Facultad de Ingeniería

Análisis de riesgo

Apunte de cátedra

Contenido

4. Análisis de riesgos

La Seguridad Informática tiene como finalidad proteger los activos de información de una organización frente a diversos eventos que puedan comprometer su confidencialidad, integridad o disponibilidad. Sin embargo, no todos los activos poseen el mismo valor ni todas las amenazas representan el mismo nivel de peligro. Por ello, antes de implementar medidas de protección, resulta necesario identificar cuáles son los riesgos existentes y determinar cuáles requieren mayor atención.

El **análisis de riesgos** es el proceso mediante el cual una organización identifica sus activos, reconoce las amenazas y vulnerabilidades que pueden afectarlos, evalúa las posibles consecuencias y establece prioridades para la implementación de controles de seguridad. Este proceso permite optimizar los recursos disponibles y orientar las inversiones hacia los riesgos más significativos.

En la actualidad, el análisis de riesgos constituye una actividad fundamental dentro de cualquier Sistema de Gestión de Seguridad de la Información (SGSI) y forma parte de normas y metodologías ampliamente utilizadas, como ISO/IEC 27005, MAGERIT y OCTAVE.

4.1. Introducción al Riesgo

La seguridad absoluta no existe. Ningún sistema informático puede garantizar que estará completamente protegido frente a todas las amenazas posibles. Siempre existirá la posibilidad de que ocurra un incidente capaz de afectar el funcionamiento de la organización.

Por esta razón, las organizaciones deben identificar los riesgos a los que están expuestas y establecer mecanismos para reducirlos hasta niveles aceptables. El análisis de riesgos proporciona una metodología sistemática para conocer esos riesgos y tomar decisiones fundamentadas sobre las medidas de seguridad que deben implementarse.

Es importante comprender que el análisis de riesgos no busca eliminar completamente todos los riesgos, ya que ello sería técnica y económicamente inviable. Su propósito consiste en identificar los riesgos existentes, evaluar su importancia y determinar la mejor estrategia para tratarlos.

El análisis de riesgos es un proceso continuo. Los sistemas informáticos evolucionan constantemente: aparecen nuevas amenazas, se incorporan tecnologías, cambian los procesos de negocio y surgen nuevas vulnerabilidades. Como consecuencia, los riesgos también cambian y deben ser evaluados periódicamente.

4.1.1. Concepto de Riesgo

En el ámbito de la Seguridad Informática, un **riesgo** es la posibilidad de que una amenaza aproveche una vulnerabilidad y produzca un incidente capaz de generar consecuencias negativas sobre uno o más activos de información.

En otras palabras, el riesgo representa la combinación entre la probabilidad de que ocurra un evento y el impacto que dicho evento tendría sobre la organización.

Una definición ampliamente aceptada establece que:

Riesgo = Probabilidad × Impacto

Esta expresión no debe interpretarse como una fórmula matemática exacta, sino como una forma sencilla de comprender que un riesgo depende de dos factores fundamentales:

- la posibilidad de que ocurra un incidente;
- las consecuencias que produciría si llegara a materializarse.

Por ejemplo, una empresa puede considerar que existe el riesgo de perder información debido a un ataque de ransomware. La probabilidad dependerá de factores como el nivel de exposición a Internet, las vulnerabilidades presentes y las medidas de protección implementadas. El impacto estará relacionado con la importancia de la información afectada, el tiempo de recuperación y las pérdidas económicas derivadas del incidente.

El análisis conjunto de ambos factores permite determinar qué riesgos requieren atención inmediata y cuáles pueden ser aceptados o tratados posteriormente.

4.1.1.1. Características del riesgo

El riesgo presenta diversas características que deben ser consideradas durante su análisis.

Es incierto

El riesgo hace referencia a un evento que podría ocurrir en el futuro. No existe certeza de que el incidente llegue a producirse, aunque sí existe la posibilidad de que ocurra.

Puede variar con el tiempo

El nivel de riesgo no permanece constante. La aparición de nuevas amenazas, la incorporación de tecnologías, la implementación de controles de seguridad o los cambios en los procesos de negocio pueden aumentar o disminuir el riesgo existente.

Por este motivo, el análisis de riesgos debe actualizarse periódicamente.

Depende del contexto

Un mismo riesgo puede tener consecuencias diferentes según la organización.

Por ejemplo, una interrupción de treinta minutos en el servicio informático puede representar una molestia menor para una pequeña empresa, mientras que para un banco o un hospital podría generar importantes pérdidas económicas y afectar la prestación de servicios esenciales.

Esto demuestra que el análisis de riesgos siempre debe realizarse considerando las características particulares de cada organización.

Puede gestionarse

Aunque no siempre es posible eliminar un riesgo, sí es posible reducir su probabilidad, disminuir su impacto o adoptar medidas para administrarlo adecuadamente.

Esta capacidad de gestión constituye uno de los principios fundamentales de la Seguridad Informática.

4.1.1.2. Ejemplo

Supóngase que una universidad almacena toda la información académica de sus estudiantes en un servidor. Una amenaza podría ser un ataque de ransomware que cifre la base de datos institucional.

Si el servidor presenta vulnerabilidades sin corregir y no existen copias de seguridad recientes, el riesgo será elevado debido a que:

- existe una posibilidad real de que el ataque ocurra;
- el impacto sobre la institución sería muy importante, ya que podrían perderse temporalmente los registros académicos y verse afectados los servicios administrativos.

En cambio, si la universidad mantiene los sistemas actualizados, utiliza autenticación multifactor para los administradores y dispone de copias de seguridad verificadas, la probabilidad de éxito del ataque disminuirá y, en caso de producirse, el impacto también será considerablemente menor.

Este ejemplo muestra que el riesgo no depende únicamente de la existencia de una amenaza, sino también de las vulnerabilidades presentes y de las medidas de protección implementadas.

4.1.2. Finalidad, Objetivos e Importancia del Análisis de Riesgos

El análisis de riesgos constituye una actividad esencial dentro de la gestión de la seguridad de la información. Su finalidad es proporcionar a la organización una visión clara de los riesgos que pueden afectar a sus activos, permitiendo tomar decisiones fundamentadas sobre las medidas de protección que deben implementarse.

Toda organización dispone de recursos limitados, ya sean económicos, humanos o tecnológicos. Por ello, resulta necesario establecer prioridades y destinar los esfuerzos hacia aquellos riesgos que podrían ocasionar mayores pérdidas o afectar el cumplimiento de los objetivos del negocio.

A diferencia de un enfoque reactivo, en el que las medidas de seguridad se implementan después de que ocurre un incidente, el análisis de riesgos permite actuar de forma preventiva, identificando anticipadamente las situaciones que representan un peligro para la organización y definiendo acciones para reducirlas hasta niveles aceptables.

Además, el análisis de riesgos no constituye una actividad aislada. Los riesgos evolucionan con el tiempo debido a la aparición de nuevas amenazas, la incorporación de tecnologías, los cambios en los procesos de negocio y las modificaciones en la infraestructura informática. Por este motivo, debe realizarse de manera periódica como parte de un proceso de mejora continua.

En la actualidad, el análisis de riesgos forma parte de las principales normas y metodologías de seguridad de la información, como **ISO/IEC 27005**, **MAGERIT** y **OCTAVE**, constituyendo uno de los pilares de los Sistemas de Gestión de Seguridad de la Información (SGSI).

4.1.2.1. Objetivos del análisis de riesgos

El análisis de riesgos persigue diversos objetivos, entre los que se destacan:

- conocer el nivel de exposición al riesgo de la organización;
- facilitar la toma de decisiones relacionadas con la seguridad;
- optimizar la utilización de los recursos disponibles;
- reducir la probabilidad y el impacto de los incidentes de seguridad;
- contribuir al cumplimiento de normas y estándares internacionales;
- favorecer la mejora continua de la seguridad de la información.

Estos objetivos permiten que las medidas de seguridad se implementen de forma planificada, priorizando los riesgos que representan un mayor impacto para la organización.

4.1.3. Riesgo, Amenaza, Vulnerabilidad e Incidente de Seguridad

En el ámbito de la Seguridad Informática es frecuente utilizar términos como **riesgo**, **amenaza**, **vulnerabilidad** e **incidente de seguridad**. Aunque estos conceptos están estrechamente relacionados, representan ideas diferentes y es importante comprender su significado para realizar correctamente un análisis de riesgos.

