qualoom®

Inspiring Technology
for People

Evaluación de seguridad de sistemas y aplicaciones: guía práctica para reducir riesgos

Área de Ciberseguridad
Fecha 19/08/2026
Versión 1.0
Clasificación: Público

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

ÍNDICE

01 Seguridad integral: la primera línea de defensa

02 Inventario y exposición tecnológica

03 Descubrimiento y priorización de riesgos

04 Validación técnica mediante pruebas estructuradas

05 Riesgos medidos, acciones priorizadas

06 Evidencia clara, decisiones seguras

07 Seguridad evolutiva y constante

qualoom®

Inspiring Technology
for People

Seguridad integral: la primera línea de defensa

La **evaluación de seguridad de sistemas y aplicaciones** es un proceso crítico para garantizar la protección de los activos tecnológicos de la organización frente a amenazas digitales. Su objetivo es identificar **vulnerabilidades, medir riesgos y establecer medidas de mitigación** que aseguren la confidencialidad, integridad y disponibilidad de la información crítica.

OWASP (Open Web Application Security Project):

Guía de riesgos y vulnerabilidades en aplicaciones web, proporcionando patrones de mitigación.

NIST (National Institute of Standards and Technology)

Referencia para la gestión de riesgos, controles de seguridad y ciberresiliencia.

ISO 27001/27002

Estándares internacionales para la implementación de sistemas de gestión de seguridad de la información (SGSI), definiendo políticas, controles y procedimientos.

qualoom®

Inspiring Technology
for People

Seguridad integral: la primera línea de defensa

Riesgos derivados de la falta de evaluación continua

Brechas de datos

Exposición de información sensible por accesos no autorizados o filtraciones.

Fallos operativos

Interrupciones de servicios críticos que afectan la continuidad del negocio.

Compromiso de integridad

Alteración no detectada de información o procesos clave que puede derivar en decisiones erróneas o daños reputacionales

Objetivo de la guía

Proporcionar un enfoque **práctico, estructurado y replicable** para evaluar la seguridad de sistemas y aplicaciones, priorizar riesgos y establecer controles efectivos.

qualoom®

Inspiring Technology
for People

Inventario y exposición tecnológica

La **identificación de activos y el análisis de la superficie de exposición** constituyen el primer paso crítico en cualquier programa de ciberseguridad. Este proceso permite **comprender qué recursos son más valiosos, cómo se comunican y qué vectores podrían ser explotados por atacantes.** Una visión precisa de los activos y su exposición es esencial para priorizar esfuerzos de protección y aplicar controles de manera efectiva.

Identificación de activos críticos

Los activos críticos incluyen todos los sistemas, aplicaciones, APIs, bases de datos y elementos de infraestructura cloud cuya indisponibilidad, alteración o compromiso podría afectar la operación o la reputación de la organización. **El inventario debe contemplar:**

Sistemas internos

ERP, CRM, servidores de aplicaciones, sistemas de respaldo.

Aplicaciones corporativas

Aplicaciones web, móviles y de escritorio.

APIs y servicios externos

Conexiones con proveedores, integraciones con plataformas externas.

Infraestructura cloud

Servicios IaaS, PaaS y SaaS, incluyendo configuraciones de seguridad asociadas.

qualoom®

Inspiring Technology
for People

Inventario y exposición tecnológica

Mapeo de flujos de información y dependencias

El siguiente paso consiste en entender cómo los activos intercambian información. Esto incluye:

- Diagramas de flujo que muestren entrada y salida de datos.
- Dependencias entre aplicaciones, servicios y bases de datos.
- Identificación de sistemas que procesan información sensible o regulada (por ejemplo, datos personales o financieros).

Detección de puntos de entrada y vectores de ataque

Es fundamental identificar todos los puntos por los que un atacante podría acceder:

- Interfaces web y APIs abiertas al público o a terceros.
- Puertos y servicios expuestos en servidores internos o cloud.
- Integraciones externas y conexiones de proveedores.
- Canales de comunicación internos que puedan ser comprometidos.

qualoom®

Inspiring Technology
for People

Inventario y exposición tecnológica

Evaluación de tecnologías legacy y riesgos asociados

Los sistemas obsoletos o sin soporte **presentan riesgos significativos:**

- Vulnerabilidades conocidas sin parches disponibles.
- Dificultad para aplicar controles de seguridad estándar.
- Integraciones con sistemas modernos que pueden ser débiles o incompatibles.

qualoom®

Inspiring Technology
for People

Descubrimiento y priorización de riesgos

La **gestión de vulnerabilidades** es un proceso sistemático para **identificar, evaluar, clasificar y mitigar debilidades** en sistemas, aplicaciones y redes antes de que puedan ser explotadas por atacantes. Una gestión efectiva permite reducir la superficie de ataque y priorizar esfuerzos según el riesgo real que representa cada vulnerabilidad para el negocio.

