UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Monografía del Seminario de NIST CSF

ASESOR:

Ariana Maybee Orué Medina

AUTORES:

Oviedo Piérola, Miguel Angel (0000-0002-4093-9931)

GRUPO: 03

ESCUELA ACADÉMICO-PROFESIONAL:

INGENIERÍA EN SISTEMAS

CICLO VI

CALLAO, DICIEMBRE 2023

UNIVERSIDAD CÉSAR VALLEJO

Índice:

I. Introducción	**4**
II. Resumen Día 1	**5**
III. Resumen Dia 2	**8**
IV. Resumen Día 3	**10**
VI. REFERENCIAS	**15**

Índice Figuras:

Figura 01. Arquitectura del marco de trabajo de ciberseguridad del NIST..... 4
Figura 02. Funciones NIST CSF..... 5
Figura 03. Riesgo e implementación en la Organización con el Framework NIST CSF....7
Figura 04. Pasos NIST CSF e ISO/IEC 27001.....9
Figura 05. Severidad de Riesgos..... 12

I. Introducción

La ciberseguridad, se ocupa de la protección de los activos digitales, desde las redes al hardware y la información que es procesada, almacenada o transportada a través los sistemas de información interconectados.

Los documentos del cual nos dio a conocer el profesor en el seminario corresponden a presentaciones sobre el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST). El Marco de Ciberseguridad del NIST (conocido también por sus siglas en inglés CSF) es una guía para mejorar la ciberseguridad y la resiliencia de las infraestructuras críticas.

El propósito de este seminario fue explicar en profundidad el CSF, incluyendo sus antecedentes, los componentes que lo conforman, recomendaciones para su implementación paso a paso en una organización, la importancia de la evaluación de riesgos, el uso de perfiles, los niveles de aplicabilidad y la gestión del ciclo de vida de este framework dentro de las organizaciones con el objetivo de evaluar problemas de seguridad y trabajar con los riesgos que traerán a la organización, enfocándose también en trabajar con otros marcos o controles como el Control CIS que trabaja con NIST a un nivel más técnico que de procesos, complementandose con sus categorías y subcategorías, por lo que a continuación se dará los resumenes de estos días conferencianles que ayudó a comprender el framework NIST, sus iguales o similares marcos de trabajo y sus complementos para implementarlo de manera efectiva .

Figura 01. *Arquitectura del marco de trabajo de ciberseguridad del NIST*

Fuente: *OEA*

II. Resumen Día 1

En el primer día el ingeniero en ciberseguridad nos empezó a explicar la definición de conceptos centrales en el ámbito de la ciberseguridad, incluyendo activos, amenazas, vulnerabilidades e impacto. Un activo hace referencia a cualquier elemento que tiene valor para una organización, como información, sistemas, infraestructura, personal y reputación. Una amenaza es un actor o acción con el potencial de dañar o comprometer los activos. Las vulnerabilidades son debilidades que pueden ser explotadas por las amenazas. Finalmente, el impacto se enfoca en las consecuencias que un incidente de seguridad puede ocasionar a una organización.

Luego, explicó que cubre buenas prácticas y estándares relevantes en el ámbito de la ciberseguridad, haciendo énfasis en la norma ISO 27032 de Ciberseguridad y el ya mencionado Marco de Ciberseguridad del NIST. La norma ISO 27032 proporciona orientación para fortalecer la seguridad de internet y diseñar sistemas de información más seguros.

Figura 02. *Funciones NIST CSF*

Fuente: *Barret (2018).*

Seguidamente, se presentan los componentes centrales del NIST CSF. Este framework está conformado por 5 Funciones (Identificar, Proteger, Detectar, Responder y Recuperar), 23 Categorías y 108 Subcategorías. Las funciones agrupan resultados de alto nivel en ciberseguridad. Por ejemplo, la función Identificar reúne la comprensión organizacional sobre manejo de activos, entorno de amenazas y gestión de riesgos. Las categorías son los objetivos estratégicos en seguridad. Algunos ejemplos de categorías son protección de datos, respuesta a

incidentes, concienciación y capacitación. Finalmente, las subcategorías presentan resultados técnicos y de gestión específicos que apoyan cada categoría.

