Aplicación del CSF del NIST

Anteriormente en este programa, aprendiste sobre los usos y beneficios del Marco de Ciberseguridad (CSF) del Instituto Nacional de Estándares y Tecnología (NIST). Hay cinco funciones básicas del marco CSF del NIST: identificar, proteger, detectar, responder y recuperar.

Imagen: 5 funciones básicas del CSF del NIST

Estas funciones ayudan a las organizaciones a gestionar los riesgos de ciberseguridad, implementar estrategias de gestión de riesgos y aprender de errores anteriores. Los planes basados en este marco deben actualizarse continuamente para estar siempre un paso por delante de las últimas amenazas de seguridad. Las funciones básicas ayudan a garantizar que las organizaciones estén protegidas contra posibles amenazas, riesgos y vulnerabilidades. Cada función se puede utilizar para mejorar la seguridad de una organización:

- **Identificar:** administrar los riesgos de seguridad a través de auditorías periódicas de redes internas, sistemas, dispositivos y privilegios de acceso para reconocer posibles brechas de seguridad o fugas de datos.
- **Proteger**: desarrollar una estrategia para resguardar los activos internos a través de la implementación de políticas, procedimientos, capacitación y herramientas que ayuden a mitigar las amenazas de ciberseguridad.
- **Detectar**: analizar posibles incidentes de seguridad y mejorar las capacidades de monitoreo para así aumentar la velocidad y la eficiencia de las detecciones.

- **Responder**: garantizar que se utilizan los procedimientos adecuados para contener, neutralizar y analizar los incidentes de seguridad e implementar mejoras en el proceso de seguridad.
- **Recuperar**: restablecer los sistemas afectados a su funcionamiento normal y restaurar los datos y activos de los sistemas que se han visto afectados por un incidente.

Algunas posibles preguntas sobre cada una de las cinco funciones principales incluyen:

Identificar	Crea un inventario de los sistemas, procesos, activos, datos, personas y capacidades de la organización que deben protegerse: ● Tecnología/Gestión de activos: ¿Qué dispositivos de hardware, sistemas operativos y software se vieron afectados? Rastrea el flujo del ataque a través de la red interna. ● Procesos/Entorno comercial: ¿Qué procesos comerciales se vieron afectados en el ataque? ● Personas: ¿Quién necesita acceso a los sistemas afectados?
Proteger	Desarrolla e implementa salvaguardas para proteger los elementos identificados y garantizar la prestación de servicios: ● Control de acceso: ¿Quién necesita acceso a los elementos afectados? ¿Cómo se bloquea el acceso a fuentes no confiables? ● Conocimiento/Capacitación: ¿Quién debe enterarse de la existencia de este ataque y cómo se puede evitar que vuelva a suceder? ● Seguridad de los datos: ¿Hay algún dato afectado que deba protegerse mejor? ● Procedimientos y protección de la información: ¿Es necesario actualizar o agregar algún procedimiento para proteger los activos de datos? ● Mantenimiento: ¿Es necesario actualizar alguno de los componentes hardware, sistemas operativos o software afectados? ● Tecnología de protección: ¿Hay alguna tecnología de protección, por ejemplo un cortafuegos (firewall) o un sistema de prevención de intrusiones (IDS), que deba implementarse para la protección frente futuros ataques?

Detectar	Diseña e implementa un sistema con las herramientas necesarias para detectar amenazas y ataques: ● Anomalías y eventos: ¿Qué herramientas podrían utilizarse para detectar y alertar al personal de seguridad de TI sobre anomalías y eventos de seguridad, por ejemplo, una herramienta del sistema de gestión de eventos e información de seguridad (SIEM)? ● Monitoreo continuo de seguridad: ¿Qué herramientas o procesos de TI se necesitan para monitorear la red en busca de eventos de seguridad? ● Proceso de detección: ¿Qué herramientas (por ejemplo, un IDS) se necesitan para detectar eventos de seguridad?
Responder	Diseña planes de acción para responder a amenazas y ataques: ● Planificación de la respuesta: ¿Qué planes de acción deben implementarse para responder a ataques similares en el futuro? ● Comunicaciones: ¿Cómo se comunicarán los procedimientos de respuesta ante eventos de seguridad dentro de la organización y con las personas directamente afectadas por el ataque, incluidos/as los/las usuarios/as finales y el personal de TI? ● Análisis: ¿Qué pasos de análisis se deben seguir en respuesta a un ataque similar? ● Mitigación: ¿Qué pasos de respuesta, como desconectar o aislar los recursos afectados, podrían usarse para mitigar el impacto de un ataque? ● Mejoras: ¿Qué mejoras se necesitan para optimizar los procedimientos de respuesta en el futuro?
Recuperar	Construye un plan e implementa el marco para recuperar y restaurar los sistemas o datos afectados: ● Planificación de la recuperación: ¿Cómo se restaurarán los recursos después de un ataque? ● Mejoras: ¿Es necesario realizar alguna mejora en los sistemas o procesos de recuperación actuales? ● Comunicaciones: ¿Cómo se comunicarán los procedimientos de restauración dentro de la organización y con las personas directamente afectadas por el ataque, incluidos/as los/las

	usuarios/as finales y el personal de TI?

El CSF del NIST y sus cinco funciones principales proporcionan un marco de planificación proactivo para aplicar medidas reactivas a las amenazas de ciberseguridad. Estas funciones son esenciales para garantizar que una organización tenga estrategias de seguridad efectivas. Una organización debe tener la capacidad de recuperarse rápidamente de cualquier daño causado por un incidente para minimizar su nivel de riesgo.