aplicación del NIST CSF

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

Image: 5 core functions of the NIST CSF

Estas funciones centrales 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 mantenerse a la vanguardia de las últimas amenazas a la seguridad. Las funciones principales 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: gestionar los riesgos de seguridad mediante auditorías periódicas de redes internas, sistemas, dispositivos y privilegios de acceso para identificar posibles brechas en la seguridad.

Proteger: Desarrollar una estrategia para proteger los activos internos mediante la implementación de políticas, procedimientos, capacitación y herramientas que ayuden a mitigar las amenazas de ciberseguridad.

Detectar: busque posibles incidentes de seguridad y mejore las capacidades de monitoreo para aumentar la velocidad y la eficiencia de las detecciones.

Responder: Garantizar que se utilizan los procedimientos adecuados para contener, neutralizar y analizar incidentes de seguridad e implementar mejoras en el proceso de seguridad.

Recuperar: devolver 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 preguntas que se deben hacer para cada una de las cinco funciones principales incluyen:

Identify	Cree un inventario de sistemas, procesos, activos, datos, personas y capacidades organizacionales que deben protegerse: Tecnología/Gestión de activos: ¿Qué dispositivos de hardware, sistemas operativos y software se vieron afectados? Rastree el flujo del ataque a través de la red interna. Proceso/Entorno empresarial: ¿Qué procesos empresariales se vieron afectados por el ataque? Personas: ¿Quién necesita acceso a los sistemas afectados?

Protect	• Desarrollar e implementar 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 de fuentes no confiables? • Concientización/Capacitación: ¿Quién debe ser consciente de este ataque y cómo evitar que vuelva a ocurrir? • Seguridad de los datos: ¿Hay algún dato afectado que deba protegerse más? • Protección de la información y procedimientos: ¿Es necesario actualizar o agregar algún procedimiento para proteger los activos de datos? • Mantenimiento: ¿Es necesario actualizar alguno de los hardware, sistemas operativos o software afectados? • Tecnología de protección: ¿Existe alguna tecnología de protección, como un firewall o un sistema de prevención de intrusiones (IPS), que deba implementarse para proteger contra futuros ataques? •
Detect	• Diseñar e implementar un sistema con las herramientas necesarias para la detección de amenazas y ataques: • Anomalías y eventos: ¿Qué herramientas podrían usarse para detectar y alertar al personal de seguridad de TI sobre anomalías y eventos de seguridad, como 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 se necesitan para detectar eventos de seguridad, como un IDS?

Respond	• Diseñar planes de acción para responder a amenazas y ataques: • Planificación de respuesta: ¿Qué planes de acción deben implementarse para responder a ataques similares en el futuro? • Comunicaciones: ¿Cómo se comunicarán los procedimientos de respuesta a eventos de seguridad dentro de la organización y con aquellos directamente afectados por el ataque, incluidos los usuarios finales y el personal de TI? • Análisis: ¿Qué pasos de análisis se deben seguir en respuesta a un ataque similar? • Mitigación: ¿Qué medidas de respuesta podrían utilizarse para mitigar el impacto de un ataque, como desconectar o aislar los recursos afectados? • Mejoras: ¿Qué mejoras se necesitan para mejorar los procedimientos de respuesta en el futuro?
Recover	• Construir un plan e implementar el marco para recuperar y restaurar los sistemas y/o datos afectados: • Planificación de 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 aquellos directamente afectados por el ataque, incluidos los usuarios finales y el personal de TI?

El NIST CSF y sus cinco funciones principales proporcionan un marco de planificación proactiva para aplicar medidas reactivas a las amenazas a la ciberseguridad. Estas funciones son esenciales para garantizar que una organización cuente con 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