T.I RESCUE

SEGURIDAD INFORMÁTICA

# AUDITORÍA INTEGRAL

www.tirescue.com
Info@tirescue.com.co
(57)315 259 2011

# ISO 27001

ISO 27001 es un estándar internacional para la gestión de la seguridad de la información. Ayuda a las organizaciones a establecer, implementar, mantener y mejorar continuamente un **Sistema de Gestión de Seguridad de la Información (SGSI).**

Su objetivo principal es identificar y gestionar los riesgos de seguridad, garantizando la **confidencialidad, integridad y disponibilidad de la información**. Además, permite cumplir con los requisitos legales y contractuales aplicables.

# ¿Qué evalúa **ISO 27001?**

www.tirescue.com

## 01 Infraestructura de TI

Gestión de activos, protección de redes, servidores y dispositivos para garantizar la seguridad de la información.

## 02 Seguridad de aplicaciones

Implementación de controles para el desarrollo seguro, evaluación de vulnerabilidades y gestión de riesgos en software y APIs.

## 03 Identidades y Accesos

Control de accesos, autenticación y gestión de identidades para proteger la confidencialidad de la información.

## 04 Seguridad en la Nube

Aplicación de políticas y controles para la protección de datos en entornos cloud, incluyendo cifrado y gestión de accesos.

## 05 Cumplimiento y gestión de riesgos

Identificación y tratamiento de riesgos de seguridad de la información, cumplimiento de normativas y auditorías de seguridad.

## 06 Seguridad operativa

Monitoreo de incidentes, gestión de eventos de seguridad y capacitación en ciberseguridad para garantizar la mejora continua.

# Metodología y **Aplicación**

El enfoque de ISO 27001 se basa en la gestión de riesgos, la implementación de controles de seguridad y la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

**01**

**Recolección de información:**
Identificación de activos, evaluación de sistemas, controles existentes y requisitos legales aplicables.

**02**

**Análisis de vulnerabilidades:**
Evaluación de riesgos y brechas de seguridad mediante herramientas automatizadas y análisis manual.

**03**

**Pruebas de seguridad:**
Simulación de escenarios de ataque y validación de la efectividad de los controles implementados.

**04**

**Evaluación de riesgos:**
Análisis del impacto y probabilidad de materialización de amenazas, con base en el contexto de la organización.

**05**

**Implementación de medidas de seguridad:**
Aplicación de controles basados en el Anexo A de ISO 27001, alineados con los riesgos identificados.

**06**

**Informe de seguridad:**
Documentación de hallazgos, recomendaciones y estrategias de mitigación para garantizar el cumplimiento del SGSI.

# Beneficios de **ISO 27001**

ISO 27001 proporciona un marco estructurado para la **gestión de la seguridad de la información**, permitiendo a las organizaciones proteger sus activos, reducir riesgos y garantizar el cumplimiento normativo.

✅ Gestión de riesgos y cumplimiento de estándares internacionales.

✅ **Evaluación integral de la seguridad de la información.**

✅ Mejora continua en la protección contra amenazas.

✅ Cumplimiento normativo y regulatorio.

✅ Priorización de acciones según el nivel de riesgo.

## 🔄 Ciclo continuo **de mejora**

La seguridad de la información es un proceso continuo. ISO 27001 impulsa la mejora constante del SGSI mediante revisiones, auditorías y ajustes en las estrategias de seguridad.

Además, puede i**ntegrarse con DevSecOps y otros marcos** para fortalecer los controles y garantizar una protección efectiva.

# 1. Infraestructura de **TI**

La seguridad de la infraestructura tecnológica es clave para proteger los sistemas críticos. ISO 27001 evalúa configuraciones, accesos y controles para minimizar riesgos y garantizar la disponibilidad de la información.

**Redes:** Análisis de configuraciones, segmentación, protección perimetral (firewalls, IDS/IPS) y conexiones seguras (VPN).

**Servidores:** Evaluación de configuraciones de seguridad, control de accesos, gestión de parches y protección de servicios expuestos.

**Dispositivos finales:** Análisis de estaciones de trabajo, laptops y dispositivos móviles para detectar vulnerabilidades y mejorar la seguridad.

✅ Una infraestructura de TI segura es la base para proteger los datos y operaciones de una organización. **La auditoría ISO 27001 permite identificar brechas de seguridad y optimizar los controles existentes**, asegurando el cumplimiento de estándares internacionales y reduciendo riesgos de ciberataques.

