TECNOLOGIAS DE LA INFORMACION Y CUBERSEGURIDAD

Inacap

Evaluación de Vulnerabilidades y Matriz de Riesgo

Seguridad de la Información

Inacap

Introducción

Objetivo: Entender el proceso de evaluación de vulnerabilidades y cómo se construye una matriz de riesgo para proteger los activos de información.

Importancia: Permite priorizar acciones para reducir los riesgos y mejorar la ciberseguridad organizacional.

Inacap

Gestión de Riesgos

En esta fase se identifican los componentes de un sistema que requieren protección, se evalúan las vulnerabilidades que los debilitan y se analizan las amenazas que podrían ponerlos en peligro. El resultado de este análisis revela el nivel de riesgo al que se enfrenta el sistema.

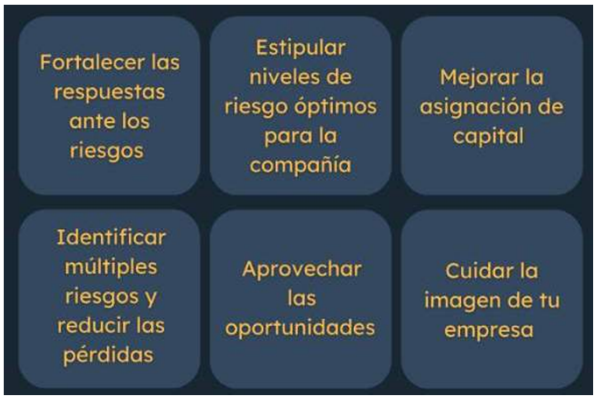
Clasificación:
En esta etapa se determina si los riesgos identificados son aceptables o no. Se evalúa la probabilidad de ocurrencia de los riesgos y el impacto que podrían tener en el sistema y en la organización en general.

En esta fase se monitorea el funcionamiento de las medidas de protección implementadas, evaluando su efectividad y asegurándose de que se cumplan correctamente. En caso de detectar deficiencias en las medidas, se realizan ajustes y se aplican sanciones en caso de incumplimiento.

Una vez clasificados los riesgos, se definen e implementan las medidas de protección necesarias. También se lleva a cabo la sensibilización y capacitación de los usuarios, para que estén conscientes de las medidas de seguridad y sepan cómo aplicarlas correctamente.

nacap

Objetivos



nacap

Evaluación de Riesgos

La evaluación de riesgos de seguridad de la información es un proceso en el cual se identifican, analizan, categorizan y priorizan las amenazas que pueden afectar el cumplimiento de los objetivos establecidos. A través de esta evaluación, se obtiene la información necesaria para tomar decisiones sobre cómo manejar dichos riesgos.

Específicamente, en el campo de la seguridad de la información, las evaluaciones de riesgos se centran en los activos de datos e información de la empresa. Por esta razón, la norma ISO 27001 requiere de manera explícita la realización de un proceso de gestión de riesgos para revisar y confirmar los controles de seguridad, en cumplimiento de las obligaciones regulatorias, legales y contractuales.

¿Para qué sirve un análisis de riesgos?

Aunque un análisis de riesgos no puede evitar que ocurran problemas, sí resulta útil para gestionarlos de manera efectiva dentro de la empresa y obtener una visión realista que considere tanto los aspectos positivos como los negativos. En resumen, un análisis de riesgos promueve una mayor confianza entre los involucrados, ya que brinda la certeza de que las decisiones y acciones tomadas son cuidadosamente evaluadas.

Además, el análisis de riesgos permite desarrollar planes de contingencia en caso de contratiempos que se opongan a lo planeado, lo cual facilita una respuesta adecuada y la implementación de acciones para superar la situación adversa.

Vertientes de un análisis de riesgos

Análisis Cualitativo	Análisis Cuantitativo
El análisis cualitativo de riesgos es una opción adecuada cuando no se dispone de una gran cantidad de datos para evaluar el riesgo, por lo que se opta por una valoración más subjetiva. En este enfoque, se tiene en cuenta el juicio personal y la experiencia acumulada hasta ese momento para considerar las amenazas del proyecto. Algunas técnicas utilizadas en el análisis cualitativo incluyen el brainstorming, cuestionarios, entrevistas, evaluación en grupos, opiniones de expertos y especialistas. Este enfoque es ideal cuando se carece de los recursos necesarios para llevar a cabo un análisis exhaustivo y suele ser utilizado por empresas pequeñas y medianas, cuyo nivel de riesgo también es bajo.	Utiliza métodos más precisos y basados en cálculos matemáticos. Requiere tiempo, personal y, en algunas ocasiones, inversión financiera para llevarlo a cabo. En este tipo de análisis, se asigna un valor numérico a las probabilidades de que algo ocurra, ya sea positivo o negativo. En ocasiones, se recomienda realizarlo después de un análisis cualitativo o de forma simultánea. Siempre que sea posible, se recomienda implementar un análisis cuantitativo de riesgos, ya que permite una evaluación más precisa de las amenazas que pueden afectar a los proyectos, ya que se basa en datos mensurables. En este análisis se utilizan herramientas como listas de verificación, matrices de control y software de gestión de riesgos.

Matriz de riesgos

La matriz de riesgos es la herramienta indicada para entender los riesgos que corre la organización. Permite comparar por nivel de riesgos las distintas tareas que se llevan a cabo. Una vez que se cuente con esa información, es posible poder tomar acciones concretas para la solución completa o disminución de los mismos.

Los riesgos son distintas situaciones o tópicos que ponen en peligro la integridad de una organización. Tanto el ámbito material, como la salud de las personas, pueden estar en riesgo.

