Fundada 2003

Skína IT Solutions

# MISI
# Metodología Integral para la Seguridad de la Información

Ing. Ricardo Naranjo Faccini, M.Sc.

2024-01-08


https://www.skinait.com/metodologia-integral-para-la-seguridad-de-la-informacion-misi-Escritos-81/

# Objetivos del encargado de la seguridad de la inf. - CISO

- **Proteger la organización antes de que ocurran incidentes.**
  - La prevención, reacción y recuperación requiere presupuesto.
- **Elegir los controles a implementar de acuerdo con la relación entre:**
  - Costo del control.
  - Tiempo de implementacion.
  - Beneficio en mitigación de los riesgos.
- **Valorar los riesgos de acuerdo con:**
  - La probabilidad de ocurrencia de los incidentes.
  - El impacto del daño o pérdida de los activos.
- **Conocer las amenazas más relevantes para la organización.**
- **Identificar las vulnerabilidades que tienen los activos.**
- **Realizar el levantamiento de un completo inventario de activos.**

# 3 formas de obtener presupuesto

- **Justificando en la ecuación U = I - E**
  - Es lo que hacen las áreas no relacionadas con riesgos.
  - Subir los ingresos:
    - Incrementando ventas.
    - Incrementando producción.
  - Incrementar el ahorro:
    - Reduciendo costos.
- **Justificando en prevención:**
  - Ya no es tan fácil, no es "natural".
  - Alertar sobre los riesgos.
  - Relación costo/beneficio de los controles.
- **Después de un incidente con un alto costo :(**

