.

En este documento ECI-CSIRT especificará los procedimientos a utilizar para detectar y responder al acceso no autorizado, o la divulgación de información privada de los Sistemas utilizados, tomando como referencia la guía para el manejo de Incidentes de Seguridad (SP-800-61) del National Institute of Standars Technology (NIST), la cual consiste en siete etapas para brindar un manejo adecuado de Incidentes de Seguridad Informática.

2 Definiciones

- **Incidente de Seguridad Informática:** Cualquier evento que amenace la Confidencialidad, Integridad y Disponibilidad de la Información dentro de una organización.

- **Tríada de la CID:** La tríada de la Confidencialidad, Integridad y Disponibilidad, es un modelo diseñado para guiar las políticas de Seguridad de la Información dentro de una organización.

- **Seguridad Informática:** Es la práctica de proteger los recursos, herramientas, equipos informáticos, aplicaciones, redes y Sistemas electrónicos, de ataques maliciosos.

- **CSIRT:** Es el Equipo de expertos responsables de dar Respuesta ante Emergencias Informáticas.

- **Logs:** Son el Registro secuencial de todos los eventos de cada Sistema, los cuales se usan para detectar y analizar los errores y problemas relativos a eventos de red y de Sistemas, como lo son los Incidentes de Seguridad, las actividades irregulares o los problemas operacionales, por ende se constituyen como una evidencia del comportamiento de cada Sistema.

- **Administradores de Sistemas:** Es la persona responsable de implementar, configurar, mantener, monitorizar, documentar y asegurar el correcto funcionamiento de un Sistema Informático, o algún aspecto de este.

- **Hosts:** También conocidos como anfitriones, se refieren a las computadoras u otros dispositivos conectados a una red que proveen y utilizan servicios de ella.

- **Malware:** Es un programa (Software) malintencionado, el cual realiza acciones dañinas en un Sistema Informático de forma intencionada y sin el conocimiento del usuario.

- **Pruebas de Penetración:** Más conocidas como "pen testing", son una práctica para poner a prueba un Sistema Informático, red o aplicación web para encontrar vulnerabilidades que un atacante podría explotar.

3 Grupo de Respuesta a Incidentes

3.1 Información de Contacto

- **CIO:** Gerson David Quintero Rodríguez, Ingeniero de Sistemas, Magíster en Seguridad Informática, gerson.quintero@escuelaing.edu.co, CIO.

- **Comandante de Respuesta a Incidentes:** Angie Daniela Ruiz Alfonso, Ingeniera de Sistemas, angie.ruiz@mail.escuelaing.edu.co, Comandante IR, Gerente CSIRT.

- **Gerente de Infraestructura:** Jorge Enrique Rodríguez Valderrama, Ingeniero de Sistemas, jorge.rodriguez-v@mail.escuelaing.edu.co, Gerente IR.

- **Gerente de Comunicaciones:** ... Pertenece al Equipo de manejo de Incidentes de Seguridad Informática.

- **Gerente de Riesgo:** ... Pertenece al equipo de manejo de Incidentes de Seguridad Informática.

- **Representante Legal:** ... Pertenece al Equipo de manejo de Incidentes de Seguridad Informática.

- **Representante de Recursos Humanos:** ... Pertenece al Equipo de manejo de Incidentes de Seguridad Informática.

- **Proveedores:** ...

- **Contactos Técnicos:** ...

3.2 Roles y Responsabilidades

- **Equipo de manejo de Incidentes de Seguridad Informática:**

  Consta de expertos legales, gerentes de riesgo, comunicaciones e infraestructura, los cuales pueden ser consultados o notificados durante la Respuesta a Incidentes, los cuales son responsables de las comunicaciones internas y externas relacionadas con Incidentes de Seguridad Informática, brindan asesoramiento sobre las actividades de Respuesta a Incidentes relacionadas con sus campos, aseguran que las actividades de Respuesta a incidentes estén de acuerdo con los requisitos legales, contractuales y reglamentarios, y participan en las pruebas del plan y procedimientos de Respuesta a Incidentes.

- **CIO (Director de Información):**

  Debe coordinar las actividades de Respuesta con los departamentos auxiliares y los recursos externos según sea necesario para minimizar el daño a los recursos de información, proporcionar al equipo de gestión de Incidentes y a otras partes interesadas actualizaciones sobre las actividades de Respuesta durante el Incidente, asegurarse de tener acuerdos con los proveedores de servicios y las políticas relacionadas con la gestión de Incidentes, definidos de forma clara y precisa, orientados siempre hacia el cumplimiento y reflejo de las expectativas y objetivos de la organización.