Un aspecto relevante que estuvo bueno en el seminario es que el CSF permite establecer Perfiles que ayudan a alinear las actividades de ciberseguridad con las prioridades y necesidades del negocio, a la vez que proporcionan una medición de progreso y oportunidades de mejora. Adicionalmente, el CSF incorpora Niveles de Implementación (Parcial, Informal, Formal, Adaptativo, Líder) que facilitan establecer una línea base y una ruta de mejora.

Otro punto cubierto es la conexión entre los riesgos organizacionales y los riesgos de ciberseguridad. Por ejemplo, una interrupción de las operaciones comerciales debido a un ataque de denegación de servicio representa una manifestación de una amenaza informática con consecuencias en los procesos de negocio. Este análisis conjunto permite demostrar el impacto tangible que los fallos de ciberseguridad pueden representar para cualquier organización, facilitando la obtención de recursos y apoyo al más alto nivel.

Finalmente, en el primer día se dieron explicaciones y representaciones gráficas de cada uno de los Niveles de Implementación del NIST CSF. Como se mencionó, estos niveles permiten determinar la situación actual de ciberseguridad y trazar una ruta de mejora sistemática. Los niveles son los siguientes:
- Parcial: Enfoque reactivo, con participación irregular de la gerencia. No se aplica en toda la institución.
- Informal: Se comunican prácticas pero no están estandarizadas ni institucionalizadas.
- Formal: Hay políticas y procesos estandarizados documentados y aprobados por la gerencia.
- Adaptativo: Se utiliza monitoreo en tiempo real, análisis de riesgo dinámico y mejora continua.
- Líder: La gerencia provee recursos para alcanzar el estado del arte en ciberseguridad, con mejoras proactivas.

Figura 03. *Riesgo e implementación en la Organización con el Framework NIST CSF*

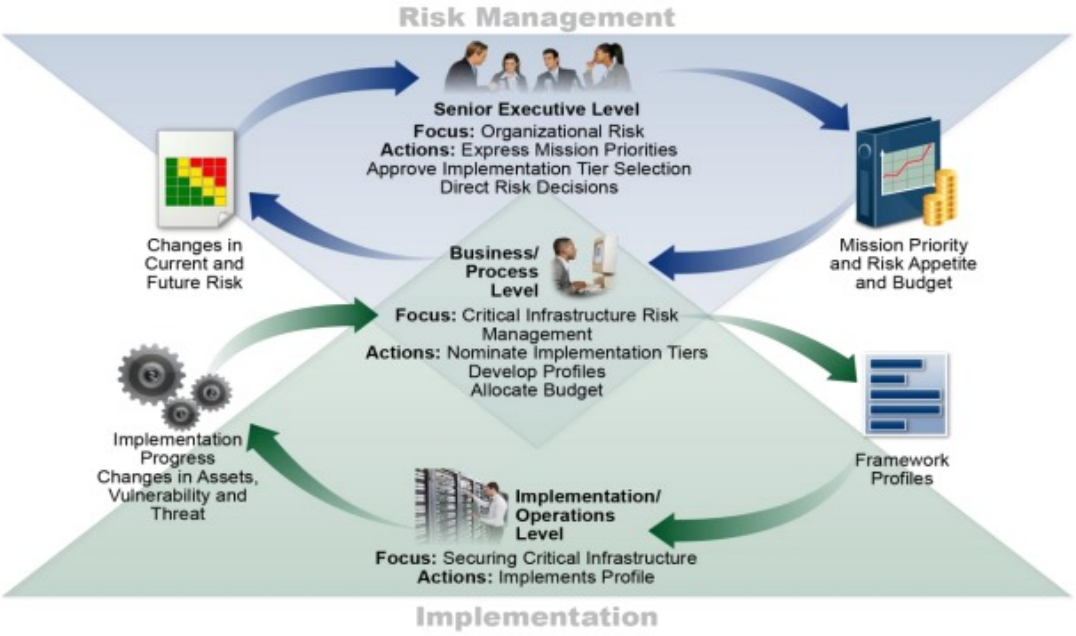


Figure 2: Notional Information and Decision Flows within an Organization

Fuente: *Barret (2018).*

Finalmente se habla de cómo afecta y se implementa el Framework NIST CSF dentro de una organización, como se adentra en las áreas de esta y su manejo desde un nivel de operación, de procesos y de nivel ejecutivo, brindándonos un gráfico claro que complementa esta explicación, donde podemos ver como es el flujo de trabajo del NIST dentro de la organización y cómo cada área o nivel de esta trabaja con él y la información que provee a nivel de procesos.

