UNIVERSIDAD AUTÓNOMA DE CHIAPAS

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN
CAMPUS 1

Licenciatura en Ingeniería en Desarrollo y Tecnologías de Software

Actividad 2.4 Explica ¿Qué es el Marco de Ciberseguridad del NIST?

7 "M"

Materia: Análisis De Vulnerabilidades

Docente: Luis Gutierrez Alfaro

ALUMNOS:

A 211387

Steven de Dios Montoya Hernández

Git:https://github.com/StevenMontoya12

TUXTLA GUTIÉRREZ, CHIAPAS

Viernes, 15 de Marzo de 2024, 23:59

Explica ¿Qué es el Marco de Ciberseguridad del NIST?

El Marco de Ciberseguridad del NIST (National Institute of Standards and Technology) es un conjunto de prácticas recomendadas para la gestión de riesgos de ciberseguridad. Este marco de referencia voluntario y flexible ayuda a las organizaciones a identificar, proteger, detectar, responder y recuperarse de incidentes de ciberseguridad.

El marco se estructura en cinco funciones principales:

1. **Identificar**: El primer paso es comprender los activos de información de la organización, es decir, todo aquello que necesita ser protegido, como datos confidenciales, sistemas informáticos y redes. A partir de esto, se realiza una evaluación de los riesgos asociados a cada activo, considerando las amenazas y vulnerabilidades existentes.

2. **Proteger:** Una vez identificados los riesgos, se implementan medidas de seguridad para proteger los activos de información
    - Controles de acceso: para determinar quién tiene acceso a qué información.
    - Seguridad perimetral: para proteger los sistemas y redes de accesos no autorizados.
    - Encriptación: para proteger la confidencialidad de la información.
    - Capacitación en seguridad: para que los empleados sean conscientes de los riesgos y las mejores prácticas de seguridad.

3. **Detectar:** Es fundamental contar con mecanismos para monitorizar los sistemas y redes de la organización para detectar actividades cibernéticas maliciosas. Esto incluye el uso de herramientas de detección de intrusiones, análisis de logs y sistemas de alerta temprana..

4. **Responder:** En caso de un incidente de ciberseguridad, es necesario tener un plan de respuesta para contener el daño y mitigar el impacto. Este plan debe incluir:
    - Pasos para aislar el sistema afectado.
    - Métodos para contener la propagación del ataque.
    - Procedimientos para restaurar los sistemas y datos afectados.
    - Comunicación con las partes interesadas.

5. **Recuperar:** El objetivo final es restaurar los sistemas y la infraestructura a su estado normal después de un incidente. Esto implica:
    - Implementar medidas de recuperación de datos.
    - Restablecer los sistemas a su configuración original.
    - Aplicar lecciones aprendidas para mejorar la postura de seguridad.

El uso del Marco de Ciberseguridad del NIST puede brindar a las organizaciones los siguientes beneficios:

Mejora la postura de seguridad: Reduce la probabilidad y el impacto de los incidentes de ciberseguridad.

Optimiza la gestión de riesgos: Permite tomar decisiones informadas sobre la inversión en seguridad.

Facilita la comunicación: Mejora la comunicación entre las partes interesadas sobre la ciberseguridad.

Aumenta la confianza: Demuestra el compromiso de la organización con la seguridad de la información.

¿Cómo implementar el Marco?

El Marco de Ciberseguridad del NIST es adaptable a las necesidades de cualquier organización. No existe una única forma de implementarlo, lo que permite personalizarlo a su contexto específico.

Para empezar, se recomienda realizar una evaluación de la madurez actual de la organización en materia de ciberseguridad. A partir de esta evaluación, se puede definir un plan de acción para implementar las prácticas del Marco de forma gradual.

Implementación del Marco en diferentes sectores:

- **Sector público:** El Marco ha sido ampliamente adoptado por agencias gubernamentales en todo el mundo. El Departamento de Seguridad Nacional de los Estados Unidos (DHS) exige que las agencias federales implementen el Marco como parte de su programa de gestión de riesgos de ciberseguridad.
- **Sector privado:** El Marco también es aplicable a empresas privadas de cualquier tamaño e industria. Algunas organizaciones líderes que han implementado el Marco incluyen: Bank of America, Boeing, Coca-Cola, ExxonMobil, General Electric, Google, Microsoft, y Walmart.
- **PyMEs:** El Marco puede ser adaptado a las necesidades específicas de las pequeñas y medianas empresas (PyMEs). Existen recursos específicos disponibles para ayudar a las PyMEs a implementar el Marco, como la Guía de Implementación del Marco de Ciberseguridad del NIST para Pequeñas Empresas.