Detección de vulnerabilidades

- Escaneos automatizados: análisis de sistemas y aplicaciones para detectar fallas conocidas o configuraciones inseguras.
- Revisión manual: análisis experto basado en OWASP Top 10 y CWE para vulnerabilidades complejas.

Identificación de configuraciones inseguras

- Contraseñas débiles o por defecto.
- Permisos excesivos en sistemas críticos.
- Servicios o puertos expuestos innecesariamente.
- Falta de segmentación de red entre sistemas críticos y periféricos.

Clasificación y priorización

- Las vulnerabilidades deben evaluarse según su criticidad, utilizando CVSS y contexto operativo. La prioridad se define combinando impacto, probabilidad de explotación y exposición del activo.

qualoom®

Inspiring Technology for People

Descubrimiento y priorización de riesgos

Tabla de vulnerabilidades

Vulnerabilidad	Criticidad	Impacto	Acción Recomendada	Estado
Inyección SQL	Crítica	Alta	Validación de entrada y parametrización de consultas	Pendiente
Contraseñas débiles	Alta	Media	Forzar uso de contraseñas fuertes y MFA	En progreso
Exposición de puerto 22	Media	Baja	Restringir acceso vía firewall y VPN	Resuelto
Configuración SSL insegura	Alta	Alta	Actualizar certificados y habilitar TLS 1.2+	Pendiente
Desbordamiento de buffer	Crítica	Alta	Revisar y reforzar manejo de memoria en código	Pendiente

qualoom®

Inspiring Technology
for People

Validación técnica mediante pruebas estructuradas

Las **pruebas de seguridad** son fundamentales para **evaluar la efectividad de los controles existentes** y detectar vulnerabilidades que podrían ser explotadas por atacantes. Estas pruebas permiten validar la seguridad de aplicaciones, sistemas y redes, complementando la identificación de vulnerabilidades. Su enfoque debe ser **estructurado y repetible**, asegurando resultados confiables y medibles.

SAST – Static Application Security Testing

- Análisis estático del código fuente sin ejecutar la aplicación.
- Permite identificar errores lógicos, vulnerabilidades de codificación y debilidades estructurales.
- Beneficio: detección temprana de fallos antes de que el código llegue a producción.

DAST – Dynamic Application Security Testing

- Evaluación de la aplicación en entornos de ejecución controlados.
- Detecta vulnerabilidades que solo se manifiestan cuando la aplicación está activa.
- Beneficio: prueba de comportamiento real frente a ataques externos.

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Validación técnica mediante pruebas estructuradas

Pentesting – Pruebas de penetración

- Simulación avanzada de ataques reales para evaluar la resistencia de sistemas y aplicaciones.
- Puede incluir redes, aplicaciones web, APIs y servicios cloud.
- Objetivo: validar la efectividad de los controles y medir el riesgo real de explotación.
- Entregable: informe con vulnerabilidades explotables, riesgo asociado y recomendaciones de mitigación.

Pruebas de carga y resistencia

- Evaluación del comportamiento de sistemas bajo condiciones extremas.
- Permite identificar cuellos de botella, fallos de rendimiento y vulnerabilidades que surgen bajo estrés.
- Útil para aplicaciones críticas o de alto tráfico que requieren disponibilidad continua.

Hardening (endurecimiento)

Revisión de configuraciones de sistemas y aplicaciones para alinearlas con buenas prácticas y estándares de seguridad. **Incluye:**

- Eliminación de servicios innecesarios
- Restricción de permisos excesivos
- Aplicación de parches y actualizaciones
- Configuración segura de servidores, bases de datos y redes

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Validación técnica mediante pruebas estructuradas

Tipo de prueba	Objetivo principal	Alcance	Momento recomendado	Ejemplos de hallazgos
SAST	Detectar vulnerabilidades en el código fuente	Código, librerías y dependencias	Durante desarrollo / CI/CD	Inyecciones, errores lógicos, funciones inseguras
DAST	Identificar vulnerabilidades en ejecución	Aplicaciones web, APIs	Pre-producción / QA	Exposición de datos, errores de autenticación, manejo de sesiones
Pentesting	Validar seguridad frente a ataques reales	Sistemas completos (redes, apps, APIs)	Pre-producción o producción controlada	Acceso no autorizado, explotación de vulnerabilidades críticas
Pruebas de carga	Evaluar rendimiento bajo estrés	Aplicaciones y servicios críticos	Pre-producción	Fallos por alta concurrencia, degradación de servicios
Hardening	Endurecer configuraciones y controles	Servidores, aplicaciones, bases de datos	Continuo	Servicios innecesarios, permisos excesivos, configuraciones inseguras

qualoom®

Inspiring Technology
for People

Riesgos medidos, acciones priorizadas

El **análisis de riesgos** es un proceso crítico dentro de cualquier programa de ciberseguridad. Su objetivo es **evaluar sistemáticamente la exposición de los activos a amenazas**, determinar el impacto potencial de su explotación y establecer prioridades claras para la mitigación. Esto permite **tomar decisiones basadas en riesgo,** asignando recursos de manera eficiente y protegiendo los activos más críticos para el negocio.