# Selección de controles

- Análisis costo-beneficio
- Matriz de Eisenhower ajustada

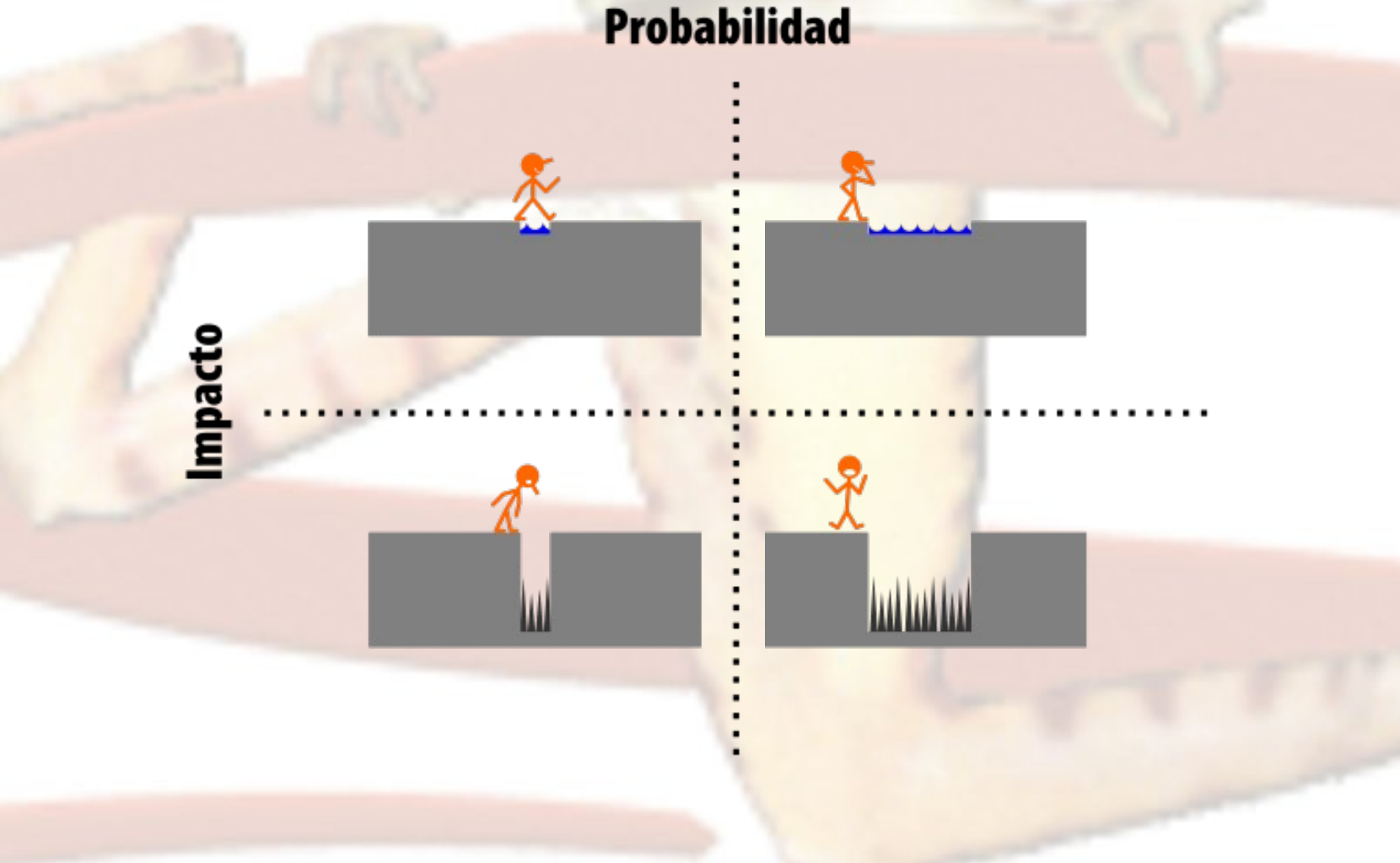
| Impacto en mitigación de riesgos | Costo de implementacion del control: Bajo | Costo de implementacion del control: Alto |
|---|---|---|
| Alto | **¡Hazlo ya!** Abordar riesgos críticos de manera eficiente, serán los primeros controles en ser implementados. | **Planealo** Justificar la inversión con un análisis costo-beneficio o evaluar la posibilidad de asumir el riesgo o tercerizarlo mediante un seguro. |
| Bajo | **Cuando se pueda** Pueden considerar ser implementados por su bajo costo, a pesar que mitigan riesgos de menor prioridad. | **Usa mejor tus recursos** Evaluar cuidadosamente antes de implementar, en la mayoría de los casos se descartan para utilizar los recursos en otras áreas. |