De manera general, la relación entre estos conceptos puede resumirse de la siguiente forma:

Un activo puede estar expuesto a una o más amenazas. Si una amenaza aprovecha una vulnerabilidad, puede producirse un incidente de seguridad que genere un impacto sobre el activo. La posibilidad de que esto ocurra constituye el riesgo.

4.1.3.1. Riesgo

El **riesgo** es la posibilidad de que una amenaza aproveche una vulnerabilidad y produzca un incidente de seguridad que afecte a uno o más activos de la organización.

El nivel de riesgo depende, principalmente, de dos factores:

- la probabilidad de que el incidente ocurra;
- el impacto que produciría sobre la organización.

Por esta razón, el riesgo suele expresarse como una combinación de ambos elementos.

4.1.3.2. Amenaza

Una **amenaza** es cualquier evento, circunstancia o agente con capacidad para causar un daño a un activo de información.

Las amenazas pueden tener distintos orígenes, como fenómenos naturales, errores humanos, fallas técnicas o acciones intencionales realizadas por personas. Por sí sola, una amenaza no implica necesariamente que se produzca un incidente. Para ello, generalmente debe existir una vulnerabilidad que pueda ser explotada.

4.1.3.3. Vulnerabilidad

Una **vulnerabilidad** es una debilidad o deficiencia presente en un activo, en un sistema o en un procedimiento que puede ser aprovechada por una amenaza.

Las vulnerabilidades pueden originarse por diversas causas, entre ellas:

- errores de configuración;
- software desactualizado;
- contraseñas débiles;
- ausencia de procedimientos;
- falta de capacitación del personal.

Cuantas más vulnerabilidades posea un activo, mayor será la probabilidad de que una amenaza logre materializarse.

4.1.3.4. Incidente de Seguridad

Un **incidente de seguridad** es un evento que compromete, o tiene el potencial de comprometer, la confidencialidad, integridad o disponibilidad de la información o de los sistemas informáticos.

Los incidentes representan la materialización de un riesgo y pueden producir pérdidas económicas, interrupción de los servicios, daño reputacional o incumplimiento de obligaciones legales. No todos los incidentes tienen la misma gravedad; su impacto

dependerá de los activos afectados y de las consecuencias que generen para la organización.

4.1.3.5. Relación entre los conceptos

Los cuatro conceptos estudiados se encuentran estrechamente relacionados y forman parte del proceso de análisis de riesgos.

La siguiente secuencia resume dicha relación:

Activo → Amenaza → Vulnerabilidad → Incidente → Impacto → Riesgo

4.1.3.6. Ejemplo integrador

Supóngase que una universidad almacena toda la información académica de sus estudiantes en un servidor.

- El **activo** es el servidor que contiene la base de datos académica.
- La **amenaza** es un ataque de ransomware.
- La **vulnerabilidad** consiste en que el sistema operativo del servidor no ha sido actualizado y presenta fallas de seguridad conocidas.
- El **incidente de seguridad** ocurre cuando el atacante aprovecha esa vulnerabilidad y cifra toda la información almacenada.
- El **impacto** se manifiesta en la interrupción de los servicios académicos, la imposibilidad de acceder a las calificaciones y los costos asociados a la recuperación de la información.
- El **riesgo** corresponde a la posibilidad de que este escenario ocurra y a las consecuencias que tendría para la universidad.

Este ejemplo muestra que los conceptos de activo, amenaza, vulnerabilidad, incidente e impacto forman parte de una misma secuencia lógica. Comprender esta relación resulta fundamental para realizar correctamente un análisis de riesgos.

4.1.4. Riesgo Inherente y Riesgo Residual

Durante el análisis de riesgos es importante distinguir entre el riesgo que existe antes de implementar medidas de seguridad y el riesgo que permanece una vez que dichas medidas han sido aplicadas. Esta diferencia permite evaluar la efectividad de los controles de seguridad y determinar si el nivel de riesgo alcanzado resulta aceptable para la organización. Por este motivo, en la gestión de riesgos se utilizan los conceptos de **riesgo inherente** y **riesgo residual**.

4.1.4.1. Riesgo Inherente

El **riesgo inherente** es el nivel de riesgo al que está expuesto un activo antes de implementar cualquier medida de protección o control de seguridad.

Representa la situación inicial, considerando únicamente la probabilidad de que una amenaza aproveche una vulnerabilidad y el impacto que produciría sobre la organización.

En otras palabras, responde a la siguiente pregunta:

¿Qué nivel de riesgo existiría si no se aplicara ningún control de seguridad?

El conocimiento del riesgo inherente permite identificar cuáles son los activos más expuestos y establecer prioridades para la implementación de medidas de protección.

4.1.4.2. Ejemplo

Una empresa almacena toda su información financiera en un servidor conectado a Internet. El servidor presenta varias vulnerabilidades conocidas, no posee autenticación multifactor y no existen copias de seguridad recientes.

En estas condiciones, el riesgo de sufrir un ataque de ransomware es elevado.

Este nivel de exposición corresponde al **riesgo inherente**, ya que todavía no se han implementado controles de seguridad para reducirlo.

4.1.4.3. Riesgo Residual

El **riesgo residual** es el nivel de riesgo que permanece después de implementar los controles de seguridad seleccionados por la organización.

Ningún control elimina completamente el riesgo. Siempre existe la posibilidad de que ocurra un incidente, aunque su probabilidad o su impacto hayan disminuido considerablemente. Por esta razón, toda organización debe determinar si el riesgo residual resulta aceptable o si es necesario incorporar nuevas medidas de protección.

En otras palabras, el riesgo residual responde a la pregunta:

¿Cuál es el nivel de riesgo que permanece después de aplicar los controles de seguridad?

4.1.4.4. Ejemplo

Continuando con el ejemplo anterior, la empresa decide implementar las siguientes medidas:

- autenticación multifactor para los administradores;
- actualización del sistema operativo;
- copias de seguridad diarias;
- software de protección contra malware.

Como consecuencia, disminuye la probabilidad de que un atacante logre comprometer el servidor y, si el incidente llegara a producirse, las copias de seguridad permitirían recuperar la información en un tiempo reducido.

El riesgo existente después de aplicar estas medidas corresponde al **riesgo residual**.

4.1.4.5. Comparación entre riesgo inherente y riesgo residual

La diferencia entre ambos conceptos puede resumirse en la siguiente tabla.

Característica	Riesgo inherente	Riesgo residual
Momento de evaluación	Antes de implementar controles	Después de implementar controles
Controles de seguridad	No se consideran	Sí se consideran
Nivel de riesgo	Generalmente mayor	Generalmente menor
Finalidad	Conocer la exposición inicial	Determinar el riesgo que permanece

4.2. Activos de Información

Toda organización posee recursos que resultan esenciales para el desarrollo de sus actividades. Estos recursos tienen un valor para la organización y, por lo tanto, deben ser protegidos frente a las amenazas que puedan comprometer su funcionamiento. En el ámbito de la Seguridad Informática, estos recursos reciben el nombre de **activos de información**. La correcta identificación y valoración de los activos constituye el punto de partida de cualquier análisis de riesgos, ya que no es posible proteger aquello que no se conoce.

Es importante destacar que un activo no se limita únicamente a los equipos informáticos o a la información almacenada en ellos. También forman parte de los activos las personas, los servicios, las aplicaciones, la documentación y cualquier otro elemento cuyo compromiso pueda afectar el cumplimiento de los objetivos de la organización.

4.2.1. Concepto de Activo

Un **activo** es cualquier recurso que posee valor para una organización y cuya pérdida, alteración, divulgación no autorizada o indisponibilidad puede generar consecuencias negativas.

En seguridad de la información, el valor de un activo no depende únicamente de su costo económico. Un activo puede ser muy valioso porque contiene información crítica, porque permite la continuidad de un servicio o porque resulta indispensable para el funcionamiento de la organización.

Por ejemplo, una base de datos de clientes puede tener un valor muy superior al del servidor donde se encuentra almacenada, ya que la información representa uno de los recursos más importantes para la empresa.

En consecuencia, el análisis de riesgos debe considerar tanto los activos tangibles como los intangibles.

4.2.1.1. Características de un activo

Los activos de información presentan una serie de características comunes que permiten comprender su importancia dentro de la organización.