III. Resumen Dia 2

El segundo día de presentaciones inicia el ingeniero explicando cómo implementar el Marco de Ciberseguridad del NIST en una organización, siguiendo una serie de pasos recomendados. Se enfatiza en que el CSF es lo suficientemente flexible para adaptarse a los distintos entornos operativos y necesidades de diferentes unidades de negocio incluso dentro de una misma compañía, además de ello se resalta que se adapta también al ISO/IEC 27001, dónde esté puede ser usado junto al NIST para su implementación dentro de una organización saldando sus similitudes y diferencias dentro de los marcos. Veamos cada uno de los pasos:

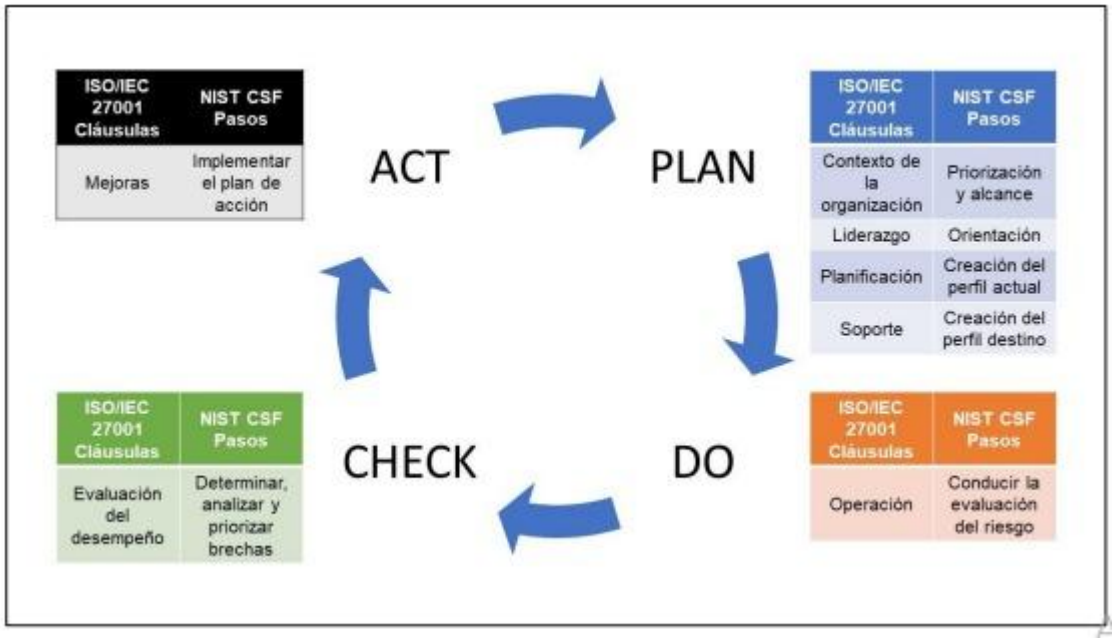
Paso 1 - Priorización y Alcance:
Consiste en que la organización identifique sus objetivos estratégicos y las prioridades de alto nivel para el negocio o misión. Con esta información, la dirección puede tomar decisiones respecto a qué inversiones en ciberseguridad realizar, a la vez que define el alcance de los sistemas y activos que soportan los procesos seleccionados como críticos.

Por ejemplo, en una institución financiera probablemente un área clave sea la banca en línea, con procesos como transacciones electrónicas, autenticación de clientes, monitoreo de fraudes y servicio al cliente. Así mismo, los activos de información vitales pueden incluir plataformas transaccionales, bases de datos centralizadas, sistemas de correlación de eventos y herramientas de soporte técnico.

