Fundada 2003

SkínaIT Solutions

MIGRI
Metodología Integral para la Gestión de Riesgos

Ing. Ricardo Naranjo Faccini, M.Sc.

2024-01-08

https://skinait.com/MIGRI-Escritos-81/

Marcos de seguridad de la información

- **Hay muchas aproximaciones**
  - ISO/IEC 27000 ; ISO/IEC 31000 y sus familias
  - NIST, ISACA COBIT 5, CRAMM, COSO, Octave, Magerit, ...
- **Cada una con sus virtudes y sus oportunidades para mejorar**
- **Dicen qué hay que hacer**
- **No dicen cómo hacerlo**

Software para Seguridad de la Información

- Mucha oferta de software técnico/táctico
  - Firewalls
  - Antivirus
  - Análisis de vulnerabilidades
  - Análisis de bitácoras
  - Monitoreo
- Poca oferta estratégica

Ciclo de vida MIGRI

Inventario de activos

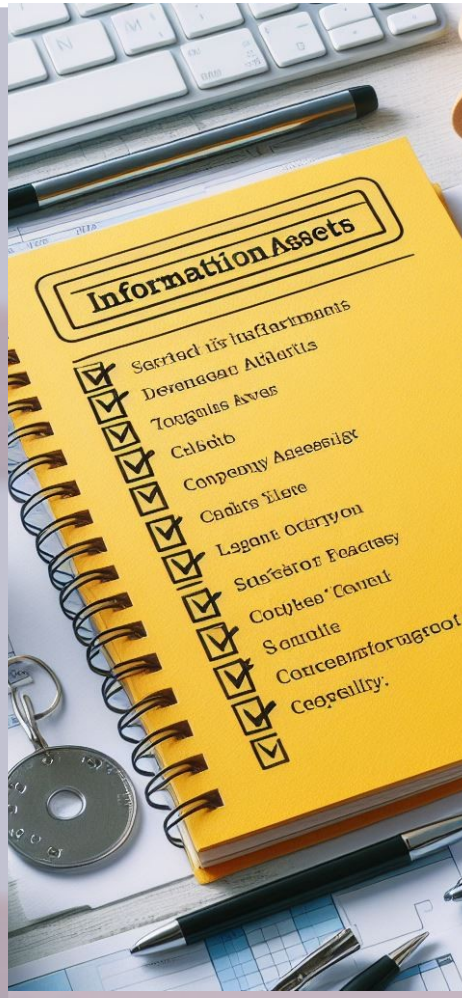
- **Clasificación / Identificación / Rotulación**
  - Información
    - Archivos / Bases de datos / Documentos importantes
    - Backups / Metadatos / Bitácoras
    - Llaves de cifrado / firmas electrónicas.
  - Hardware
    - Servidores / Computadores / Dispositivos de almacenamiento.
    - Portátiles / Móviles / IoT / Ciberfísicos / Domótica
    - Redes / enrutadores / gateways / firewalls / appliances
  - Software
    - Desktop / Motores de base de datos / Web / Cloud / Apps.
  - Servicios
    - Web / email / ssh / ERP / CRM / LMS / Mesa de ayuda / RDP

