TECNOLOGIAS DE LA INFORMACION Y CUBERSEGURIDAD

nacap

Controles de mitigación y gestión de riesgos basados en análisis de vulnerabilidad

Seguridad de la Información

nacap

Objetivo

Proporcionar controles de mitigación y gestión de riesgos basados en análisis de vulnerabilidades es fundamental para asegurar la seguridad de sistemas, redes y datos en entornos informáticos.

nacap

CVSS

Sigla	Acrónimo	En español
C	Common	Común
V	Vulnerabilty	Vulnerabilidades
S	Scoring	Puntuación
S	System	Sistema

Sistema común de puntuación de vulnerabilidades

nacap

¿Qué es un análisis de vulnerabilidad?

Este proceso implica identificar y evaluar vulnerabilidades en sistemas, redes o aplicaciones.

Las vulnerabilidades pueden ser debilidades en el diseño, implementación, configuración o uso de tecnologías que podrían ser explotadas por amenazas.

nacap

Fases Análisis Vulnerabilidad

Recopilación de información	- Identificación de activos: Enumerar todos los activos críticos de la organización, incluyendo hardware, software, datos y recursos humanos. - Evaluación de activos: Clasificar los activos según su importancia y criticidad para la operación del negocio.
Detección de vulnerabilidades	Escaneo de vulnerabilidades: Utilizar herramientas automatizadas y manuales para identificar vulnerabilidades en los sistemas y aplicaciones. Bases de datos de vulnerabilidades: Consultar bases de datos como CVE (Common Vulnerabilities and Exposures), NVD (National Vulnerability Database), y OWASP para obtener información sobre vulnerabilidades conocidas.
Evaluación de la severidad de las vulnerabilidades	Aplicar el sistema de puntuación CVSS para evaluar la gravedad de cada vulnerabilidad. CVSS mide tres grupos de métricas: Métricas básicas: Miden las cualidades intrínsecas de una vulnerabilidad. Métricas temporales: Ajustan la puntuación en función de factores temporales como la disponibilidad de exploits o parches. Métricas ambientales: Consideran las características del entorno de la organización que afectan la gravedad de la vulnerabilidad.

¿Qué es métrica?

Una métrica en seguridad de la información es una medida cuantitativa o cualitativa que se utiliza para evaluar el estado, rendimiento y efectividad de las políticas, controles y prácticas de seguridad dentro de una organización.

Las métricas permiten monitorear, comparar y tomar decisiones basadas en datos, con el fin de gestionar los riesgos, garantizar el cumplimiento de normativas y mejorar la postura de seguridad a lo largo del tiempo.



¿Qué es métrica?

Ejemplos de métricas en Seguridad de la Información
Métricas de desempeño: Miden la eficiencia de las medidas de seguridad implementadas. Por ejemplo, el tiempo promedio para detectar un incidente de seguridad o el tiempo que se tarda en aplicar un parche de seguridad.
Métricas de cumplimiento: Se utilizan para evaluar si se están cumpliendo las políticas y regulaciones de seguridad, como el porcentaje de usuarios que completan la formación en seguridad cibernética.
Métricas de incidentes: Se enfocan en los incidentes de seguridad y ayudan a comprender la frecuencia y la gravedad de estos, como el número de intentos de intrusión detectados o la cantidad de malware detectado en un periodo determinado.
Métricas de vulnerabilidad: Miden cuán vulnerables son los sistemas ante posibles amenazas, como el número de vulnerabilidades sin parchear o el tiempo promedio para remediar una vulnerabilidad.

nacap

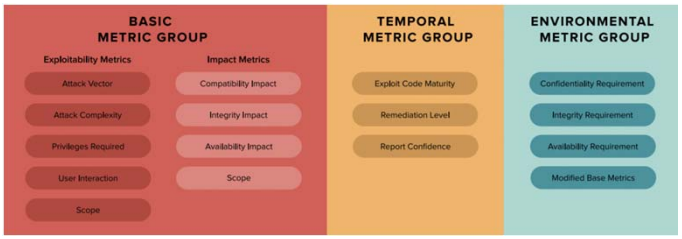
Herramienta de cálculo CVSS

CVSS proporciona una metodología estandarizada para evaluar la severidad de las vulnerabilidades, lo que permite a las organizaciones priorizar los riesgos y planificar las acciones de mitigación de manera eficiente.