Paso 2 – Orientar:
Una vez definido el alcance, la organización identifica todos los sistemas, activo primario y de apoyo, tecnologías y recursos humanos relacionados con ese foco establecido para la ciberseguridad. Adicionalmente, se determinan los requisitos legales, regulatorios y contractuales relevantes para ese dominio. Finalmente, se establecen las amenazas y vulnerabilidades críticas de ese ambiente operativo. Esto permite orientar las siguientes actividades en torno a necesidades y riesgos específicos. Por ejemplo, en caso de que un hacker lance un ataque al sistema, responderá los controles de defensa mitigando o evitando a la información, tras ello se va a recopilar la información del ataque para un futuro realizar un parche contra esta vulnerabilidad y teniendo en cuenta que este cambio no afecte el rendimiento del sistema. Sin estos preparativos, cabe decir que el personal técnico no sabrá cómo actuar antes, durante y después del hecho.

Paso 3 - Crear un Perfil Actual:
En este paso la organización desarrolla un perfil de ciberseguridad de línea base, describiendo el grado de cumplimiento existente para cada una de las Funciones, Categorías y Subcategorías que establece el NIST CSF en su núcleo.

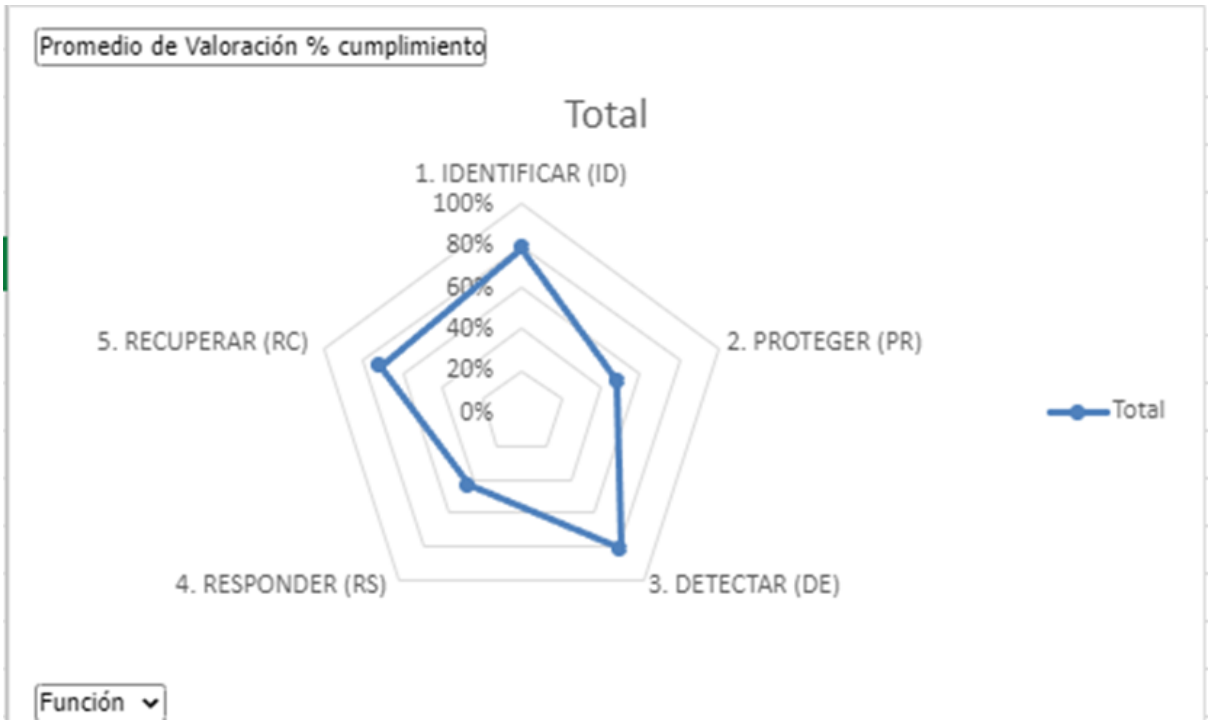
Figura 04. *Pasos NIST CSF e ISO/IEC 27001*