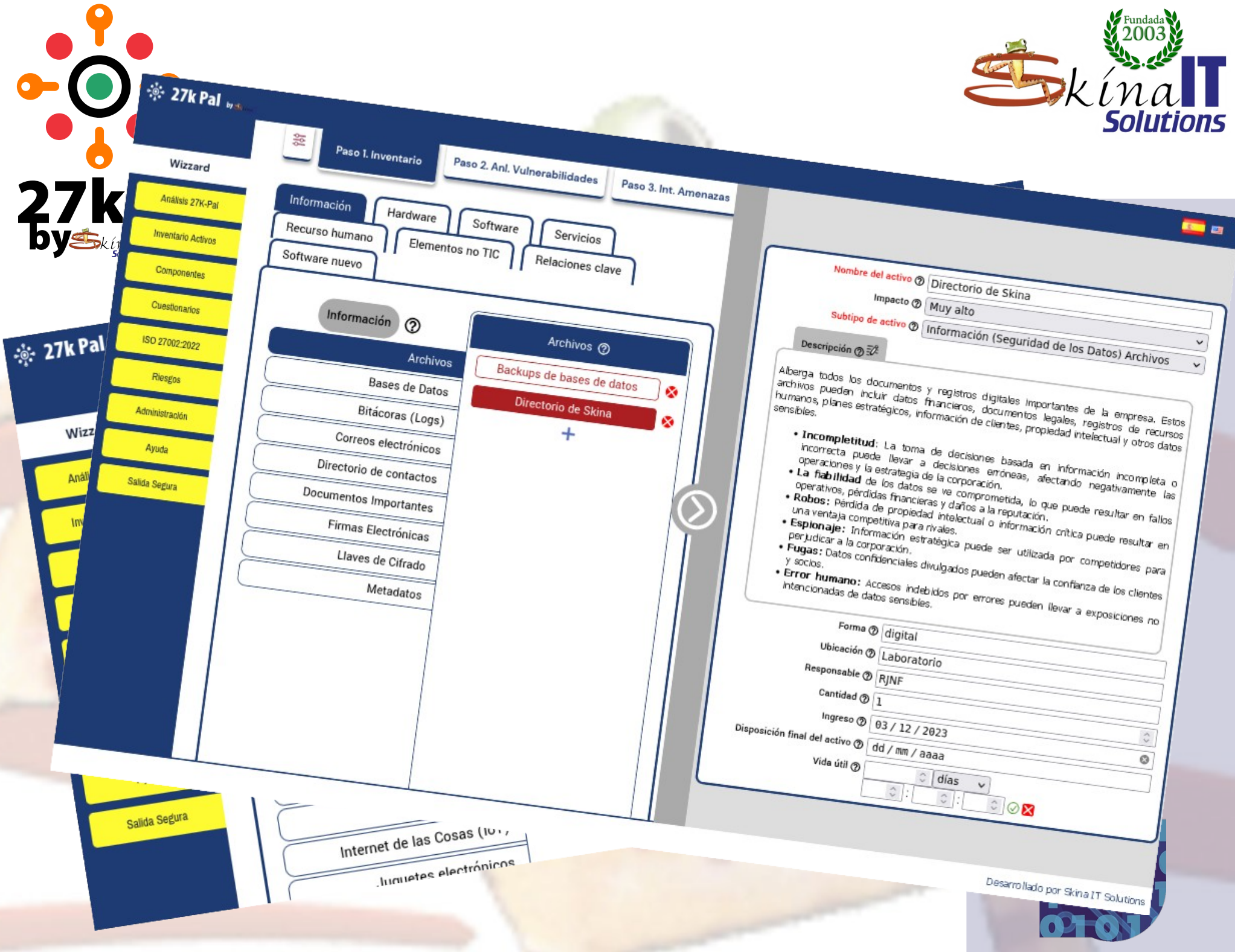
Inventario de activos

- **Incluír elementos NO-TIC**
  - Fluído eléctrico.
  - Conectividad
    - Internet - servidores onLine/Cloud.
  - Infraestructura.
  - Buen nombre / Reputación.
  - Relaciones con (directorio):
    - Directivos, implicados, clientes, proveedores
    - Pares, entes de control.
  - Personal con condiciones especiales.
  - Secretos industriales.
  - Propiedad intelectual.

Inventario de activos

- **Determinar el grado de impacto que produciría:**
  - Integridad:
    - Que la información no esté completa o sea errónea.
    - Daños / Mala calidad de la información.
  - Confidencialidad:
    - Que la información sea conocida por personas no autorizadas.
    - Robos / Espionaje / Fugas / Error humano
  - Disponibilidad:
    - Que no se tenga acceso oportuno a la información.
    - Bloqueos / Denegación de servicio / Lentitud.
  - Privacidad
    - Que los datos personales sean almacenados o publicados sin autorizacion
  - No repudio
    - Que quienes hayan tratado los datos "se hagan los locos".




