UNIVERSIDAD AUTÓNOMA DE CHIAPAS

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN
CAMPUS 1

ING. EN DESARROLLO Y TECNOLOGÍAS DE SOFTWARE

7 “M”

OPT.2 - ANÁLISIS DE VULNERABILIDADES

SUB2

ACTIVIDAD 2.4 EXPLICA ¿QUÉ ES EL MARCO DE CIBERSEGURIDAD DEL NIST?

ALUMNO: MARCO ANTONIO ZÚÑIGA MORALES – A211121

DOCENTE: DR. LUIS GUTIÉRREZ ALFARO

TUXTLA GUTIÉRREZ, CHIAPAS
MARTES, 12 DE MARZO DE 2024

Índice

Introducción

En la era digital, donde las amenazas cibernéticas evolucionan constantemente, establecer un marco robusto de ciberseguridad es esencial para proteger los activos y la información crítica de las organizaciones. El Marco de Ciberseguridad del NIST (Instituto Nacional de Estándares y Tecnología de los Estados Unidos) ofrece una guía estratégica para desarrollar, implementar y mantener prácticas de seguridad informática eficaces. Este documento proporciona una vista a los componentes clave y la implementación del Marco de Ciberseguridad del NIST, destacando su importancia en la gestión de riesgos de ciberseguridad en las organizaciones modernas.

El Marco de Ciberseguridad del NIST es un conjunto de políticas y prácticas recomendadas diseñadas para ayudar a las organizaciones a mejorar su seguridad cibernética y gestionar los riesgos de manera eficiente. Este marco ofrece un lenguaje común y un enfoque sistemático para la ciberseguridad, facilitando la colaboración y el entendimiento entre diferentes partes interesadas dentro de una organización y con sus socios externos.

Este documento tiene como objetivo proporcionar una visión general de los aspectos fundamentales del Marco de Ciberseguridad del NIST, facilitando a las organizaciones el desarrollo de estrategias de seguridad informática eficientes y adaptadas a sus necesidades específicas. Al seguir las directrices del NIST, las entidades pueden fortalecer significativamente su postura de ciberseguridad, mejorando su capacidad para gestionar y mitigar los riesgos en el cambiante paisaje de amenazas cibernéticas.

Desarrollo

¿Qué es el Marco de Ciberseguridad del NIST?

El Marco de Ciberseguridad del NIST (Instituto Nacional de Estándares y Tecnología de los Estados Unidos) es una guía comprensiva diseñada para ayudar a las organizaciones de todos los tamaños y sectores a gestionar y mitigar los riesgos de ciberseguridad. Establecido para promover una mayor protección y seguridad de las infraestructuras críticas en los Estados Unidos, el Marco se ha convertido en una referencia global para las mejores prácticas de seguridad cibernética.

El propósito del Marco es doble: primero, proporcionar un conjunto de estándares, pautas y prácticas para ayudar a las organizaciones a gestionar y reducir sus riesgos cibernéticos de manera eficiente; y segundo, fomentar la comunicación y la cooperación tanto dentro de las organizaciones como entre ellas y sus partes interesadas. Esto se logra mediante la creación de un lenguaje común que permite a todos los involucrados comprender, gestionar y expresar los riesgos de ciberseguridad de manera efectiva y coherente.

Una de las fortalezas del Marco de Ciberseguridad del NIST es su flexibilidad; está diseñado para ser adaptado y aplicado según las necesidades específicas de cada organización, teniendo en cuenta su tamaño, sector, riesgo de ciberseguridad y recursos disponibles. Esto hace que el Marco no solo sea accesible para grandes corporaciones con recursos significativos, sino también para pequeñas y medianas empresas.

La implementación del Marco permite a las organizaciones comprender mejor sus activos y sistemas críticos, identificar y priorizar riesgos, desarrollar estrategias robustas de protección, detectar y responder de manera efectiva a incidentes de seguridad, y recuperarse de estos para minimizar el impacto en el negocio.