Fuente: *Cabezas Juárez (2020).*

Esto crea una fotografía de las capacidades instaladas actualmente, identificando fortalezas y debilidades de la situación de partida. Ayuda a evitar suposiciones erróneas respecto a las salvaguardas implementadas contra amenazas detectadas previamente. Representa una valoración inicial fundamental para la planificación y medición de progreso posterior. Del cual, es necesario usar referencias como el CIS o COBIT para realizar un proceso que nos permite completar el núcleo de marco de trabajo, cada uno de estos tienen sus criterios y ventajas pero se recomienda aplicar ambos para tener una mejor perspectiva, por ejemplo se nos plantean una lista de vanguardia, que permite diferenciar el tipo de empresa segun su experiencia TI, denominado perfil el cual va ser un requisito para cada vanguardia limitando a las empresas los controles que van a tener, dentro de este tambien esta el tipo de activo como dispositivos y la funcion ya antes mencionada, tras desarrollar nos permitra completar nuestro nucleo de marco de trabajo.

Figura 5. Gráfico Radial – NIST CSF



Fuente: Gutiérrez (2019)

En la anterior figura, Muestra el resultado de aplicar estas dos referencias, el cual se puede entender las características que posee el software, el cual se puede dar que en caso se de un ataque, es altamente posible detectar, pero con una posibilidad de proteger del 35%, alto porcentaje de recuperación y entre sus otras funciones el identificar al atacante y como responde.

IV. Resumen Día 3

En el dia 3 el ingeniero habló sobre el seguimiento de los pasos que se implementan para el NIST CSF en el cual se quedó en el Paso 4 del Marco de Ciberseguridad NIST el cual implica realizar una evaluación exhaustiva de riesgos considerando tanto la probabilidad de que ocurran incidentes de seguridad como su impacto potencial en los objetivos y operaciones de negocio de la organización.

La evaluación puede utilizar la metodología general de gestión de riesgos ya existente en la compañía o construirse sobre análisis previos de amenazas. El objetivo es obtener una comprensión profunda de los escenarios específicos de riesgo cibernético aplicables al contexto único de la empresa.

Para estimar la probabilidad se estudian factores como:

- Vulnerabilidades preexistentes en sistemas de TI, apps web y otros activos digitales que pueden ser explotadas.

- Capacidad y motivación de amenazas internas y externas identificadas.

- Efectividad de controles de seguridad actuales e identificación de brechas significativas.

- Incidentes de seguridad previamente materializados y causas raíz.

En relación al impacto potencial se analiza:

- Información, sistemas y procesos críticos que se verían afectados ante un incidente.

- Pérdidas financieras directas e indirectas como multas regulatorias, daños reputacionales, etc.

- Gravedad de interrupciones en operaciones de negocio y provisión de servicios.

- Aspectos legales y de cumplimiento normativo según la industria.

Idealmente la probabilidad e impacto deben categorizarse cuantitativamente mediante data histórica y modelación de escenarios. De no ser viable, se emplea una valoración cualitativa con apoyo de expertos internos y externos.

Se dio una representación estructurada de los factores de riesgo analizados, sus interrelaciones y cómo en conjunto impactan el perfil general de riesgo cibernético que enfrenta la organización.

Paso 5 - Perfil Objetivo

Una vez comprendidos los requerimientos de seguridad impuestos por factores como la estrategia de negocio, obligaciones regulatorias y los resultados de la evaluación de amenazas y riesgos; el siguiente paso es establecer un Perfil Objetivo dentro del Marco de Seguridad.

Este Perfil representa el estado deseado a futuro de madurez en ciberseguridad para los sistemas de información y procesos de negocio críticos, permitiendo satisfacer las prioridades estratégicas, requerimientos normativos y tolerancia al riesgo definidos por la alta dirección.

Para construir este Perfil Objetivo, se realiza una selección de los resultados y referencias específicas dentro de cada categoría y subcategoría del Núcleo del Marco NIST que aplican al contexto particular de la organización y sus objetivos de seguridad trazados para el mediano plazo de 1-2 años.