# Seguridad de **Aplicaciones**

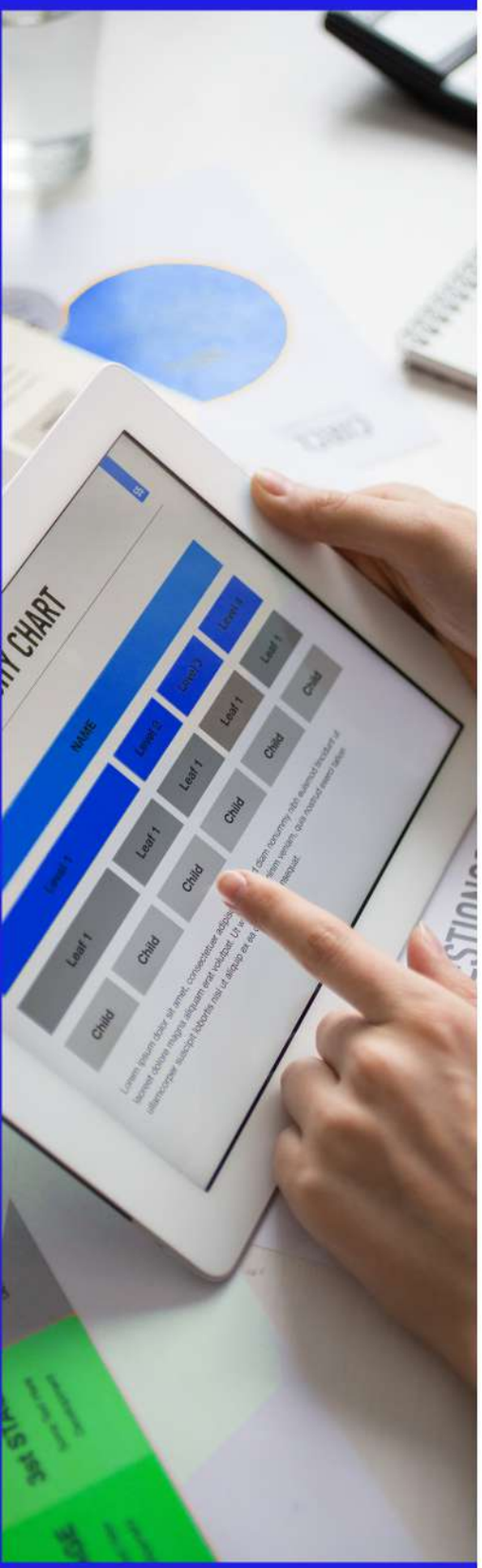
Este enfoque está alineado con los controles del Anexo A de ISO 27001, que incluyen el desarrollo seguro, la gestión de vulnerabilidades y la protección de la información en aplicaciones.

Las aplicaciones son un objetivo frecuente de ataques, por lo que su seguridad debe ser gestionada y evaluada de manera continua según ISO 27001.


**Pruebas de seguridad en aplicaciones:** Evaluación de la seguridad en software y aplicaciones web/móviles mediante análisis estáticos, dinámicos y pruebas de penetración.

**Gestión de vulnerabilidades:** Identificación y mitigación de fallos como inyecciones SQL, XSS, fallos en autenticación y errores de configuración.

**Seguridad de APIs:** Implementación de controles de acceso, cifrado en la transmisión de datos y validación de integridad en las interfaces.



# Seguridad de **Aplicaciones**

Incorporar estos controles en el SGSI optimiza la gestión de accesos, garantizando trazabilidad y respuesta efectiva ante incidentes.

ISO 27001 garantiza una gestión segura de identidades y accesos, minimizando riesgos y protegiendo la información crítica. **Al restringir accesos no autorizados, se refuerza la confidencialidad, integridad y disponibilidad** de los datos.

**Control de accesos:** Asignación de permisos según roles para limitar el acceso solo a lo necesario.

La norma promueve el uso de MFA, privilegios mínimos y monitoreo continuo para prevenir ataques como el robo de credenciales. Auditorías periódicas y políticas de acceso fortalecen la seguridad y el cumplimiento normativo.

**Autenticación segura:** Uso de MFA y contraseñas fuertes para prevenir robos de credenciales.


**Gestión de sesiones:** Bloqueo, expiración y monitoreo de accesos para evitar riesgos.


ISO 27001 impulsa la adopción de controles de seguridad dentro del SGSI, fortaleciendo la protección de la información en entornos cloud. **Su implementación reduce riesgos de exposición y asegura que los accesos, configuraciones y almacenamiento** de datos cumplan con estándares de seguridad.

Aplicar estos controles permite mitigar vulnerabilidades antes de que se conviertan en amenazas críticas, asegurando la continuidad operativa y la resiliencia de los sistemas ante posibles ataques o fallos de seguridad.

# Seguridad en **la Nube**

ISO 27001 establece controles para proteger los entornos cloud, asegurando configuraciones seguras, gestión de accesos adecuada y protección de datos. **Su implementación garantiza el cumplimiento normativo y minimiza riesgos de exposición.**

**Configuraciones seguras:** Prevención de configuraciones incorrectas que puedan exponer información sensible en entornos como AWS, Azure y GCP.

**Control de accesos:** Aplicación del principio de privilegios mínimos y autenticación reforzada para evitar accesos no autorizados.

**Monitoreo y auditoría:** Uso de herramientas de logging, alertas y auditoría para detectar amenazas y responder a incidentes de manera oportuna.

# Cumplimiento y **Gestión de Riesgos**

ISO 27001 proporciona un **marco estructurado** para la identificación, evaluación y tratamiento de riesgos de seguridad de la información, asegurando el cumplimiento normativo y la mejora continua.

**Evaluación de riesgos:** Análisis de amenazas y vulnerabilidades en los activos de información para definir controles adecuados.

**Monitoreo y mejora continua:** Uso de herramientas de auditoría y evaluación para detectar desviaciones y optimizar la seguridad.