# Identificación y valoración de riesgos

Fundada 2003

Skína IT Solutions

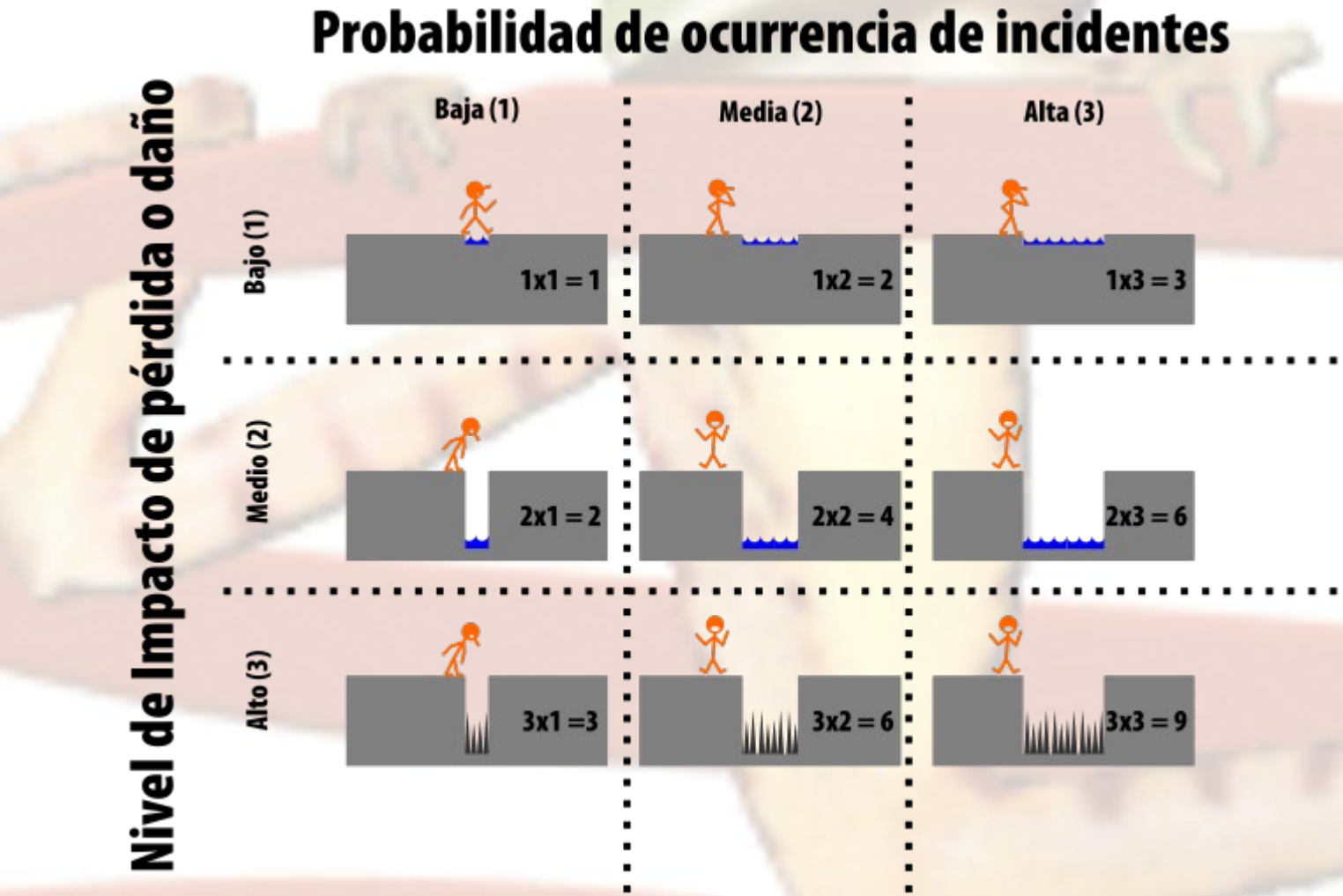
## Cruzar la probabilidad de ocurrencia de un incidente con el impacto de perder un activo

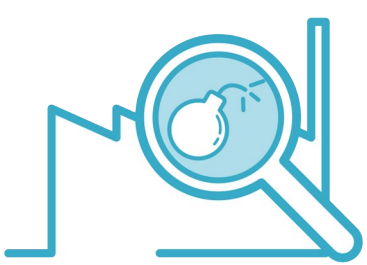



CO COLOMBIA

# Identificación y valoración de riesgos

## El puntaje genera un valor para priorizar



# Inteligencia de amenazas

- **Mirar hacia afuera**
  - ¿Cómo han atacado a mis vecinos?
  - ¿Cómo han atacado a mi competencia?
  - ¿Cómo han atacado mi sector?
  - ¿Qué dicen las autoridades?
  - ¿Qué dicen los expertos?
- **Las amenazas no se pueden controlar**
  - Existe y existirán sin importar cuántos recursos inviertas
- **Se calcula la probabilidad de ocurrencia de los incidentes**

# Inteligencia de amenazas

Fundada 2003
SkínaIT Solutions

## Tipos de incidentes que afectan la seguridad de la información.


Acceso no autorizado


Malware

Fugas de información

Denegación de servicios


Dirigidos a sitios Web


Inyección de código

Errores humanos


Intrínsecos al software


Dirigidos a móviles


Dirigidos a niños


Acústicos


Secuestro, fraude o suplantación

# Análisis de vulnerabilidades

- Cada elemento del inventario
- Las vulnerabilidades se controlan mediante la inversión de recursos:
  - Temporales (tiempo)
  - Humanos (conocimiento)
  - Económicos ($$$, tecnología)
- Se calcula la exposición de los activos a las amenazas.
- Niveles de exposición porcentuales.