Poseen valor para la organización

Todo activo contribuye, de una u otra forma, al cumplimiento de los objetivos institucionales. Su valor puede ser económico, operativo, legal o estratégico.

Deben ser protegidos

Los activos pueden verse afectados por amenazas naturales, accidentales o intencionales. Por este motivo, requieren la implementación de medidas de seguridad adecuadas para preservar su confidencialidad, integridad y disponibilidad.

Pueden depender de otros activos

En muchas ocasiones, un activo necesita de otros para poder funcionar correctamente.

Por ejemplo, una aplicación de gestión depende del servidor donde se ejecuta, de la base de datos que almacena la información y de la red que permite el acceso de los usuarios.

Esta relación de dependencia resulta importante durante el análisis de riesgos, ya que un incidente sobre un activo puede afectar indirectamente a otros.

Requieren una valoración

No todos los activos poseen la misma importancia. Por ello, durante el análisis de riesgos será necesario determinar cuáles son los activos más críticos para la organización y asignarles una valoración acorde con su importancia.

Ejemplo

Considérese una universidad que dispone de un sistema informático para la gestión académica.

Entre sus activos pueden identificarse los siguientes:

- la base de datos de estudiantes;
- el servidor donde se ejecuta el sistema;
- la aplicación de gestión académica;
- la red institucional;
- la documentación técnica;
- el personal responsable de administrar el sistema.

Aunque todos estos elementos forman parte del sistema de información, no poseen el mismo valor para la organización. La pérdida de la base de datos académica, por ejemplo, tendría un impacto considerablemente mayor que la pérdida de un equipo de uso administrativo. Este ejemplo pone de manifiesto la necesidad de identificar y valorar adecuadamente los activos antes de comenzar el análisis de riesgos.

4.2.2. Clasificación de los Activos

Los activos pueden clasificarse de diferentes maneras según el criterio utilizado. Una clasificación adecuada facilita su identificación, organización y posterior valoración durante el análisis de riesgos.

No existe una única clasificación universal; sin embargo, la mayoría de las metodologías y normas internacionales agrupan los activos en categorías similares.

4.2.2.1. Información

La información constituye el activo más importante para la mayoría de las organizaciones. Puede encontrarse almacenada en formato digital o físico e incluye bases de datos, documentos, registros, contratos, historiales, planos, informes y cualquier otro conjunto de datos relevante para el funcionamiento de la organización.

La protección de este activo constituye el principal objetivo de la Seguridad de la Información.

4.2.2.2. Hardware

Comprende todos los dispositivos físicos utilizados para el procesamiento, almacenamiento y transmisión de la información.

Entre ellos pueden mencionarse:

- servidores;
- computadoras personales;
- notebooks;
- dispositivos móviles;
- equipos de red;
- dispositivos de almacenamiento;
- impresoras.

La pérdida o el deterioro del hardware puede afectar la disponibilidad de los servicios informáticos.

4.2.2.3. Software

Incluye todos los programas utilizados por la organización para desarrollar sus actividades.

Entre ellos se encuentran:

- sistemas operativos;
- aplicaciones de gestión;
- bases de datos;
- software de seguridad;
- herramientas de desarrollo;
- aplicaciones ofimáticas.

El software puede presentar vulnerabilidades que incrementen el nivel de riesgo si no se mantiene correctamente actualizado.

4.2.2.4. Servicios

Los servicios representan las funciones que permiten el funcionamiento normal de la organización.

Por ejemplo:

- servicio de correo electrónico;
- servicio web institucional;
- acceso a Internet;
- servicio de autenticación;
- almacenamiento en la nube.

La interrupción de estos servicios puede afectar significativamente la continuidad de las actividades.

4.2.2.5. Personas

Las personas también constituyen un activo fundamental.

Se incluyen:

- usuarios;
- administradores;
- personal técnico;
- directivos;
- proveedores;
- consultores.

Además de utilizar los sistemas, las personas intervienen en la toma de decisiones, la administración de la información y la aplicación de los controles de seguridad.

4.2.2.6. Instalaciones e infraestructura

Comprenden los espacios físicos y la infraestructura necesaria para el funcionamiento de los sistemas informáticos.

Por ejemplo:

- centros de datos;
- salas de servidores;
- oficinas;
- cableado estructurado;
- sistemas eléctricos;
- sistemas de climatización.

4.2.3. Valoración de Activos

Una vez identificados los activos de información, es necesario determinar la importancia que cada uno tiene para la organización. Este proceso recibe el nombre de **valoración de activos**.

La valoración permite conocer cuáles son los activos más importantes y establecer prioridades para su protección. De esta forma, la organización puede asignar sus recursos de seguridad de manera más eficiente, concentrando los esfuerzos en aquellos activos cuya pérdida o afectación produciría mayores consecuencias.

La valoración de activos constituye una de las primeras etapas del análisis de riesgos y está presente en las principales metodologías de gestión de riesgos, como **MAGERIT**, **ISO/IEC 27005**, **OCTAVE** y **NIST SP 800-30**.

4.2.3.1. Concepto de Valoración de Activos

La **valoración de activos** consiste en determinar la importancia que posee un activo para la organización considerando las consecuencias que tendría su pérdida, alteración, destrucción o indisponibilidad.

El objetivo de la valoración no es establecer el precio económico del activo, sino medir el impacto que produciría sobre la organización si dicho activo dejara de cumplir correctamente su función. Por esta razón, dos activos con un costo económico similar pueden tener valores muy diferentes desde el punto de vista de la seguridad.

Por ejemplo, una computadora utilizada para tareas administrativas puede tener un valor inferior al de un servidor que almacena la base de datos institucional, aunque ambos equipos tengan un costo de adquisición semejante. La diferencia radica en el impacto que produciría la pérdida de cada uno de ellos.

4.2.3.2. Criterios para valorar un activo

No existe un único criterio para valorar un activo. Cada organización puede definir los aspectos que considere más relevantes según sus necesidades y el tipo de información que administra.

Entre los criterios más utilizados se encuentran los siguientes:

Valor económico

Corresponde al costo de adquisición, mantenimiento o reemplazo del activo. Este criterio suele aplicarse principalmente a los activos físicos, como servidores, equipos de comunicaciones o dispositivos de almacenamiento. Sin embargo, el valor económico no siempre refleja la verdadera importancia del activo para la organización.

Importancia para la operación

Evalúa el grado en que el activo resulta necesario para el funcionamiento normal de la organización. Un activo cuya indisponibilidad interrumpa procesos críticos tendrá una valoración superior a otro cuya ausencia genere únicamente inconvenientes menores.

Valor de la información

Cuando el activo contiene información, resulta necesario considerar el valor de dicha información.

Entre los aspectos más importantes se encuentran:

- la **confidencialidad** de los datos;
- la **integridad** de la información;
- la **disponibilidad** requerida para el normal desarrollo de las actividades.

Estas tres propiedades constituyen la base de la seguridad de la información y son utilizadas por la mayoría de las metodologías de análisis de riesgos para valorar activos de información.

Requisitos legales y normativos

Algunos activos contienen información cuya protección se encuentra regulada por leyes, contratos o normas específicas. La pérdida o divulgación de esta información puede generar sanciones legales, responsabilidades administrativas o perjuicios económicos para la organización.

Impacto sobre la imagen institucional

Existen activos cuya pérdida puede afectar la reputación o la confianza que clientes, proveedores o ciudadanos depositan en la organización. En muchos casos, el daño reputacional puede resultar incluso más importante que las pérdidas económicas directas.

4.2.3.3. Valoración mediante la tríada CIA

En muchas metodologías de análisis de riesgos, el valor de un activo se determina evaluando la importancia de sus tres propiedades fundamentales:

- Confidencialidad.

- Integridad.
- Disponibilidad.

Cada propiedad recibe una puntuación según una escala previamente definida por la organización.

Por ejemplo:

Valor	Nivel
0	Sin importancia
1	Muy baja
2	Baja
3	Media
4	Alta
5	Muy alta

Supóngase que se desea valorar una serie de activos.