ISO 27001 establece un enfoque basado en la gestión de riesgos dentro del SGSI, permitiendo a las organizaciones r**educir amenazas,** cumplir con regulaciones y fortalecer su postura de seguridad.

# Seguridad **Operativa**

ISO 27001 establece controles para garantizar la **protección, monitoreo y respuesta a incidentes de seguridad**, asegurando la disponibilidad, integridad y confidencialidad de la información.

## Evaluación y Respuesta en la **Seguridad de la Información**

ISO 27001 establece controles para garantizar la protección, monitoreo y respuesta a incidentes de seguridad, asegurando la disponibilidad, integridad y confidencialidad de la información.

**Protección de activos:** Aplicación de controles para la seguridad en redes, servidores y estaciones de trabajo, evitando accesos no autorizados.

**Monitoreo continuo:**
Uso de herramientas de SIEM, registros de auditoría y detección de anomalías para identificar actividades sospechosas.

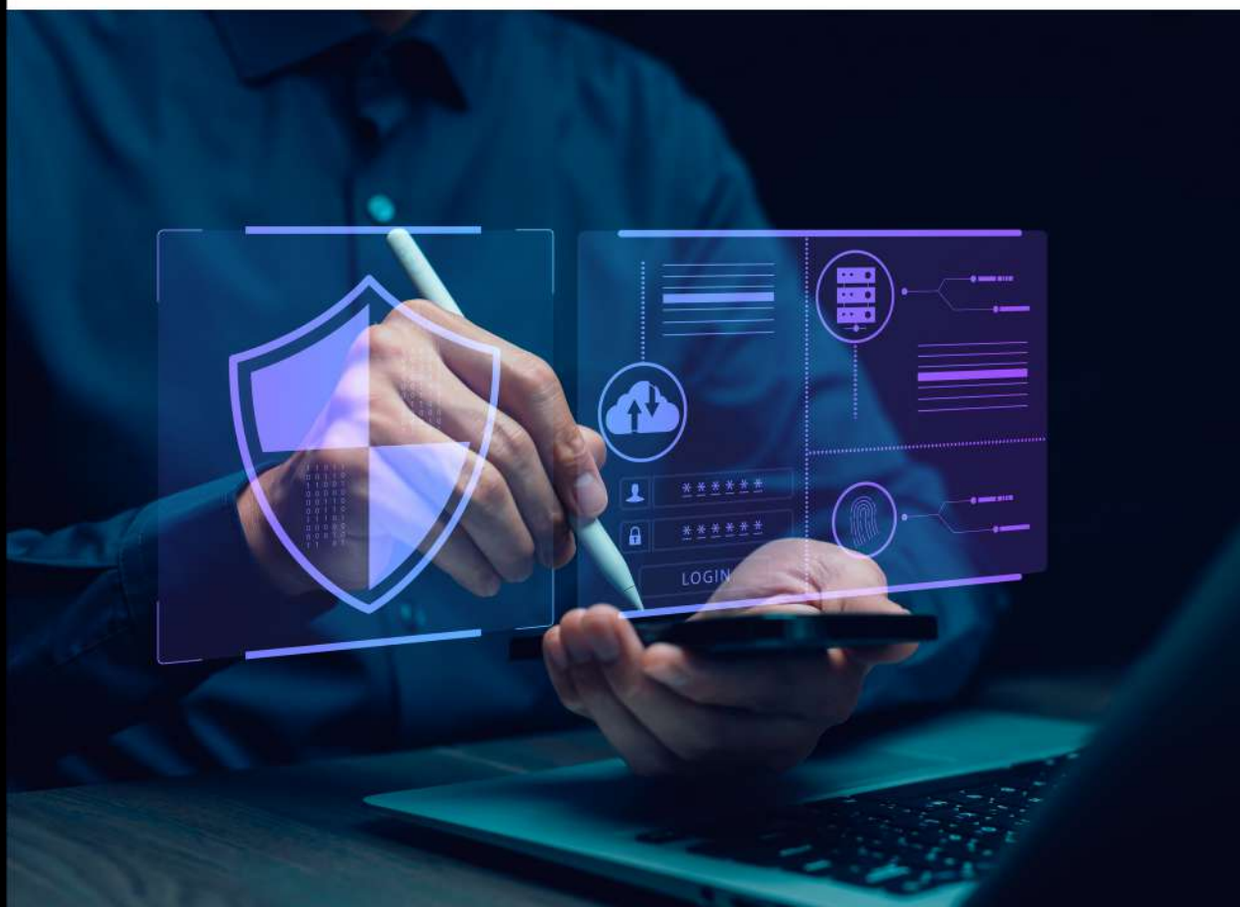
**Gestión de incidentes:** Implementación de procesos para detección, análisis y respuesta ante eventos de seguridad.

**Mejora continua:** Evaluaciones periódicas y auditorías para optimizar la seguridad operativa dentro del SGSI.

ISO 27001 impulsa la adopción de estos controles, permitiendo a las organizaciones responder de manera eficiente a amenazas y mantener la resiliencia operativa.

