FACULTAD DE INGENIERÍA

Universidad Nacional de Jujuy

Unidad 4

Análisis de Riesgos

Apunte de Cátedra · Seguridad y Auditoría Informática

Contenidos de la Unidad 4

4.1 Introducción al Análisis de Riesgos

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.

Seguridad absoluta no existe

Siempre habrá riesgo residual

Recursos limitados

Hay que priorizar los riesgos más significativos

Proceso continuo

Los riesgos cambian con el tiempo y la tecnología

Base de SGSI

Presente en ISO 27005, MAGERIT y OCTAVE

4.1.1 Concepto de Riesgo

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.

Riesgo ≈ Probabilidad × Impacto

No es una fórmula matemática exacta, sino una forma de comprender que el riesgo depende de dos factores: la posibilidad de que ocurra un incidente y las consecuencias si se materializa.

4.1.1.1 Características del Riesgo

1

Es incierto

Hace referencia a un evento futuro. Existe posibilidad, no certeza.

2

Varía con el tiempo

Nuevas amenazas, incorporación de tecnologías o implementación de controles modifican el nivel de riesgo.

3

Depende del contexto

El mismo evento tiene impacto distinto según la organización (banco vs. oficina pequeña).

4

Puede gestionarse

Se puede reducir su probabilidad, disminuir su impacto o administrarlo.

4.1.2 Finalidad y Objetivos del Análisis de Riesgos

Proporcionar una visión clara de los riesgos para tomar decisiones fundamentadas sobre las medidas de protección.

Conocer la exposición

Identificar el nivel de riesgo de la organización

Facilitar decisiones

Orientar las inversiones en seguridad

Optimizar recursos

Priorizar riesgos más significativos

Reducir probabilidad e impacto

Disminuir la posibilidad y las consecuencias de incidentes

Cumplir normas

Apoyar ISO 27001/27005 y otras estándares

Mejora continua

Evaluar riesgos de forma periódica

4.1.3 Riesgo, Amenaza, Vulnerabilidad e Incidente

Riesgo

Posibilidad de que una amenaza aproveche una vulnerabilidad y produzca un incidente que afecte a uno o más activos. Depende de probabilidad e impacto.

Amenaza

Evento, circunstancia o agente con capacidad para causar daño a un activo (natural, humano, técnico o intencional).

Vulnerabilidad

Debilidad o deficiencia en un activo, sistema o procedimiento que puede ser aprovechada por una amenaza.

Incidente de seguridad

Evento que compromete (o puede comprometer) la confidencialidad, integridad o disponibilidad de la información o los sistemas.

Relación entre los conceptos

Activo → Amenaza → Vulnerabilidad → Incidente → Impacto → Riesgo

Ejemplo: Universidad que almacena información académica de los estudiantes en un servidor

Activo:	Servidor con la base de datos académica
Amenaza:	Ataque de ransomware
Vulnerabilidad:	Sistema operativo sin actualizar
Incidente:	El atacante cifra toda la información
Impacto:	Interrupción de servicios, pérdida temporal de registros, costos de recuperación
Riesgo:	Posibilidad de que ocurra este escenario y sus consecuencias

4.1.4 Riesgo Inherente y Riesgo Residual

Riesgo Inherente

Nivel de riesgo al que está expuesto un activo antes de implementar cualquier control de seguridad.

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

Permite conocer la exposición inicial y priorizar medidas.

Riesgo Residual

Nivel de riesgo que permanece después de implementar los controles de seguridad seleccionados.

Pregunta:
¿Cuál es el riesgo que queda después de aplicar los controles?

Ningún control elimina el riesgo por completo. Se evalúa si el residual es aceptable.

Comparación: Inherente vs Residual

Característica	Riesgo Inherente	Riesgo Residual
Momento de evaluación	Antes de implementar controles	Después de implementar controles
Controles	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

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

Características de un activo

Poseen valor

Económico, operativo, legal o estratégico

Deben protegerse

Expuestos a amenazas naturales, accidentales o intencionales

Pueden depender de otros

Una aplicación depende del servidor, red y base de datos

Requieren valoración

No todos tienen la misma criticidad

4.2.2 Clasificación de los Activos

Información

En formato digital o físico.
Bases de datos, documentos, registros, contratos, historiales

Hardware

Dispositivos físicos utilizados para el procesamiento, almacenamiento y transmisión de la información.
Servidores, PCs, notebooks, equipos de red, almacenamiento