Evaluación del impacto

Cada activo debe analizarse en términos de **Confidencialidad, Integridad y Disponibilidad (CIA)**

Confidencialidad

Qué tan grave sería la exposición de información sensible si se accede sin autorización.

Integridad

El efecto de la alteración no autorizada de datos o procesos críticos.

Disponibilidad

La consecuencia de que un sistema deje de estar operativo para los usuarios o procesos de negocio.

qualoom®

Inspiring Technology for People

Riesgos medidos, acciones priorizadas

Probabilidad de explotación y exposición

No todas las vulnerabilidades representan el mismo riesgo: es fundamental evaluar:

Probabilidad de explotación

Qué tan fácil es que un atacante pueda aprovechar la vulnerabilidad.

Exposición del activo

Cuán accesible está el activo para un atacante (internet, red interna, proveedores, terceros).

Tipos de riesgo y priorización

Tipo	Descripción	Priorización
BAJO	Riesgos menores; monitoreo y control continuo.	monitoreo continuo y auditorías periódicas, documentación de excepciones.
MEDIO	Riesgos moderados; mitigación planificada.	plan de mitigación programado, actualización de políticas, revisión de configuraciones.
ALTO	Riesgos significativos que deben mitigarse a corto plazo.	aplicación de controles compensatorios, segmentación de red, monitorización reforzada.
CRÍTICO	Vulnerabilidades con alto impacto y alta probabilidad de explotación; requieren acción inmediata.	Remediación inmediata, parcheo de vulnerabilidades críticas, bloqueo de accesos inseguros.

qualoom®

Inspiring Technology
for People

Evidencia clara, decisiones seguras

La **documentación de seguridad** permite registrar de forma estructurada los hallazgos identificados durante las evaluaciones, asegurando **trazabilidad, seguimiento y control** del riesgo. Una correcta documentación facilita la remediación técnica y garantiza la consistencia de los procesos de seguridad.

Informe técnico de vulnerabilidades

Cada vulnerabilidad debe documentarse de manera homogénea, incluyendo:

- **Descripción técnica del hallazgo**
- **Evidencia asociada**
- **Nivel de riesgo**
- **Activos afectados**
- **Recomendación de mitigación**

Esta información permite a los equipos técnicos analizar y corregir los riesgos de forma eficiente.

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Evidencia clara, decisiones seguras

Trazabilidad y seguimiento

La documentación debe reflejar el estado de cada vulnerabilidad (pendiente, en progreso, mitigada), asegurando que los riesgos críticos sean tratados y verificados.

Reporting ejecutivo

Los reportes ejecutivos presentan el estado de la seguridad de forma **clara y visual,** mediante indicadores clave (KPIs):

- **Tasa de cierre de vulnerabilidades**
- **Tiempo promedio de remediación**
- **Incidentes asociados a configuraciones inseguras**

Estos reportes permiten a la dirección **tomar decisiones informadas y priorizar acciones de seguridad.**

Más información www.qualoom.es

qualoom®

Inspiring Technology
for People

Seguridad evolutiva y constante

La **mejora continua en ciberseguridad** es esencial para mantener la eficacia de los controles frente a un entorno de amenazas dinámico. La seguridad debe gestionarse como un **proceso permanente,** no como una acción puntual.

La aplicación del **ciclo PDCA (Plan–Do–Check–Act)** permite estructurar este proceso mediante la planificación de controles, su implementación, la verificación periódica de su efectividad y la corrección de desviaciones detectadas.

La **automatización de evaluaciones de seguridad** facilita la detección temprana de vulnerabilidades, reduce errores operativos y garantiza consistencia en los controles aplicados.

La integración de la seguridad en los **pipelines de desarrollo y despliegue (DevSecOps)** permite incorporar controles desde las fases iniciales del ciclo de vida del software, reduciendo riesgos en producción.

La revisión periódica de políticas, configuraciones y métricas de seguridad permite **medir el nivel de madurez** y orientar acciones de mejora continua.

qualoom®

Inspiring Technology
for People

Evalúa riesgos y **mejora tu ciberseguridad.**

CONTACTA CON NOSOTROS

www.qualoom.es

contacto@qualoom.es

(+34) 91 236 4808

Más información www.qualoom.es