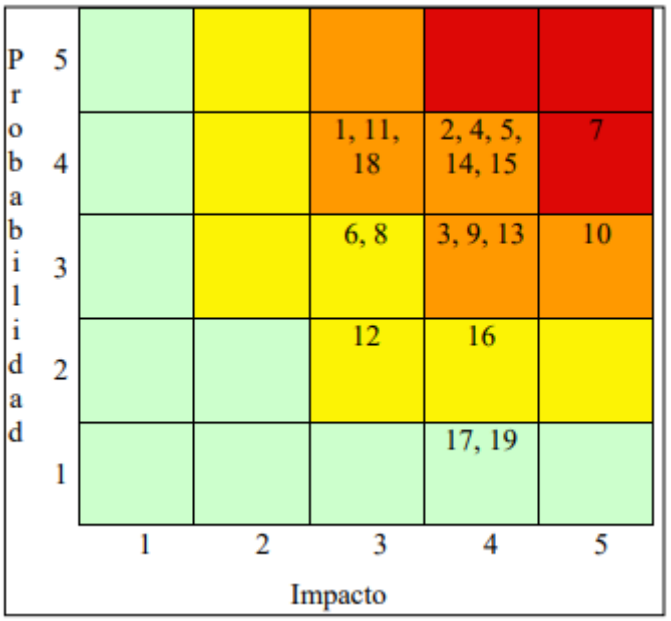
Su adopción debe ser medida de forma continua a través de indicadores clave para monitorear su efectiva implementación. Este Perfil Objetivo constituye una hoja de ruta para guiar iniciativas de inversión en seguridad de información por los próximos años.

Paso 6 - Análisis de Gaps

Contando con un panorama del estado actual (Perfil Actual) y el estado objetivo deseado de madurez en ciberseguridad (Perfil Objetivo), se identifican y analizan en detalle las diferencias o gaps existentes entre ambos perfiles. Cada brecha se examina considerando el contexto específico de la organización.

Luego las brechas individuales se agrupan y priorizan de acuerdo a su criticidad e impacto potencial, dependencias entre controles, factibilidad de implementación, alineación estratégica; para construir una hoja de ruta que defina el camino de iniciativas para alcanzar el estado futuro deseado.

Figura 06. *Severidad de Riesgos.*



Fuente: *Mendoza & Vega (2019).*

V. Conclusiones

Las conclusiones que se tuvieron serán divididas sobre los días abarcados por la ponencia (Seminario de Ciberseguridad):

Dia 1:

El primer día de presentaciones finalizó cubriendo sólidamente los fundamentos del Marco de Ciberseguridad del NIST, incluyendo su estructura con Funciones, Categorías y Subcategorías, la posibilidad de establecer Perfiles, los distintos Niveles de Implementación, ejemplos de conexión entre los riesgos de negocio y de ciberseguridad, así como ejemplos específicos de cada Nivel de Implementación del Framework.

El documento permite tener claridad sobre el lenguaje común que provee el NIST CSF para abordar la ciberseguridad desde múltiples disciplinas, funciones, pasos, facilitando así la comunicación con los altos directivos de cualquier organización.

Dia 2:

La presentación del segundo día se centró en recomendaciones prácticas para ejecutar la implementación del NIST CSF dentro de cualquier organización, siguiendo los pasos de la priorización, el enfoque en el contexto específico de la organización, y determinación de la línea base de seguridad informática.

Esto permite sentar las bases para la mejora sistemática al clarificar el estado actual de los procesos, los procesos más relevantes para el negocio o misión, los sistemas críticos que los apoyan y los riesgos cibernéticos asociados a estos mismos. Sobre este diagnóstico se pueden planear medidas técnicas, operacionales y de gestión para reducir algunas brechas y madurar el nivel de ciberseguridad dentro de la organización y dentro del margen ejecutivo.

Dia 3:

En el último día, el ingeniero nos habla de la implementación efectiva del Marco de Ciberseguridad de NIST, el cual les permite a las organizaciones reducir su exposición a riesgos en el ciberespacio de forma medible, sistemática y adaptada a sus prioridades estratégicas, ejecutivas, realidades operativas y limitaciones del presupuesto asignado al área en cuestión.

Seguir los pasos de priorización, evaluación de amenazas, determinación de brechas respecto a un perfil objetivo y ejecución de planes de acción iterativos, posibilita converger sólidamente hacia un estado de ciber-resiliencia sostenido dentro de nuestra organización.

