Unidad 3

viernes, 24 de noviembre de 2023 10:26

Marco

- Se desarrolla el funcionamiento confiable de la infraestructura crítica en EE.UU.
- Es un enfoque priorizado, flexible, repetible, basado en el desempeño y costo efectivo, que incluye medidas de seguridad de la información y controles para identificar, evaluar y gestionar los riesgos.
- Identifica estándares de seguridad aplicables a todos los sectores de infraestructuras críticas.
- Ayuda a los responsables de infraestructuras críticas a inventariar y gestionar riesgos.
- Establece criterios para la definición de métricas para el control de desempeño.
- Establece controles para la protección al realizar prácticas de ciberseguridad.
- Identifica áreas de mejora orientadas al desarrollo de estándares.
- Priorizar recursos.

- Infraestructura crítica: Sistemas o activos, físicos o virtuales, tan vitales que su daño tendrían un gran impacto en la seguridad de la nación, económica y/o salud.

Componentes

- Framework Core: Conjunto de actividades de ciberseguridad, resultados y referencias comunes en todos los sectores de infraestructura crítica.
- Perfiles: Resultados que se basan en las necesidades empresariales.
- Niveles de implementación: Contexto sobre cómo una organización considera el riesgo y los procesos para gestionarlo.
  - Nivel 1 Parcial: Gestión de riesgos. Baja participación externa.
  - Nivel 2 Riesgo Informado: Participación de gestión de riesgos. Aumento de concientización. Participación de terceros informalmente.
  - Nivel 3 Repetible: Gestión de riesgos formalizada. Programas transversales a la organización. Participación de terceros.
  - Nivel 4 Adaptativo: Prácticas basadas en lecciones aprendidas. Mejora continua. Colaboración activa con terceros.

Cómo utilizar:

- Cuando se deba identificar, evaluar y administrar el riesgo.

- Complementar operaciones y medidas existentes.
- Aplicable a lo largo del ciclo de vida de los sistemas.
- Aplicable para revisión básica. Comparar medidas actuales con las medidas del núcleo del marco. Crear un perfil actual de en qué medida están logrando los resultados y cómo mejorar.
- ¿Cómo estamos?

APLICAR EL NIST CSF

PASO 1: Priorización y Alcance

Identificar objetivos empresariales y prioridades.
Determinar el alcance de los sistemas y activos.
Revisar políticas de negocio.

PASO 2: Orientación

Identificar sistemas, activos, requisitos y enfoque del riesgo.
¿Sistemas involucrados?
¿Activos involucrados?
¿Qué amenazas son aplicables?
¿Qué vulnerabilidades hay sobre el sistema?
Identificar amenazas y vulnerabilidades.

PASO 3: Crear un perfil actual

Qué resultados de las categorías del marco se están logrando actualmente?
Categorías
Procesos
- ○ ¿Se tienen procesos para inventariar los activos físicos de la organización?

Personas
- ○ ¿Las personas que participan en los procesos de inventario se encuentran capacitadas para ello?

Tecnologías
- ○ ¿Se cuenta con un software centralizado para inventariar los activos físicos de la organización?

Personas

Nivel	Puntuación	Descripción
Inadecuado	0	- La actividad no se puede realizar debido a que el personal tiene habilidades limitadas. - La actividad no se puede realizar debido a la falta de disponibilidad de personal. - Ningún personal es responsable de completar la actividad .
Carente	1	- El personal actual tiene habilidades limitadas que solo les permiten realizar una pequeña parte de las actividades - El personal realiza las actividades en la medida en que tienen disponibilidad, pero requiere muchos recursos y le restan responsabilidades.
Adecuado	2	- El personal actual tiene las habilidades para realizar la mayoría de las responsabilidades asociadas con la actividad - El personal realiza las actividades en la medida en que tienen disponibilidad, pero requiere muchos recursos y le restan responsabilidades.
Informal	3	- La mayoría de las responsabilidades asociadas con la actividad se pueden realizar con la cantidad actual de personal y base de conocimientos sin una carga significativa. - El personal es responsable de realizar la actividad sin ser asignado formalmente .
Formal	4	- El personal tiene habilidades y experiencia suficientes para completar la actividad en su totalidad con poca carga. - El personal ha sido explícitamente designado roles y responsabilidades para completar la actividad .