  Puede aprobar el cierre de Incidentes de gravedad moderada o crítica, pero debe trabajar con el Comandante IR para evaluar periódicamente la efectividad del Plan y CSIRT, para asegurarse de que las lecciones aprendidas se apliquen, y los gerentes de CSIRT tengan la autoridad necesaria para incautar activos y detener los servicios rápidamente para contener un Incidente de gravedad moderada o crítica.

- **CSIRT/Equipo de Respuesta a Incidentes de Seguridad Informática:**

  - **Comandante de Respuesta a Incidentes:**

    El Gerente de Respuesta a Incidentes supervisa y determina la prioridad de las acciones durante la detección, el análisis y la contención del Incidente, y es el responsable de transmitir los requisitos especiales de los Incidentes de alta gravedad al resto de la organización, así como de comunicar el impacto potencial al CIO y de comprender los acuerdos de nivel de servicio vigentes con terceros y el papel que estos pueden desempeñar en escenarios de Respuesta específicos.

  - **Miembros del Equipo de Respuesta a Incidentes:**

    El Gerente de Respuesta a Incidentes cuenta con el apoyo de un equipo de técnicos que trabajan directamente con los sistemas de información afectados para investigar la hora, la ubicación y los detalles del incidente. Los miembros del equipo suelen estar compuestos por expertos en la materia (PYME), personal de Tecnología de la Información de alto nivel, terceros, expertos forenses externos o socios de seguridad.

    • Deben asegurar que las herramientas estén configuradas y administradas correctamente para alertar sobre Incidentes o eventos de Seguridad, además de conocer los acuerdos a nivel de servicio con los proveedores de servicios.

    • Deben comprender los Planes y Procedimientos de Respuesta a Incidentes para responder adecuadamente, al igual que desarrollar continuamente habilidades de gestión de Respuesta a Incidentes y participar en las pruebas del Plan y los Procedimientos de Respuesta a Incidentes.

• Deben ayudar en la Repuesta a incidentes según se solicite, teniendo en cuenta que las responsabilidades del CSIRT tienen prioridad sobre las funciones normales, recopilan información relevante sobre incidentes según lo solicite el comandante de IR, asegurándose de que la recolección de pruebas, la cadena de custodia y la preservación sean las adecuadas.

• Deben analizar el tráfico de la red en busca de señales de denegación de servicio, denegación de servicio distribuida u otros ataques externos, revisar los archivos de registro de los sistemas críticos para detectar actividad inusual, al igual que supervisar las aplicaciones y los servicios empresariales para detectar signos de ataque.

• Si es necesario, deben consultar con personal de Seguridad de la Información calificado para obtener asesoramiento.

4 Etapas de un Incidente de Seguridad Informática

La Respuesta a Incidentes de Seguridad Informática tiene como objetivo un enfoque dirigido a la detección de un Incidente, al igual que a su mitigación y su recuperación. Para lograr este objetivo, el modelo propuesto para la gestión de Incidentes de Seguridad de la información involucra las siguientes etapas de manera cíclica como lo muestra la figura 1 :

