Matriz de Riesgos

"La ciberseguridad no falla por falta de tecnología, sino por falta de gestión del riesgo"

Desliza →

Matriz de Riesgos

Qué es?

Una matriz de riesgos es una herramienta de gestión que permite visualizar, priorizar y comunicar los riesgos que amenazan la seguridad de la información de una organización.

Se construye al evaluar la probabilidad de ocurrencia de un evento adverso y el impacto potencial que tendría sobre los activos de información, los procesos de negocio y la continuidad operativa.

Ingrid Mora

Matriz de Riesgos

Objetivo

- Identificar y evaluar riesgos sobre activos de información.
- Priorizar medidas de tratamiento y mitigación.

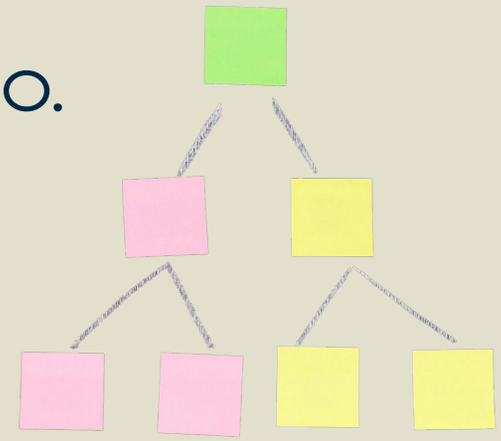
- Proveer trazabilidad y evidencia frente a auditores y reguladores.
- Facilitar que la dirección tome decisiones informadas y estratégicas.

Ingrid Mora

Matriz de Riesgos

Estructura básica

- Activos: datos, sistemas, procesos.
- Amenazas y vulnerabilidades: qué podría suceder y cómo.
- Valoración: impacto × probabilidad.



- Controles: alineados al Anexo A (2022) de la 27001.
- Plan de tratamiento: aceptar, transferir, evitar o mitigar.

Ingrid Mora

Matriz de Riesgos

¿Para qué sirve realmente?

- Justifica inversiones en seguridad con base en riesgos reales.
- Fortalece la cultura de riesgos y sensibiliza a toda la organización.
- Conecta la ciberseguridad con la estrategia empresarial.
- Asegura cumplimiento normativo y contractual, generando confianza en clientes y socios.

Ingrid Mora

Matriz de Riesgos

¿Quién la implementa?

El CISO o equipo de seguridad lidera el proceso, pero su validación corresponde a la alta dirección.

Esto garantiza que el riesgo sea un tema de negocio, no solo de tecnología.

Ingrid Mora

Matriz de Riesgos

Factores a considerar

- Contexto y apetito de riesgo de la organización.
- Requisitos legales y regulatorios
  (ej. GDPR, o leyes locales).
- Evaluaciones periódicas, porque los riesgos evolucionan.
- Integración con ISO/IEC 27005
  (gestión de riesgos de seguridad de la información)
  y ISO 31000
  (gestión de riesgos corporativos).

Ingrid Mora

En Resumen

La matriz de riesgos no es un requisito burocrático, es la pieza que transforma la seguridad en gobernanza y convierte la 27001 en una **ventaja competitiva**.

“La ciberseguridad no se improvisa: se gestiona. ¿Tu organización ya tiene una matriz de riesgos que guíe la implementación de ISO/IEC 27001?

El momento de construirla es ahora.”

Si quieres conocer como te beneficia y te impacta, contáctame y conversamos.

Email: imora@wafratransformation.com

WAFRA

Ingrid Mora