**NIST Cybersecurity framework (CSF)**

El **CSF** es un marco voluntario que consta de Estándares, directrices y mejores prácticas para gestionar el riesgo de ciberseguridad. Este framework es ampliamente respetado y esencial para mantener la seguridad independientemente de la organización para la que trabaje. El CSF consta de cinco importantes funciones básicas, Identificar, Proteger, Detectar, Responder y Recuperar

Imagínese que una mañana recibe una notificación de alto riesgo de que una estación de trabajo ha sido comprometida. Identifica la estación de trabajo, y descubre que hay un dispositivo desconocido conectado a ella. Bloquea el dispositivo desconocido de forma remota para detener cualquier amenaza potencial y proteger a la organización. A continuación, elimina la estación de trabajo infectada para evitar la propagación del daño y utiliza herramientas para detectar cualquier comportamiento adicional del Agente de amenaza e identificar el dispositivo desconocido. Responde investigando el incidente para determinar quién utilizó el dispositivo desconocido, cómo se produjo la amenaza, qué se vio afectado y dónde se originó el ataque. En este caso, descubre que un empleado estaba cargando su teléfono infectado utilizando un puerto USB de su portátil de trabajo. Por último, hace todo lo posible para recuperar cualquier archivo o dato que se viera afectado y corregir cualquier daño que la amenaza causara a la propia estación de trabajo.

Como demuestra el ejemplo anterior, las funciones centrales del NIST (CSF) proporcionan orientación específica y dirección para los profesionales de la seguridad. Este marco se utiliza para desarrollar planes para manejar un incidente de forma adecuada y rápida para disminuir el riesgo, proteger a una organización contra una amenaza, y mitigar cualquier vulnerabilidad potencial. El NIST (CSF) también se expande a la protección de el gobierno federal de los Estados Unidos con la publicación especial del NIST, o SP 800-53. Proporciona un marco unificado para proteger la seguridad de los sistemas de Información dentro del gobierno federal, incluyendo los sistemas proporcionados por empresas privadas para uso del gobierno federal.

El CSF del NIST se centra en cinco funciones principales: identificar, proteger, detectar, responder y recuperar.

Estas funciones principales ayudan a las organizaciones a gestionar los riesgos de ciberseguridad, implementar estrategias de gestión de riesgos y aprender de los errores anteriores. Básicamente, cuando se trata de operaciones de Seguridad, las funciones del CSF del NIST son clave para garantizar que una organización esté protegida contra posibles amenazas, riesgos y vulnerabilidades.

* La primera función principal es **identificar**, que está relacionada con la gestión del riesgo de ciberseguridad y su efecto en las personas y los activos de una organización. Por ejemplo, como analista de seguridad, es posible que se le pida que supervise los sistemas y dispositivos de la red interna de su organización para identificar posibles problemas de seguridad.
* La segunda función principal es **proteger**, que es la estrategia que se utiliza para proteger a una organización mediante la implementación de políticas, procedimientos, capacitación y herramientas que ayudan a mitigar las amenazas de ciberseguridad. Por ejemplo, como analista de Seguridad, usted y su equipo pueden encontrarse con amenazas y ataques nuevos y desconocidos. Por esta razón, es esencial estudiar los datos históricos y realizar mejoras en las políticas y los procedimientos.
* La tercera función principal es **detectar**, lo que significa identificar posibles incidentes de Seguridad y mejorar las capacidades de monitoreo para aumentar la velocidad y la eficiencia de las detecciones. Por ejemplo, como analista, es posible que se le pida que revise la configuración de una nueva herramienta de seguridad para asegurarse de que marca un riesgo bajo, medio o alto y, a continuación, que avise al equipo de seguridad sobre cualquier posible amenaza o incidente.
* La cuarta función es **responder**, lo que significa asegurarse de que se utilizan los procedimientos adecuados para contener, neutralizar y analizar los incidentes de seguridad e implementar mejoras en el proceso de seguridad. Como analista, podrías trabajar con un equipo para recopilar y organizar datos para documentar un incidente y sugerir mejoras en los procesos para evitar que el incidente vuelva a ocurrir.
* La quinta función principal es la **recuperación**, que es el proceso de devolver los sistemas afectados a su funcionamiento normal. Por ejemplo, como analista de seguridad de nivel básico, puede trabajar con su equipo de seguridad para restaurar los sistemas, los datos y los activos, como los archivos financieros o legales, que se han visto afectados por un incidente, como una infracción.