Qué es CVSS

Es un sistema estándar para medir la gravedad de las vulnerabilidades en software y sistemas informáticos. Su objetivo es proporcionar una forma consistente y objetiva de calificar las vulnerabilidades, lo que ayuda a las organizaciones a priorizar la remediación de las amenazas según su nivel de riesgo.

Tiene tres componentes principales: Base, Temporal y Environmental. Cada uno de ellos proporciona diferentes niveles de evaluación.



Métricas CVSS

Métricas	Definición
Métricas base	Evalúan las propiedades intrínsecas de una vulnerabilidad
Métricas temporales	Ajustan la puntuación en función de factores como la disponibilidad del parche o la madurez del exploit.
Métricas Environmental (ambientales)	Refina aún más la puntuación para reflejar las necesidades específicas de entorno y seguridad de un organismo

Puntuaciones CVSS

Las puntuaciones base de CVSS se determinan mediante la evaluación de la explotabilidad de vulnerabilidades, el impacto en la Confidencialidad, Integridad y Disponibilidad y el alcance del efecto.

Factores como el Vector de Ataque, los Privilegios Requeridos y el posible impacto en todo el sistema se evalúan para generar una puntuación de gravedad entre 0 y 10.

Puntuaciones CVSS métricas base

Métricas base **Impacto: ¿Qué tan grave sería si un atacante explotara la vulnerabilidad? Se clasifica en tres áreas: Confidencialidad (C), Integridad (I), y Disponibilidad (A).**	
Confidencialidad ¿Qué tan comprometida estaría la confidencialidad de los datos?	Ninguno (0) : No hay impacto. Parcial (5) : Se puede acceder a parte de la información. Completo (10): Se accede a toda la información confidencial.
Integridad ¿Qué tan afectada sería la capacidad de mantener la integridad de los datos?	Ninguno (0) : No hay impacto. Parcial (5) : Se pueden modificar parcialmente los datos. Completo (10) : Los datos se pueden modificar completamente.
Disponiblidad ¿Qué tan afectada estaría la disponibilidad del sistema o servicio?	Ninguno (0): No hay impacto. Parcial (5): El sistema se ve afectado parcialmente, algunos servicios pueden no estar disponibles. Completo (10): El sistema completo es inaccesible.

Puntuaciones CVSS métricas base

Complejidad del Ataque (AC): ¿Qué tan difícil es explotar la vulnerabilidad?
Baja (10): Es fácil de explotar, no se requieren habilidades especiales ni configuración.
Alta (5): Requiere condiciones o configuraciones específicas o un mayor nivel de habilidad por parte del atacante.

nacap

Puntuaciones CVSS métricas base

Privilegios Requeridos (PR): ¿El atacante necesita privilegios previos para explotar la vulnerabilidad?
Ninguno (10): El atacante no necesita tener privilegios previos.
Bajos (5): El atacante necesita privilegios limitados (por ejemplo, una cuenta de usuario estándar)
Altos (0): El atacante necesita privilegios elevados (por ejemplo, administrador o root).

nacap

Puntuaciones CVSS métricas base

Vector de Ataque (AV): ¿Cómo se explota la vulnerabilidad?
Red (10): La vulnerabilidad se puede explotar de forma remota a través de la red.
Local (5): Se necesita acceso físico o local al sistema afectado
Adyacente (5): El atacante debe estar en una red local (por ejemplo, una red Wi-Fi compartida).
Físico (0): El atacante necesita tener acceso físico al dispositivo para explotarlo.

nacap

Puntuaciones CVSS métricas base

Interacción de Usuario (UI): ¿El atacante necesita que un usuario realice alguna acción?
Ninguna (10): El atacante puede explotar la vulnerabilidad sin intervención del usuario.
Requerida (5): El usuario necesita realizar alguna acción, como hacer clic en un enlace o abrir un archivo.

Puntuaciones CVSS Métricas temporal

Estas métricas se ajustan con el tiempo, teniendo en cuenta la existencia de parches, si la vulnerabilidad está siendo activamente explotada, etc. Se evalúan de la siguiente forma:

Exploitabilidad (E): ¿Existen herramientas para explotar la vulnerabilidad?
Ninguna (0): No existe un exploit conocido.
Baja (1): Existen exploits disponibles, pero no son fáciles de usar.
Alta (2): Existen exploits ampliamente disponibles.

nacap

Puntuaciones CVSS Métricas temporal

Solución Temporal (RL): ¿Hay alguna mitigación temporal disponible?
Ninguna (0): No hay solución temporal disponible.
Parcial (1): Hay una mitigación parcial.
Completa (2): Hay una solución temporal disponible que bloquea la vulnerabilidad.

nacap

Puntuaciones CVSS Métricas temporal

Fase de Madurez (RC): ¿El parche o la corrección está disponible?
No Corrección (0): No hay corrección disponible.
Parcial (1): Hay una corrección parcial disponible.
Completa (2): Hay una corrección disponible.