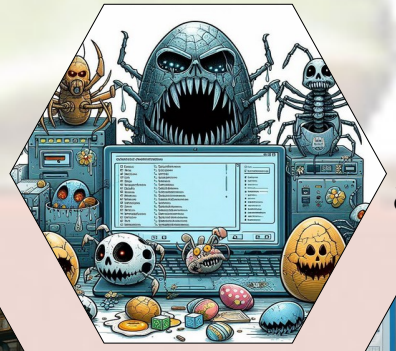
# Análisis de vulnerabilidades

Fundada 2003

SkínaIT Solutions

Áreas clave sin protección

Mala configuración



Obsolescencia, daños y descomposición

Falta de alternativas de abastecimiento


Control de acceso inadecuado


Software vulnerable

Interrupción de suministros

Negligencia o ingenuidad del personal

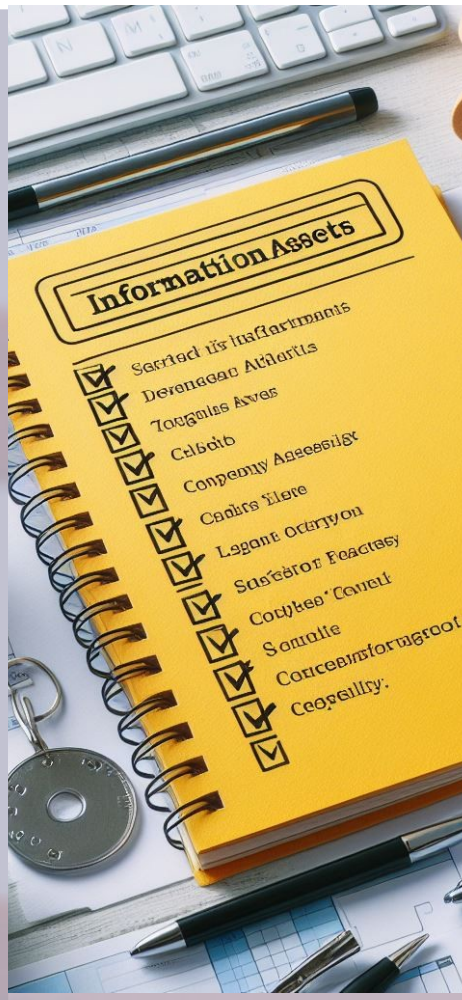
Deficiente monitoreo, detección y vigilancia

Falta de confidencialidad

CO COLOMBIA

# Inventario de activos

- **Saber qué hay que proteger es el primer paso para protegerlo**
- **Se calcula el impacto de incidentes por:**
  - Confidencialidad
    - Robo, filtraciones o fugas
  - Integridad
    - Activo no confiable, no veraz o incompleto
  - Disponibilidad
    - Bloqueo o pérdida del activo
- **Mantener actualizado el inventario**
  - Adquisición
  - Disposición / daño / pérdida / obsolescencia



# Implementación de controles

- **ISO:IEC 27002:2022**
  - Organizacionales: 37 controles
  - Personas: 8 controles
  - Físicos: 14 controles
  - Tecnológicos: 34 controles
- **Registro del progreso de la implementación.**
- **Comparar mes a mes los avances en mitigación de riesgos.**
- **Monitoreo de la mitigación de los riesgos.**

# Ciclo de vida MISI

# Facilitamos el proceso

- Guia a través de toda la metodología MISI
- Inventario de activos
- Análisis de vulnerabilidades
- Inteligencia de amenazas
- Priorización de riesgos
- Selección de controles
- Trazabilidad del proceso de montaje

27k Pal by SkínaIT Solutions

CO COLOMBIA

# Muchas Gracias

¿Preguntas?

ventas@skinait.com

http://www.skinait.com