Estructura central del Marco de Ciberseguridad del NIST

La estructura central del Marco de Ciberseguridad del NIST está diseñada para ofrecer un enfoque coherente y comprensible hacia la gestión de la ciberseguridad. Está organizada alrededor de cinco Funciones principales que, en conjunto, proporcionan un marco para la gestión eficaz de los riesgos de ciberseguridad. Estas Funciones ayudan a las organizaciones a comprender sus operaciones de ciberseguridad y a planificar sus respuestas a incidentes de seguridad.
Las cinco Funciones son:

1. **Identificar**

    - **Objetivo:** Comprender el entorno organizacional para gestionar eficazmente los riesgos cibernéticos.
    - **Actividades Clave:** Identificación de recursos críticos, evaluación de riesgos y análisis de dependencias.

2. **Proteger**

    - **Objetivo:** Implementar salvaguardas para asegurar la continuidad de servicios críticos.
    - **Actividades Clave:** Control de acceso, formación y concienciación, protección de datos, y mantenimiento de la seguridad operacional.

3. **Detectar**

    - **Objetivo:** Identificar rápidamente actividades cibernéticas anómalas.
    - **Actividades Clave:** Monitoreo continuo, detección de anomalías y eventos, y evaluación de seguridad en tiempo real.

4. **Responder**

    - **Objetivo:** Actuar efectivamente ante incidentes cibernéticos detectados.
    - **Actividades Clave:** Planificación de respuesta, comunicación, análisis de incidentes, y mitigación de impactos.

5. **Recuperar**

    - **Objetivo:** Restaurar operaciones normales tras un incidente cibernético.
    - **Actividades Clave:** Recuperación de sistemas y activos, reducción del impacto en stakeholders, y aprendizaje de lecciones para futuras estrategias de protección y resiliencia.

Niveles de implementación del Marco del NIST

Para ayudar a las organizaciones del sector privado a medir su progreso hacia la implementación del marco de ciberseguridad del NIST, el marco identifica cuatro niveles de implementación:

- **Nivel 1 – Parcial**
    - **Descripción:** Implementación ad-hoc y reactiva de controles de ciberseguridad. Conocimiento limitado de los riesgos de ciberseguridad.
    - **Características:** Conciencia inicial, falta de procesos planificados.
- **Nivel 2 - Riesgo Informado**
    - **Descripción:** Conciencia aumentada sobre los riesgos de ciberseguridad. Comunicación informal de la información, sin procesos de gestión de riesgos estructurados.
    - **Características:** Mayor conciencia, falta de enfoque proactivo y repetible.
- **Nivel 3 – Repetible**
    - **Descripción:** Comprensión clara de los riesgos, con un plan de gestión de riesgos implementado. Acciones para monitorear y responder a ciberataques están establecidas.
    - **Características:** Plan de gestión de riesgos establecido, prácticas de respuesta mejoradas.
- **Nivel 4 – Adaptable**
    - **Descripción:** La organización es ciberresiliente, aprende de experiencias pasadas y se adapta proactivamente a nuevas amenazas. Incorpora la gestión del riesgo de ciberseguridad en la toma de decisiones y la cultura organizativa.
    - **Características:** Ciberresiliencia, adaptabilidad frente a nuevas amenazas, integración del riesgo de ciberseguridad en la cultura y decisiones organizacionales.

Establecimiento de un programa de gestión de riesgos de ciberseguridad acorde al Marco del NIST

El establecimiento de un programa de gestión de riesgos de ciberseguridad acorde al Marco de Ciberseguridad del NIST es un proceso estructurado que ayuda a las organizaciones a identificar, gestionar y mitigar los riesgos relacionados con la seguridad de la información. Este enfoque sistemático se basa en la comprensión de la gestión de riesgos como un componente integral de la gobernanza organizacional, orientado a proteger los sistemas, activos, datos y capacidades.