27k Pal
Wizzard
Análisis 27K-Pal
Inventario Activos
Componentes
Cuestionarios
ISO 27002:2022
Riesgos
Administración
Ayuda
Salida Segura
Paso 1. Inventario
Paso 2. Anl. Vulnerabilidades
Paso 3. Int. Amenazas
Información
Hardware
Software
Servicios
Recurso humano
Elementos no TIC
Relaciones clave
Software nuevo
Información
Archivos
Bases de Datos
Bitácoras (Logs)
Correos electrónicos
Directorio de contactos
Documentos Importantes
Firmas Electrónicas
Llaves de Cifrado
Metadatos
Archivos
Backups de bases de datos
Directorio de Skina
Internet de las Cosas (IoT)
Juguetes electrónicos
Nombre del activo
Directorio de Skina
Impacto
Muy alto
Subtipo de activo
Información (Seguridad de los Datos) Archivos
Descripción
Alberga todos los documentos y registros digitales importantes de la empresa. Estos archivos pueden incluir datos financieros, documentos legales, registros de recursos humanos, planes estratégicos, información de clientes, propiedad intelectual y otros datos sensibles.
• Incompletitud: La toma de decisiones basada en información incompleta o incorrecta puede llevar a decisiones erróneas, afectando negativamente las operaciones y la estrategia de la corporación.
• La fiabilidad de los datos se ve comprometida, lo que puede resultar en fallos operativos, pérdidas financieras y daños a la reputación.
• Robos: Pérdida de propiedad intelectual o información crítica puede resultar en una ventaja competitiva para rivales.
• Espionaje: Información estratégica puede ser utilizada por competidores para perjudicar a la corporación.
• Fugas: Datos confidenciales divulgados pueden afectar la confianza de los clientes y socios.
• Error humano: Accesos indebidos por errores pueden llevar a exposiciones no intencionadas de datos sensibles.
Forma
digital
Ubicación
Laboratorio
Responsable
RJNF
Cantidad
1
Ingreso
03 / 12 / 2023
Disposición final del activo
dd / mm / aaaa
Vida útil
días
Desarrollado por Skina IT Solutions

Ciclo de vida MIGRI

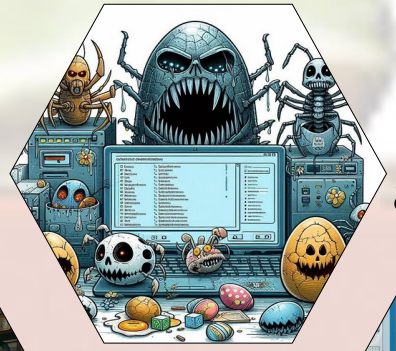
Análisis de vulnerabilidades

- Para cada elemento del inventario
- Las vulnerabilidades se pueden controlar 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

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

Análisis de vulnerabilidades

- **Áreas clave sin protección**
  - Equipos sin supervisión en áreas sin restricción
  - Circulación de personal no autorizado en áreas restringidas
  - Dispositivos de red o cables en áreas sin restricción
  - Puntos finales en áreas sin restricción

- **Gestión inadecuada de control de acceso, autenticación y autorización**
  - En equipos de red
  - En equipos
  - Al software
  - A los datos
  - De los usuarios

Análisis de vulnerabilidades

- **Obsolescencia, daños y descomposición**
  - Falta de mantenimiento preventivo o correctivo de puntos finales
  - Falta de mantenimiento preventivo o correctivo de equipos de red
  - Fragilidad de los materiales que componen la red
  - Fragilidad de los materiales de los equipos
  - Fragilidad de los materiales de los medios de almacenamiento

Análisis de vulnerabilidades

- **Deficiente monitoreo, detección y vigilancia**
  - En la red
  - En puntos finales
  - De las aplicaciones
  - En los datos
- **Falta de confidencialidad**
  - Transmisión de datos por la red sin protección
  - Aplicativos que transmiten datos sin protección
  - Almacenamiento de datos sin protección

Análisis de vulnerabilidades

- **Negligencia o ingenuidad del personal**
  - Del personal de administración del software
  - Del personal de administración de medios de almacenamiento
  - De los usuarios
  - Del personal de auditoría y supervisión
  - Ingenuidad y/o falta de formación sobre seguridad

Análisis de vulnerabilidades

- **Software vulnerable**
  - Existencia de funcionalidades inadecuadas en el software
  - Uso de software desactualizado u obsoleto
  - Bugs, fallos y errores en el software
  - Malas prácticas de adquisición de software
  - Malas prácticas de desarrollo de software
  - Software sin funcionalidades básicas de seguridad

Análisis de vulnerabilidades

- **Falta de alternativas de abastecimiento**
  - Falta de recurso humano alternativo
  - Falta de alternativas de abastecimiento
  - Pérdida de vigencia de las certificaciones
  - Desaparición de entidad de certificación