Software

Programas utilizados por la organización para desarrollar sus actividades. SO, aplicaciones, bases de datos, herramientas de seguridad

Servicios

Permiten el funcionamiento normal de la organización. Correo, web, Internet, autenticación, almacenamiento en nube

Personas

Constituyen un activo fundamental.
Usuarios, administradores, directivos, proveedores, consultores

Instalaciones e infraestructura

Espacios físicos y la infraestructura necesaria para el funcionamiento de los sistemas informáticos. Centros de datos, salas de servidores, cableado, sistemas eléctricos

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 no es establecer el precio económico, sino medir el impacto sobre la organización si el activo dejara de cumplir su función.

Ejemplo

Una computadora administrativa y un servidor que almacena la base de datos institucional pueden tener un costo de adquisición similar. Sin embargo, el valor desde el punto de vista de la seguridad es muy distinto: la pérdida del servidor produce un impacto mucho mayor sobre la organización.

4.2.3.2 Criterios para valorar un activo

No existe un único criterio. Cada organización define los aspectos más relevantes según sus necesidades.

Valor económico

Costo de adquisición, mantenimiento o reemplazo. Útil para activos físicos, pero no siempre refleja la verdadera importancia.

Importancia para la operación

Grado en que el activo es necesario para el funcionamiento normal. Indisponibilidad de procesos críticos = mayor valoración.

Valor de la información

Cuando el activo contiene información resulta necesario considerar el valor de dicha información.
Confidencialidad, integridad y disponibilidad de los datos que contiene el activo (base de la tríada CIA).

Requisitos legales y normativos

Información regulada por leyes, contratos o normas. Su pérdida puede generar sanciones o responsabilidades.

Impacto sobre la imagen

Pérdida que afecta la reputación o la confianza de clientes, proveedores o ciudadanos. A veces más grave que el daño económico.

4.2.3.3 Valoración mediante la tríada CIA

En muchas metodologías el valor de un activo se determina evaluando la importancia de sus tres propiedades fundamentales: Confidencialidad, Integridad y Disponibilidad. Cada una recibe una puntuación según una escala definida por la organización.

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

Suponiendo 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

Valor del Activo = Confidencialidad + Integridad + Disponibilidad
Ejemplo: Base de Datos → 5 + 5 + 4 = 14

En el ejemplo se utiliza la suma de las puntuaciones, aunque algunas metodologías aplican ponderaciones diferentes, como por ejemplo, consideran el valor máximo de los tres atributos o el promedio.

Métodos de Valoración de Activos

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

Cualitativos

Categorías descriptivas para expresar la importancia de los activos (Bajo, Medio, Alto, Crítico). Fáciles de aplicar; útiles en organizaciones pequeñas o cuando falta información estadística.

Semicuantitativos

Asignan números a escalas cualitativas (1–5 o 1–10). Facilitan la comparación. No representan valores económicos reales, sino niveles relativos. Muy usados en la práctica.

Cuantitativos

Intentan expresar el valor del activo mediante datos objetivos: costo de adquisición, reemplazo, pérdidas estimadas, impacto financiero, costos de interrupción. Más precisos, pero requieren más información y análisis.

4.2.4 Inventario de Activos

Documento que reúne información organizada sobre los activos de la organización. Permite conocer qué activos existen, dónde se encuentran, quién es responsable y cuál es su nivel de importancia. Es base para identificar amenazas, vulnerabilidades y controles.

Información habitual en un inventario

Identificador del activo	Nombre o descripción	Tipo de activo
Ubicación	Responsable / propietario	Nivel de criticidad
Observaciones	Dependencias con otros activos	Estado / versión

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

4.3.1 Clasificación de las Amenazas

Naturales

Fenómenos de la naturaleza fuera del control de la organización: terremotos, inundaciones, incendios naturales, tormentas, cortes de energía por clima.

Accidentales

Sin intención de causar daño: eliminación accidental de datos, errores de configuración, fallas de hardware, pérdida de dispositivos, interrupciones inesperadas.

Intencionales

Son aquellas realizadas deliberadas para obtener beneficio o causar perjuicio: ataques informáticos, malware, fraude, sabotaje, robo, espionaje, phishing, acceso no autorizado.

4.3.2 Clasificación de las Vulnerabilidades

Técnicas

Debilidades relacionadas con la infraestructura tecnológica, el software, el hardware o las redes de comunicación. SO sin actualizar, software con fallas conocidas, contraseñas predeterminadas, configuraciones incorrectas, puertos abiertos, ausencia de antivirus/firewall.