Activo	Confidencialidad	Integridad	Disponibilidad	Valor
Base de Datos	5	5	4	14
Servidor	4	4	5	13
Computadoras	2	3	2	7

Para la base de datos se tendría

Propiedad	Valor
Confidencialidad	5
Integridad	5
Disponibilidad	4

Entonces

Valor del Activo = Confidencialidad + Integridad + Disponibilidad

Para el caso de la Base de Datos, Valor = 5 + 5 + 4 = 14

Existen distintas formas de combinar los valores de la tríada CIA. En este ejemplo se utiliza la suma de las puntuaciones, aunque algunas metodologías aplican ponderaciones diferentes o consideran el valor máximo de los tres atributos.

4.2.3.4. Métodos de Valoración

Las metodologías de análisis de riesgos no establecen un único procedimiento para valorar los activos. La elección del método dependerá del tipo de organización, de la información disponible y del nivel de detalle requerido durante el análisis.

De manera general, los métodos de valoración pueden clasificarse en **cualitativos**, **semicuantitativos** y **cuantitativos**.

Métodos cualitativos

Los métodos cualitativos utilizan categorías descriptivas para expresar la importancia de los activos, evitando el uso de cálculos matemáticos.

Es habitual emplear escalas como:

- Bajo
- Medio
- Alto
- Crítico

Su principal ventaja es la facilidad de aplicación, por lo que suelen utilizarse en organizaciones pequeñas o cuando no se dispone de información suficiente para realizar mediciones más precisas.

Métodos semicuantitativos

Los métodos semicuantitativos asignan valores numéricos a escalas previamente definidas con el fin de facilitar la comparación entre activos.

Por ejemplo, una organización podría utilizar una escala de 1 a 5 o de 1 a 10 para representar el nivel de importancia de cada activo. Aunque emplean números, estos no representan valores económicos reales, sino niveles relativos definidos por la propia organización.

Este tipo de métodos constituye un punto intermedio entre la valoración cualitativa y la cuantitativa, siendo uno de los enfoques más utilizados en la práctica.

Métodos cuantitativos

Los métodos cuantitativos intentan expresar el valor del activo mediante datos objetivos y medibles.

Para ello pueden considerarse aspectos como:

- costo de adquisición;
- costo de reemplazo;
- pérdidas económicas estimadas;
- impacto financiero sobre la organización;
- costos derivados de la interrupción del servicio.

Estos métodos proporcionan resultados más precisos, aunque requieren una mayor cantidad de información y un análisis más complejo. En consecuencia, suelen emplearse en organizaciones de gran tamaño o en proyectos donde resulta necesario estimar económicamente las pérdidas derivadas de un incidente de seguridad.

4.2.3.5. Ejemplos de valoración

La siguiente tabla muestra una posible valoración de algunos activos pertenecientes a una universidad.

Activo	Criticidad	Justificación
Base de datos académica	Crítico	Contiene la información de estudiantes, docentes y calificaciones.
Servidor institucional	Alto	Aloja los principales servicios informáticos de la universidad.
Sitio web institucional	Medio	Su indisponibilidad afecta la comunicación, pero no impide el funcionamiento interno.
Equipo de una oficina administrativa	Bajo	Puede ser reemplazado sin afectar significativamente las actividades.

Este ejemplo demuestra que la criticidad depende del impacto que tendría la pérdida o indisponibilidad del activo y no únicamente de su costo económico.

Considérese una empresa que desea valorar algunos de sus activos de información.

Activo	Método utilizado	Resultado
Servidor principal	Cualitativo	Crítico
Base de datos de clientes	Cualitativo	Crítico
Sistema de correo electrónico	Semicuantitativo	8/10
Computadora administrativa	Semicuantitativo	4/10
Centro de datos	Cuantitativo	Valor económico estimado

En este ejemplo puede observarse que una misma organización puede utilizar distintos métodos de valoración según las características del activo y el nivel de precisión que requiera el análisis.

No existe un método universalmente mejor que otro; la elección dependerá de las necesidades de la organización y de la metodología de análisis de riesgos adoptada.

4.2.4. Inventario de Activos

Una vez identificados y valorados los activos de información, es recomendable registrarlos en un **inventario de activos**.

El inventario es un documento que reúne información organizada sobre los activos de la organización y facilita su administración a lo largo del tiempo.

Disponer de un inventario actualizado permite conocer qué activos existen, dónde se encuentran, quién es responsable de ellos y cuál es su nivel de importancia para la organización. Además, constituye una herramienta fundamental para las etapas posteriores del análisis de riesgos, ya que las amenazas, vulnerabilidades y controles de seguridad se analizan sobre la base de los activos previamente identificados.

4.2.4.1. Información que contiene un Inventario de Activos

No existe un formato único para elaborar un inventario de activos. Cada organización puede adaptarlo a sus necesidades y a la metodología de gestión de riesgos que utilice.

Sin embargo, habitualmente un inventario contiene información como la siguiente:

- identificador del activo;
- nombre o descripción;
- tipo de activo;
- ubicación;
- responsable o propietario;
- nivel de criticidad;
- observaciones.

Dependiendo del tamaño de la organización, también pueden incorporarse otros datos, como la fecha de adquisición, el estado del activo, la versión del software, las dependencias con otros activos o cualquier otra información que facilite su administración.

4.2.4.2. Ejemplo de Inventario de Activos

Identificador	Activo	Tipo	Responsable	Criticidad
A-001	Base de datos académica	Información	Dirección de Sistemas	Crítico
A-002	Servidor principal	Hardware	Dirección de Sistemas	Alto
A-003	Plataforma educativa	Software	Área Académica	Alto
A-004	Sitio web institucional	Software	Área de Comunicación	Medio
A-005	Impresora administrativa	Hardware	Secretaría Administrativa	Bajo

Este ejemplo tiene únicamente fines ilustrativos. En una organización real, el inventario suele contener una cantidad considerablemente mayor de información y adaptarse a las necesidades particulares de la institución.

Una vez elaborado el inventario de activos, la organización dispone de una visión clara de los recursos que deben protegerse. A partir de esta información es posible continuar con el análisis de riesgos, identificando las amenazas y las vulnerabilidades que pueden afectar a cada uno de estos activos.

4.3. Clasificación de amenazas y vulnerabilidades

Los activos de información se encuentran expuestos a diversos eventos que pueden afectar su funcionamiento o comprometer la seguridad de la información. Estos eventos reciben el nombre de **amenazas**. Sin embargo, una amenaza por sí sola no siempre provoca un incidente. Para que esto ocurra, generalmente debe existir una **vulnerabilidad** que pueda ser aprovechada.

Por este motivo, las amenazas y las vulnerabilidades constituyen dos conceptos estrechamente relacionados dentro del análisis de riesgos y deben estudiarse de manera conjunta.

4.3.1. Clasificación de las Amenazas

Las amenazas pueden clasificarse de diferentes maneras. En este apunte se utilizará una clasificación sencilla basada en su origen o intencionalidad, distinguiendo entre **amenazas naturales, accidentales e intencionales**.

4.3.1.1. Amenazas naturales

Son aquellas originadas por fenómenos de la naturaleza y que escapan al control de la organización.

Algunos ejemplos son:

- terremotos;
- inundaciones;
- incendios provocados por causas naturales;
- tormentas eléctricas;
- fuertes vientos;
- cortes prolongados del suministro eléctrico ocasionados por fenómenos climáticos.

Aunque estas amenazas no pueden evitarse, es posible reducir sus consecuencias mediante medidas de prevención y planes de contingencia.

4.3.1.2. Amenazas accidentales

Son aquellas que se producen sin intención de causar daño. Generalmente tienen su origen en errores humanos, fallas técnicas o descuidos durante las actividades cotidianas.

Entre las más frecuentes se encuentran:

- eliminación accidental de información;
- errores de configuración;
- instalación incorrecta de software;
- fallas de hardware;
- interrupciones inesperadas de servicios;
- pérdida accidental de dispositivos de almacenamiento.

Este tipo de amenazas representa una de las principales causas de incidentes de seguridad en las organizaciones.

4.3.1.3. Amenazas intencionales

Son aquellas realizadas deliberadamente con el propósito de obtener un beneficio o causar un perjuicio a la organización.

Algunos ejemplos son:

- ataques informáticos;
- malware;
- fraude;
- sabotaje;
- robo de equipos;
- espionaje;
- phishing;
- acceso no autorizado a los sistemas.

Las amenazas intencionales suelen requerir medidas de protección más complejas, ya que son ejecutadas por personas que buscan vulnerar los controles de seguridad establecidos.

4.3.2. Clasificación de las Vulnerabilidades

Las vulnerabilidades pueden agruparse en cuatro categorías principales.