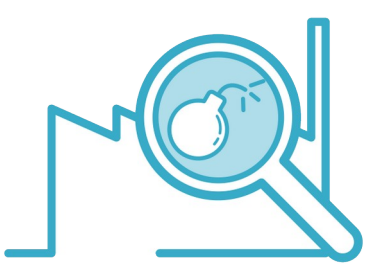
27k Pal

by Skína IT Solutions

Fundada 2003

Skína IT Solutions

Ciclo de vida MIGRI



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

Inteligencia de amenazas

- **Accidentes industriales**
  - Explosiones
  - Corrosión
- **Desastres naturales**
  - Sismos
  - Incendios
  - Inundaciones
- **Afectación ambiental**
  - Polvo
  - Sal marina
  - Plagas

Inteligencia de amenazas

- **Acceso no autorizado**
  - Ataques a contraseñas
    - Diccionario, fuerza bruta, sniffing, rainbow
  - Dumpster diving
  - Hoaxes (Falsos avisos o engaños)
  - Ingeniería social
  - Phishing
    - Spear phishing
    - Whaling
  - Robo de credenciales
  - Shoulder surfing
  - Tailgating

Inteligencia de amenazas

- **Malware**
  - Gusanos
  - Ransomware
  - Troyanos
  - Virus
- **Fugas de información**
  - Fugas de información confidencial
  - Fugas de propiedad intelectual
  - Keyloggers
  - Leaks (filtraciones)
  - Man in the middle (MITM)
  - Publicación accidental de información
  - Spyware

Inteligencia de amenazas

- **Denegación de servicios**
  - Ataques de amplificación
  - Ataques de inundación
  - DDoS
  - DoS
  - Zip Bomb
- **Dirigidos a sitios web**
  - Clickjacking
  - Cross Site Scripting (XSS)
  - Directory traversal
  - Sesión falsa
  - URL injection (%20)

Inteligencia de amenazas

- **Inyección de código**
  - Clickjacking
  - Cross Site Scripting (XSS)
  - Directory traversal
  - Sesión falsa
  - URL injection (%20)
- **Secuestro, fraude y suplantación**
  - Spoofing
    - Suplantación de identidad, Ataques de spoofing, Vishing, Skimming, Carding, Troll farms, Dialers, Cryptocurrency scam, Boicots, Fake news (noticias falsas), Deep Fakes,
  - Hijacking
    - Session Hijacking, Clickjacking, DNS Hijacking, Email Hijacking, Account Hijacking.

Inteligencia de amenazas

- **Acústicos**
  - Asistentes de voz
  - Sonidos de teclados numéricos
  - Ultrasónicos
- **Dirigidos a niños**
  - Cyberbullying
  - Grooming
  - Retos en redes sociales
  - Toy Cracking

Inteligencia de amenazas

- **Dirigidos a móviles**
  - Juice-jacking
  - Malware para OS de móviles
  - SIMjacking o SIM swap scam
  - SMShing
  - Screen Hacking
  - WiFi falsas o redes trampa

Inteligencia de amenazas

- Intrínsecos al software
  - Backdoors
  - Bugs
  - Cracking
  - Easter eggs
  - Exploits
  - Piratería de software
  - Race conditions (Time of check/Time of use, Read-Modify-Write)
  - Rogueware