Humanas

Se originan por acciones u omisiones de las personas que utilizan o administran los sistemas de información. Contraseñas débiles, compartir credenciales, abrir enlaces sospechosos, errores de configuración, manipulación incorrecta de información confidencial.

Físicas

Son aquellas relacionadas con la protección de las instalaciones, el equipamiento y los recursos físicos de la organización. Ausencia de controles de acceso físico, falta de CCTV, sin detección/extinción de incendios, cableado expuesto, equipos sin protección.

Organizativas

Se producen cuando la organización presenta deficiencias en la gestión de la seguridad de la información. Inexistencia de políticas de seguridad, procedimientos no documentados, falta de responsabilidades, ausencia de auditorías, sin planes de continuidad.

4.3.3 Relación entre Amenazas y Vulnerabilidades

Una amenaza representa la posibilidad de un evento perjudicial; una vulnerabilidad es la debilidad que permite que se materialice. En general, una amenaza necesita aprovechar una vulnerabilidad para producir un incidente.

Amenaza + Vulnerabilidad → Posibilidad de incidente de seguridad

Incendio (natural)	+ Sin detectores / extinción (física)
Ciberdelincuente (intencional)	+ Contraseñas débiles (humana)
Atacante (intencional)	+ Error de configuración (técnica)
Diversos incidentes	+ Ausencia de políticas (organizativa)

4.4 Proceso de Análisis de Riesgos

Proceso sistemático que permite identificar, evaluar y tratar los riesgos. Su finalidad es facilitar la toma de decisiones sobre las medidas de seguridad para proteger los activos.

1. **Definir el Alcance**
2. **Identificar Activos**
3. **Identificar Amenazas**
4. **Vulnerabilidades y Controles**
5. **Evaluar el Riesgo**
6. **Tratar el Riesgo**

Paso 1. Definir el Alcance

Todo análisis debe comenzar definiendo claramente qué parte de la organización será objeto del estudio. El alcance establece los límites y evita evaluar sistemas o recursos fuera del proyecto.

¿Qué vamos a analizar?

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.

Paso 2. Identificar los Activos

Se identifican los activos que poseen valor para la organización. Se elabora o actualiza el inventario y se verifica la **valoración** de cada uno, identificando aquellos cuya pérdida generaría mayores consecuencias.
Se apoya en el trabajo del apartado 4.2 Activos de Información.

¿Qué debemos proteger?

En esta etapa se consolida el inventario de activos (identificador, tipo, ubicación, responsable, criticidad) y se confirma la **valoración** según criterios económicos, operativos, legales y la tríada CIA.

Paso 3. Identificar las Amenazas

Se identifican las amenazas que podrían afectar a los activos previamente listados. Las amenazas pueden ser naturales, accidentales o intencionales (apartado 4.3). Se busca determinar todos los eventos que podrían comprometer la seguridad de los activos analizados.

¿Qué puede afectar a los activos?

Naturales

Terremotos, inundaciones, tormentas...

Accidentales

Errores humanos, fallas técnicas...

Intencionales

Ataques, malware, fraude, phishing...

Paso 4. Identificar Vulnerabilidades y Controles

Se analizan las vulnerabilidades presentes en los activos y los controles de seguridad existentes para determinar el nivel de protección actual de la organización.

Vulnerabilidades

Debilidades que pueden ser aprovechadas por una amenaza.

¿Qué vulnerabilidades presentan los activos?

Técnicas · Humanas · Físicas · Organizativas

Controles de seguridad

Medidas técnicas, físicas u organizativas que previenen incidentes o reducen probabilidad/impacto.

Ejemplos: firewall, MFA, antivirus, backups, políticas, capacitación, IDS, control de acceso.

¿Qué vulnerabilidades presentan los activos? ¿Qué controles de seguridad existen para reducir el riesgo?

Paso 5. Evaluar el Riesgo

Con la información de los pasos anteriores se estima el nivel de cada riesgo para establecer prioridades de tratamiento.
Pregunta: **¿Qué tan importante es el riesgo?**

Modelo 1

Valor del Activo × Probabilidad de la Amenaza

Útil en análisis introductorios y ejercicios académicos.

Cuanto mayor el valor del activo o la probabilidad, mayor el riesgo.