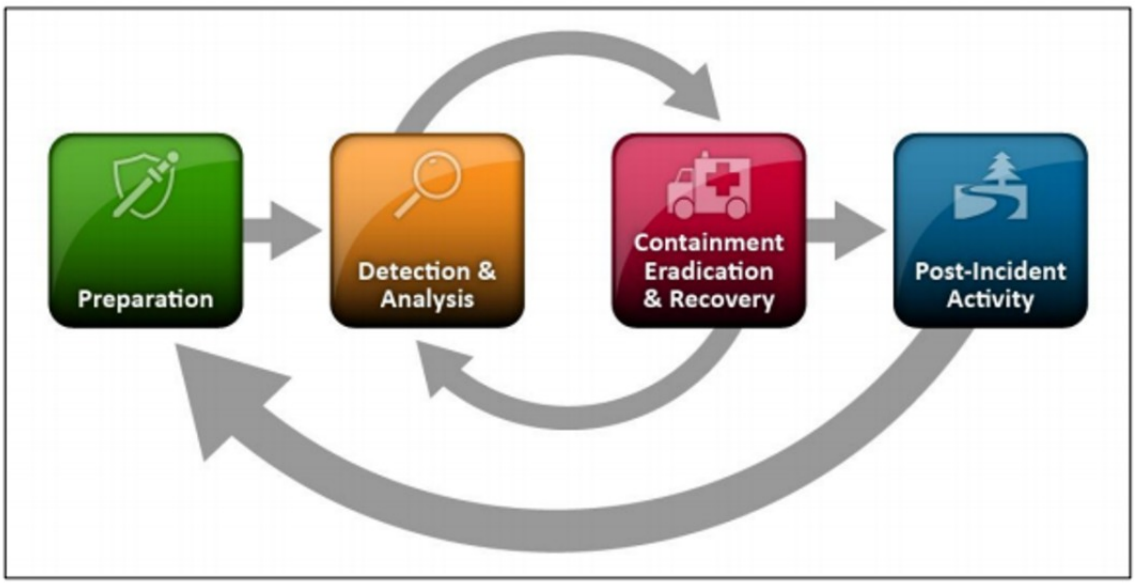

Figure 1: Etapas de Respuesta a Incidentes NIST

Para definir las actividades de este Plan de Respuesta a Incidentes de Seguridad Informática se incorporan componentes definidos por el NIST, los cuales están diseñados para detectar a tiempo, evaluar, gestionar las vulnerabilidades y eventos que vulneren la Seguridad de la Información, los equipos tecnológicos y las aplicaciones en general.

4.1 Preparación

Se debe tener conformado un equipo con los conocimientos y experiencia necesarios para dar Respuesta a los Incidentes de Seguridad Informática, con el fin de definir a quién se debe acudir y por cuál medio se debe reportar cualquier Incidente dentro de la organización, además se debe tener un plan claro y preciso que detalle de manera secuencial los pasos a seguir en caso de materialización de un Incidente, contar con el Hardware y Software necesario para el análisis de los Incidentes y la documentación de toda la infraestructura tecnológica de la organización.

4.2 Detección

Se deben identificar el o los Incidentes, teniendo en cuenta los vectores de ataque, los indicadores que pueden ser señales de un Incidente de Seguridad Informática y los compartimientos que son o no "normales" dentro de la organización.

4.3 Análisis

El equipo debe de la manera más rápida analizar y validar cada Incidente, con el fin de priorizarlos dada su criticidad y relevancia, lo cual influye drásticamente en la toma de decisiones oportunas, las cuales tienen en cuenta la probabilidad de ocurrencia, el impacto y la recuperabilidad de la organización ante el Incidente.

En la figura 2 podemos evidenciar que el impacto funcional y la probabilidad de la materialización del Incidente en la organización se mide en: Ninguno (blanco), Bajo (verde), Medio (amarillo) y Alto (rojo). Priorizando así la atención de los riesgos ALTOS que necesitan mitigación por medio de planes correctivos debido a su fuerte impacto, luego se tienen en cuenta los riesgos MEDIOS que necesitan planes de prevención y por último se atienden los riesgos BAJOS que necesitan de constante monitoreo para su detección.

