Área Tecnologías de Información y Ciberseguridad

nacap

Vulnerabilidad/Amenaza /Riesgo

Seguridad de la Información

nacap

Conceptos preliminares

Conceptos
VULNERABILIDAD
AMENAZA
RIESGO

nacap

Vulnerabilidad

Vulnerabilidad
Es una debilidad o falla en un sistema, aplicación, red o proceso que puede ser explotada por un atacante para comprometer la confidencialidad, integridad o disponibilidad de la información. vulnerabilidad es una puerta abierta que puede ser aprovechada para realizar un ataque.
Software: Errores en el código que permiten a un atacante ejecutar acciones no autorizadas.
Hardware: Deficiencias en los dispositivos físicos que pueden ser explotadas.
Procesos: Falta de políticas o procedimientos de seguridad que permitan a un atacante acceder a recursos sensibles.
Redes: Deficiencias en la infraestructura de red, como configuraciones inseguras o protocolos débiles.

Al identificar y corregir vulnerabilidades, las organizaciones pueden reducir el riesgo de sufrir ataques y proteger mejor sus activos y datos.

Amenazas

Amenazas
Es cualquier factor, evento o acción que tiene el potencial de causar daño o afectar negativamente la confidencialidad, integridad o disponibilidad de la información. Es una posible causa de un incidente de seguridad que puede explotar una vulnerabilidad en el sistema.
Amenazas naturales: Desastres naturales como terremotos, inundaciones, tormentas, incendios, etc., que pueden dañar los sistemas físicos y comprometer la información.
Humanas - Maliciosas: Son acciones deliberadas de individuos o grupos (por ejemplo, hackers, ciberdelincuentes) que intentan explotar vulnerabilidades para robar, alterar o destruir información.
Humanas -No maliciosas: Son eventos o acciones accidentales causadas por errores humanos, como la pérdida de un dispositivo de almacenamiento, el envío de un correo electrónico a la persona equivocada o la mala configuración de un sistema.
Amenazas tecnológicas: Se refieren a fallas o defectos en el hardware, software o infraestructura tecnológica que pueden ser explotados por atacantes, como un software desactualizado o fallos en la red.

Riesgo

Riesgo
Probabilidad de que una amenaza explote una vulnerabilidad y cause un daño o impacto a los activos de información. Posibilidad de que un incidente de seguridad afecte la confidencialidad, integridad o disponibilidad de los datos, sistemas o redes de una organización.

- Amenaza: Es cualquier evento o acción que pueda comprometer la seguridad de la información, como un ciberataque, un fallo de hardware, desastres naturales, o errores humanos.

- Vulnerabilidad: Son debilidades o fallos en los sistemas, procesos o controles de seguridad que pueden ser explotados por una amenaza para causar daño. Por ejemplo, una vulnerabilidad puede ser un software desactualizado que permite un acceso no autorizado.

- Impacto: Es el efecto o daño que ocurre si una amenaza explota una vulnerabilidad. Esto puede incluir la pérdida de datos sensibles, daño a la reputación de la empresa, o interrupciones en los servicios.

nacap

Riesgo

Fórmula general del riesgo
Riesgo = Probabilidad de la amenaza × Impacto del evento

Tipos de riesgos comunes en la seguridad de la información:
Riesgos de confidencialidad: Exposición no autorizada de datos sensibles, como el robo de información personal o empresarial.
Riesgos de integridad: Alteración o modificación no autorizada de la información, lo que puede llevar a decisiones erróneas o daños operacionales.
Riesgos de disponibilidad: Pérdida de acceso a los datos o sistemas, lo que puede paralizar operaciones, como en un ataque de denegación de servicio (DDoS).

nacap

Gestión del Riesgo

Gestión del Riesgo
L a gestión del riesgo en seguridad de la información implica identificar, evaluar y mitigar los riesgos para minimizar su impacto en los activos de la organización. Esto puede incluir:
- Prevención: Implementar medidas para reducir la probabilidad de que ocurra un incidente.
- Mitigación: Limitar las consecuencias de un incidente si llegara a suceder.
- Aceptación: Reconocer ciertos riesgos y decidir no tomar medidas adicionales si el impacto es bajo o manejable.