# OWASP

El Open Web Application Security Project (OWASP) es una iniciativa global dedicada a mejorar la **seguridad del software.** Proporciona metodologías, herramientas y documentación para evaluar, identificar y mitigar vulnerabilidades en aplicaciones web. Nuestro enfoque se basa en las mejores prácticas de OWASP para analizar riesgos, fortalecer la **seguridad de las aplicaciones** y proporcionar recomendaciones estratégicas para mitigar amenazas y mejorar la resiliencia de los sistemas.



# ¿Qué evalúa **OWASP?**

www.tirescue.com

## 01 Seguridad en aplicaciones

Identificación de vulnerabilidades en aplicaciones web, incluyendo ataques como inyección SQL, XSS y autenticación insegura.

## 02 Seguridad en APIs

Evaluación de riesgos en APIs expuestas, detección de fallos en autenticación, autorización y validación de datos.

## 03 Identidades y Accesos

Análisis de mecanismos de autenticación, sesiones y control de accesos para evitar brechas de seguridad.

## 04 Seguridad en la Nube

Evaluación de configuraciones de seguridad en entornos cloud para evitar exposición de datos sensibles.

## 05 Vulnerabilidades y Cumplimiento

Revisión de riesgos de seguridad y alineación con estándares como OWASP Top 10 y ASVS.

## 06 Seguridad operativa

Monitoreo de amenazas, respuesta a incidentes y capacitación en ciberseguridad para desarrollo seguro.

# Metodología y **Aplicación**

OWASP proporciona un marco estructurado para evaluar, identificar y mitigar vulnerabilidades en aplicaciones web y sistemas digitales.

El enfoque de OWASP sigue un proceso sistemático que detecta vulnerabilidades, evalúa riesgos y propone soluciones. Desde la recolección de información hasta el informe final, garantiza una seguridad integral y efectiva.

**Recolección de información:**
Análisis de la arquitectura y seguridad de la aplicación.

**Escaneo de vulnerabilidades:**
Uso de herramientas para detectar fallos en el sistema.

**Pruebas de penetración:**

Simulación de ataques para evaluar la resistencia de la aplicación.

**01**

**Análisis de riesgos:**
Evaluación del impacto y probabilidad de ataques.

**02**

**Informe de seguridad:**
Hallazgos, recomendaciones y soluciones basadas en OWASP.

# Beneficios de **OWASP**

OWASP proporciona un enfoque estructurado para mejorar la seguridad de las aplicaciones web, reduciendo riesgos y fortaleciendo la protección contra ciberataques.

✅ Basado en estándares globales de seguridad.

✅ Evaluación integral de vulnerabilidades en aplicaciones y APIs.

✅ Reducción del riesgo de ataques como inyección SQL, XSS y CSRF.

✅ Cumplimiento de normativas y buenas prácticas de seguridad.

✅ Implementación de medidas correctivas según el impacto.

## Seguridad desde el **diseño**

La seguridad debe incorporarse desde el inicio del desarrollo de software. OWASP promueve enfoques como Security by Design y DevSecOps, integrando controles de seguridad en cada fase del ciclo de vida de desarrollo (SDLC). Esto permite identificar y mitigar vulnerabilidades antes de que lleguen a producción, reduciendo riesgos y costos.

# Seguridad en **la Nube**

Las configuraciones inseguras en la nube pueden exponer datos sensibles. Evaluamos la seguridad de entornos cloud para prevenir riesgos y accesos no autorizados.

Configuración Segura: Revisión de permisos, roles y acceso a recursos en la nube.

Protección de Datos: Cifrado en tránsito y en reposo para evitar filtraciones.

Seguridad en APIs y Servicios Cloud: Control de autenticación y validación de accesos.

- Monitoreo y Registro: Análisis de logs y detección de actividad sospechosa.

- Cumplimiento y Normativas: Verificación de alineación con estándares como ISO 27001, NIST y PCI.

# 1. Seguridad en **Aplicaciones Web**

Las aplicaciones web son un objetivo frecuente de ataques cibernéticos. Evaluamos su seguridad para identificar vulnerabilidades y prevenir riesgos que comprometan la integridad de los sistemas.

## Aspectos evaluados:

- **Inyección SQL (SQLi):** Prevención de manipulación en bases de datos.
- **Cross-Site Scripting (XSS):** Bloqueo de scripts maliciosos en el navegador.
- **Autenticación y Sesiones:** Protección contra accesos no autorizados.
- **Validación de Datos:** Evita inyección de código y ejecución de comandos.
- **Configuraciones de Seguridad:** Cifrado, almacenamiento seguro y cabeceras HTTP.

# Seguridad de **APIs**

Las APIs conectan sistemas y datos, pero su exposición puede ser un riesgo. Evaluamos su seguridad para evitar accesos no autorizados y filtraciones de información.

**Autenticación y Autorización:** Protección contra accesos indebidos con OAuth, JWT y API keys seguras.

**Validación de Entradas:** Prevención de ataques como inyección de código y manipulación de datos.

**Gestión de Errores:** Evita la exposición de información sensible en respuestas del servidor.

**Control de Tasa y Restricciones:** Protección contra abusos y ataques de denegación de servicio (DoS).

**Cifrado de Datos:** Uso de HTTPS, TLS y almacenamiento seguro para proteger la información.

# Identidades y **Accesos**

El control de identidades es clave para evitar accesos no autorizados. Evaluamos los mecanismos de autenticación y gestión de sesiones para proteger los sistemas.