Casos de éxito:

- **Bank of America:** Implementó el Marco para mejorar su postura de seguridad y reducir el riesgo de sufrir un incidente cibernético.
- **Boeing:** Utiliza el Marco para proteger sus sistemas y datos de amenazas cibernéticas.
- **Google:** Ha implementado el Marco en sus operaciones globales para proteger la información de sus usuarios.

El Marco de Ciberseguridad del NIST es una herramienta invaluable para cualquier organización que busca protegerse de las amenazas cibernéticas. Su enfoque flexible y adaptable lo convierte en una solución viable para empresas de todos los tamaños y sectores.

La implementación del Marco puede ayudar a mejorar significativamente la postura de seguridad de una organización, reducir el riesgo de sufrir un incidente cibernético y aumentar la confianza de sus clientes y socios.

Estructura central del Marco de Ciberseguridad del NIST

El Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) es una guía ampliamente utilizada en la industria para fortalecer la ciberseguridad de las organizaciones. La estructura central del Marco de Ciberseguridad del NIST consta de tres componentes principales: el Core (Núcleo), el Tiers (Niveles) y el Profile (Perfil).

Core (Núcleo):

El Núcleo es el componente esencial del marco y está compuesto por cinco funciones principales: Identificar, Proteger, Detectar, Responder y Recuperar (Identity, Protect, Detect, Respond y Recover, en inglés). Estas funciones representan las actividades clave que una organización debe llevar a cabo para gestionar y mejorar su postura de ciberseguridad.

Cada una de estas funciones se divide en categorías y subcategorías que proporcionan detalles específicos sobre las acciones y controles asociados a cada función.

Entre los que entra el núcleo, es Identificar, Proteger Detectar, Responder, Recuperar.

Tiers (Niveles):

Los Niveles o Tiers representan la capacidad de gestión de riesgos de una organización y su enfoque de implementación del marco. Hay cuatro niveles en total: Básico, Intermedio, Avanzado y Adaptativo.

Cada nivel refleja un grado creciente de madurez en la implementación de las funciones del Núcleo. Los niveles ayudan a las organizaciones a evaluar su posición actual y establecer metas para mejorar su ciberseguridad.

- **Básico (Tier 1):** Las organizaciones en este nivel tienen un enfoque reactivo y no cuentan con una gestión formalizada de la ciberseguridad.

- **Intermedio (Tier 2):** Se caracteriza por un enfoque más proactivo en la gestión de riesgos, con procesos documentados y una mayor conciencia de la ciberseguridad.

- **Avanzado (Tier 3):** Las organizaciones en este nivel tienen un enfoque avanzado y centrado en la gestión integral de la ciberseguridad, con procesos continuos de mejora y adaptación.

- **Adaptativo (Tier 4)**: Este nivel implica una capacidad de respuesta ágil y continua a medida que evolucionan las amenazas y las tecnologías. La organización se adapta rápidamente a los cambios en el entorno de ciberseguridad.

Profile (Perfil):

El Perfil permite a las organizaciones personalizar el marco según sus necesidades y circunstancias específicas. Los perfiles son configuraciones adaptadas del Núcleo y los Tiers para abordar los objetivos de ciberseguridad y los riesgos particulares de una organización.

Al crear un perfil, las organizaciones pueden identificar y seleccionar las categorías y subcategorías del Núcleo que son relevantes para sus operaciones, así como establecer metas específicas de Tiers.

- Los perfiles son configuraciones específicas del Núcleo y los Tiers que las organizaciones utilizan para personalizar el marco según sus necesidades y objetivos. Al desarrollar un perfil, las organizaciones pueden seleccionar las categorías y subcategorías del Núcleo que son relevantes y establecer metas específicas de Tiers.
- El perfil permite a las organizaciones alinear el Marco de Ciberseguridad del NIST con sus objetivos comerciales y adaptarlo a su contexto operativo particular.

Niveles de implementación del Marco del NIST

El Marco de Ciberseguridad del NIST (National Institute of Standards and Technology) define cuatro niveles de implementación para ayudar a las organizaciones a medir su progreso en la gestión de riesgos de ciberseguridad. Estos niveles son:

1. Parcial:
La organización está familiarizada con el Marco del NIST y puede haber implementado algunos aspectos de control en algunas áreas de la infraestructura.
No se ha realizado una evaluación completa de la madurez de la organización en materia de ciberseguridad.
No existe un plan formal para implementar el Marco de forma completa.