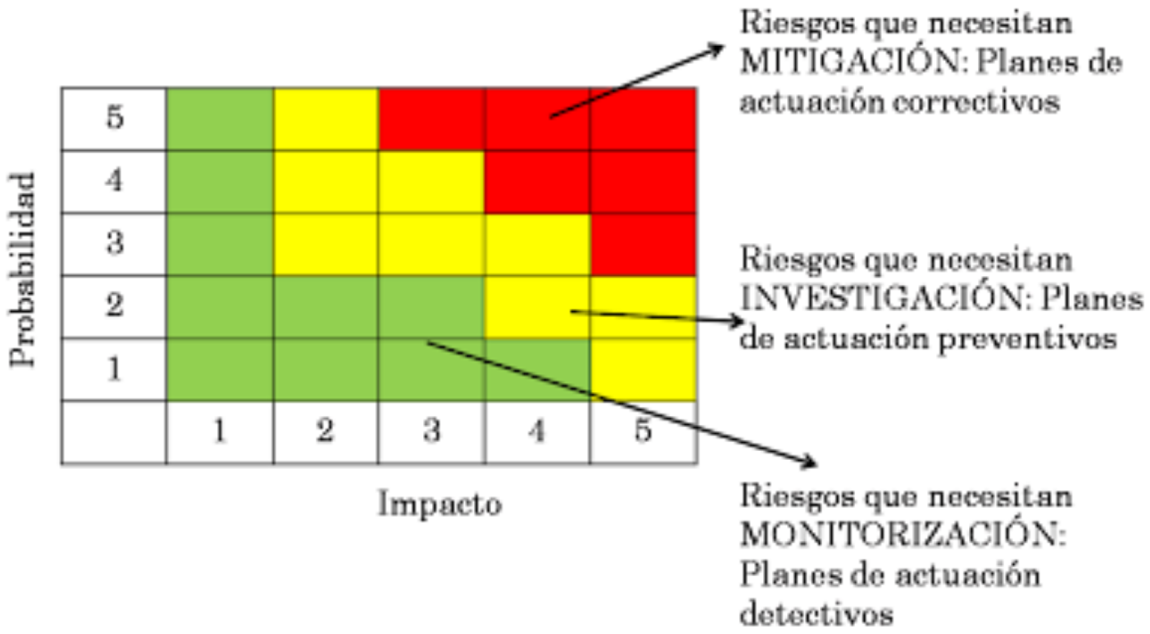

Figure 2: Matriz de Riesgos Informáticos

Es de gran utilidad tener una política de retención de Logs por un tiempo específico debido a que muchas veces los Incidentes de Seguridad Informática se detectan un tiempo después de su materialización o para poder correlacionar eventos usando los Logs de varios Sistemas, al igual que tener sincronizados los relojes de los Sistemas para evitar mayores dificultades durante el análisis y recolectar posibles datos adicionales en el tráfico de red.

4.4 Contención

Las estrategias de contención varían según el tipo de Incidente y se deben tener establecidas por separado, con sus respectivos criterios y documentos, los cuales deben

ser claros para la toma de decisiones oportunas, pero en todo caso se deben mantener las evidencias intactas, para evitar y prevenir un daño mayor.

4.5 Erradicación

Se deben identificar todos los Hosts afectados dentro de la organización para poder ser enmendados, ya sea eliminando malware, usuarios maliciosos o que han sido vulnerados, realizando pruebas de penetración, etc. Esto quiere decir que luego de la contención se debe erradicar el Incidente de Seguridad Informática, aunque hay casos donde puede realizarse en la siguiente etapa.

4.6 Recuperación

Los Administradores de Sistemas se encargan de restaurar su operación normal, verificando que todo funcione de manera correcta y si se puede, remedian las vulnerabilidades con el fin de prevenir algún otro Incidente.

4.7 Actividad Posterior al Incidente

Esta etapa final es la que se conoce como aprender y mejorar, debido a que el equipo ve como se desempeñó, que se debe y no repetir, el tiempo utilizado, el manejo de las evidencias, la evolución tanto en conocimientos de nuevas amenazas como en nuevas tecnologías, las lecciones aprendidas, logrando así mejorar las medidas de Seguridad en la organización y todo el proceso de Respuesta a Incidentes de Seguridad Informática, con el fin de prevenir que se materialice nuevamente otro Incidente similar. Por ende, se recomienda documentar lo siguiente:

Preparar un Informe de Seguimiento del Incidente que incluya:

- Una estimación económica del impacto.
- Las medidas adoptadas durante el incidente.
- Las medidas de seguimiento necesarias para eliminar o mitigar la vulnerabilidad.
- Las políticas o procedimientos que requieren actualización.
- Las medidas adoptadas para reducir al mínimo las pérdidas o la exposición negativa.
- El registro cronológico y los registros de auditorías de sistemas que existan.

Es fundamental trabajar con las Autoridades Locales, si el incidente fue causado por agentes externos. O en caso contrario, trabajar con la Administración para determinar las medidas disciplinarias necesarias, si el incidente se generó internamente.

5 Casos de Uso

5.1 Detección

INCIDENTES	EVENTOS
Acceso no Autorizado	Múltiples intentos fallidos de Login, Compromiso del usuario administrador, Acceso a Información por personas no autorizadas, Asignación y control de roles.
Código Malicioso	Uso de disposivos de almacenamiento, Acceso a páginas inseguras, Vulnerabilidades a nivel de red que faciliten la propagación, Phishing.
Ataque por Vulnerabilidades	Aplicaciones o software desactualizadas
Denegación del Servicio	SYN Flood.
Divulgación de la Información	Vulnerabilidades en aplicaciones y servidores.
Intento de Intrusión	Software que proporciona acceso y control remoto.
Actividad de Reconocimiento	Sondas, Escaneo de puertos, Mapeo de recursos.