nacap

Gestión del Riesgo/ etapas

1.- Identificación del riesgo
- Definir objetivos corporativos y operativos (permitirá identificar eventos que potencien su capacidad de alcanzar los objetivos estratégicos de la organización)
- Inventario de los riesgos mas relevantes. El mejor proceso para listar los riesgos de manera rigurosa es crear una lista de chequeo para reconocerlos, hacer sesiones de brainstorming o entrevistas individuales con el equipo. La idea es reconocer todos los posibles riesgos: financieros, operativos, reputacionales, económicos, ambientales, tecnológicos y de fraude.
- Identificar factores de riesgo Causas probables de cada riesgo, es decir, aquellos factores que hicieron que el riesgo apareciera por primera vez. Es posible que se encuentre una o muchas causas, pero de cualquier forma lo importante es saber de dónde provienen.
- Especificar las medidas de control actuales Probablemente, algunos de los riesgos ya tengan algunas medidas y controles internos para mitigar su impacto. Con el fin de que sean efectivos, estos controles internos deben estar orientados por políticas, procedimientos o prácticas, esto permitirá saber si los controles existentes son adecuados o si es necesario implementar controles adicionales.
- Definir responsabilidades A cada riesgo le es asignado un responsable que garantice que los controles internos estén funcionando y que las acciones de tratamiento relevantes se lleven a cabo de manera oportuna. Estas asignaciones se realizan con el objetivo de monitorear regularmente un evento de riesgo y optimizarlo periódicamente.

nacap

Gestión del Riesgo

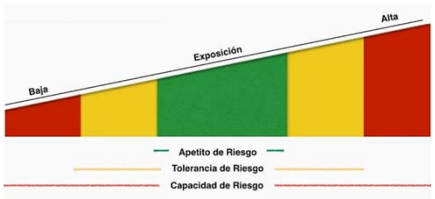
2. Evaluación de riesgos
- Evaluar la probabilidad de que ocurran los riesgos Para obtener el resultado de la evaluación de un riesgo, es necesario analizar la posibilidad de que un riesgo ocurra, teniendo en cuenta cada uno de los controles que están en funcionamiento. Recuerda que los criterios pueden ser diferentes para cada uno de los riesgos.
- Evaluar el impacto de los riesgos El impacto de un riesgo se calcula según el nivel de gravedad. Definir criterios para evaluarlo es más complejo que para calcular la probabilidad de que ocurran, pues en muchas ocasiones esta evaluación se realiza de manera cualitativa.
- Resultado final de evaluación El resultado final de combinar las evaluaciones de probabilidad y de impacto se obtiene multiplicando los coeficientes de cada una en una matriz de evaluación de riesgos. Dividir la matriz en bloques de colores ayuda a que quede más visible el resultado cuantitativo.
- Priorizar los riesgos y definir el apetito al riesgo Es difícil evitar todos los riesgos, por eso, deben priorizarse para saber cuáles deben ser tratados primero. Para esto define primero cuál es el nivel de apetito y de tolerancia de la organización a los riesgos. Al definir las prioridades, se puede tener un panorama complementario de los riesgos e identificar aquellos que son más urgentes.

nacap

Gestion del riesgo /Apetito del Riesgo

El apetito del riesgo en seguridad de la información es la cantidad de riesgo que una organización está dispuesta a aceptar o tolerar en sus actividades, procesos y sistemas, teniendo en cuenta sus objetivos, recursos y la necesidad de proteger sus activos de información.

Define los límites dentro de los cuales una organización está dispuesta a operar, considerando el impacto potencial que los riesgos pueden tener sobre sus activos, reputación o continuidad del negocio.



Apetito/ Tolerancia
Apetito del riesgo: Es la cantidad total de riesgo que una organización está dispuesta a aceptar a nivel general para alcanzar sus objetivos. Es una visión más estratégica y de largo plazo.
Tolerancia al riesgo: Es el nivel específico de riesgo que la organización puede aceptar en situaciones particulares sin comprometer su seguridad, operatividad o estabilidad. Es más detallada y se refiere a situaciones concretas.

nacap

Apetito/ Tolerancia/capacidad

Apetito del riesgo	Tolerancia al riesgo	Capacidad de Riesgo
Nivel de riesgo que la empresa quiere aceptar	tolerancia es la desviación respecto a este nivel.	La capacidad es el máximo de riesgo que una organización puede soportar en la persecución de sus objetivos.

Si una empresa está lanzando un nuevo producto, podría estar dispuesta a asumir un mayor riesgo en áreas como la tecnología o la innovación para aprovechar una oportunidad de mercado. Sin embargo, en términos de protección de datos personales de sus clientes, la empresa podría tener un apetito de riesgo muy bajo debido a las implicaciones legales y reputacionales que conlleva cualquier vulneración de esa información.

Gestión del Riesgo

3.-Tratamiento de los riesgos
- Define el tipo de respuesta al riesgo Hay cuatro formas de responder a un riesgo: tolerar, transferir, tratar y eliminar. La conveniencia de cada una depende de las características de cada riesgo y, sobre todo, del nivel de prioridad que se le asigne. Excepto para aquellos que se definen como tolerables, es necesario contar con un plan de acción que ayude a mitigar, prevenir, reducir o transferir el riesgo.
- Crea acciones para mitigar el impacto Crear un plan de mitigación para todos los riesgos que quieras tratar. El propósito de estas acciones no es eliminar los riesgos, sino reducirlos a un nivel aceptable. Asimismo, evalúa la relación costo-beneficio a la hora de tratar cada riesgo.