Modelo 2

Probabilidad × Impacto

El más usado en metodologías modernas. Permite construir matrices de riesgo.

Un incidente poco probable pero muy grave puede equipararse a uno frecuente de impacto bajo.

Paso 6. Tratar el Riesgo

¿Qué haremos con el riesgo identificado? Se decide cómo gestionarlo según su nivel, los recursos disponibles y las políticas de la organización.

Evitar	Eliminar la fuente del riesgo (retirar servidor obsoleto, cancelar servicio riesgoso).
Mitigar	Implementar controles que reduzcan probabilidad o impacto (firewall, MFA, backups, capacitación).
Transferir	Trasladar consecuencias a un tercero (seguro informático, externalización).
Aceptar	Asumir el riesgo cuando es aceptable o el costo de reducirlo supera el beneficio.

4.5 Matriz de Riesgos

Herramienta gráfica o tabular que clasifica los riesgos según la probabilidad de materialización y el impacto sobre la organización. Facilita la priorización de controles. Cada riesgo combina Activo + Amenaza + Vulnerabilidad.

R1	Servidor BD · Ransomware · SO sin actualizar
R2	Servidor BD · Corte de energía · Ausencia de UPS
R3	Servidor BD · Robo · Sala sin control de acceso

4.5.2 Tipos de Valoración del Riesgo

Cualitativa

Clasifica con categorías descriptivas (Bajo, Medio, Alto, Crítico). Útil cuando no hay datos estadísticos o se necesita un análisis rápido.

Semicuantitativa

Asigna valores numéricos a escalas cualitativas (1–5). Permite cálculos sencillos y comparación entre riesgos. Muy usada en trabajos prácticos.

Cuantitativa

Utiliza datos estadísticos, probabilidades reales y pérdidas económicas. Requiere mucha información; usada en organizaciones que pueden estimar pérdidas.

4.5.3 – 4.5.4 Probabilidad e Impacto

Probabilidad

Posibilidad de que una amenaza aproveche una vulnerabilidad.

- Baja: rara vez ocurre
- Media: puede ocurrir ocasionalmente
- Alta: ocurre con frecuencia

Se consideran: antecedentes, exposición, vulnerabilidades conocidas, frecuencia de ataques similares.

Impacto

Consecuencias del incidente sobre la organización.

- Bajo: inconvenientes menores
- Medio: interrupciones parciales
- Alto: pérdidas importantes o procesos críticos

Puede ser económico, operativo, legal o reputacional.

4.5.5 Construcción e interpretación de la matriz

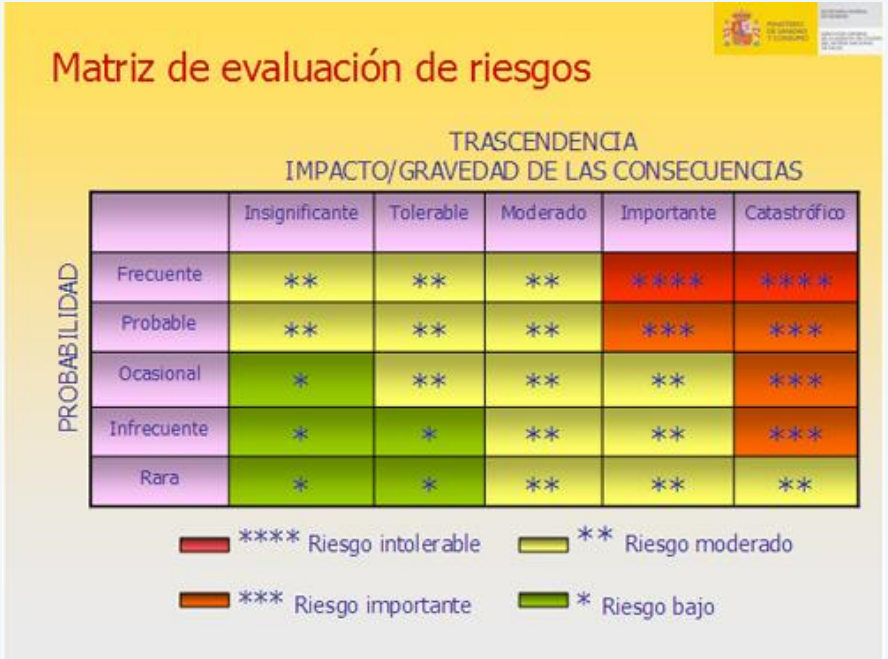
Impacto / Prob.	Baja	Media	Alta
Alto	Medio	**Alto**	**Crítico**
Medio	Bajo	Medio	**Alto**
Bajo	Bajo	Bajo	Medio

Interpretación: Bajo → monitorear · Medio → controles · Alto → acciones cortoplazo · Crítico → atención inmediata

La matriz no elimina el riesgo; es una herramienta de apoyo para priorizar y tomar decisiones.

