GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

BASADA EN LA NORMA ISO/IEC 27001

Ing. María de los Ángeles Cicerone
Universidad Tecnológica Nacional – Facultad Regional Córdoba
Argentina
Mayo 2025

¿QUÉ ES LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN?

Proceso sistemático para identificar, analizar, evaluar y tratar riesgos que afectan la confidencialidad, integridad y disponibilidad de la información.

NORMAS ISO RELEVANTES

01

- ISO/IEC 27001: Requisitos del SGSI, incluye la gestión de riesgos como elemento central.

02

- ISO/IEC 27005: Guía específica para la gestión de riesgos.

03

- ISO/IEC 27002: Controles de seguridad aplicables como tratamiento de riesgos.

PROCESO DE GESTIÓN DE RIESGOS (ISO/IEC 27005)

1. ESTABLECER EL CONTEXTO

2. IDENTIFICACIÓN DE RIESGOS

3. ANÁLISIS DE RIESGOS

4. EVALUACIÓN DE RIESGOS

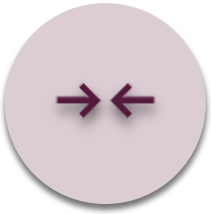
5. TRATAMIENTO DE RIESGOS

IDENTIFICACIÓN DE RIESGOS

ACTIVOS

AMENAZAS

VULNERABILIDADES



IMPACTO

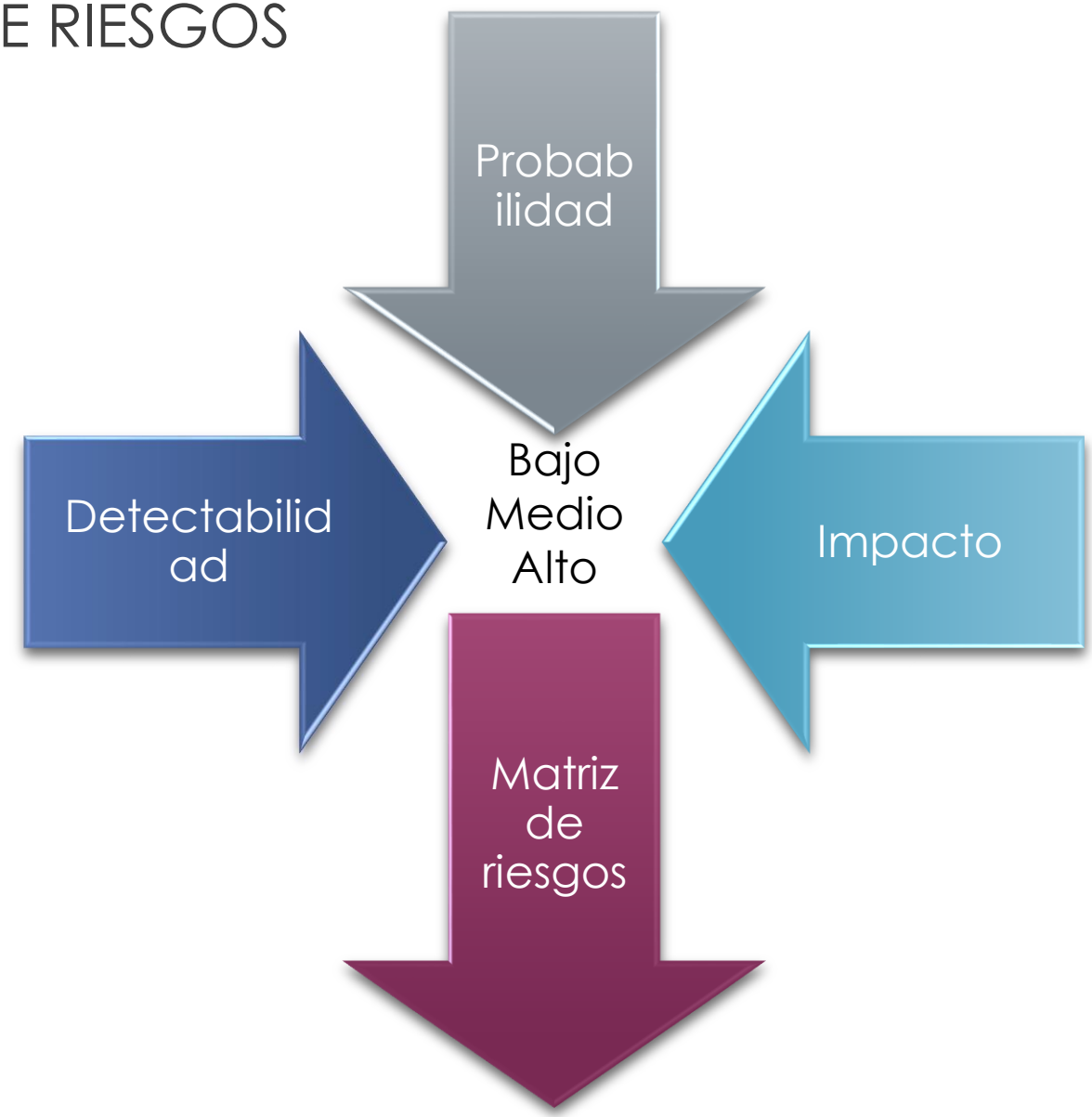
Servidor
de timestamp

Ataque DoS

Falta de protección

Indisponibilidad
del servicio

EVALUACIÓN DE RIESGOS



TRATAMIENTO DEL RIESGO

Opciones:

- Reducir (implementar controles)
- Evitar (cambiar procesos)
- Transferir (seguro, outsourcing)
- Aceptar (riesgo residual controlado)

REGISTRO Y REVISIÓN

- Registro de riesgos documentado y actualizado

- Evaluación periódica

- Parte del ciclo de mejora continua del SGSI (PDCA)

BENEFICIOS DE UNA BUENA GESTIÓN DE RIESGOS

- REDUCCIÓN DE INCIDENTES

- CUMPLIMIENTO NORMATIVO

- TOMA DE DECISIONES INFORMADA

PREGUNTAS / CIERRE

- • ¿Qué otros riesgos existen o conoces como frecuentes?
- • ¿Están siendo gestionados adecuadamente?

MUCHAS GRACIAS!

Contacto: Ing. María de los Ángeles Cicerone

angelescicerone@gmail.com

UTN | FACULTAD REGIONAL CÓRDOBA