Disertación NIST

El documento trata sobre los potenciales cambios que se generaran en el mist 2.0.

Proporciona un amplio espectro sobre las amenazas siendo un recurso utilizado ampliamente a nivel mundial, sigue siendo eficaz para ministrar la gobernanta y gestión del riesgo en seguridad, mejorando la comunicación a nivel estratégico a través de las tecnologías, se nutre a través del aporte del mundo académico, gobierno e industria, en el lapso de los últimos 9 años, ha sido un documento vivo, que está en modificación con la participación de los entes antes descritos.

En la estructura fundamental, el MCA, fue concebido como guía en el marco en ciberseguridad, sin embargo su empleo ha sido más amplio, llegando hacer un documento de referencia utilizado por múltiples fuentes desde lo gubernamental hasta el ente comercial, haciendo un “llamado a la acción”, buscando la sinergia a través de la preguntas, consultas y los aportes en el conocimiento para proteger la infraestructura crítica.

Dentro de las principales actuaciones del MCA se tiene:

1. Aumentar la colaboración y el compromiso internacional. A través de la políticas y directrices se pretendería mejorar el ítem de la ciberseguridad, donde en algunos países, han tomado como referencia y otros de manera obligada los lineamientos dados por esta guía, por último, esta ha mantenido su estrecha relación a través de los institutos de normas internacionales, buscando estándares para su utilización.
2. El MC2 seguirá siendo un Contexto entre lo actual-vigente y lo venidero:   
   Velará por mantener el nivel de detalle actual, buscando la sencillez y practicidad de los procedimientos.
3. Relación del NIST aprovechara s contexto con otros marcos normativos.
4. Herramienta de referencia de la Ciberseguridad y Privacidad en línea: buscara marcos normativos y directrices para ser interfaz con los usuarios.
5. Referencia Informativas en Línea Actualizables.

Posibles Actualizaciones del MCA 2.0:

* Mapeos, y desarrollo de estos.
* Mantener La neutralidad con respecto a la tecnología y proveedores, reflejando los cambios en las prácticas en ciberseguridad, en lo referente a IT (Information technology); IoT (Internet de las Cosas); OT (Operation Technology).

El MCA 2.0 Incluirán Orientaciones sobre ampliación del Marco. En referencia a este tema, abordará más necesidades en lo organizacional y en lo No Prescriptivo, vario arios enfoques.

Pretende ampliar los ejemplos de las subcategorías del MCA, Elaborar un perfil del MCA, también compartir los perfiles entre entidades gubernamentales y Privadas, con el fin de compartir para sectores, amenazas y otros casos. Se resalta también como el NIST a través del repositorio, incluir enfoques de implementación, mapeo, herramientas, casos de estudio y casos de éxito.

Otro tema relevante será que el MSC 2.0, buscará la gobernanza de la ciberseguridad, a través de identificar y como utilizar el Marco. Se incluirá una herramienta nueva de Gobernanza, siendo esta fundamental para gestionar y reducir el riesgo en ciberseguridad, determinando prioridades y tolerancia al riesgo en toda la cadena de valor relacionada. Esto es vital para que la actividad de la organización se pueda identificar, proteger, detectar responder y recuperarse.

Otro tema relevante, definitivamente se constituye en la relación del riesgo y su gestión. Y como afectara está a la cadena de suministros.

El CSF 2.0 se enfocará en la medición y evaluación en ciberseguridad y los programas a través de ejemplos.

Se actualizará la Guía de medición del rendimiento del NIST para la seguridad de la información.

Como conclusión esa GUIA busca proporcionar los mecanismos para el manejo de los riesgos en Ciberseguridad, a través de la colaboración e intercambio de información en la plataforma, con un creciente rigor y sofisticación, en el proceso de la gestión del riesgo y los programas para anticipar en los ecosistemas amplios, por ultimo incluye el enfoque del contexto de la gobernanza y la participación externa, para mejorar el sistema.

EE. UU. El Marco de Ciberseguridad del NIST **ayuda a los negocios de todo tamaño a comprender mejor sus riesgos de ciberseguridad, administrar y reducir sus riesgos, y proteger sus redes y datos**. Este Marco es voluntario.