Procesos

Nivel	Puntuación	Descripción
Sin proceso	0	- Las tareas asociadas a esta actividad no se realizan.
Ad-Hoc	1	- No hay documentación asociada a la actividad. - Las tareas asociadas con esta actividad se realizan de manera ad hoc .
Definido	2	- Existe alguna documentación escrita para abordar la actividad. - la documentación solo se implementa parcialmente o se sigue en la práctica .
Repetible	3	- Existe documentación apropiada para abordar la actividad. - La actividad se realiza principalmente de acuerdo con la documentación.
Formal	4	- Existe la documentación adecuada para abordar la actividad y se alinea con la política y los estándares de la organización - la actividad se realiza de acuerdo con la política y estándares de la organización

Madurez de los procesos

Tecnología

Title	Score	Description
Indisponible	0	- La tecnología apropiada requerida para realizar esta actividad no está disponible dentro del departamento.
No coincidente	1	- El propósito principal de la tecnología que se utiliza para completar la actividad no es el propósito previsto.
Limitado	2	- La tecnología es capaz y está configurada para realizar algunas de las actividades requeridas. - Hay una infraestructura limitada, capacidad de computación o licencias de software disponibles para el departamento para realizar la actividad requerida .
Aceptable	3	- La tecnología es capaz y está configurada para realizar la mayor parte de la actividad requerida. - Hay suficiente infraestructura, capacidad de computación y licencias de software disponibles para el departamento para realizar la actividad requerida .
Óptimo	4	- La actividad se puede completar en su totalidad con la tecnología. - La función principal de la tecnología es realizar la actividad requerida. - Hay una amplia infraestructura, capacidad de computación y licencias de software disponibles para el departamento para realizar la actividad requerida .

ID.AM: Reconocer dispositivos, software y recursos para identificar incidentes.

- ¿Cuál es el nivel de personal de TI para priorizar, rastrear e inventariar los activos?
- ¿Cuál es el nivel de la organización para priorizar, rastrear e inventariar los activos?
- ¿Cuál es el nivel de los recursos tecnológicos para priorizar, rastrear e inventariar los activos?

#	Evaluación	Definición
0	No comenzado	No se ha iniciado ningún progreso para lograr los resultados de la hoja de ruta definidos a partir del perfil del estado objetivo.
1	No logrado	Hay poca evidencia o ninguna evidencia del logro de los resultados definidos en el perfil de estado objetivo.
2	Parcialmente logrado	Existe cierta evidencia de un enfoque y algún logro de los resultados definidos en el perfil del estado objetivo. Algunos aspectos de las actividades requeridas para lograr el perfil de estado objetivo pueden no estar completamente definidos.
3	Logrado	Existe evidencia de un enfoque sistemático y un logro significativo de los resultados definidos en el perfil del estado objetivo. Pueden existir algunas debilidades en el proceso para lograr el resultado deseado.
4	Completamente logrado	Existe evidencia de un enfoque completo y sistemático y un logro completo de los resultados definidos en el perfil del estado objetivo. No existen debilidades significativas en el proceso para lograr el resultado deseado.

30

PASO 4: Evaluación de riesgos

Analizar probabilidad e impacto de los riesgos.

#	Activo comprometido	Vulnerabilidad	Amenaza	Agente de amenaza	Objetivo de ciberseguridad comprometido	Probabilidad	Impacto	Riesgo	Control	Probabilidad	Impacto	Riesgo residual
R1	Base de datos SIAC	Cliente SIAC sin inventariar que se encuentra en notebook personal del encargado de archivo de RC.	Suplantación del encargado de archivo RC para la modificación de la base de datos	Ex - estudiante enojado	Integridad	Alta	Muy Alto	Extremo	CIS 1.1 Establecer y mantener un detallado inventario de activos empresariales CIS1.2 Gestionar activos no autorizados A.8.1.2 Propiedad de los activos	Baja	Muy Alto	Medio

PASO 5: Crear un perfil objetivo

Describir los resultados deseados de las categorías del marco.