5.2 Análisis

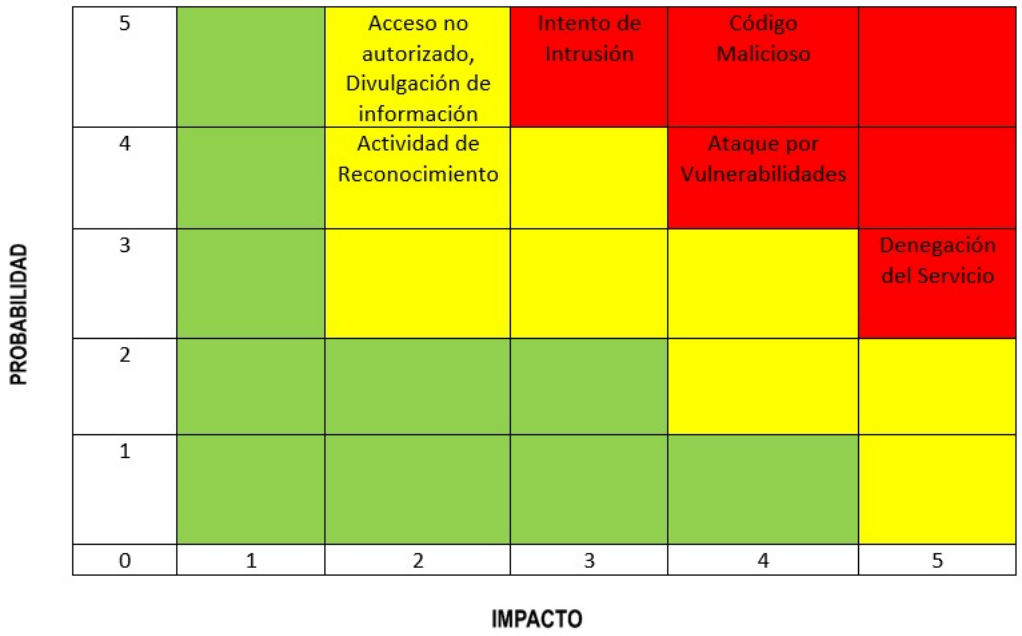

Figure 3: Priorización de los Incidentes

5.3 Contención

INCIDENTES	ESTRATEGIA
Acceso no Autorizado	Bloqueo de la cuenta, Despido del funcionario, Apagado de la máquina.
Código Malicioso	Bloqueo de puertos, Desconexión de la red de los equipos afectados, Actualización de herramientas y softwares de detección, Monitoreo y control del tráfico de red.
Ataque por Vulnerabilidades	Actualización de Aplicaciones o software, Realizar respaldos de la información.
Denegación del Servicio	Detectar y bloquear el origen del ataque, Reconfigurar routers para minimizar el efecto.
Divulgación de la Información	Restringir el acceso a carpetas compartidas, Deshabilitar sistemas de almacenamiento portátil, Bloqueo de URLs o correos electrónicos,
Intento de Intrusión	Software que proporciona acceso y control remoto.
Actividad de Reconocimiento	Bloqueo de puertos,

5.4 Erradicación y Recuperación

INCIDENTES	ESTRATEGIA
Acceso no Autorizado	Restauración de equipos y servicios, Recuperación de los Datos, Restauración de Backups.
Malware	Corrección de Efectos, Restauración de Backups, Actualización de Antivirus.
Ataque por Vulnerabilidades	Actualización de Aplicaciones o software, Restauración de Backups.
Denegación del Servicio	Restitución del servicio caido, Restauración de Backups.
Intento de Intrusión	Restauración de equipos y servicios, Recuperación de los Datos, Restauración de Backups.

5.5 Actividad Posterior al Incidente

Realizar el Informe de Seguimiento del Incidente y seguir las recomendaciones dadas en cada Incidente.

6 References

[1] C. de la República, *Ley 1341 del 2009*, http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html#:~:text=de%20la%20competencia.-,6.,7., Artículo 6.