ASENTEC

DOCUMENTO CONFIDENCIAL — EJEMPLO

INGENIERÍA DE SISTEMAS Y CIBERSEGURIDAD

Informe de Auditoría de Seguridad · Protocolo 0-Trust

Evaluación de infraestructura, aplicaciones y redes corporativas. Diagnóstico técnico, priorización de riesgo y plan de acción — no solo problemas, soluciones.

CLIENTE	SECTOR	FECHA	REF.
Empresa Ejemplo S.L.	Servicios profesionales	Julio 2026	AST-AUD-0000

01 · RESUMEN EJECUTIVO

Estado general de seguridad

ASENTEC

Este documento resume los resultados de la auditoría de seguridad realizada sobre la infraestructura de **Empresa Ejemplo S.L.**, cubriendo sistemas locales y cloud, aplicaciones web expuestas a internet, y la red corporativa de oficina. El objetivo no es solo enumerar vulnerabilidades, sino ofrecer un plan de acción priorizado por impacto real sobre el negocio.

2	4	6	3
HALLAZGOS CRÍTICOS	HALLAZGOS ALTOS	HALLAZGOS MEDIOS	HALLAZGOS BAJOS

Valoración general

La infraestructura evaluada presenta una base razonable de controles perimetrales, pero se han identificado **debilidades críticas en la gestión de accesos y en la exposición de servicios a internet** que requieren corrección inmediata. Ninguno de los hallazgos críticos ha sido, hasta la fecha de este informe, objeto de explotación conocida — la ventana de actuación preventiva sigue abierta.

Alcance de la evaluación

01

Enterprise System Audits

SISTEMAS LOCALES Y CLOUD

Evaluación de arquitecturas locales y cloud, identificando configuraciones erróneas y vectores de escalada de privilegios.

02

Aplicaciones web y APIs

PRUEBAS DE PENETRACIÓN

Pruebas estáticas y dinámicas sobre los activos digitales expuestos a internet.

03

Redes de oficina

WIFI, ETHERNET Y PERÍMETRO FÍSICO

Blindaje de infraestructuras de conectividad corporativa y puntos de acceso físico a la red.

> Este es un informe de ejemplo con datos ficticios, generado para ilustrar el formato y el nivel de detalle de las auditorías de Asentec. No corresponde a ningún cliente real.

Detalle de vulnerabilidades

Cada hallazgo se clasifica por severidad en función de su probabilidad de explotación y el impacto potencial sobre la continuidad del negocio, no únicamente sobre criterios técnicos.

SEVERIDAD	HALLAZGO	IMPACTO EN EL NEGOCIO	ÁREA
CRÍTICO	Puerto de escritorio remoto (RDP) expuesto directamente a internet sin VPN ni MFA	Acceso no autorizado a servidores internos; riesgo directo de ransomware	Perímetro / Red
CRÍTICO	Cuentas de administrador con contraseñas sin caducidad ni política de complejidad	Escalada de privilegios y movimiento lateral en caso de compromiso	Identidad y accesos
ALTO	Firmware de firewall perimetral desactualizado (2 versiones de seguridad pendientes)	Exposición a vulnerabilidades públicamente documentadas	Perímetro / Red
ALTO	Copias de seguridad accesibles desde la misma red que protegen	Pérdida total de datos en caso de ransomware (backup también cifrado)	Continuidad
MEDIO	Red WiFi de invitados sin segmentación respecto a la red corporativa	Posible pivote desde dispositivos externos hacia sistemas internos	Red de oficina
MEDIO	Ausencia de autenticación multifactor en el correo corporativo	Mayor exposición a phishing y compromiso de cuentas	Identidad y accesos
BAJO	Certificados TLS con expiración inferior a 30 días en dos subdominios	Interrupción de servicio y advertencias de seguridad a usuarios	Aplicaciones web

Tabla no exhaustiva — el informe completo incluye evidencias técnicas, capturas y detalle de reproducción para cada hallazgo.

Plan de acción priorizado

No entregamos solo problemas. Este plan ordena las acciones correctivas por impacto y urgencia real de negocio, no por orden de aparición técnica.

INMEDIATO · 0–7 DÍAS

Cerrar la exposición crítica

- Retirar el acceso RDP directo a internet y sustituirlo por VPN con MFA obligatorio
- Forzar política de contraseñas y caducidad en todas las cuentas de administrador

CORTO PLAZO · 30 DÍAS

Reducir superficie de ataque

- Actualizar firmware del firewall perimetral a la última versión estable
- Aislar las copias de seguridad en un segmento de red independiente (air-gap lógico)
- Activar MFA en correo corporativo y accesos cloud críticos

MEDIO PLAZO · 90 DÍAS

Consolidar la postura de seguridad

- Segmentar la red WiFi de invitados de la red corporativa
- Automatizar la renovación de certificados TLS
- Formación de concienciación en phishing para el equipo

Seguimiento

Cada fase se cierra con una validación técnica por parte de Asentec para confirmar que la corrección se ha aplicado correctamente y no introduce nuevos riesgos. El cliente recibe un informe de cierre por cada bloque de acciones completado.

SIGUIENTE PASO

¿Hablamos de la seguridad real de tu infraestructura?

Este ha sido un informe de ejemplo. Una auditoría real de Asentec incluye evidencias técnicas completas, capturas de cada hallazgo y una sesión de presentación de resultados con tu equipo.

EMAIL CORPORATIVO

proyectos@asentec.es

HORARIO

Lunes – Viernes, 09:00–18:00

ÁREA DE SERVICIO

EMEA

© 2026 Asentec — Este documento es un ejemplo comercial con datos ficticios y no constituye una auditoría real. Todo el contenido es confidencial y propiedad de Asentec.