De los niveles del perfil actual

Se plantean las siguientes metas:

- Nivel 1 en el primer año
- Nivel 2 en el segundo año
- Nivel 3 en el tercer año.

PASO 6: Determinar y priorizar brechas

Comparar el perfil actual y objetivo para definir brechas con el perfil objetivo.
Determinar los recursos necesarios para abordar brechas (dinero y trabajo)
Mejoras.

Tenemos que ID.AM:

- Perfil actual: Nivel 0 - No comenzado
- Perfil objetivo: Nivel 3 - Logrado

Identificador	Función	Pregunta	Situación actual: **Inadecuado**	Primer año - Perfil Objetivo ID.AM: **No logrado**	Segundo año - Perfil Objetivo ID.AM: **Parcialmente logrado**	Tercer año - Perfil Objetivo ID.AM: **Logrado**
ID.AM. Pe-1	Identificar	¿Cuál es el nivel del personal de TI de su departamento para priorizar, rastrear e inventariar los activos de TI (incluidos los dispositivos físicos, el software)?		Implementación de controles: • CIS 1.1 Establecer y mantener un detallado inventario de activos empresariales Otras actividades: • Capacitar a los encargados del inventario en el proceso de inventario de activos	Definición del proceso de inventario. Contratar personal para labores de tecnología. Compra de software de gestión de inventario. Implementar software de gestión de inventario. Capacitar a las personas en el nuevo software de inventario y proceso. Personal se le asigna funciones asociadas en la medida de lo posible.	El personal prioriza, rastrea y hace inventario de los activos de TI sin ser asignado formalmente. Contratar personal para labores de ciberseguridad. Capacitación continua del capital humano en los procesos y tecnología de la organización. Auditoría de los procesos relacionados.

PASO 7: Implementar el plan de acción

Qué acciones tomar para abordar las brechas.
Ajustar al contexto

Gestión del riesgo

Riesgo: Probabilidad de que ocurra el daño y las consecuencias.
IRM: Gestión del riesgo de la información (Identificar, reducir, implementar mecanismos, priorizar)

Objetivos del análisis del riesgo:

- Identificar valor de activos.
- Identificar vulnerabilidades y amenazas.
- Cuantificar la probabilidad e impacto.

- Balancear entre impacto de amenazas y costos de contramedidas.

El riesgo tiene una
- Pérdida potencial: Lo que se pierde si un agente de amenaza explota una vulnerabilidad. (corrupción de datos, divulgación, etc.)
- Pérdida tardía: Consecuencias luego de explotar la vulnerabilidad (pérdida de reputación, pérdida de mercado, penalización).

Metodologías de la gestión del riesgo:
- NIST 800-30 Risk Management
- Facilitated Risk Analysis Process
- OCTAVE
- AS/NZS 4360
- ISO/IEC 27005
- Failure Modes and Effect
- Fault tree analysis
- CRAMM
- ISO/IEC 31000

El análisis de riesgo tiene dos enfoques
- Cuantitativo: Monetario.
- Cualitativo: Asigna clasificación a los riesgos (alto, medio bajo).

Atributo	Cuantitativo	Cualitativo
No requiere cálculos		X
Requiere cálculo complejos	X	
Requiere un alto grado de supuestos		X
Proporciona áreas generales e indicaciones de riesgos		X
Es fácil para automatizar y evaluar	X	
Usado para el seguimiento de la performance del manejo de riesgo	X	
Permite un análisis costo/beneficio	X	
Usa métricas verificables y objetivas	X	
Provee opiniones de los individuos que mejor conocen los procesos		X
Muestra las perdidas que pueden ser producidas en un año	X	

Una compañía invierte para disminuir el riesgo total a un nivel aceptable, lo que significa que siempre queda un riesgo residual.

Amenazas x Vulnerabilidad x Valor activo = Riesgo total
Riesgo total x brecha de control = riesgo residual
Riesgo total – controles = riesgo residual

Para manejar el riesgo, se puede transferir (compañía de seguros), evitar, reducir o aceptar.