Inteligencia de amenazas

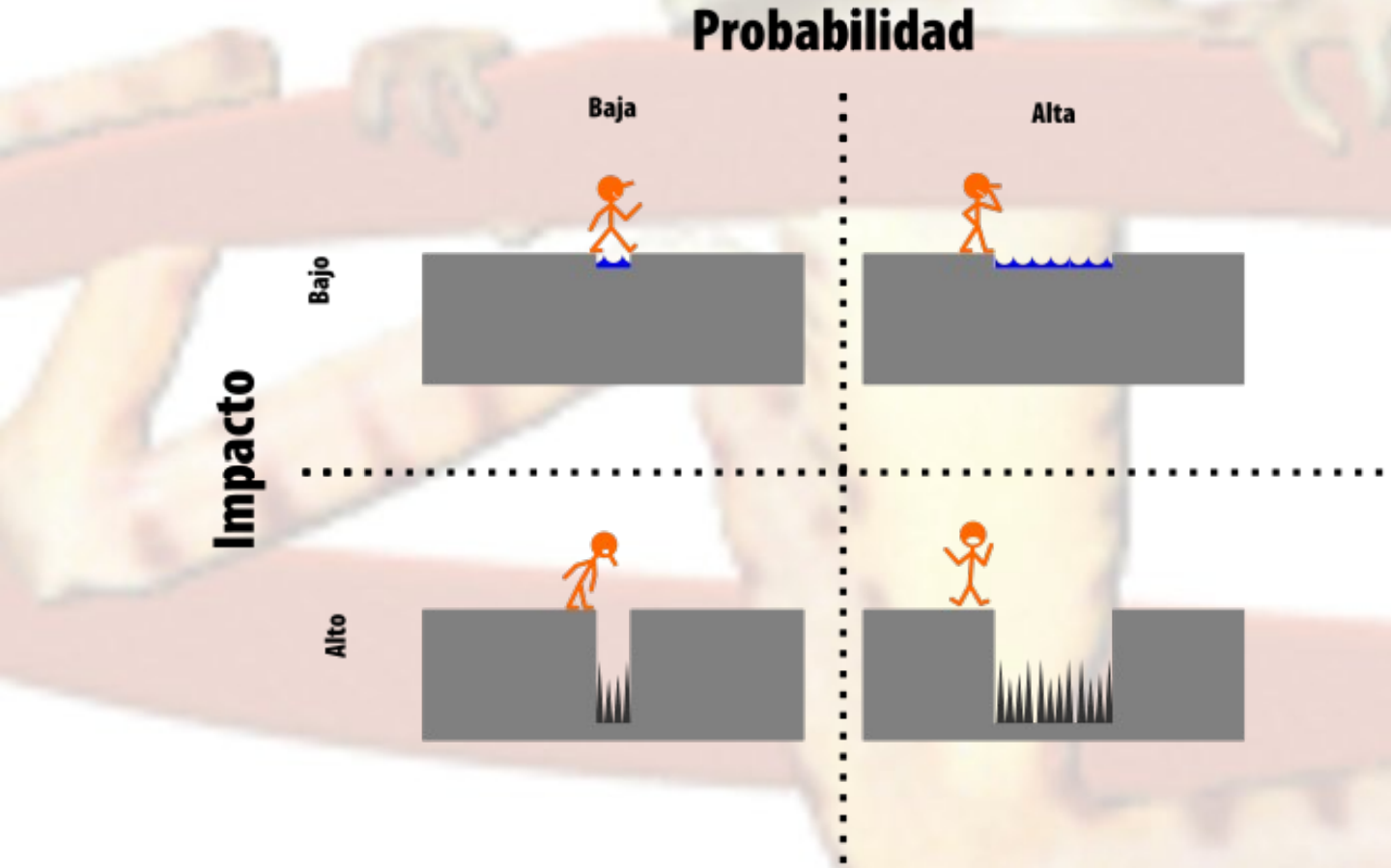
- **Errores humanos**
  - Envío accidental de información confidencial
  - Errores de configuración
  - Pérdida de dispositivos
- **Otros tipos de amenazas**
  - APT (Advanced persistent threats)
  - Botnets
  - Cryptojacking
  - Jackpotting
  - OSINT (Opensource Intelligence)
  - Recuperadores de claves WEP y WPA
  - Rootkits
  - SPAM
  - Wipers