- Autenticación Segura: Implementación de MFA, gestión de contraseñas y estándares como OAuth y SAML.

- Control de Accesos: Aplicación del principio de mínimo privilegio y revisión de permisos.

**Gestión de Sesiones:** Protección contra secuestro de sesión y exposición de tokens.

**Registro y Monitoreo:** Detección de intentos de acceso sospechosos y auditoría de eventos críticos.

**Protección contra Ataques:**

Prevención de ataques como fuerza bruta y reutilización de credenciales.

# Evaluación de **Vulnerabilidades y Cumplimiento**

Identificar y corregir vulnerabilidades es clave para reducir riesgos. Evaluamos el nivel de seguridad de los sistemas y su alineación con estándares de la industria.

- Detección de Vulnerabilidades: Análisis automatizado y manual de fallos de seguridad.
- Cumplimiento de Estándares: Verificación con OWASP Top 10, ASVS, ISO 27001 y NIST.
- Gestión de Riesgos: Priorización de vulnerabilidades según impacto y explotación.
- Aplicación de Parches: Revisión de actualizaciones críticas y configuraciones seguras.
- Reportes y Recomendaciones: Informes detallados con soluciones y mejoras de seguridad.

## Aspectos evaluados:

**Monitoreo de Amenazas:** Detección de ataques en tiempo real.

**Respuesta a Incidentes:** Planes de acción ante brechas de seguridad.

**Capacitación en Ciberseguridad:** Formación para reducir riesgos humanos.

**Gestión de Logs y Auditorías:** Registro y análisis de eventos críticos.

**Mejora Continua:** Revisión periódica de controles y políticas de seguridad.

La seguridad operativa **no solo previene ataques**, sino que permite detectar, responder y mejorar ante nuevas amenazas. Monitorear sistemas, gestionar incidentes y capacitar al personal reduce riesgos. Auditorías y revisiones constantes garantizan que la seguridad evolucione frente a las amenazas cibernéticas.