Nos habla que la clave para el éxito es comprender que no se trata de un proyecto temporal sino de un proceso de mejora continua e iterativo con métricas claras, revisión de efectividad periódica y apoyo integral de la alta dirección.

Por último se nos recalca en centrarse en reducir la exposición a incidentes de alto impacto y viabilidad, esto permite usar eficientemente recursos limitados para cerrar las brechas de ciberseguridad más críticas, creando una cultura positiva de gestión de riesgos y cumplimiento proactivo con estándares globales como el ISO 27001.

Y por último la conclusión final:

En conclusión, las presentaciones sobre el Marco de Ciberseguridad del NIST entregan información muy valiosa tanto a nivel estratégico como táctico. A nivel estratégico, resaltan la importancia de vincular la ciberseguridad con la gestión de riesgo organizacional para conseguir patrocinio y recursos desde los altos mandos de esta. También enfatiza la necesidad de orientar la ciberseguridad hacia los procesos de negocio críticos, centrándose en estos más que en la parte técnica.

A nivel táctico, el NIST provee orientación técnica muy sólida para evaluar la postura de ciberseguridad, identificar carencias, establecer una línea base y construir un plan de remediación por etapas. Los perfiles permiten adaptar el Marco a cada contexto del negocio.

En definitiva,la aplicación del Framework NIST CSF permite a una organización diseñar, implementar y mantener un programa de seguridad de la información personalizado, que refuerce sus políticas organizacionales y esté alineado con sus prioridades institucionales centrales.

Comentario:
Este taller nos metió en el mundo del Marco de Ciberseguridad del NIST. Descubrimos la sorprendente flexibilidad de este marco, su habilidad para adaptarse a diversos entornos y su conexión con ISO/IEC 27001. Los pasos prácticos, desde la priorización hasta la creación de perfiles, resultaron ser una guía clara y aplicable para implementar medidas de seguridad de manera efectiva.

Hemos explorado la evaluación de riesgos, también destaca la importancia de comprender la probabilidad e impacto de los incidentes. Esta perspectiva subrayó la complejidad y la necesidad de una comprensión profunda para fortalecer nuestra ciberseguridad. También nos proporcionó herramientas prácticas para construir una postura sólida en ciberseguridad.

Nos llamó la atención la importancia de los perfiles objetivo y actual en el marco NIST. La idea de crear un perfil actual de seguridad y luego establecer un perfil

objetivo para el futuro realmente resuena como un enfoque integral y medible para mejorar la ciberseguridad. Esta conexión estratégica entre el estado actual y el deseado es clave para construir una resiliencia cibernética a largo plazo.

Incluir un caso real donde se haya vulnerado la información de una empresa. (PROPONER CONTROL Y/O SOLUCIÓN).

Caso real:

En noviembre de 2014, Sony Pictures Entertainment, una división de Sony, fue víctima de un ciberataque. Este notable evento tuvo un impacto significativo en la empresa en múltiples niveles.

El grupo detrás del ataque, identificándose como "Guardianes de la Paz", orquestó una operación masiva con el objetivo de filtrar una amplia gama de información clasificada. La filtración incluyó materiales confidenciales como datos financieros, registros de empleados, películas inéditas y otros materiales confidenciales. Un aspecto particularmente sorprendente del ciberataque fue el exitoso robo de datos confidenciales y la posterior divulgación de correos electrónicos privados de altos ejecutivos de Sony.

Los correos electrónicos filtrados, que provocaron controversia y dañaron la imagen de la empresa, revelaron discusiones delicadas y declaraciones polarizadoras sobre íconos de la industria del entretenimiento, incluidos actores, directores y personal de alto rango.Una comedia conocida como "La Entrevista", que se burlaba del líder norcoreano Kim Jong-un, fue retirada por la fuerza tras un ataque. La película estaba prevista para su estreno inicialmente; sin embargo, las fuerzas de paz, que se cree que tienen conexiones con Corea del Norte, amenazaron con dañar los cines que proyectaban la película. Esta debacle provocó discusiones sobre la censura y el derecho a expresarse.