4.3.2.1. Vulnerabilidades técnicas

Son debilidades relacionadas con la infraestructura tecnológica, el software, el hardware o las redes de comunicación. Generalmente aparecen como consecuencia de errores de configuración, fallas de diseño, software desactualizado o ausencia de medidas de protección adecuadas.

Algunos ejemplos son:

- sistemas operativos sin actualizar;
- software con fallas de seguridad conocidas;
- contraseñas predeterminadas;
- configuraciones incorrectas de servidores;
- puertos de red innecesariamente abiertos;
- ausencia de antivirus o firewall.

Las vulnerabilidades técnicas constituyen una de las principales causas de los incidentes de seguridad informática.

4.3.2.2. Vulnerabilidades humanas

Se originan por acciones u omisiones de las personas que utilizan o administran los sistemas de información.

En la mayoría de los casos no responden a una intención maliciosa, sino al desconocimiento, la falta de capacitación o el incumplimiento de procedimientos.

Entre los ejemplos más frecuentes se encuentran:

- utilización de contraseñas débiles;
- compartir credenciales con otros usuarios;
- abrir archivos o enlaces sospechosos;
- errores durante la configuración de sistemas;
- manipulación incorrecta de información confidencial.

La capacitación permanente de los usuarios constituye una de las medidas más efectivas para reducir este tipo de vulnerabilidades.

4.3.2.3. Vulnerabilidades físicas

Son aquellas relacionadas con la protección de las instalaciones, el equipamiento y los recursos físicos de la organización.

Estas vulnerabilidades permiten que una amenaza afecte directamente a los activos mediante el acceso físico o la falta de protección ambiental.

Algunos ejemplos son:

- ausencia de controles de acceso físico;
- falta de cámaras de vigilancia;
- inexistencia de sistemas de detección o extinción de incendios;
- cableado expuesto;
- equipos ubicados en lugares sin protección.

Muchas de estas vulnerabilidades pueden reducirse mediante la aplicación de las medidas estudiadas en la **Unidad 2: Seguridad Física**.

4.3.2.4. Vulnerabilidades organizativas

Se producen cuando la organización presenta deficiencias en la gestión de la seguridad de la información.

Generalmente están relacionadas con la ausencia de normas, procedimientos o mecanismos de control.

Entre las más comunes se encuentran:

- inexistencia de políticas de seguridad;
- procedimientos no documentados;
- falta de asignación de responsabilidades;
- ausencia de auditorías periódicas;
- inexistencia de planes de continuidad o recuperación.

Las vulnerabilidades organizativas suelen afectar a toda la organización y, por ello, requieren un enfoque de gestión que involucre tanto aspectos técnicos como administrativos.

4.3.3. Relación entre Amenazas y Vulnerabilidades

Las amenazas y las vulnerabilidades son conceptos diferentes, pero estrechamente relacionados. Una amenaza representa la posibilidad de que ocurra un evento perjudicial, mientras que una vulnerabilidad constituye la debilidad que permite que dicha amenaza llegue a materializarse.

En términos generales, una amenaza necesita aprovechar una vulnerabilidad para producir un incidente de seguridad.

Por ejemplo:

- Un **incendio** constituye una amenaza natural. La ausencia de detectores de humo o de sistemas de extinción representa una vulnerabilidad física que incrementa el riesgo de daños.
- Un **ciberdelincuente** constituye una amenaza intencional. El uso de contraseñas débiles representa una vulnerabilidad humana que facilita el acceso no autorizado.
- Un **error de configuración** puede convertirse en una vulnerabilidad técnica que sea aprovechada por un atacante para comprometer un servidor.
- La **ausencia de políticas de seguridad** constituye una vulnerabilidad organizativa que incrementa la probabilidad de que ocurran distintos tipos de incidentes.

Puede resumirse esta relación mediante la siguiente expresión conceptual:

Amenaza + Vulnerabilidad = Posibilidad de que ocurra un incidente de seguridad

Por este motivo, durante el análisis de riesgos no basta con identificar las amenazas existentes; también resulta imprescindible detectar las vulnerabilidades presentes en la organización para definir los controles de seguridad más adecuados.

4.3.4. Ejemplo Integrador

La siguiente tabla presenta algunos ejemplos de la relación entre activos, amenazas y vulnerabilidades.

Activo	Amenaza	Vulnerabilidad
Base de datos institucional	Malware	Sistema operativo sin actualizar
Servidor principal	Incendio	Ausencia de sistema automático de extinción
Correo electrónico corporativo	Phishing	Usuarios sin capacitación en ciberseguridad
Oficina administrativa	Robo	Falta de control de acceso físico

Activo	Amenaza	Vulnerabilidad
Sistema de gestión académica	Acceso no autorizado	Contraseñas débiles

Este tipo de análisis permite comprender que una amenaza no siempre genera un incidente. Para que el daño se produzca, normalmente debe existir una vulnerabilidad que pueda ser aprovechada. Identificar y corregir dichas vulnerabilidades constituye uno de los principales objetivos del análisis de riesgos.

4.4. Proceso de Análisis de Riesgos

Una vez identificados y valorados los activos de información, y comprendidos los conceptos de amenaza y vulnerabilidad, el siguiente paso consiste en realizar el **análisis de riesgos**.

El **análisis de riesgos** es un proceso sistemático que permite identificar, evaluar y tratar los riesgos que pueden afectar a una organización. Su finalidad es proporcionar información que facilite la toma de decisiones sobre las medidas de seguridad que deben implementarse para proteger los activos de información.

Aunque existen diferentes metodologías, la mayoría sigue una secuencia similar de actividades. En este apunte se utilizará el proceso representado en la siguiente figura.

4.4.1. Paso 1. Definir el Alcance

Todo análisis de riesgos debe comenzar definiendo claramente qué parte de la organización será objeto del estudio. El alcance establece los límites del análisis y evita evaluar sistemas, procesos o recursos que no forman parte del proyecto. Dependiendo de las necesidades de la organización, el análisis puede abarcar:

- toda la organización;

- un área específica;
- un sistema de información;
- una aplicación;
- un centro de cómputos;
- un servicio informático.

También se establecen los objetivos del análisis, los responsables y el período de tiempo considerado.

La pregunta que se responde en este paso es:

¿Qué vamos a analizar?

4.4.2. Paso 2. Identificar los Activos

Una vez definido el alcance, se identifican los activos que poseen valor para la organización. En esta etapa se elabora o actualiza el inventario de activos y se verifica la valoración realizada sobre cada uno de ellos, identificando aquellos recursos cuya pérdida o afectación podría generar mayores consecuencias para la organización. Esta actividad se apoya en el trabajo realizado en el apartado **4.2 Activos de Información**.

La pregunta que responde este paso es:

¿Qué debemos proteger?

4.4.3. Paso 3. Identificar las Amenazas

El siguiente paso consiste en identificar las amenazas que podrían afectar a los activos previamente identificados. Las amenazas pueden ser naturales, accidentales o intencionales, según lo desarrollado en el apartado **4.3**. En esta etapa se busca determinar todos los eventos que podrían comprometer la seguridad de los activos analizados.

La pregunta correspondiente es:

¿Qué puede afectar a los activos?

4.4.4. Paso 4. Identificar Vulnerabilidades y Controles de Seguridad

Una vez identificadas las amenazas, se analizan las vulnerabilidades presentes en los activos y los controles de seguridad existentes para determinar el nivel de protección actual de la organización.

Las **vulnerabilidades** representan las debilidades que pueden ser aprovechadas por una amenaza para producir un incidente.

Los **controles de seguridad** son las medidas técnicas, físicas u organizativas destinadas a prevenir incidentes, disminuir su probabilidad de ocurrencia o reducir el impacto que podrían ocasionar.

Algunos ejemplos de controles de seguridad son:

- firewall;
- autenticación multifactor;
- antivirus;
- copias de seguridad;
- políticas de seguridad;
- capacitación del personal;
- sistemas de detección de intrusos;
- controles de acceso físico y lógico.

Durante este paso se responde a las siguientes preguntas:

¿Qué vulnerabilidades presentan los activos?

¿Qué controles de seguridad existen para reducir el riesgo?

La información obtenida permitirá determinar posteriormente el nivel de riesgo.