Como realizar una matriz de riesgos

El proceso general de una matriz de riesgos cuenta con cinco pasos generales:

- Identificación de riesgos
- Cálculo de exposición al riesgo
- Identificación de controles
- Cálculo de riesgo residual
- Aceptación o rechazo del riesgo residual

Elementos de la matriz de riesgos informáticos

Concepto	Definición
Actividad	Se explicita la actividad o tarea que realizan los trabajadores de la empresa. Siempre conviene tener un listado de todas las actividades que se llevan a cabo, sean estas rutinarias o no. Es un plus poder llenar esta sección con la participación misma de los trabajadores.
Probabilidad	Las posibilidades de que el riesgo se convierta en una realidad, de que llegue a producir el daño potencial. Puede expresarse de manera cualitativa o cuantitativa. Es decir, con conceptos generados (poco posible, muy posible, nulo) o directamente en números, si es cuantitativo.
Riesgo	Es la situación o evento, el cual es incierto, pero se sabe que tiene un impacto negativo. También se puede conceptualizar como la posibilidad de sufrir un daño de tipo físico o material por la exposición a un peligro específico.
Peligro	Es de donde viene el riesgo. La situación u objeto específico.
Magnitud de daño / Severidad	s el índice que indicará que nivel de impacto que habrá si este peligro potencial termina concretándose.

Matriz de riesgos

Matriz de Riegos		Probabilidad de amenaza					
Elementos de informacion	Magnitud daño	Criminalidad		Sucesos fisicos		Negligencia	
		Robo	Virus	Incendio	Falta energia	Compartir contraseñas	No cifrar datos
		3	4	2	3	4	3
Datos e informacion							
RRHH	3	9	12	6	9	12	9
Finanzas	4	12	16	8	12	16	12
Sistemas de Información							
Computadores	2	6	8	4	6	8	6
Laptops	3	9	12	6	9	12	9
Personal							
Coordinador	4	12	16	8	12	16	12
personal Técnico	3	9	12	6	9	12	9

Administración de los Riesgos relevantes identificados

Una vez identificados los riesgos que no cumplen con los criterios de aceptabilidad, se iniciará para éstos el proceso de administración del riesgo, el cual contempla las siguientes etapas:

- Identificar las medidas para la Administración de Riesgos.
- Evaluar la viabilidad de las medidas para la Administración de Riesgos.
- Preparar los planes para las medidas de Administración de Riesgos.
- Implementación de las medidas para la Administración de Riesgos.

Identificar las medidas para la Administración de Riesgos

Se definirán, según el orden de priorización determinado durante el proceso de evaluación del riesgo, las diferentes medidas que puedan existir para administrar el riesgo.

Evitar el riesgo	**No ejecutar las acciones que involucran la materialización del riesgo.** **Esta decisión se debe analizar con mucho cuidado, ya que, de no definirse adecuadamente, puede aumentar la exposición de otros riesgos. Todos los riesgos que seleccionen bajo este criterio deben ser adecuadamente documentados e informados a la Administración Superior.**

Identificar las medidas para la Administración de Riesgos

Reducir la probabilidad	**Definición de medidas que colaboren con la minimización de la probabilidad presentada, a través de la evaluación del riesgo controlado, como revisiones preventivas y condiciones contractuales, entre otros.**

Identificar las medidas para la Administración de Riesgos

Reducir consecuencia	Definición de medidas que colaboren con la minimización de la consecuencia presentada a través de la evaluación del riesgo controlado, como planeamiento de contingencia y planes de recuperación, entre otros.

Identificar las medidas para la Administración de Riesgos

Transferir el riesgo	Definir medidas mediante las cuales, terceros asuman parte o la totalidad del riesgo que se desea administrar, por ejemplo, la adquisición de seguros.

Evaluar la viabilidad de las Medidas para la Administración de Riesgos

Se deberá analizar la viabilidad de cada una de las medidas de administración del riesgo que han sido propuestas, con la finalidad de seleccionar y priorizar las medidas que mejor se ajustan a la ejecución de planes de acción propuestos para cada riesgo tecnológico que se ha identificado.

Criterios de evaluación
La relación costo-beneficio de llevar a cabo la recomendación de la medida de mitigación.
La capacidad e idoneidad de los entes participantes, internos y externos.
El cumplimiento del interés público
La viabilidad jurídica, técnica y operacional de las alternativas propuestas para mitigar el riesgo.

Importante

Las medidas de control para la administración del riesgo se priorizarán sobre la base la base de aquellas que satisfagan de la mejor manera posible estos criterios de evaluación y permitan asegurar el cumplimiento de los objetivos de los procesos, que se pueden estar viendo afectados por dichos incidentes o riesgos.

Preparar los planes para las Medidas de Administración de Riesgos

Para cada una de las medidas, cuya viabilidad haya sido definida como apropiada, se deberá registrar los acuerdos establecidos como tratamientos y planes de acción que pretendan mitigar los riesgos.

Para rastrear los riesgos identificados, los riesgos residuales y los nuevos riesgos, así como realizar una revisión con el fin de mejorar la gestión del riesgo, se deben de implementar los planes de respuesta al riesgo.

Seguimiento y monitoreo

Debe existir personal de Gestión de Riesgo que realice las auditorías de riesgos para garantizar los resultados de las respuestas a riesgos para que sean eficaces y que los procesos de riesgos se realicen.

Una herramienta técnica que funciona para el proceso de seguimiento y control de los riesgos es realizar las siguientes actividades:

- Gestionar los recursos asignados para Contingencia (lo que se ha gestionado en forma separada para cubrir riesgos relacionados al tiempo y al costo).
- Rastrear el conjunto de condiciones (Disparadores) que se asignaron a cada riesgo.
- Rastrear el riesgo.
- Rastrear el cumplimiento que se definió en el Plan de Gestión de Riesgo.