Respuesta: Para evitar que los correos se filtres se puede realizar una implementación usando API, el cual evitará recibir correo basura (SPAM), protegerá contra los malware y phishing, privacidad, reputación y las normativas, para el sistema de logueo tiene una autenticación y autorización, para los datos tiene va encriptar los datos y tiene un sistema de flirteo de datos, asi como un DPL para evitar que los datos se pueden perder, esto seria en cuanto a la seguridad de los correos, si quiere proteger los datos de personal como el cliente,propongo utilizar un agente endpoint que protegerá contra amenazas cibernéticas, realizará encriptación de los dispositivos y datos, tienes actualizaciones y parches que mejorar sus servicios, y monitisara y analizará las actividades para detectar comportamientos anómalos que amenacen la seguridad, tiene la poder gestionar las opciones de seguridad, por último tiene un control de incidentes que permite mitigar el daño y identificar la amenaza durante el ataque.

No está demás decir que es la transiciones de datos se debe de encriptar los datos así como la ruta final de este que permite dificultar al atacantes obtener una información valiosa

Cinco controles de seguridad (tipo legal, tipo de software, tipo físico)

1. Políticas de Seguridad y Cumplimiento Legal:
   - Tipo Legal: Implementa políticas de seguridad que cumplan con las regulaciones y leyes pertinentes en tu industria y ubicación geográfica. Asegúrate de tener procesos para la gestión de datos personales y confidenciales, cumpliendo con normativas como GDPR, HIPAA, o regulaciones locales.

2. Firewalls y Software de Seguridad:
   - Tipo de Software: Instala firewalls y software de seguridad en todos los sistemas. Configura reglas de firewall para restringir el tráfico no deseado y asegurar que solo los servicios necesarios estén expuestos. Utiliza soluciones antivirus y antimalware actualizadas.

3. Control de Acceso Físico:
   - Tipo Físico: Implementa controles de acceso físico en lugares críticos, como centros de datos y salas de servidores. Utiliza sistemas de cerraduras electrónicas, tarjetas de acceso y sistemas biométricos para garantizar que solo personas autorizadas tengan acceso a áreas sensibles.

4. Actualizaciones y Parches de Software:
   - Tipo de Software: Establece un proceso de gestión de parches y actualizaciones para todos los sistemas y software en tu entorno. Mantente al día con las últimas actualizaciones de seguridad para mitigar vulnerabilidades conocidas y proteger contra amenazas cibernéticas.

5. Cámaras de Vigilancia y Monitoreo Ambiental:
   - Tipo Físico: Implementa cámaras de vigilancia y sistemas de monitoreo ambiental en ubicaciones críticas. Esto no solo proporciona seguridad física, sino que también ayuda a detectar y responder rápidamente a eventos inusuales, como intrusiones o condiciones ambientales adversas.

VI. REFERENCIAS

Aguilar Araujo, C. E., Lau Alayo, E. R., Olivera Kalinowski, S., & Polanco Ramos, C. A. (2017). Propuesta de implantación del Cyber Security Framework (CSF) del NIST, usando COBIT, en Honda del Perú. Universidad ESAN. https://repositorio.esan.edu.pe/handle/20.500.12640/1200

Mendoza Silva, L. F., & Vega Gallegos, G. R. (2019). Evaluación de la capacidad de detección y respuesta a riesgos de ciberseguridad, caso de la empresa Sisc. https://repositorio.up.edu.pe/handle/11354/2250

Barrett, M. (2018), Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST Cybersecurity Framework. https://www.nist.gov/cyberframework

Cabezas Juárez, I. C. (2020). Implementación de un framework de ciberseguridad compuesto por normas y controles para proteger la información de las pequeñas y medianas empresas en Lima. Universidad San Martín de Porres. https://renati.sunedu.gob.pe/handle/sunedu/2847596

Gutiérrez, M. (Abril del 2019). *Gráfico Radial – NIST CSF* [Captura]. Checklist NIST CSF 1.1. https://onedrive.live.com/edit.aspx?resid=CFC9F6EC235610B1!1340&cid=cfc9f6ec235610b1&authkey=!APPSuX41ei6sWYw&CT=1701867971891&OR=ItemsView