4.4.5. Paso 5. Evaluar el Riesgo

Con la información obtenida en los pasos anteriores se procede a evaluar cada uno de los riesgos identificados. Esta evaluación permite determinar cuáles representan una mayor amenaza para la organización y, por lo tanto, cuáles requieren una atención prioritaria.

La pregunta que responde este paso es:

¿Qué tan importante es el riesgo?

La evaluación del riesgo consiste en estimar el nivel de riesgo asociado a cada situación analizada, con el fin de establecer prioridades para su tratamiento.

Las metodologías de análisis de riesgos no utilizan un único criterio para evaluar el riesgo. Dependiendo del contexto y del nivel de detalle requerido, pueden emplearse distintos modelos de evaluación. Los dos enfoques más difundidos son los que se presentan a continuación:

- **Valor del activo y probabilidad de la amenaza.**
- **Probabilidad de ocurrencia e impacto del incidente.**

Ambos modelos buscan estimar la importancia del riesgo, aunque utilizan criterios diferentes.

4.4.5.1. Modelo basado en el Valor del Activo y la Probabilidad de la Amenaza

En los análisis de riesgos de carácter introductorio suele utilizarse un modelo sencillo en el que el riesgo depende del valor del activo y de la probabilidad de que una amenaza llegue a materializarse.

Este modelo puede expresarse mediante la siguiente relación:

Riesgo = Valor del Activo × Probabilidad de la Amenaza

En este caso:

- el **valor del activo** representa la importancia que tiene dicho recurso para la organización;
- la **probabilidad** indica la posibilidad de que una amenaza afecte al activo.

Cuanto mayor sea el valor del activo o mayor sea la probabilidad de ocurrencia de la amenaza, mayor será el nivel de riesgo obtenido.

Aunque se trata de un modelo sencillo, resulta muy útil para comprender los fundamentos del análisis de riesgos y suele emplearse en actividades académicas y análisis preliminares.

4.4.5.2. Modelo basado en Probabilidad e Impacto

Otro modelo ampliamente utilizado consiste en evaluar el riesgo considerando dos factores:

- la **probabilidad** de que ocurra un incidente;
- el **impacto** que dicho incidente tendría sobre la organización.

En este caso, el riesgo aumenta cuando existe una alta probabilidad de ocurrencia o cuando las consecuencias del incidente son significativas.

En este modelo, la probabilidad representa la posibilidad de que ocurra un incidente de seguridad, mientras que el impacto mide las consecuencias que dicho incidente produciría sobre la organización.

Por ejemplo, un incidente con baja probabilidad, pero consecuencias muy graves puede representar un riesgo similar al de otro incidente que ocurre con frecuencia, pero cuyo impacto es reducido.

Este enfoque es el más utilizado por las metodologías modernas, ya que permite construir matrices de riesgo y establecer prioridades para la implementación de controles de seguridad.

4.4.5.3. Comparación entre ambos modelos

Aunque ambos modelos utilizan criterios diferentes, persiguen el mismo objetivo: estimar el nivel de riesgo para establecer prioridades y facilitar la toma de decisiones. La siguiente tabla resume sus principales características.

Modelo	Factores considerados	Aplicación principal
Valor del Activo × Probabilidad	Valor del activo y probabilidad de la amenaza	Análisis introductorios y ejercicios didácticos
Probabilidad × Impacto	Probabilidad e impacto	Metodologías modernas y matrices de riesgos

Ambos modelos son válidos y ampliamente utilizados. La elección dependerá de la metodología adoptada, del tipo de organización y del nivel de detalle que se desee alcanzar durante el análisis.

4.4.6. Paso 6. Tratar el Riesgo

Finalmente, la organización decide qué acciones implementará para gestionar los riesgos evaluados. El objetivo consiste en reducir el riesgo hasta un nivel aceptable mediante la incorporación o mejora de controles de seguridad.

La pregunta correspondiente es:

¿Qué haremos con el riesgo identificado?

Una vez evaluados los riesgos, la organización debe decidir cómo gestionarlos. Esta decisión dependerá del nivel de riesgo obtenido, de los recursos disponibles y de las políticas de seguridad de la organización. Las estrategias más utilizadas para el tratamiento del riesgo son las siguientes:

- **Evitar**: Consiste en eliminar la fuente del riesgo, dejando de realizar la actividad que lo origina o retirando el activo cuando este ya no resulta necesario para la organización. Esta estrategia elimina completamente el riesgo, aunque en la práctica suele aplicarse únicamente cuando el activo o el proceso pueden ser reemplazados o dejar de utilizarse sin afectar el funcionamiento de la organización.
  Ejemplo: dejar de utilizar un servidor obsoleto, retirar un software que presenta vulnerabilidades críticas, cancelar un servicio que ya no es necesario, decidir no implementar una tecnología que representa un riesgo elevado.
- **Mitigar**: Consiste en implementar controles de seguridad que reduzcan la probabilidad de ocurrencia del incidente o disminuyan su impacto.
  Ejemplo**:** instalar un firewall, aplicar actualizaciones de seguridad o capacitar al personal.
- **Transferir**: Consiste en trasladar total o parcialmente las consecuencias del riesgo a un tercero.
  Ejemplo**:** contratar un seguro informático o externalizar un servicio especializado.

- **Aceptar**: Consiste en asumir el riesgo cuando su nivel es considerado aceptable o cuando el costo de reducirlo supera el beneficio esperado.
  Ejemplo: aceptar el riesgo asociado al uso de un equipo antiguo cuya sustitución no resulta económicamente conveniente.

4.5. Matriz de Riesgos

La evaluación de los riesgos genera información sobre la probabilidad de ocurrencia de los incidentes y el impacto que estos podrían producir sobre la organización. Para facilitar su análisis y priorización, esta información suele representarse mediante una **matriz de riesgos**.

La matriz de riesgos es una herramienta ampliamente utilizada en seguridad de la información y en otras disciplinas relacionadas con la gestión de riesgos. Su principal objetivo consiste en clasificar los riesgos según su nivel de criticidad, permitiendo identificar cuáles requieren una atención inmediata y cuáles pueden aceptarse o mantenerse bajo monitoreo.

Es importante destacar que la matriz **no evalúa activos de forma aislada**, sino que evalúa los **riesgos identificados** durante el análisis.

Cada riesgo surge de la combinación de tres elementos:

- un **activo** que posee valor para la organización;
- una **amenaza** capaz de afectar dicho activo;
- una o más **vulnerabilidades** que pueden ser aprovechadas por la amenaza.

Por este motivo, un mismo activo puede estar asociado a varios riesgos diferentes.

Por ejemplo:

Riesgo	Activo	Amenaza	Vulnerabilidad
R1	Servidor de Base de Datos	Ransomware	Sistema operativo sin actualizar
R2	Servidor de Base de Datos	Corte de energía	Ausencia de UPS
R3	Servidor de Base de Datos	Robo	Sala sin control de acceso

Cada uno de estos riesgos será evaluado de forma independiente y podrá ocupar una posición distinta dentro de la matriz.

4.5.1. Concepto

Una **matriz de riesgos** es una representación gráfica o tabular que permite clasificar los riesgos según dos factores fundamentales:

- la **probabilidad** de que un riesgo llegue a materializarse;
- el **impacto** que dicho incidente produciría sobre la organización.

La combinación de ambos factores permite determinar el nivel de criticidad del riesgo y establecer prioridades para la implementación de controles de seguridad.

La matriz no elimina el riesgo ni lo reduce por sí misma; constituye una herramienta de apoyo para la toma de decisiones durante la gestión del riesgo.

4.5.2. Tipos de Valoración del Riesgo

Las metodologías de análisis de riesgos no utilizan un único criterio para evaluar los riesgos. Dependiendo del nivel de detalle requerido y de la información disponible, pueden emplearse distintos enfoques de valoración.

Los más utilizados son los siguientes.

4.5.2.1. Valoración cualitativa

Clasifica los riesgos mediante categorías descriptivas, por ejemplo:

- Bajo
- Medio
- Alto
- Crítico

No realiza cálculos numéricos y resulta apropiada cuando no se dispone de información estadística suficiente o cuando se requiere un análisis rápido.

4.5.2.2. Valoración semicuantitativa

Asigna valores numéricos a escalas cualitativas.

