dcsaudit

Auditoría técnica de seguridad · Windows, Linux y Active Directory · Sin instalar nada

CLIENTE

—

PREPARADO POR

DCSeguridad Consultoría IT & Ciberseguridad

Una auditoría técnica de seguridad de sus equipos, servidores y red, ejecutada en una sola visita, **sin instalar nada**. Le entregamos un informe con los puntos débiles ordenados por gravedad y la solución concreta de cada uno.

243
Controles de seguridad

21
Bloques temáticos

ENS
Categoría media

23
Críticos

73
Gravedad alta

113
Medios

34
Bajos e informativos

Contenido

1 Qué es dcsaudit

dcsaudit es una auditoría técnica de seguridad de los equipos, servidores y red de su empresa. Se ejecuta en una sola visita, **sin instalar nada** en sus sistemas, y produce un informe con los puntos débiles ordenados por gravedad, cada uno con su explicación en lenguaje de negocio y su solución concreta.

OK

La auditoría inicial es gratuita y sin compromiso. El informe es suyo y puede resolverlo con quien quiera, incluido su proveedor actual. Regalamos el diagnóstico: usted decide qué hacer con él.

Es una herramienta propia de DCSeguridad, pensada para **PYMEs de 20 a 50 equipos** sin departamento de seguridad propio, que nunca han auditado sus sistemas o hace mucho que no lo hacen.

Los 243 controles están mapeados al **Esquema Nacional de Seguridad (ENS)**, con nivel objetivo **categoría media**. La auditoría cubre configuración e infraestructura de Windows, Linux y Active Directory; **no incluye pentesting** (explotación de fallos).

2 Qué revisamos

La auditoría evalúa **243 controles** organizados en **21 bloques temáticos**, sobre Windows (196 controles) y Linux (47 controles). Cada control está clasificado por gravedad y mapeado al Esquema Nacional de Seguridad.

Alcance	Controles
Controles totales	**243**
Windows	196
Linux	47
Bloques temáticos	21
Mapeados al Esquema Nacional de Seguridad (ENS)	243 (todos)
Con referencia CIS verificada	96
De criterio propio (gestión, estado, infraestructura)	147

Por gravedad: • CRÍTICO 23 críticos • AVISO 73 de gravedad alta • 113 medios • 21 bajos • 13 informativos.

INFO

Que 147 controles sean de criterio propio no es una carencia. CIS es un benchmark de configuración del sistema operativo; buena parte de la auditoría trata de gestión, estado operativo e infraestructura (copias, salud del directorio, herramientas de control remoto, verificación activa) que CIS no cubre ni pretende cubrir.

3 Los 21 bloques

Los textos en cursiva son ejemplos reales de hallazgos, explicados en lenguaje de negocio tal como aparecen en el informe.

3.1 Windows (196 controles)

1 · Antivirus y EDR 17 controles · 4 críticos

No basta con comprobar que hay un antivirus instalado: verificamos que funciona de verdad —protección permanente activa, definiciones al día, sin excepciones peligrosas— y que no se puede desactivar desde el propio equipo.

> «El antivirus está instalado pero apagado. A efectos prácticos el equipo está desprotegido, con el agravante de que aparenta estar protegido y nadie lo revisa.»

2 · Copias de seguridad 17 controles · 2 críticos

Si existen, si la última terminó correctamente, con qué frecuencia y, sobre todo, dónde se guardan (si un ransomware las alcanzaría) y si el correo está copiado.

> «Hay un sistema de copias instalado, pero lleva tiempo sin completar ninguna correctamente. Es peor que no tener copias, porque todo el mundo cree que están hechas.»

3 · Software y estado de soporte 12 controles · 1 crítico

Inventario completo del software, sistema operativo y aplicaciones fuera de soporte, y versiones antiguas olvidadas al actualizar.

> «Cada mes se publican fallos nuevos que en este equipo ya no se corregirán nunca. El riesgo no se mantiene, crece de forma continua.»

4 · Active Directory e identidad 28 controles · 2 críticos

El corazón del dominio: administradores, delegaciones peligrosas, cuentas de servicio con credenciales almacenadas y contraseñas anotadas en fichas de usuario.

> «Hay contraseñas escritas en texto claro en la ficha del usuario. Cualquier persona del dominio, sin ningún permiso especial y sin herramientas, puede consultarlas.»

5 · Contraseñas y bloqueo 18 controles · 1 crítico

Política real de contraseñas: longitud mínima, caducidad, bloqueo por intentos y cuentas exentas.