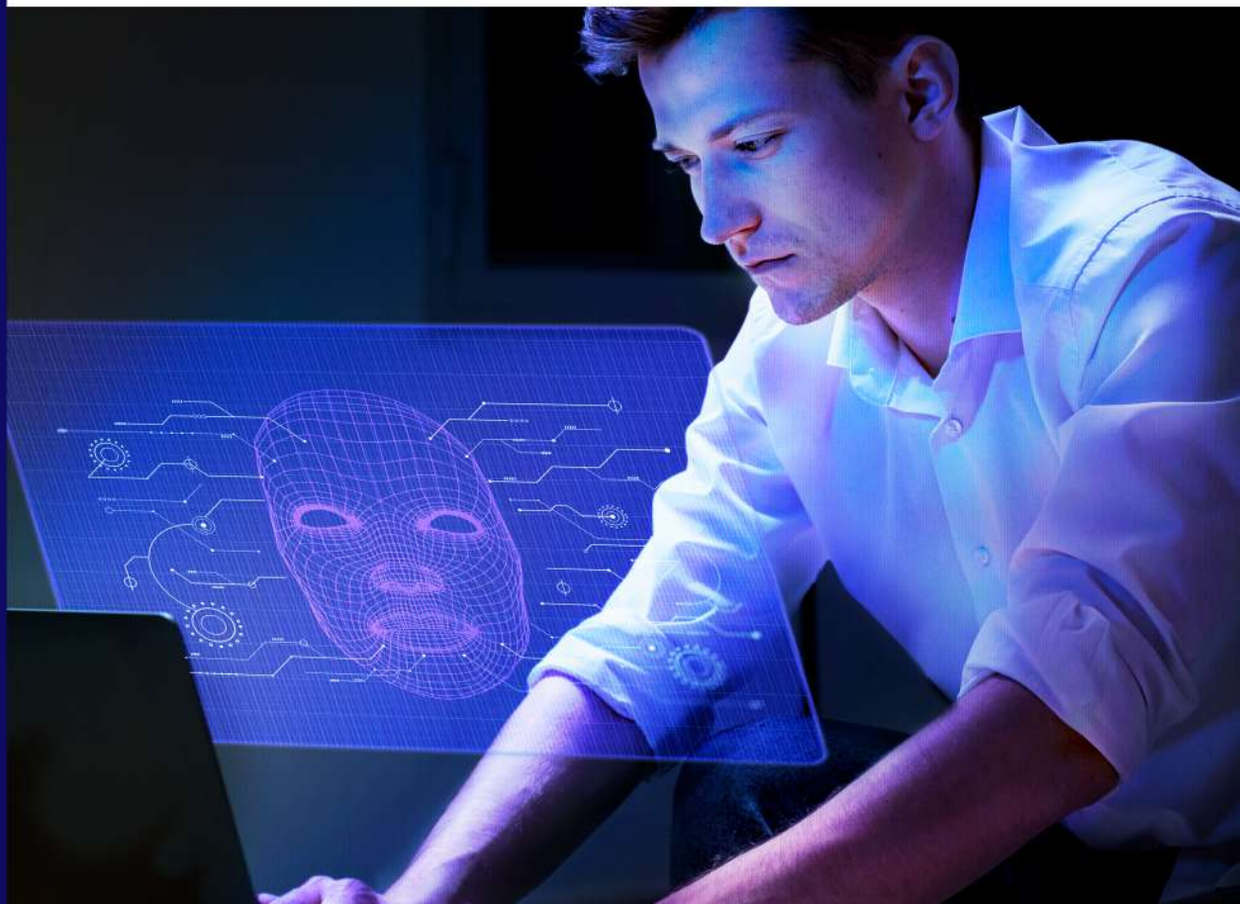
# Seguridad **Operativa**

Una buena seguridad no solo depende de herramientas, sino de monitoreo constante y respuesta efectiva a incidentes.

# Red Team

Las **auditorías y consultorías de seguridad ofensiva** que ofrecemos están basadas en metodologías avanzadas utilizadas en pruebas de penetración y simulaciones de ataques dirigidos a infraestructuras corporativas. **Nuestro enfoque se centra en la evaluación de la seguridad de entornos empresariales**, con énfasis en la explotación de vulnerabilidades en Active Directory, escalada de privilegios, movimiento lateral y técnicas de evasión.

A través de nuestras certificaciones en Red Team, aplicamos estrategias prácticas para identificar fallos de seguridad, evaluar riesgos y proporcionar recomendaciones efectivas para mejorar la postura de ciberseguridad de su organización.



# ¿Qué evalúa **Red Team?**

www.tirescue.com

## 01 Reconocimiento y Enumeración

Recopilación de información sobre la organización, dominios, empleados y sistemas expuestos.

## 02 Explotación de infraestructura

Identificación y explotación de vulnerabilidades en redes, servidores y estaciones de trabajo.

## 03 Active Directory y Movimiento Lateral

Abuso de Active Directory (AD), escalada de privilegios y técnicas de movimiento lateral.

## 04 Evasión de Defensas

Bypass de antivirus (AV), EDR y soluciones de seguridad para evitar detección.

## 05 Persistencia y Exfiltración

Creación de puertas traseras y extracción de información crítica sin ser detectado.

## 06 Detección y Respuesta

Evaluación de la capacidad del equipo de seguridad para detectar y responder a ataques.

# Metodología de **Ataques**

Un análisis Red Team no solo identifica vulnerabilidades, sino que simula ataques reales para evaluar la postura de seguridad de una organización.

Este enfoque sigue el ciclo de vida de un ataque avanzado, incluyendo:

**01** **Reconocimiento (OSINT):**Recopilación de información pública sobre la organización, empleados, dominios y sistemas expuestos en internet.

**02** **Enumeración y Mapeo:**Identificación de servicios, redes, aplicaciones y estructuras de Active Directory. Uso de herramientas como BloodHound, LDAP queries, Nmap y Shodan.

**03** **Explotación de Vulnerabilidades:**Uso de exploits y técnicas de ataque para vulnerar sistemas y credenciales con herramientas como Metasploit, CrackMapExec y Burp Suite.

**04** **Movimiento Lateral:** Expansión del acceso dentro de la red, compromiso de más sistemas y servidores Windows/Linux.

Un análisis Red Team no solo identifica vulnerabilidades, sino que simula ataques reales para evaluar la postura de seguridad de una organización.


**Evasión de Defensas:** Bypass de Antivirus (AV), Endpoint Detection & Response (EDR), logging y SIEM.

**Persistencia y Exfiltración:** Mantenimiento del acceso con puertas traseras, túneles C2 (Cobalt Strike, Sliver, Covenant) y extracción de información sensible.

Un análisis Red Team no solo identifica vulnerabilidades, sino que simula ataques reales para evaluar la postura de seguridad de una organización.

**Evaluación de Detección y Respuesta:** Análisis de la capacidad del SOC, Blue Team y SIEM para detectar ataques.

**Reporte y Recomendaciones:** Documentación detallada de hallazgos, tácticas utilizadas y soluciones de mitigación.

# Beneficios de **Red Teaming**

Nuestro enfoque de Red Teaming permite evaluar la postura de seguridad de una organización mediante la simulación de **ataques avanzados**, ayudando a reducir riesgos y fortalecer la resiliencia frente a amenazas reales.

✅ Simula **ataques reales y avanzados**.

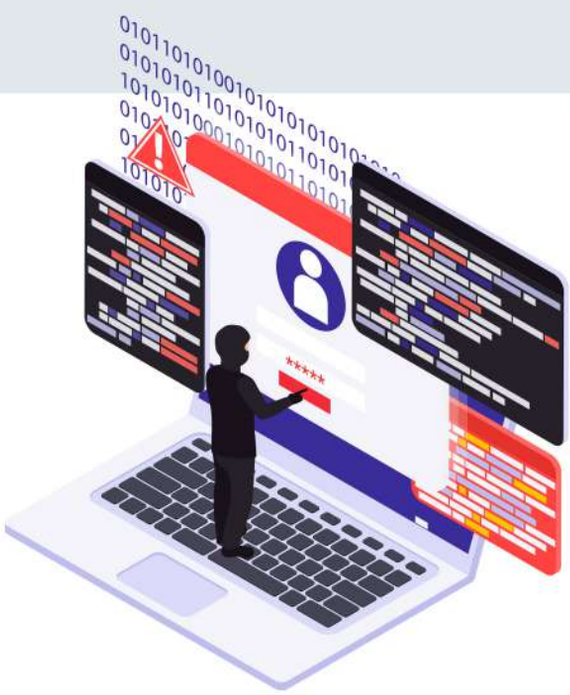
✅ Evalúa la seguridad en **Active Directory**.