Por ejemplo:

Nivel	Valor
Muy bajo	1
Bajo	2
Medio	3
Alto	4
Muy alto	5

Estos valores permiten realizar cálculos sencillos y comparar los distintos riesgos. Es el enfoque más utilizado en trabajos prácticos y en muchas metodologías de análisis de riesgos.

4.5.2.3. Valoración cuantitativa

Utiliza datos estadísticos, probabilidades reales y pérdidas económicas para calcular el riesgo con mayor precisión.

Este enfoque requiere una gran cantidad de información y suele emplearse en organizaciones donde resulta posible estimar económicamente las pérdidas asociadas a un incidente.

4.5.3. Determinación de la Probabilidad

Antes de construir la matriz es necesario determinar la **probabilidad de ocurrencia** de cada riesgo.

La probabilidad representa la posibilidad de que una amenaza aproveche una vulnerabilidad y afecte al activo analizado.

Una escala sencilla puede ser la siguiente.

Nivel	Descripción
Baja	La amenaza rara vez ocurre o no existen antecedentes conocidos.
Media	La amenaza puede ocurrir ocasionalmente.
Alta	La amenaza ocurre con frecuencia o existen muchas posibilidades de que ocurra.

Para determinar la probabilidad suelen analizarse aspectos como:

- antecedentes de incidentes similares;
- exposición del activo;
- existencia de vulnerabilidades conocidas;
- frecuencia de ataques similares;
- características del entorno tecnológico.

4.5.4. Determinación del Impacto

El impacto representa las consecuencias que tendría un incidente sobre la organización.

Estas consecuencias pueden ser:

- económicas;
- operativas;
- legales;
- reputacionales.

Una escala sencilla puede ser la siguiente.

Nivel	Descripción
Bajo	Produce inconvenientes menores y no afecta significativamente las operaciones.
Medio	Genera interrupciones parciales o pérdidas moderadas.
Alto	Produce pérdidas importantes o afecta procesos críticos.

Para determinar el impacto suelen analizarse aspectos como:

- indisponibilidad del servicio;

- pérdida de información;
- pérdidas económicas;
- incumplimiento legal;
- daño a la imagen institucional;
- interrupción de procesos críticos.

4.5.5. Construcción de la Matriz

Una vez determinados la probabilidad y el impacto de cada riesgo, estos valores se combinan para obtener el nivel de criticidad.

La siguiente tabla presenta un ejemplo simplificado de una matriz de riesgos.

Impacto / Probabilidad	**Baja**	**Media**	**Alta**
Alto	Medio	Alto	Crítico
Medio	Bajo	Medio	Alto
Bajo	Bajo	Bajo	Medio

Cada organización puede definir la cantidad de niveles y los criterios de clasificación de acuerdo con la metodología adoptada.

4.5.6. Interpretación de la Matriz

Una vez construida la matriz, cada riesgo queda clasificado según su nivel de criticidad.

En términos generales:

- **Riesgo Bajo:** puede aceptarse o mantenerse bajo monitoreo.
- **Riesgo Medio:** requiere seguimiento e implementación de algunos controles.
- **Riesgo Alto:** demanda acciones correctivas en el corto plazo.
- **Riesgo Crítico:** requiere atención inmediata debido al impacto que podría generar sobre la organización.

La matriz facilita la asignación de recursos y permite priorizar la implementación de controles de seguridad.

4.5.7. Ejemplo de Valoración Cualitativa

Supóngase el siguiente riesgo identificado durante el análisis.

Elemento	**Descripción**
Activo	Servidor de Base de Datos
Amenaza	Ransomware
Vulnerabilidad	Sistema operativo sin actualizar

Luego del análisis se concluye que:

- la probabilidad de ocurrencia es **Alta**, debido a que el servidor está expuesto a Internet y presenta vulnerabilidades conocidas;
- el impacto es **Alto**, ya que la pérdida del servidor afectaría procesos críticos de la organización.

Al ubicar el riesgo en la matriz, se obtiene un **riesgo Crítico**.

4.5.8. Ejemplo de Valoración Semicuantitativa

Muchas organizaciones prefieren asignar valores numéricos a cada criterio para facilitar la comparación entre distintos riesgos. Supóngase que se utiliza la siguiente escala para valorar los activos y la probabilidad de las amenazas.

4.5.8.1. Valor del activo

Nivel	Valor
Muy bajo	1
Bajo	2
Medio	3
Alto	4
Muy alto	5

4.5.8.2. Probabilidad de la amenaza

Nivel	Valor
Muy baja	1
Baja	2
Media	3
Alta	4
Muy alta	5

Durante el análisis se obtiene la siguiente información.

Elemento	Valor
Activo	Servidor de Base de Datos
Valor del activo	5
Amenaza	Ransomware
Probabilidad	4

En este ejemplo se utiliza el siguiente modelo de evaluación:

Riesgo = Valor del Activo × Probabilidad de la Amenaza

Por lo tanto:

Riesgo = 5 × 4 = 20

La organización establece la siguiente clasificación.

Resultado	Nivel
1 – 5	Bajo
6 – 10	Medio
11 – 15	Alto
16 – 25	Crítico

Como el resultado obtenido es **20**, el riesgo se clasifica como **Crítico**.

4.5.9. Tratamiento del riesgo

Al tratarse de un riesgo crítico, la organización decide aplicar la estrategia de **Mitigar el riesgo**.

La mitigación consiste en implementar controles que reduzcan la probabilidad de ocurrencia del incidente o disminuyan su impacto.

Para ello se decide:

- actualizar el sistema operativo;
- fortalecer las políticas de copias de respaldo;
- implementar autenticación multifactor para los administradores;
- mejorar el monitoreo del servidor.

Estas medidas no eliminan completamente el riesgo, pero permiten reducirlo hasta un nivel aceptable para la organización.

Observación: En este ejemplo se seleccionó la estrategia de Mitigar porque el servidor de base de datos constituye un activo crítico para la organización. No resulta posible eliminar el activo (evitar el riesgo), ni aceptar un riesgo de nivel crítico, mientras que transferir el riesgo no resolvería el problema operativo. Por ello, la alternativa más adecuada consiste en reducir el riesgo mediante la implementación de controles de seguridad.

4.6. Metodologías para el Análisis de Riesgos

Hasta el momento se ha estudiado un proceso general para realizar un análisis de riesgos. Sin embargo, en la práctica, las organizaciones suelen apoyarse en metodologías específicas que proporcionan procedimientos, criterios y herramientas para identificar, evaluar y tratar los riesgos de forma sistemática.

Una **metodología de análisis de riesgos** establece un conjunto de pasos, técnicas y recomendaciones que permiten realizar evaluaciones de manera ordenada y consistente.

Además, facilita que distintos analistas obtengan resultados comparables al aplicar criterios comunes.

Existen numerosas metodologías desarrolladas por organismos internacionales, gobiernos y entidades especializadas en seguridad de la información. Algunas de las más utilizadas son MAGERIT, OCTAVE e ISO/IEC 27005.

4.6.1. MAGERIT

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) fue desarrollada por el **Consejo Superior de Administración Electrónica del Gobierno de España** y constituye una de las metodologías más difundidas en el ámbito de habla hispana.

Su principal objetivo es ayudar a las organizaciones a identificar los riesgos que afectan a sus sistemas de información y establecer las medidas necesarias para reducirlos.

El proceso propuesto por MAGERIT incluye, entre otras actividades:

- identificación de los activos;
- valoración de los activos;
- identificación de amenazas;
- identificación de vulnerabilidades;
- evaluación del riesgo;
- selección de controles para reducir el riesgo.

Una característica importante de MAGERIT es que presta especial atención a la valoración de los activos y al análisis de las amenazas que pueden afectar a cada uno de ellos.

4.6.2. OCTAVE

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) fue desarrollado por el **Software Engineering Institute (SEI)** de la Universidad Carnegie Mellon.

A diferencia de otras metodologías, OCTAVE pone un fuerte énfasis en la participación del personal de la organización durante el proceso de análisis.

Esta metodología considera que quienes conocen mejor los procesos de negocio son las propias personas que trabajan en ellos, por lo que participan activamente en la identificación de los activos críticos, las amenazas y los riesgos.

Entre sus principales características se destacan:

- enfoque orientado al negocio;
- participación de distintas áreas de la organización;
- identificación de activos críticos;
- análisis de amenazas y vulnerabilidades;

- elaboración de estrategias para el tratamiento del riesgo.