> «Se puede probar contraseñas contra una cuenta indefinidamente, sin límite y sin que el sistema reaccione.»

6 · Políticas de seguridad del sistema 19 controles · 2 críticos

Protocolos obsoletos activos (SMBv1), contraseñas legibles en memoria y firma de comunicaciones.

> «[SMBv1] es el protocolo que usaron los grandes ataques de ransomware que paralizaron empresas en toda Europa.»

7 · Servicios y tareas programadas 9 controles · 1 crítico

Servicios que corren con cuentas de dominio privilegiadas, permisos de escritura sobre binarios y tareas con credenciales guardadas.

> «La contraseña de una cuenta con permisos totales sobre la empresa está almacenada en el equipo para que un programa pueda arrancar solo.»

8 · Estado de parcheo 9 controles

Actualizaciones de seguridad pendientes, actualizaciones automáticas deshabilitadas, servidor de actualizaciones (WSUS) inaccesible y actualizaciones que fallan repetidamente.

«Faltan correcciones para fallos de seguridad ya publicados y documentados.»

9 · Red 15 controles · 1 crítico

Qué protege la conexión, servicios expuestos a internet, DNS correcto, salida a internet sin restricción y firewall de Windows.

«Hay servicios de la empresa alcanzables desde cualquier punto del mundo. Los buscadores especializados en localizar equipos expuestos los indexan en cuestión de horas.»

10 · Cifrado de disco 7 controles · Windows y Linux

Portátiles cifrados y, sobre todo, si la clave de recuperación está guardada en algún sitio.

«El disco está cifrado, pero la clave para recuperarlo no está guardada en ningún sitio. El día que el equipo pida esa clave, y acaba pasando, no habrá forma de recuperarlo.»

11 · Registro y auditoría 12 controles

Si el sistema anota quién entra, quién falla al entrar y quién crea o modifica cuentas, para poder reconstruir un incidente.

«Si mañana ocurre un incidente, no habrá forma de reconstruir qué pasó.»

12 · Acceso remoto 9 controles · 1 crítico

Escritorio remoto publicado en internet y herramientas de control remoto olvidadas por proveedores.

«Es hoy la principal vía de entrada del ransomware en pequeñas y medianas empresas.»

13 · Recursos compartidos y permisos 8 controles · 1 crítico

Permisos de carpetas de red: la carpeta de nóminas o contabilidad accesible por toda la plantilla.

«Hay carpetas de red que cualquier persona de la empresa puede abrir, y en algunos casos modificar o borrar.»

14 · Verificación activa de protección perimetral 6 controles

Comprueba de verdad si la red bloquea amenazas: fichero de prueba EICAR (inofensivo, reconocido por todos los antivirus), inspección de tráfico cifrado y protección antisuplantación. Requiere autorización firmada (ver sección 5).

«El filtrado funciona con las conexiones sin cifrar, pero hoy prácticamente todo internet va cifrado. La protección existe sobre el papel y no en la práctica.»

21 · Salud del directorio 11 controles · 4 críticos

Que el Active Directory esté sano: servicios críticos del controlador, roles FSMO, replicación, SYSVOL/NETLOGON y registros DNS del dominio.

«Uno de los servicios que sostienen el dominio no está funcionando. Mientras siga así, los usuarios pueden no poder iniciar sesión.»

3.2 Linux (47 controles)

15 · SSH 11 controles · 1 crítico

Acceso remoto seguro: contraseñas vacías, acceso directo como root y permisos de claves.

> «Se puede entrar al servidor directamente como administrador total, desde cualquier sitio y sin identificarse antes como una persona concreta.»

16 · Privilegios y sudo 6 controles · 1 crítico

Cuentas con identificador de superusuario ocultas, elevación sin contraseña y registro de comandos.

> «Hay una segunda cuenta que es administrador total del servidor sin llamarse root. Es una forma clásica de dejar una puerta trasera.»

17 · Cuentas y contraseñas locales 10 controles · 1 crítico

Cuentas sin contraseña, contraseñas mal protegidas y caducidad.

> «Se puede acceder con esas cuentas sin escribir contraseña alguna.»

18 · Servicios, red y cortafuegos 7 controles

Cortafuegos activo, política por defecto y parámetros de red.

> «El servidor acepta conexiones de cualquier equipo de la red hacia cualquier servicio. Es el equivalente a dejar la puerta abierta dentro de casa.»

19 · Registro y auditoría Linux 5 controles

Sistema de auditoría, retención de registros y envío externo.

