**ACTIVIDAD N° 1 DISERTACIÓN NIST CYBERSECURITY FRAMEWORK 2.0**

Icono

Descripción generada automáticamente

Autor.

Mauricio Ruiz Castaño

Escuela superior de guerra “General Rafael Reyes Prieto”

Maestría de Ciberseguridad y Ciberdefensa

Jaider Ospina Navas

Gestión de Riesgo Cibernético

Bogotá 2023

La evolución de los riesgos en el ciberespacio son cada día más rápidos, así mismo es necesario que las personas que trabajamos para obtener un mundo más seguro y ciberresiliente estemos en constante búsqueda de nuevas alternativas de combatir a los cibercriminales, es por esto que la National Institute of Standards and Technology ha diseña gran variedad de herramientas conceptuales, que permites que los profesionales tengamos de primera la información necesaria para minimizar el riesgo desde las más pequeñas empresas hasta las mas grandes, pasando por los distintos sectores industriales y llagando hasta la utilización por personas naturales, un ejemplo de estas el Cybersecurity Framework “CSF”, en esta ocasión analizare los aspectos relevantes en el cambio de versión 2 lanzada en el 2023.

Uno de los puntos más relevantes es el cambio de nombre y con esto su alcance dado que anteriormente se enfocaba en infraestructuras criticas y en esta nueva versión su alcance va desde pequeñas instituciones hasta grandes instituciones, colegios y instituciones estatales, así como la aplicación en cualquier lugar del mundo, ya que es independiente del sector, tipo o tamaño.

Por otro lado busca que se afiance el compromiso con la cooperación internacional, su estructura mantiene los niveles de detalles “flexible, simple y fácil de usar”, manteniendo la imparcialidad sobre el uso de herramientas, tecnologías y proveedores, se guarda la independencia de la tecnología utilizada como “TI, IoT, TO, servicios en la nube. Así como la incorporación de capa de red de dispositivos IoT, tecnología 5G y la migración de la criptografía Post-Cuántica, se da alta importación a la gestión y respuesta y recuperación ante incidentes de ciberseguridad para mantener la resiliencia y restauración de los servicios.

Otro de los temas relevantes en el CSF 2.0 es la gestión de identidad y en mantener la orientación y ampliación para la implementación de Framework, se adicionales ejemplos de implementación de las subcategorías

Se agregarán ejemplos de la implementación del framework, lo que ayudara a las personas en el entendimiento de como implementar y adecuar a la organización, es de suma importancia la adopción del framework para el desarrollo seguro, así como la gestión de riesgos de inteligencia artificial, dejando ver la relevancia que se le da a las tecnologías emergentes. Cobra también relevancia la actualización del sitio web con información que permite orientar al momento de implementar, mapear perfiles, herramientas, casos de éxito que permitan de una manera más ágil la toma de decisiones en las organizaciones.

Un apartado importante y a la cual se le presta gran atención es la gobernanza en ciberseguridad, ampliando su contenido e incluyendo nuevas funciones de “Gobierno” para mejorar los resultados de la gestión de riesgos cibernéticos, se mejora las aclaraciones sobre la gestión de riesgos para analizar, priorizar, responder y monitorear los riesgos, así mismo se enfatiza la importancia de gestión de riesgos en la cadena de suministros, así como la medición y evaluación de la ciberseguridad con una adición de los niveles de implementación del framwork.

Como se evidencia en la nueva versión del Framework de ciberseguridad 2.0 tienen cambios significativos, los cuales ayudaran en el desarrollo de actividades en pro de proteger nuestros activos en el ciberespacio y volver las organizaciones ciber-resiliente ante la creciente evolución de las amenazas cibernéticas.