Análisis cuatitativo

Expectativa de pérdida única SLE: Pérdida potencial si ocurre una amenaza.
- Valor activo * Factor de exposición EF
- EF: % de pérdida una vez realizada la amenaza

Por ejemplo, si un data warehouse tiene por valor $80.000.000, y se estima que si ocurre un incendio, el 25% del warehouse puede ser dañado, esto quiere decir que el SLE es:
– SLE =Valor activo x Factor de exposición
– SLE= $80.000.000 * 25% = $20.000.000
Esto quiere decir que la perdida potencial es de $20.000.000 si el incendio se produce.

Expectativa de pérdida anual ALE
- SLE *Ratio anualizado de ocurrencia ARO
- ARO: Frecuencia de una amenaza en 12 meses. 0,0 (nunca) a 1,0 (1 vez al año) a más de 1 (muchas veces en el año)

Por ej: si la probabilidad de incendio y que dañe el data warehouse es de una cada diez años, el valor de ARO es 0,1

Por ej: si la probabilidad de incendio y que dañe el data warehouse es de una cada diez años, el valor de ARO es 0,1

Entonces si el SLE=20.000.000, ARO=0,1 entonces el ALE=2.000.000

El ALE le permite determinar a una empresa si puede gastar esa cantidad o menos anualmente para proteger. Gastar más que eso no es buena opción.

Beneficio del control: ALE antes del control - ALE después del control - Valor control(incluye mantención, capacitación, instalación, etc.)

Si el ALE (Expectativa de perdida anual) de la amenaza de un hacker derribando un webserver es $6.000.000 antes de implementar el control

El ALE es $1.500.000 después de implementado el control.

Mientras que el costo de mantención y operación del control es de $325.000

– $6.000.000 - $1.500.000 - $325.000

Entonces el beneficio de este control para la compañía es de $4.175.000 anualmente.

Análisis cuantitativo

Ranking de alto, medio, bajo o del 1/5, 1/10

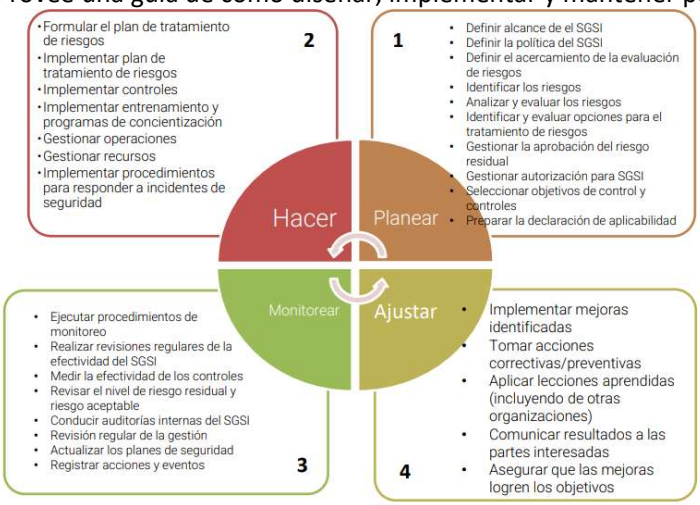
Frameworks de Seguridad

Construir una fortaleza de mecanismos de protección de todo tipo en capas.

Serie ISO/IEC 27000

Nace de estándar británico BS7799.

Provee una guía de cómo diseñar, implementar y mantener políticas, procesos y tecnologías para manejas riesgos y activos.



COBIT

Desarrollado por ISACA.

Marco de gobierno de las tecnologías de la información.

ITIL

Estándar de facto para las prácticas del manejo de los servicios TI.

CIS Control

Conjunto de acciones priorizadas y focalizadas para las prácticas de la defensa organizacional.

- Ofensiva informa a la defensa
- Identificar puntos críticos
- Factibilidad
- Métricas
- Adaptativo

Gobierno de la seguridad de la información

Sistema que dirige y controla las actividades de una organización relacionadas a la ciberseguridad.