> «El servidor no registra quién accede, qué comandos se ejecutan ni qué ficheros se modifican. Tras un incidente no habrá nada que analizar.»

20 · Endurecimiento base Linux 7 controles

Permisos de ficheros del sistema, control de acceso obligatorio (SELinux/AppArmor) y protección del gestor de arranque.

> «Quien tenga acceso físico al servidor puede arrancarlo en modo mantenimiento y obtener control total sin conocer ninguna contraseña, en menos de un minuto.»

4 Qué NO hacemos

En seguridad, la transparencia es parte del servicio. Estas son nuestras garantías:

OK

- **No instalamos nada.** El colector se ejecuta una vez y se va. No queda ningún programa, servicio ni agente residente en sus equipos.
- **No modificamos ninguna configuración.** La auditoría solo lee. No cambia absolutamente nada en sus sistemas.
- **No accedemos ni mostramos contraseñas.** Aunque detectamos contraseñas mal guardadas, el informe cita la cuenta o el equipo afectado, **nunca el valor**. Las contraseñas no viajan al servidor ni se almacenan.
- **No hacemos fuerza bruta ni ataques.** No probamos credenciales, no explotamos fallos, no hay pentesting.
- **No dejamos sus datos expuestos.** La evidencia se cifra y se aplica una frontera de privacidad estricta.

5 Comprobaciones activas: solo con su permiso

La mayor parte de la auditoría es lectura pasiva. **Solo 5 controles** realizan comprobaciones activas (verificación de perímetro, salida a internet y herramientas de control remoto sin autorización).

> ⚠ **ATENCIÓN**
> Esos 5 controles **solo se ejecutan si usted marca una casilla de autorización explícita** en el documento firmado. Nada intrusivo ocurre sin permiso expreso y por escrito.

6 Cómo funciona

1. **Visita.** Se ejecuta un colector (un único programa que no se instala) en los equipos y servidores a auditar, Windows y Linux.
2. **El colector recoge datos y se va.** No deja rastro, no modifica nada, no guarda contraseñas.
3. **El servidor de DCSeguridad evalúa** los datos recogidos contra los 243 controles.
4. **Se genera el informe** con los hallazgos ordenados por gravedad, cada uno con su explicación en lenguaje de negocio y su solución concreta.
5. **Revisión humana.** El informe pasa por un flujo borrador → revisado → entregado: una persona lo revisa antes de entregarlo. Nunca se entrega automático.
6. **Entrega y conversación.** El informe es suyo.

> ⓘ **INFO**
> Todo control que no se pudo evaluar se marca como no evaluado, nunca como conforme. La auditoría no da por bueno lo que no ha podido comprobar.

7 Valor y precio

> ✓ **OK**
> Una auditoría técnica de este alcance tiene un valor de mercado de **1.800€ a 3.500€**. La ofrecemos **sin coste y sin compromiso** como primer paso. El informe es suyo y puede resolverlo con quien quiera, incluido su proveedor actual.

dcsaudit encaja como **auditoría técnica de configuración e infraestructura con cumplimiento ENS, sin pentesting**: más profunda que una revisión básica (243 controles mapeados a ENS, Windows + Linux + Active Directory, informe con remediación priorizada), sin llegar a la explotación de vulnerabilidades.

Tipo de auditoría (mercado español 2026)	Rango
Revisión básica (sin pentesting)	800€ – 2.000€
Auditoría de vulnerabilidades + informe	1.500€ – 4.000€
Auditoría básica de infraestructura	2.000€ – 5.000€
Auditoría de cumplimiento RGPD/NIS2	2.000€ – 6.000€
Auditoría completa con pentesting	5.000€ – 12.000€
dcsaudit — valor de mercado equivalente	**1.800€ – 3.500€**

El coste de no hacerlo. El coste medio de recuperación tras un ciberataque en una PYME española ronda los **42.000€**, frente a los 2.000€–8.000€ de una auditoría preventiva. Los problemas más frecuentes del sector coinciden con los que detecta la herramienta:

78%
Sistemas sin actualizar

65%
Contraseñas débiles

52%
Copias no funcionales

44%
Accesos de ex-empleados sin revocar

8 Contacto

Producto	dcsaudit · `dcsaudit.dcseguridad.es`
Empresa	DCSeguridad · Consultoría IT & Ciberseguridad
Web	www.dcseguridad.com
Correo	hola@dcseguridad.com
Teléfono	910 053 662

Auditoría inicial gratuita y sin compromiso. El informe es del cliente.