El marco de ciberseguridad del NIST proporciona una guía paso a paso sobre cómo establecer o mejorar su programa de gestión de riesgos de seguridad de la información:

1. **Prioridades y alcance:** cree una idea clara del alcance del proyecto e identifique las prioridades. Establezca los objetivos de la misión o los objetivos comerciales de alto nivel, las necesidades del negocio y determine la tolerancia al riesgo de la organización.

2. **Orientación:** haga un balance de los activos y sistemas de la organización e identifique las regulaciones aplicables, el enfoque del riesgo y las amenazas a las que estaría expuesta la organización.

3. **Cree un perfil actual:** un perfil actual es un ejemplo de cómo la organización está gestionando el riesgo en la actualidad, según lo definido por las categorías y subcategorías del CSF.

4. **Realice una evaluación de riesgos:** evalúe el entorno operativo, los riesgos emergentes y la información sobre amenazas de ciberseguridad para determinar la probabilidad y gravedad de un evento de ciberseguridad que pueda afectar a la organización.

5. **Cree un perfil objetivo:** un perfil objetivo representa la meta de gestión de riesgos del equipo de seguridad de la información.

6. **Determine, analice y priorice las brechas:** al identificar las brechas entre el perfil actual y el perfil objetivo, el equipo de seguridad de la información puede crear un plan de acción que incluya hitos y recursos medibles (personas, presupuesto, tiempo) necesarios para cubrir estas brechas.

7. **Implemente un plan de acción:** implemente el plan de acción definido en el Paso 6.

Conclusión

En conclusión, el Marco de Ciberseguridad del NIST representa una piedra angular en los esfuerzos de las organizaciones para fortalecer su postura de ciberseguridad en un panorama digital que evoluciona rápidamente. A través de su estructura articulada en torno a las cinco Funciones fundamentales de Identificar, Proteger, Detectar, Responder y Recuperar, el Marco ofrece un enfoque cohesivo y estratégico para la gestión de la ciberseguridad. Este enfoque no solo permite a las organizaciones abordar de manera eficaz los desafíos de seguridad actuales sino también anticiparse y adaptarse a las amenazas emergentes.

La adaptabilidad del Marco, junto con la conceptualización de niveles de madurez en su implementación, facilita a las organizaciones de todo tipo y tamaño la integración de prácticas de seguridad robustas y personalizadas. Estos niveles de madurez sirven como un espejo en el cual las organizaciones pueden reflejarse para evaluar su progreso en la implementación del Marco y, en consecuencia, afinar su enfoque hacia una gestión de riesgos de ciberseguridad más eficiente y dinámica.

El establecimiento de un programa de gestión de riesgos de ciberseguridad acorde al Marco del NIST no es un fin en sí mismo, sino un proceso continuo de mejora y adaptación. Este proceso requiere un compromiso organizacional con la evaluación constante y la recalibración de estrategias de seguridad en función de las cambiantes dinámicas del entorno cibernético. Al adoptar y adaptar el Marco del NIST, las organizaciones pueden no solo salvaguardar sus activos críticos contra las amenazas cibernéticas actuales sino también fomentar una cultura de seguridad resiliente que esté preparada para enfrentar los desafíos del futuro.

Referencias Bibliográficas

Ciberseg. (2021, 17 septiembre). *¿Qué es el marco de Ciberseguridad del NIST?* Ciberseguridad. https://ciberseguridad.com/herramientas/marco-ciberseguridad-nist/

Gómez, J. A. (2024, 6 febrero). *Marco de Ciberseguridad Del NIST: Qué es y Cómo Implementarlo*. https://www.deltaprotect.com/blog/marco-ciberseguridad-nist

Marco de ciberseguridad del NIST. (2021, 9 noviembre). Comisión Federal de Comercio. https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist

NIST Cybersecurity Framework. (s. f.). Cyberzaintza. https://www.ciberseguridad.eus/ciberpedia/marcos-de-referencia/nist-cybersecurity-framework

¿Qué es el marco de ciberseguridad del NIST? | *IBM*. (s. f.). https://www.ibm.com/mx-es/topics/nist