✅ Prueba la capacidad de detección del **SOC y Blue Team**.

✅ Identifica vulnerabilidades antes que un **atacante real**.

## 🔄 Más allá de la simulación: Red Team en acción

Evaluamos la resiliencia de tu empresa frente a **ataques reales**, probando evasión de defensas, acceso persistente y explotación de vulnerabilidades en entornos on-premise y cloud. Además, fortalecemos al **Blue Team** y analizamos el impacto en la continuidad del negocio.



# Estrategia Red Team:
# **Evaluación y Ataque**

El Red Team evalúa la seguridad de una organización simulando ataques reales. Desde la planificación hasta la ejecución, mide la respuesta del equipo de seguridad y proporciona informes con mejoras y asesoría para fortalecer defensas.

### 1️⃣ Definición del Alcance

Determinar qué sistemas y redes serán atacados.

Se define si será un ataque sigiloso (Red Team puro) o con participación del equipo interno para entrenamiento (Purple Team)

### 2️⃣ Simulación de Ataque

Ejecución de técnicas de hacking ético y ataques dirigidos.

Uso de herramientas como Mimikatz, Rubeus, SharpHound, Cobalt Strike, Burp Suite y Metasploit.

### 3️⃣ Evaluación de Seguridad y Respuesta

Se mide si el SOC y los equipos de seguridad detectan el ataque.

Se analizan los registros en SIEM y firewalls.

El **informe Red Team** presenta hallazgos detallados, pruebas de concepto y un resumen ejecutivo del impacto del ataque, junto con estrategias de mejora. Además, se ofrece asesoría para mitigar vulnerabilidades y fortalecer la seguridad a través de ejercicios **Purple Team,** optimizando la defensa contra futuras amenazas.

### 4 Informe Técnico y Ejecutivo

Informe técnico con hallazgos detallados y pruebas de concepto (PoC).

Resumen ejecutivo con impacto del ataque y estrategias de mejora.

### 5 Mitigación y Entrenamiento

Se asesora sobre la corrección de vulnerabilidades.

Se realizan ejercicios Purple Team para mejorar defensas.

# Seguridad de **Aplicaciones**

El Red Team de TI Rescue e**valúa vulnerabilidades en aplicaciones**, accesos e identidades, **simulando ataques reales** para mejorar la seguridad y prevenir brechas.

Nuestra metodología analiza permisos, autenticación y políticas de cuentas para detectar accesos no autorizados y prevenir ataques como robo de credenciales y escalación de privilegios. **Evaluamos configuraciones débiles en Active Directory, nubes y aplicaciones**, probando técnicas como evasión de MFA, password spraying y fuerza bruta.

También identificamos credenciales expuestas en leaks y bases de datos comprometidas, ayudando a fortalecer las defensas y minimizar riesgos. Nuestro enfoque mejora la resiliencia ante ataques dirigidos y refuerza la seguridad de accesos en entornos corporativos.

**Control de accesos:**

Evaluación de permisos en Active Directory y cloud (AWS, Azure, Google Cloud).

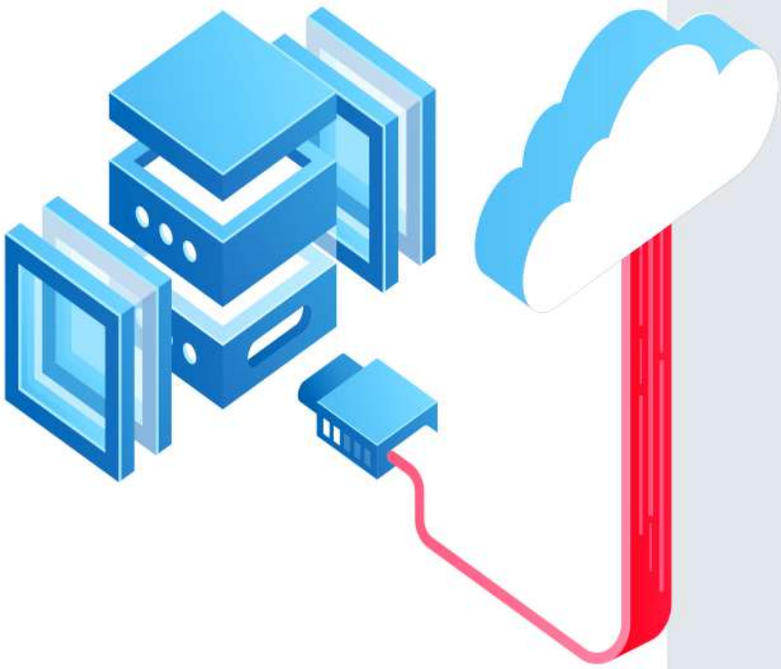
**Autenticación:**

Simulación de ataques de password spraying, brute force y MFA bypass.

