**Aplicación del CSF del NIST**

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 CSF del NIST: identificar, proteger, detectar, responder y recuperar.



*Imagen: 5 funciones principales del NIST CSF*

Estas funciones básicas ayudan a las organizaciones a gestionar los riesgos de ciberseguridad, implementar estrategias de gestión de riesgos y aprender de los errores anteriores. Los planes basados en este marco deben actualizarse continuamente para adelantarse a las últimas amenazas de 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:** Gestione los riesgos de seguridad a través de 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 a través de la implementación de políticas, procedimientos, capacitación y herramientas que ayuden a mitigar las amenazas de ciberseguridad.
* **Detectar**: Escanee en busca de posibles incidentes de seguridad y mejore las capacidades de supervisión para aumentar la velocidad y la eficiencia de las detecciones.
* **Responder**: Asegurar que se utilicen los procedimientos adecuados para contener, neutralizar y analizar los incidentes de seguridad e implementar mejoras en el proceso de seguridad.
* **Recuperar**: Devolver los sistemas afectados al funcionamiento normal y restaurar los datos y activos de los sistemas que se han visto afectados por un incidente.

Estas son algunas de las preguntas que se pueden hacer para cada una de las cinco funciones principales:

|  |  |
| --- | --- |
| Identificar | Cree 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? 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 acceder a los sistemas afectados? |
| Proteger | Desarrollar e implementar salvaguardas para proteger los artículos identificados y garantizar la prestación de servicios:   * Control de acceso: ¿Quién necesita acceder a los elementos afectados? ¿Cómo se bloquea el acceso a las fuentes que no son de confianza? * Concienciación/formación: ¿Quién debe ser consciente de este ataque y cómo evitar que vuelva a ocurrir? * Seguridad de los datos: ¿Hay algún dato afectado que deba ser más seguro? * Protección de la información y procedimientos: ¿Es necesario actualizar o agregar algún procedimiento para proteger los activos de datos? * Mantenimiento: ¿Es necesario actualizar el hardware, los sistemas operativos o el software afectados? * Tecnología de protección: ¿Existen tecnologías de protección, como un firewall o un sistema de prevención de intrusiones (IDS), que deban implementarse para protegerse contra futuros ataques? |
| Detectar | Diseñar e implementar un sistema con las herramientas necesarias para la detección de amenazas y ataques:   * Anomalías y eventos: ¿Qué herramientas se podrían utilizar para detectar y alertar al personal de seguridad de TI de anomalías y eventos de seguridad, como una herramienta de 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? |
| Responder | Diseñar 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 a eventos de seguridad dentro de la organización y con las personas directamente afectadas 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 pasos de respuesta se podrían usar para mitigar el impacto de un ataque, como la desconexión o el aislamiento de los recursos afectados? * Mejoras: ¿Qué mejoras se necesitan para mejorar los procedimientos de respuesta en el futuro? |
| Recuperar | Construir un plan e implementar el marco para recuperar y restaurar los sistemas y/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 los usuarios finales y el personal de TI? |

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