2. Riesgo informado:
La organización es más consciente de los riesgos de ciberseguridad y comparte información de manera informal.
Se ha realizado una evaluación inicial de la madurez de la organización en materia de ciberseguridad.
Existe un plan informal para implementar el Marco de forma gradual.

3. Repetible:
La organización ha implementado las prácticas del Marco de forma consistente en toda la organización.
Se han realizado evaluaciones regulares de la madurez de la organización en materia de ciberseguridad.
Existe un plan formal para mejorar continuamente la implementación del Marco.

4. Adaptativo:
La organización ha integrado el Marco en su cultura y procesos de negocio.
La organización puede adaptar y mejorar continuamente las prácticas del Marco para responder a las amenazas emergentes.
La organización es un líder reconocido en la gestión de riesgos de ciberseguridad.

¿Cómo determinar el nivel de implementación?
Para determinar el nivel de implementación actual de una organización, se recomienda realizar una evaluación de la madurez en materia de ciberseguridad. Esta evaluación debe considerar los siguientes aspectos:

- **Conocimiento del Marco del NIST:** ¿En qué medida la organización está familiarizada con el Marco?
- **Implementación de las prácticas del Marco:** ¿Cuántas prácticas del Marco se han implementado?
- **Madurez de la gestión de riesgos:** ¿Qué tan maduro es el proceso de gestión de riesgos de la organización?
- **Cultura de seguridad:** ¿Existe una cultura de seguridad dentro de la organización?

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 del NIST puede ayudar a las organizaciones a mejorar significativamente su postura de seguridad y reducir el riesgo de sufrir un incidente cibernético.

Es importante recordar que la implementación del Marco es un proceso continuo que requiere un compromiso a largo plazo por parte de la alta dirección y de todos los empleados de la organización.

El Marco de Ciberseguridad del NIST (National Institute of Standards and Technology) ofrece una guía completa para establecer un programa de gestión de riesgos de ciberseguridad efectivo. A continuación se presenta un resumen de los pasos clave para la implementación del Marco:

1. Priorizar y determinar el alcance:

Es fundamental definir los objetivos de negocio y las prioridades de alto nivel de la organización para establecer un programa efectivo.

Luego, se deben identificar los activos de información críticos y los riesgos asociados a ellos. Esto permitirá determinar el alcance del programa de gestión de riesgos, incluyendo las áreas de la organización que se abordarán.

2. Orientación:

Es importante que la organización se familiarice con el Marco del NIST y sus componentes para comprender su funcionamiento.

Luego, se deben seleccionar las prácticas del Marco que mejor se adapten a las necesidades y características específicas de la organización.

Finalmente, se debe desarrollar un plan de implementación para las prácticas del Marco, definiendo cómo se implementarán y en qué plazo.

3. Crear un perfil actual:

Para evaluar la situación actual de la organización en materia de ciberseguridad, se debe realizar una evaluación de la madurez.

Esta evaluación permitirá identificar las brechas entre la situación actual y el estado deseado, lo que servirá como base para la planificación de mejoras.

4. Realizar una evaluación de riesgos:

Es fundamental identificar las amenazas y vulnerabilidades relevantes para la organización, teniendo en cuenta su contexto y sector.

Luego, se debe evaluar el impacto potencial de los incidentes de ciberseguridad para comprender las posibles consecuencias.

Finalmente, se debe calcular el riesgo de cada amenaza y vulnerabilidad, considerando la probabilidad de ocurrencia y el impacto potencial.

5. Crear un perfil objetivo:

Con base en la evaluación previa, se debe definir el estado deseado de la gestión de riesgos de ciberseguridad en la organización.

Esto implica establecer objetivos específicos y medibles para la mejora, definiendo qué se quiere lograr y cómo se medirá el progreso.

6. Determinar, analizar y priorizar las brechas:

Luego de definir el perfil objetivo, se deben identificar las brechas entre la situación actual y el estado deseado.

Es importante analizar las causas de las brechas para comprender por qué existen y qué se puede hacer para solucionarlas.

Finalmente, se deben priorizar las brechas en función del riesgo, enfocando los esfuerzos en las que representen un mayor peligro para la organización.

