**FUERZAS MILITARES DE COLOMBIA**

**ESCUELA SUPERIOR DE GUERRA**

**MAESTRÍA CIBERSEGURIDAD Y CIBERDEFENSA**



**ACTIVIDAD No.2**

**DISERTACIÓN DOCUMENTO NIST CYBERSECURITY FRAMEWORK 2.0**

**Juan Camilo Botonero Rodriguez**

**GESTIÓN DE RIESGOS CIBERNÉTICOS**

**Docente Jaider Ospina Navas**

**COHORTE 14**

**AGOSTO, 2023**

El documento "NIST Cybersecurity Framework 2.0 Concept Paper" (NIST, 2023) es un análisis integral de las posibles actualizaciones significativas que se están contemplando para la versión 2.0 del Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST). El propósito fundamental del documento es convocar contribuciones adicionales y opiniones sobre la estructura y dirección del Marco antes de avanzar hacia la redacción de un borrador de la versión 2.0 del mismo. Esta iniciativa refleja el compromiso del NIST en asegurar que el Marco de Ciberseguridad siga siendo relevante y efectivo en el panorama en constante evolución de la ciberseguridad.

El documento presenta un resumen detallado de los cambios potenciales que se están considerando para la versión 2.0 del Marco de Ciberseguridad de NIST. Estos cambios abarcan diversas áreas, desde la ampliación del alcance y aplicaciones del Marco hasta la expansión de la orientación sobre la implementación y la introducción de una mayor emfasis en la gobernanza y la gestión de riesgos en la ciberseguridad. Cada uno de estos cambios está diseñado para mejorar la utilidad, la aplicabilidad y la flexibilidad del Marco, asegurando que continúe siendo una herramienta efectiva para organizaciones de diferentes sectores, tamaños y tipos.

**Análisis de los Cambios Propuestos**

* **Ampliación del Alcance y Aplicaciones del Marco:**

Una de las propuestas clave es cambiar el título del Marco de Ciberseguridad para reflejar su uso en una variedad más amplia de organizaciones, en contraposición a su enfoque original en infraestructuras críticas. Esto se alinea con la creciente adopción del Marco en diversas industrias. Además, se busca expandir el alcance del Marco para beneficiar a organizaciones de distintos tamaños y tipos, alentando su aplicación más allá de las infraestructuras críticas.

* **Mantenimiento de la Estructura del Marco y Conexiones con Otros Marcos:**

El documento subraya la importancia de mantener el nivel actual de detalle del Marco, que ha demostrado ser flexible y adaptable a diferentes contextos organizativos. Además, se destaca la relación del Marco de Ciberseguridad con otros marcos desarrollados por el NIST, como el Marco de Gestión de Riesgos y el Marco de Privacidad. La introducción de la Herramienta de Referencia de Ciberseguridad y Privacidad de NIST busca mejorar la forma en que se accede y se relaciona con los recursos y estándares relevantes.

* **Mayor Orientación sobre la Implementación del Marco:**

El documento reconoce la demanda de una orientación más sólida para la implementación del Marco. Se propone la inclusión de ejemplos prácticos de cómo implementar las subcategorías del Marco para lograr los resultados deseados. Estos ejemplos ayudarán a las organizaciones a comprender mejor cómo aplicar las recomendaciones del Marco en su contexto específico.

* **Énfasis en la Gobernanza de la Ciberseguridad y la Gestión de Riesgos de la Cadena de Suministro:**

El Marco de Ciberseguridad 2.0 busca incorporar una nueva función de gobierno para enfatizar la importancia de la gobernanza en la ciberseguridad. Esta adición refleja la creciente conciencia sobre la necesidad de una gestión sólida de la ciberseguridad a nivel organizativo.

* **Hincapié en la Gestión de Riesgos de la Cadena de Suministro de Ciberseguridad (C-SCRM):**

El documento subraya la expansión de la cobertura de la cadena de suministro de ciberseguridad en el Marco. Esta actualización es una respuesta directa a los desafíos actuales relacionados con la seguridad en la cadena de suministro.

* **Avances en la Medición y Evaluación de la Ciberseguridad:**

El Marco de Ciberseguridad 2.0 también busca avanzar en la comprensión y la implementación de la medición y la evaluación de la ciberseguridad. Esto incluye la clarificación de cómo el Marco puede respaldar la medición y la evaluación de los programas de ciberseguridad, junto con ejemplos concretos y una actualización de la Guía de Medición del Rendimiento de la Seguridad de la Información de NIST.

El "NIST Cybersecurity Framework 2.0 Concept Paper" (NIST, 2023) presenta una visión amplia y detallada de las posibles actualizaciones significativas que se están considerando para la versión 2.0 del Marco de Ciberseguridad de NIST. Estas actualizaciones se enfocan en ampliar el alcance del Marco, mejorar la orientación sobre la implementación y fortalecer la gobernanza y la gestión de riesgos. Cada cambio propuesto tiene como objetivo asegurar que el Marco siga siendo una herramienta valiosa y adaptable para organizaciones de diversas industrias y tamaños en el cambiante paisaje de la ciberseguridad.

**Referencias**

National Institute of Standards and Technology. (2023). NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework. January 19, 2023.