Análisis de mecanismos débiles de autenticación en aplicaciones y redes.

**Políticas de cuentas y sesiones:**

Detección de credenciales expuestas en bases de datos y leaks.
Evaluación de persistencia a través de cuentas de servicio y tokens de sesión.



# Red Team en **la Nube**

El Red Team de TI Rescue evalúa la seguridad en la nube **identificando configuraciones inseguras, accesos mal gestionados y riesgos de exposición** de datos. Simulamos ataques reales en entornos AWS, Azure y GCP para medir la resiliencia y prevenir brechas de seguridad.

La seguridad en la nube no solo depende de configuraciones adecuadas, sino de controles de detección y respuesta ante ataques. **Evaluamos la capacidad de defensa mediante simulaciones de acceso no autorizado, detección de credenciales expuestas y explotación de configuraciones débiles**. Implementamos auditoría, logging y monitoreo avanzado para prevenir filtraciones y accesos indebidos.

**Exposición de datos sensibles:** Bases de datos, buckets S3 y almacenamiento mal configurado.

**Permisos excesivos:** Cuentas con privilegios innecesarios y sin controles de acceso adecuados.

**Falta de auditoría y monitoreo:** Logging y alertas mal configuradas, facilitando accesos no detectados.

# Red Team en la Nube:
# **Amenazas y Seguridad**

✅ **Ataques en Cloud:**
Simulación de ataques a identidades, accesos y almacenamiento en AWS, Azure y GCP.

✅ **Infraestructura como Código (IaC):**
Evaluación de errores en Terraform, CloudFormation y CI/CD.

✅ **Persistencia y Exfiltración:**
Análisis de backdoors en instancias, contenedores y buckets S3.

✅ **Automatización de Red Teaming:**
Uso de herramientas como Pacu y Prowler para detección de riesgos.

El **Red Team** de TI Rescue evalúa la seguridad en la nube con simulaciones de ataques avanzados en AWS, Azure y GCP. Analizamos identidades, acceso, infraestructura como código (IaC) y resiliencia ante amenazas, utilizando herramientas como Pacu y Prowler.

Nuestro enfoque incluye pruebas de persistencia en entornos cloud, detección de bucket takeover, ataques a pipelines de CI/CD y explotación de errores en configuraciones IAM. **Estas simulaciones permiten identificar brechas de seguridad antes de que sean explotadas por actores malintencionados.**

# Retorno de la inversión en **Auditorías de Seguridad**

En términos financieros, **la auditoría baja la pérdida anual esperada al reducir la probabilidad y/o el impacto de un incidente**, y además evita costos ocultos como horas de recuperación, reprocesos, consultorías de emergencia y paradas de servicio.

- **Riesgo reducido:** baja la probabilidad y/o el impacto de incidentes (ransomware, fuga de datos, caída de servicios).
- **Ahorros operativos:** menos incidentes, menos horas de soporte/recuperación, menos interrupciones.
- **Aceleración de cumplimiento:** menos hallazgos, auditorías externas más rápidas, más contratos (clientes exigen ISO/controles).
- **Mejor priorización:** se invierte en remediar lo que más reduce riesgo (alto impacto / alta probabilidad).

Su valor está en que **identifica, valida y prioriza** las brechas que pueden convertirse en incidentes costosos **(interrupciones, fuga de datos, ransomware, fraudes)**, y permite corregirlas antes de que impacten la operación.

# **Justificación Financiera**
del Proyecto

Para medir el retorno de esta auditoría, analizamos dos variables: el impacto de un evento crítico y el ahorro por optimización de procesos.

**1. Impacto Económico por Indisponibilidad (El Riesgo)**

✅ **Pérdida de Productividad:** 40 empleados X $50.000/hora (costo promedio carga prestacional) = $2.000.000 / **hora**

✅ **Lucro Cesante (Ventas/Operación no realizada):** Estimado de $3.500.000 **/ hora**

✅ **Costo de Recuperación:** (Horas técnicas externas + recargos de urgencia) = $2.500.000

**Total riesgo (**Caída única de 4 horas)**: $24.500.000 COP**

**2. Retorno de Inversión (ROI) Anual**

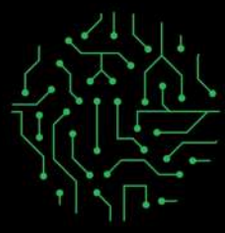
La auditoría se paga sola al eliminar gastos ocultos.

✅ **$18M — Ahorro en Soporte:** Menos fallos técnicos y menos pagos por urgencias externas.

✅ **$10M — Ganancia en Tiempo:** Recuperamos horas de trabajo perdidas en procesos lentos o manuales.

✅ **$4M — Riesgo Legal y Cumplimiento:** Mitigamos sanciones, demandas y costos por incidentes.

**Total ahorro: $32.000.000 / año**



T.I RESCUE

SEGURIDAD INFORMATICA

**WWW.TIRESCUE.COM**

Expertos en Ciberseguridad