Puntaje Métricas de Impacto Ambiental

Estas métricas permiten ajustar el puntaje base de acuerdo con el impacto específico en un entorno particular, como la infraestructura de una organización.

Metricas impacto ambiental
Impacto de Confidencialidad, Integridad y Disponibilidad (C, I, A): Se ajustan de acuerdo a la importancia del sistema o servicio afectado en el entorno de la organización.
Modificador de Privilegios (PR) y Vector de Ataque (AV): También pueden ser ajustados dependiendo de cómo se aplica la vulnerabilidad en el entorno de la organización.

¿Y cómo se asignan puntajes?



nacap

1.- Evaluacion Impacto

Paso 1
Comienza asignando un valor para las métricas de impacto (Confidencialidad, Integridad, Disponibilidad) según la gravedad que tenga para el sistema o los datos comprometidos.
Luego, asigna el vector de ataque (AV), la complejidad del ataque (AC), los privilegios necesarios (PR), y si requiere o no interacción del usuario (UI).

nacap

2.- Sumar puntos

Paso 2
Calcula la puntuación base. Para esto, se suman los valores de las métricas que has asignado y se aplican las fórmulas matemáticas correspondientes (que están bien documentadas en el sitio oficial del CVSS).
El puntaje final se calcula utilizando una fórmula matemática que combina los valores de las métricas de impacto y las métricas de exploitabilidad.

3.-Ajustar con las Métricas Temporales y Ambientales:

Si la vulnerabilidad ya tiene un exploit conocido, o si existen soluciones o parches, se ajusta la puntuación temporalmente.
Finalmente, ajusta la puntuación según el impacto ambiental si es necesario.

CVSS **Base Score** (Puntuación Base)

La Base Score refleja la gravedad de la vulnerabilidad en un estado "normal", sin tener en cuenta factores que puedan cambiar con el tiempo o con el entorno. Se calcula a partir de varias métricas que describen las características de la vulnerabilidad, tales como:

Impacto: El daño que puede causar la vulnerabilidad si es explotada (por ejemplo, pérdida de confidencialidad, integridad o disponibilidad).

Explotabilidad: Qué tan fácil es para un atacante explotar la vulnerabilidad (por ejemplo, si requiere acceso remoto o si es necesaria la interacción del usuario).