4.6.3. ISO/IEC 27005

La norma **ISO/IEC 27005** forma parte de la familia de normas ISO/IEC 27000 relacionadas con la gestión de la seguridad de la información.

Su propósito consiste en proporcionar directrices para realizar la gestión de riesgos dentro de un Sistema de Gestión de Seguridad de la Información (SGSI).

La norma no establece una metodología única, sino que describe un proceso general que puede adaptarse a las características y necesidades de cada organización.

Las principales etapas propuestas son:

- establecimiento del contexto;
- identificación de riesgos;
- análisis de riesgos;
- evaluación de riesgos;
- tratamiento de riesgos;
- comunicación del riesgo;
- seguimiento y revisión continua.

ISO/IEC 27005 es ampliamente utilizada por organizaciones que implementan la norma ISO/IEC 27001 para la gestión de la seguridad de la información.

4.6.4. Comparación de las principales metodologías

Aunque las metodologías analizadas presentan diferencias en su enfoque, todas persiguen el mismo objetivo: identificar los riesgos que afectan a la organización y proporcionar criterios para tratarlos de manera adecuada.

La siguiente tabla resume sus principales características.

Metodología	Origen	Principal característica
MAGERIT	Gobierno de España	Gran énfasis en la valoración de activos y el análisis sistemático de riesgos.
OCTAVE	Carnegie Mellon University	Prioriza la participación del personal y el conocimiento del negocio.
ISO/IEC 27005	Organización Internacional de Normalización (ISO)	Proporciona directrices para la gestión de riesgos dentro de un SGSI.

4.6.5. Selección de una metodología

No existe una metodología que resulte adecuada para todas las organizaciones.

La elección dependerá de diversos factores, entre ellos:

- el tamaño de la organización;
- la complejidad de los sistemas de información;
- los recursos disponibles;
- los requisitos legales y normativos;
- el nivel de detalle requerido para el análisis.

En muchos casos, las organizaciones adaptan estas metodologías a sus propias necesidades, combinando elementos de varias de ellas.

Observación

En este apunte se presentó un **proceso general de análisis de riesgos** con fines didácticos. Dicho proceso es compatible con las etapas propuestas por metodologías ampliamente utilizadas, como MAGERIT, OCTAVE e ISO/IEC 27005. En la práctica, cada organización selecciona o adapta la metodología que mejor se ajusta a sus necesidades y contexto.

4.7. Políticas de Seguridad

Una vez identificados, evaluados y tratados los riesgos de una organización, resulta necesario establecer reglas que permitan proteger sus activos de información y reducir la probabilidad de que dichos riesgos se materialicen. Estas reglas se formalizan mediante las **Políticas de Seguridad**.

Las políticas de seguridad constituyen uno de los principales instrumentos de gestión de la seguridad de la información, ya que establecen las directrices generales que deben cumplir todos los miembros de una organización para proteger la información y los recursos tecnológicos.

4.7.1. Concepto

Una **Política de Seguridad** es un documento formal aprobado por la dirección de una organización que establece los principios, objetivos y normas generales destinadas a proteger la información y los sistemas informáticos.

Su finalidad es proporcionar un marco de referencia para la implementación de controles de seguridad y orientar el comportamiento de todos los usuarios de la organización.

Las políticas de seguridad indican **qué debe hacerse**, mientras que los procedimientos describen **cómo debe realizarse** cada actividad.

Por ejemplo, una política puede establecer que:

- todos los usuarios deberán utilizar credenciales personales para acceder a los sistemas;
- las copias de seguridad deberán realizarse diariamente;
- el acceso al centro de cómputos estará restringido al personal autorizado.

Las políticas de seguridad se elaboran considerando los resultados obtenidos durante el análisis de riesgos. De esta manera, las amenazas y vulnerabilidades identificadas permiten definir las medidas organizativas necesarias para reducir los riesgos a niveles aceptables.

4.7.2. Características de una Política de Seguridad

Para que una política de seguridad resulte efectiva debe cumplir una serie de características básicas.

Aprobada por la dirección

La política debe contar con el respaldo de la máxima autoridad de la organización, garantizando su cumplimiento por parte de todo el personal.

Clara y comprensible

Debe redactarse utilizando un lenguaje sencillo y preciso, evitando ambigüedades que puedan dificultar su interpretación.

Aplicable

Las normas establecidas deben ser realistas y posibles de implementar dentro de la organización.

Difundida

Todos los usuarios deben conocer la política y comprender las responsabilidades que les corresponden.

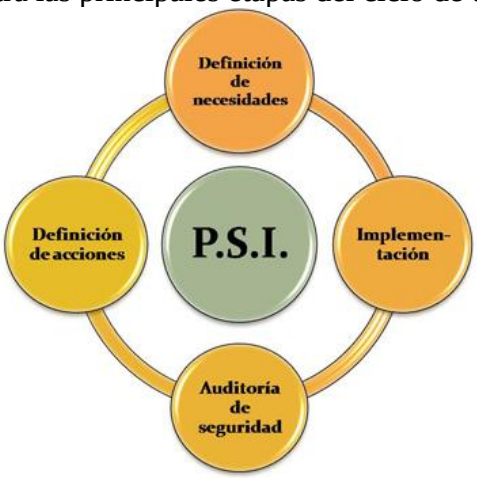
Actualizada

La política debe revisarse periódicamente para adaptarse a los cambios tecnológicos, organizativos y a la aparición de nuevos riesgos.

4.7.3. Ciclo de una Política de Seguridad

La elaboración de una Política de Seguridad de la Información constituye un proceso continuo. Una vez implementada, debe evaluarse periódicamente para verificar su eficacia y adaptarla a las nuevas necesidades de la organización.

La siguiente figura muestra las principales etapas del ciclo de una Política de Seguridad.



4.7.3.1. Paso 1. Definición de necesidades

En esta etapa se analizan las necesidades de seguridad de la organización considerando:

- los activos de información;
- los riesgos identificados;
- los requisitos legales y normativos;
- los objetivos de la organización.

El propósito es determinar los aspectos que deberán contemplarse en la política de seguridad.

4.7.3.2. Paso 2. Definición de acciones

Con base en las necesidades identificadas, se establecen las reglas, lineamientos y medidas generales que deberán cumplirse para proteger la información y los sistemas.

4.7.3.3. Paso 3. Implementación

La política aprobada se pone en práctica mediante su difusión dentro de la organización, la capacitación de los usuarios y la implementación de los controles necesarios para su cumplimiento.

4.7.3.4. Paso 4. Auditoría de seguridad

Finalmente, se verifica el cumplimiento y la eficacia de la política mediante auditorías de seguridad.

Los resultados obtenidos permiten detectar oportunidades de mejora y actualizar la política cuando aparecen nuevos riesgos o cambian las necesidades de la organización, reiniciando nuevamente el ciclo.

4.7.3.5. Ejemplo

Como resultado del análisis de riesgos realizado para una Universidad, podrían establecerse las siguientes políticas de seguridad:

- Todos los usuarios deberán utilizar contraseñas robustas y no compartirlas con otras personas.
- Se realizarán copias de seguridad diarias de la base de datos académica.
- Los servidores deberán mantenerse actualizados con los últimos parches de seguridad.
- El acceso al centro de cómputos estará restringido únicamente al personal autorizado.
- Las cuentas de usuario inactivas durante un período prolongado serán deshabilitadas.

Estas políticas constituyen medidas organizativas orientadas a disminuir la probabilidad de que los riesgos identificados durante el análisis lleguen a materializarse.

4.8. Bibliografía básica

- **Calder, A.** *IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002*. Kogan Page.
- **ISO/IEC 27005.** *Information Security Risk Management*. International Organization for Standardization.
- **INCIBE.** *Gestión de Riesgos de Seguridad de la Información*. Instituto Nacional de Ciberseguridad de España.
- **MAGERIT v3.0.** *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Consejo Superior de Administración Electrónica, Gobierno de España.
- **NIST Special Publication 800-30 Rev. 1.** *Guide for Conducting Risk Assessments*. National Institute of Standards and Technology.
- **OCTAVE Allegro.** *Improving the Information Security Risk Assessment Process*. Software Engineering Institute, Carnegie Mellon University.
- **Stallings, W.** *Seguridad Informática: Principios y Práctica*. Pearson.
- **Whitman, M. E.; Mattord, H. J.** *Principles of Information Security*. Cengage Learning.