7. Implementar el plan de acción:

El plan de acción desarrollado en la etapa 2 se debe implementar de forma gradual y priorizada, comenzando por las prácticas que tengan un mayor impacto en la reducción del riesgo.

Es importante monitorizar y evaluar el progreso de la implementación de forma regular para asegurar que se está logrando el objetivo deseado.

Adicionalmente, se deben realizar ajustes al plan de acción según sea necesario, adaptándolo a las nuevas necesidades y riesgos que puedan surgir.

8. Revisión y mejora continua:

El programa de gestión de riesgos de ciberseguridad debe ser revisado y actualizado de forma regular para asegurar que se mantiene actualizado y efectivo.

Es importante incorporar las lecciones aprendidas de los incidentes de ciberseguridad para mejorar las prácticas de gestión de riesgos.

Adicionalmente, se debe buscar la mejora continua de las prácticas, implementando nuevas medidas y estrategias para proteger la organización de las amenazas emergentes.

Conclusión
El Marco de Ciberseguridad del NIST (National Institute of Standards and Technology) es una herramienta fundamental para la gestión de riesgos de ciberseguridad en organizaciones de cualquier tamaño.

- Este marco flexible y voluntario ofrece una guía completa para:
- Identificar los activos de información de la organización y los riesgos asociados.
- Proteger los activos de información mediante la implementación de medidas de seguridad.
- Detectar actividades cibernéticas maliciosas a través de la monitorización de los sistemas y redes.
- Responder a los incidentes de ciberseguridad de forma eficaz y eficiente.
- Recuperarse de los incidentes de ciberseguridad y restaurar la normalidad en la organización.

Estructura central:

El Marco se estructura en torno a tres elementos principales:

- Funciones: cinco actividades y procesos que una organización debe realizar para gestionar el riesgo de ciberseguridad (identificar, proteger, detectar, responder y recuperar).

- Categorías: 23 áreas de enfoque dentro de cada función.

- Subcategorías: 108 prácticas específicas dentro de cada categoría.

Niveles de implementación:

El Marco del NIST define cuatro niveles de implementación para ayudar a las organizaciones a medir su progreso en la gestión de riesgos de ciberseguridad:

- **Parcial:** La organización está familiarizada con el Marco y puede haber implementado algunos aspectos de control.
- **Riesgo informado:** La organización es más consciente de los riesgos y comparte información de manera informal.
- **Repetible:** La organización ha implementado las prácticas del Marco de forma consistente.
- **Adaptativo:** La organización ha integrado el Marco en su cultura y procesos de negocio.

Establecimiento de un programa de gestión de riesgos:

Para establecer un programa de gestión de riesgos de ciberseguridad acorde al Marco del NIST, se recomienda seguir estos pasos:

Priorizar y determinar el alcance: Definir los objetivos de negocio, identificar los activos de información críticos y determinar el alcance del programa.

Orientación: Familiarizarse con el Marco, seleccionar las prácticas del Marco y desarrollar un plan de implementación.

Crear un perfil actual: Realizar una evaluación de la madurez actual de la organización en materia de ciberseguridad.

Realizar una evaluación de riesgos: Identificar las amenazas y vulnerabilidades, evaluar el impacto potencial y calcular el riesgo.

Crear un perfil objetivo: Definir el estado deseado de la gestión de riesgos de ciberseguridad.

Determinar, analizar y priorizar las brechas: Identificar las brechas entre la situación actual y el estado deseado, analizar las causas y priorizarlas en función del riesgo.

Implementar el plan de acción: Implementar las prácticas del Marco de forma gradual y priorizada, monitorizar el progreso y realizar ajustes al plan según sea necesario.

Revisión y mejora continua: Revisar y actualizar el programa de forma regular, incorporar las lecciones aprendidas de los incidentes de ciberseguridad y buscar la mejora continua de las prácticas.

Referencias Bibliográficas

National Institute of Standards and Technology. (2014). Framework for improving critical infrastructure cybersecurity. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r4

Comisión Federal de Comercio. (2023). Marco de ciberseguridad del NIST. https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist

National Institute of Standards and Technology. (2014). Framework for improving critical infrastructure cybersecurity. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r4
National Institute of Standards and Technology. (2014). Framework for improving critical infrastructure cybersecurity. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r4

National Institute of Standards and Technology. (2014). Framework for improving critical infrastructure cybersecurity. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r4

National Institute of Standards and Technology. (2014). Framework for improving critical infrastructure cybersecurity. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r4

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