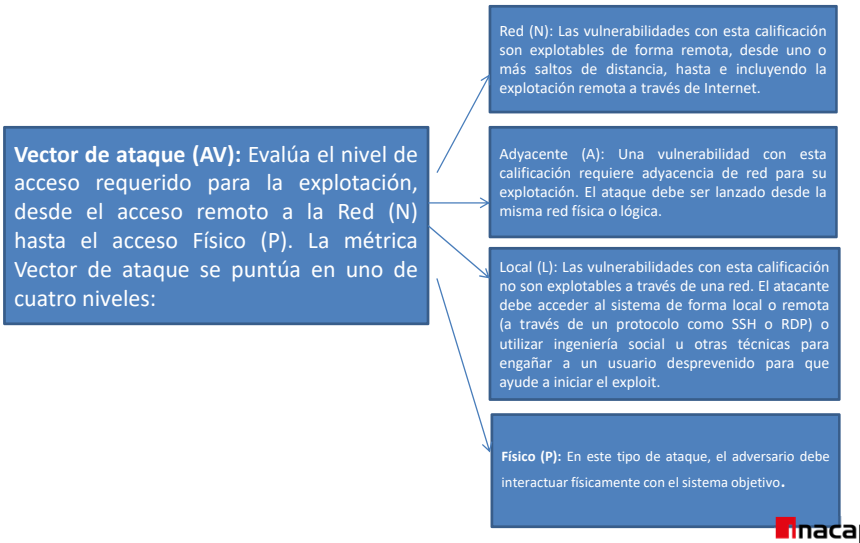
nacap

Métricas de puntuación base

Métrica	Traducción	Qué describe
Confidentiality (C)	Confidencialidad	¿Cuánto se ve afectada la confidencialidad del sistema? (Ninguna, Parcial, Completa)
Integrity (I)	Integridad	¿Cuánto se ve afectada la integridad del sistema? (Ninguna, Parcial, Completa)
Availability (A)	Disponiblidad	¿Cuánto se ve afectada la disponibilidad del sistema? (Ninguna, Parcial, Completa)
Attack Vector (AV):	Vector de ataque	¿Dónde y cómo se puede explotar la vulnerabilidad? (Red, Local, Físico, etc.)
Attack Complexity (AC)	Complejidad del ataque	¿Qué tan difícil es llevar a cabo el ataque? (Bajo, Alto)
Privileges Required (PR)	Privilegios requeridos	¿Qué privilegios o permisos son necesarios para explotar la vulnerabilidad?
User Interaction (UI)	Interacción de usuario	¿El ataque requiere interacción por parte de un usuario? (Ninguna, Requiere interacción)
Scope (S)	Alcance	¿La explotación de la vulnerabilidad afecta a la confidencialidad, integridad o disponibilidad de otros componentes? (No cambia, Cambia)

nacap

Métricas de Explotabilidad



Métricas complejidad de ataque

Complejidad de Ataque	Clasificación
mide la dificultad de explotación, con Baja (L) que no requiere condiciones especiales y Alta (H) que necesita condiciones previas específicas. Esta métrica indica condiciones más allá del control de los atacantes que deben existir para explotar la vulnerabilidad. Más comúnmente, esto se refiere a la interacción requerida del usuario o a configuraciones específicas del sistema de destino	Bajo (L): No se requieren condiciones previas específicas para la explotación.
	Alto (H): Las condiciones más allá del control de los atacantes deben existir para un ataque exitoso. Para este tipo de ataque, el atacante debe completar una serie de pasos preparatorios para obtener acceso. Esto podría incluir recopilar datos de reconocimiento, superar mitigaciones o convertirse en un hombre en el medio.

Métrica Privilegios requeridos

Privilegios requeridos	
Indica el nivel de privilegios que necesita el atacante, que van desde Ninguno (N) a Alto (H).	Ninguno (N): No se requiere ningún privilegio o acceso especial para llevar a cabo el ataque.
	Bajo (L): El atacante requiere privilegios básicos de nivel “user” para aprovechar el exploit.
	Alto (H): Se requieren privilegios de acceso administrativos o similares para un ataque exitoso.

nacap

Métricas de puntuación base

Con esta información, se genera un puntaje entre 0.0 y 10.0, donde: 0.0 indica una vulnerabilidad mínima o sin impacto.10.0 indica una vulnerabilidad crítica, con un alto impacto y fácil de explotar.



nacap

Temporal Score (Puntuación Temporal)

- La Temporal Score tiene en cuenta factores que pueden cambiar con el tiempo, como por ejemplo:

Tipo de factor	Descripción
Existencia de un parche	Si existe una solución disponible para mitigar la vulnerabilidad.
Explotación en el mundo real	Si ya se está explotando activamente esa vulnerabilidad en ataques reales.
Disponibilidad de una solución temporal	Si existen medidas de mitigación temporales.

nacap

Environmental Score (Puntuación Ambiental)

Environmental Score considera el contexto específico del entorno en el que se encuentra la vulnerabilidad. Factores como:

Importancia de los activos afectados: Si la vulnerabilidad afecta a un sistema crítico o a uno menos importante.

Control de mitigación existente: Si ya existen medidas de seguridad que reducen el impacto de la vulnerabilidad.

Este componente ayuda a ajustar la puntuación según las particularidades de la organización, proporcionando una visión más contextualizada del riesgo.

nacap

Ejemplo de cómo se calcula CVSS:

Supongamos una vulnerabilidad permite a un atacante ejecutar código arbitrario de manera remota sin autenticación.
Aquí la puntuación base podría ser:

- Impacto en Confidencialidad (C): Completo 10)
- Impacto en Integridad (I): Completo (10)
- Impacto en Disponibilidad (A): Completo (10)
- Vector de ataque (AV): Red (10)
- Complejidad de ataque (AC): Baja (10)
- Requerimiento de privilegios (PR): Ninguno (10)
- Interacción de usuario (UI): Ninguna (10)

Explicación caso anterior

Métrica	Grado	Descripción
Impacto en Confidencialidad (C):	10	"Impacto Completo" (10) significa que la vulnerabilidad permitiría al atacante acceder y obtener toda la información confidencial del sistema, sin restricciones.
Impacto en Integridad (I)	10	Un "Impacto Completo" (10) en Integridad implica que el atacante podría modificar o alterar completamente los datos en el sistema, afectando la confiabilidad y exactitud de la información.
Impacto en Disponibilidad (A)	10	Un "Impacto Completo" (10) en Disponibilidad significa que el atacante podría dejar el sistema completamente inoperativo o afectarlo de manera que no se pueda acceder a él.