Ciclo de vida MIGRI

Identificación y valoración de riesgos

Fundada 2003
SkínaIT Solutions

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

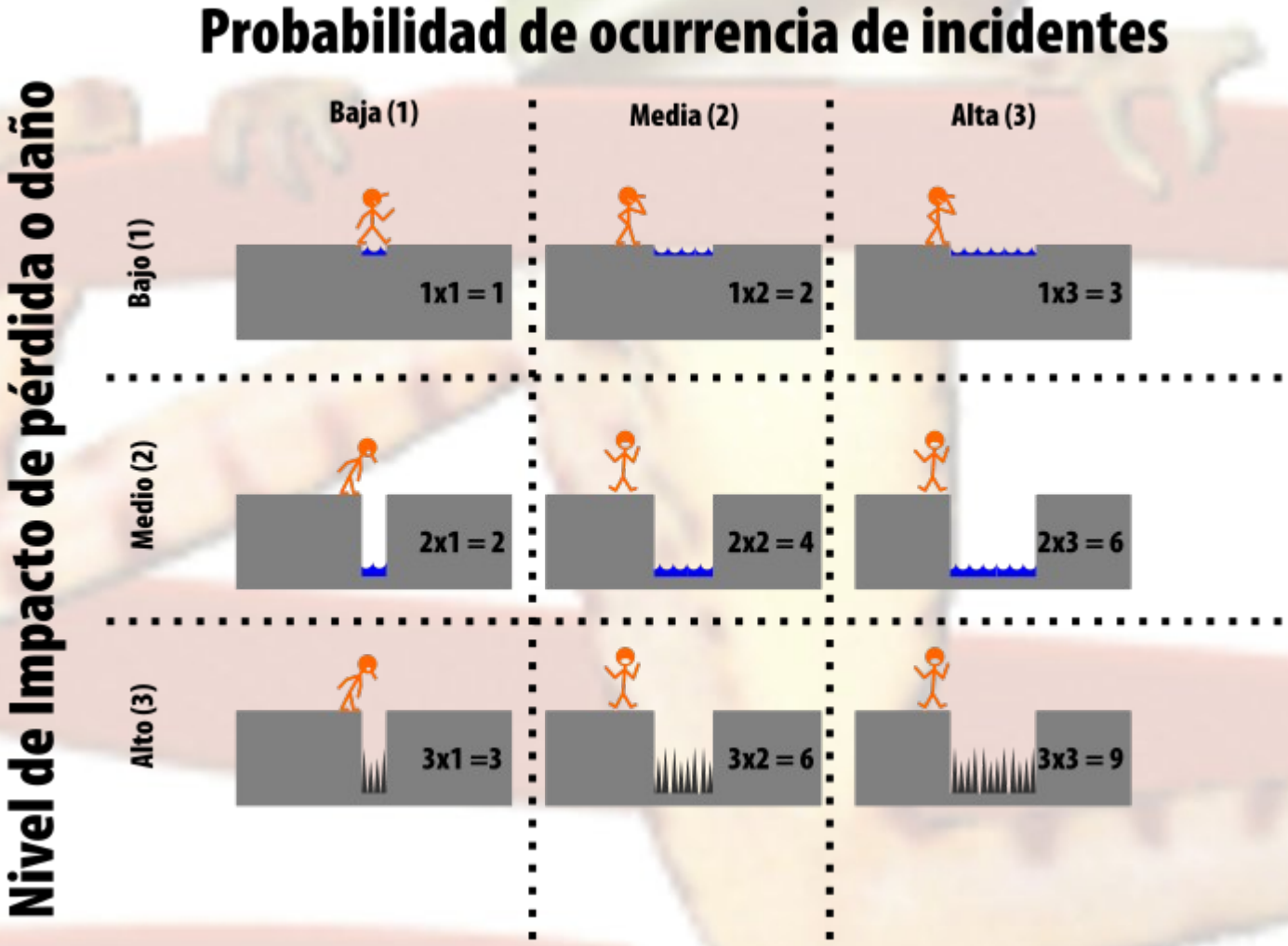


CO COLOMBIA

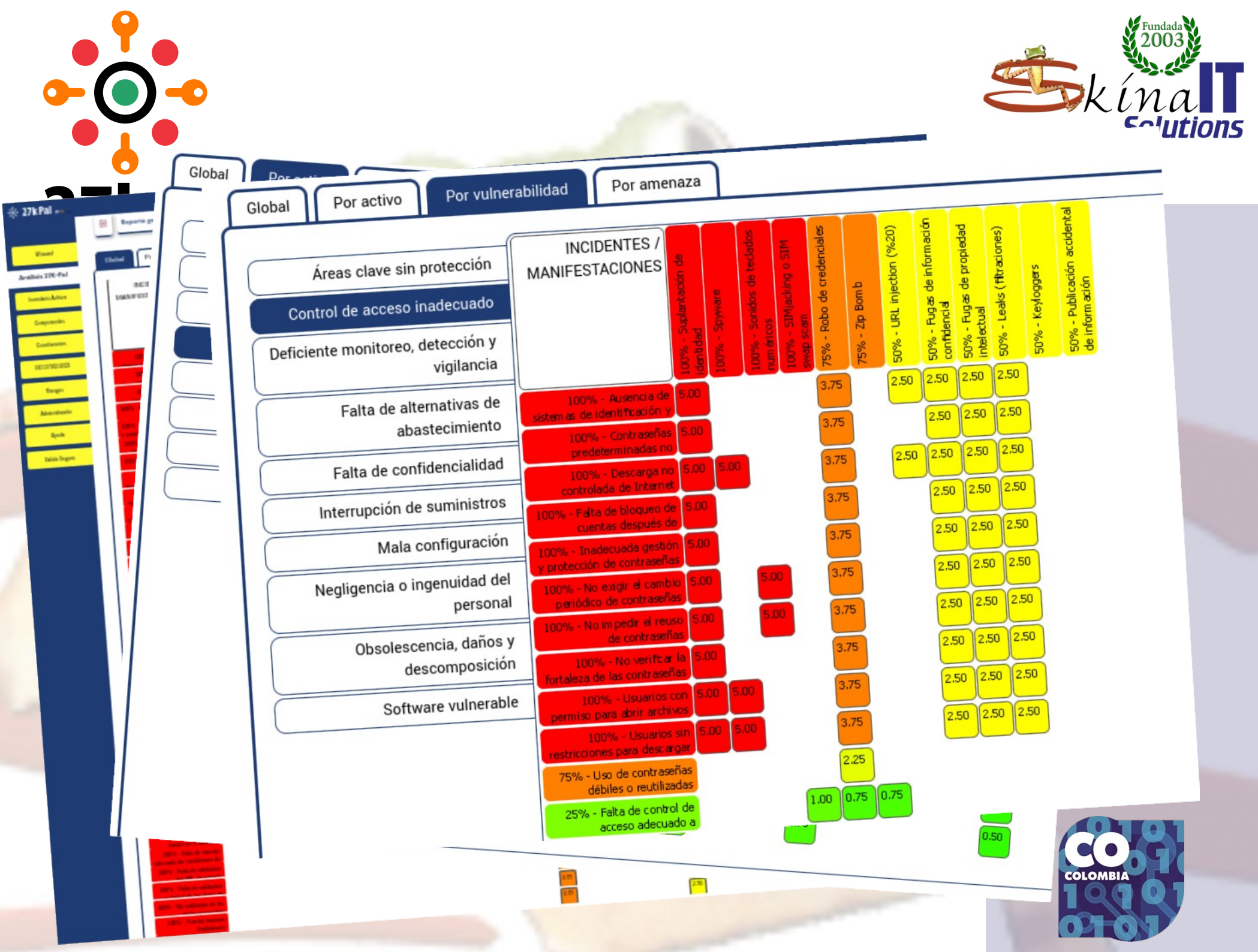
Identificación y valoración de riesgos

Fundada 2003
SkínaIT Solutions

El puntaje genera un valor para priorizar



CO COLOMBIA


Global
Por activo
Por vulnerabilidad
Por amenaza
Áreas clave sin protección
Control de acceso inadecuado
Deficiente monitoreo, detección y vigilancia
Falta de alternativas de abastecimiento
Falta de confidencialidad
Interrupción de suministros
Mala configuración
Negligencia o ingenuidad del personal
Obsolescencia, daños y descomposición
Software vulnerable
INCIDENTES / MANIFESTACIONES
100% - Suplantación de identidad
100% - Spyware
100% - Sonidos de teclados numéricos
100% - SIMjacking o SIM swap scam
75% - Robo de credenciales
75% - Zip Bomb
50% - URL injection (%20)
50% - Fugas de información confidencial
50% - Fugas de propiedad intelectual
50% - Leaks (filtraciones)
50% - Keyloggers
50% - Publicación accidental de información
100% - Ausencia de sistemas de identificación y
100% - Contraseñas predeterminadas no
100% - Descarga no controlada de Internet
100% - Falta de bloqueo de cuentas después de
100% - Inadecuada gestión y protección de contraseñas
100% - No exigir el cambio periódico de contraseñas
100% - No impedir el reuso de contraseñas
100% - No verificar la fortaleza de las contraseñas
100% - Usuarios con permiso para abrir archivos
100% - Usuarios sin restricciones para descargar
75% - Uso de contraseñas débiles o reutilizadas
25% - Falta de control de acceso adecuado a

Ciclo de vida MIGRI

Selección de controles

- Análisis costo-beneficio
- Matriz de Eisenhower ajustada

Costo de implementacion del control

Impacto en mitigación de riesgos	Bajo	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.

Ciclo de vida MIGRI

Implementación de controles

- Registro del progreso de la implementación.
- Monitoreo de la mitigación de los riesgos.
- Comparación del estado de los riesgos en dos momentos diferentes.
  - Al inicio del proceso
  - Trimestralmente
  - Anualmente
  - Al final del proceso

Ciclo de vida MIGRI

Muchas Gracias

¿Preguntas?

ventas@skinait.com

https://skinait.com