4.5.5 Construcción e interpretación de la matriz

Matriz de Análisis de Riesgo		Probabilidad de Amenaza					
Elementos de Información	Magnitud de Daño	Criminalidad		Sucesos físicos		Negligencia	
		Robo	Virus	Incendio	Falta de Corriente	Compartir contraseñas	No cifrar datos críticos
Datos e Información							
RR.HH							
Finanzas							
Sistema e Información							
Computadoras							
Portátiles							
Personal							
Coordinador							
Personal técnico							



4.5.8 Ejemplo de valoración semicuantitativa

Riesgo = Valor del Activo × Probabilidad de la Amenaza

Datos del análisis

Activo: Servidor de Base de Datos
Valor del activo: 5 (muy alto)
Amenaza: Ransomware
Probabilidad: 4 (alta)

Cálculo y clasificación

Riesgo = 5 × 4 = 20

Escala:
1–5 Bajo · 6–10 Medio
11–15 Alto · 16–25 Crítico

Resultado: Crítico

Tratamiento: Mitigar (actualizar SO, backups, MFA, monitoreo). No se puede evitar ni aceptar un riesgo crítico sobre un activo esencial.

4.6 Metodologías para el Análisis de Riesgos

MAGERIT — Gobierno de España

Énfasis en valoración de activos y análisis sistemático de amenazas y riesgos. Muy difundida en el ámbito hispanohablante.

OCTAVE — Carnegie Mellon (SEI)

Prioriza la participación del personal y el conocimiento del negocio. Identifica activos críticos con enfoque organizacional.

ISO/IEC 27005 — ISO

Directrices para la gestión de riesgos dentro de un SGSI. Proceso general adaptable: contexto, identificación, análisis, evaluación, tratamiento y seguimiento.

4.6.4 Comparación de metodologías

Metodología	Origen	Principal característica
MAGERIT	Gobierno de España	Valoración de activos y análisis sistemático
OCTAVE	Carnegie Mellon	Participación del personal y enfoque de negocio
ISO/IEC 27005	ISO	Directrices para riesgos dentro de un SGSI

No existe una metodología única. La elección depende del tamaño, complejidad, recursos y requisitos de la organización. Muchas adaptan o combinan elementos de varias.

4.7 Políticas de Seguridad

Documento formal aprobado por la dirección que establece los principios, objetivos y normas generales destinadas a proteger la información y los sistemas informáticos. Las políticas de seguridad indican qué debe hacerse, mientras que los procedimientos describen cómo debe realizarse cada actividad.

Características de una política efectiva

- Aprobada por la dirección: Respaldo de la máxima autoridad
- Clara y comprensible: Lenguaje sencillo, sin ambigüedades
- Aplicable: Realista y posible de implementar
- Difundida: Todos los usuarios la conocen
- Actualizada: Revisión periódica ante nuevos riesgos

4.7.3 Ciclo de una Política de Seguridad (etapas)

1. **Definición de necesidades**
   se analizan las necesidades de seguridad de la organización considerando: activos, riesgos, requisitos legales y objetivos

2. **Definición de acciones**
   Con base en las necesidades identificadas, se establecen las reglas y lineamientos generales de protección

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. **Auditoría de seguridad**
   Se verifica el cumplimiento y la eficacia de la política mediante auditorías de seguridad. Y se reinicia nuevamente el ciclo

Ejemplo: Políticas derivadas del análisis de riesgos

Como resultado del análisis de riesgos de una universidad, podrían establecerse:

1. Todos los usuarios deberán utilizar contraseñas robustas y no compartirlas.
2. Se realizarán copias de seguridad diarias de la base de datos académica.
3. Los servidores deberán mantenerse actualizados con los últimos parches de seguridad.
4. El acceso al centro de cómputos estará restringido únicamente al personal autorizado.
5. Las cuentas de usuario inactivas durante un período prolongado serán deshabilitadas.
6. Se implementará autenticación multifactor para cuentas administrativas.