Explicación caso anterior

Métrica	Grado	Descripción
Vector de ataque (AV): Red	10	Un Vector de ataque por Red (valor 10) significa que la vulnerabilidad puede ser explotada de forma remota a través de la red, es decir, sin necesidad de tener acceso físico al sistema afectado. Esto aumenta mucho el riesgo, ya que puede ser explotado desde cualquier lugar.
Complejidad de ataque (AC)	10	Un valor de Baja (10) implica que no se requieren habilidades especiales o un entorno particular para llevar a cabo el ataque. El atacante puede realizarlo sin grandes dificultades.
Requerimiento de privilegios (PR)	10	Un valor de Ninguno (10) significa que el atacante no necesita ningún privilegio especial. Puede llevar a cabo el ataque sin tener cuentas de usuario o permisos administrativos, lo que lo hace aún más peligroso.
Interacción de usuario (UI)	10	Un valor de Ninguna (10) significa que no se necesita ninguna intervención del usuario; el ataque se puede llevar a cabo de forma completamente automática por parte del atacante.

nacap

Implementación y monitoreo de controles

1. Planificación de la implementación
Priorizar vulnerabilidades: Basar la implementación de controles en la prioridad de las vulnerabilidades, comenzando por aquellas con puntuaciones CVSS más altas.
Asignación de recursos: Asegurar que se asignen los recursos necesarios para implementar los controles de mitigación de manera efectiva.

nacap

Implementación y monitoreo de controles

2. Monitoreo y revisión continua
Monitoreo de la efectividad: Establecer mecanismos para monitorear la efectividad de los controles implementados y realizar ajustes según sea necesario.
Reevaluación periódica: Realizar evaluaciones periódicas de vulnerabilidades y actualizar la matriz de riesgo para reflejar cambios en el entorno y en las amenazas.



Recuperación ante desastres

La mejora de las tecnologías en la recuperación ante desastres (DR, por sus siglas en inglés) es crucial para asegurar la continuidad del negocio y la protección de los activos críticos en caso de incidentes graves.



nacap

Planificación de la Recuperación ante Desastres (DRP)

¿Qué hacer?
Definición de requisitos: Identificar y documentar los requisitos específicos de recuperación ante desastres para cada sistema crítico y servicio de la organización.
Evaluación de riesgos: Realizar evaluaciones de riesgos para determinar las amenazas potenciales y los posibles impactos en las operaciones
Establecimiento de objetivos de recuperación: Definir objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO) para guiar la implementación de tecnologías de DR.

nacap

Tecnologías de Recuperación ante Desastres

Ejemplos
Replicación y redundancia Implementar tecnologías que permitan la replicación de datos y sistemas críticos en ubicaciones geográficamente dispersas para garantizar la disponibilidad continua.
Copia de seguridad y restauración Automatizar procesos de copia de seguridad y restauración para asegurar la integridad y disponibilidad de los datos críticos.
Virtualización y contenedores Utilizar virtualización y contenedores para facilitar la rápida recuperación y la migración de cargas de trabajo entre entornos de infraestructura.

Estandarización y mejores prácticas

Normativas y estándares	Auditorías y pruebas
Asegurarse de que las propuestas de mejoras tecnológicas cumplan con normativas y estándares relevantes de la industria, como ISO 22301 para la gestión de continuidad del negocio.	**Realizar auditorías periódicas y pruebas de recuperación ante desastres para validar la efectividad de las soluciones implementadas y garantizar la preparación del equipo ante emergencias.**

CAPACITACION	MEJORA CONTINUA
Entrenamiento del personal: Capacitar al personal en los procedimientos de recuperación ante desastres y en el uso de las tecnologías implementadas. Concienciación sobre la seguridad: Promover una cultura de seguridad informática que enfatice la importancia de la preparación para desastres y la protección de datos críticos.	Revisión periódica: Evaluar regularmente las capacidades de recuperación ante desastres y actualizar las propuestas de mejora tecnológica en función de nuevas amenazas y tecnologías emergentes. Feedback y ajustes: Utilizar retroalimentación del proceso de recuperación ante desastres e incidentes simulados para ajustar y mejorar continuamente las estrategias y tecnologías implementadas.