DCSeguridad

DCSaudit

AUDITORÍA DE SEGURIDAD GRATUITA.

243 controles técnicos · Windows, Linux y Active Directory · Sin instalar nada, sin tocar nada

SIN COSTE · SIN COMPROMISO

Ejecución en una sola visita · Informe con hallazgos ordenados por gravedad · ENS categoría media

REF. DCS-COM-AUD-01

dcsaudit.dcseguridad.es · 2026

ÍNDICE.

UNA FOTOGRAFÍA CLARA DEL ESTADO DE SU IT.

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

Se ofrece **gratuita y sin compromiso** como primer paso. El informe es del cliente y puede resolverlo con quien quiera, incluido su proveedor actual.

Gratuita

0 € · sin compromiso posterior. Es nuestra manera de que conozca cómo trabajamos antes de contratar nada. Si al terminar no continúa con nosotros, sus datos se eliminan.

Sin instalar nada

El colector se ejecuta una vez y se va. No queda ningún programa, servicio ni agente residente. No modificamos nada: la auditoría solo lee.

Informe con soluciones

243 controles, ordenados por gravedad, cada uno explicado en lenguaje de negocio y con la solución concreta. Revisado por una persona antes de entregarse.

QUÉ HAY DETRÁS DE ESTA AUDITORÍA.

CONTROLES TÉCNICOS EN TOTAL

243

196 Windows · **47** Linux · **21** bloques temáticos

DISTRIBUCIÓN POR GRAVEDAD

Críticos	23
Gravedad alta	73
Medios	113
Bajos	21
Informativos	13

243

MAPEADOS A ENS

Nivel objetivo: ENS categoría media.

96

CON REFERENCIA CIS VERIFICADA

Benchmark de configuración del SO.

147

DE CRITERIO PROPIO

Gestión, estado operativo e infraestructura.

BLOQUES REVISADOS EN WINDOWS Y ACTIVE DIRECTORY.

196 controles Windows + 11 de salud del directorio + 7 de cifrado (compartidos con Linux).

01 · Antivirus y EDR

17 controles · **4 críticos**

Que funciona de verdad: protección permanente, definiciones al día, sin excepciones peligrosas.

02 · Copias de seguridad

17 controles · **2 críticos**

Última copia OK, dónde se guardan (¿alcanzables por ransomware?), si el correo está copiado.

03 · Software y soporte

12 controles · **1 crítico**

Inventario, sistema operativo y aplicaciones fuera de soporte, versiones antiguas olvidadas.

04 · Active Directory

28 controles · **2 críticos**

Administradores, delegaciones peligrosas, cuentas de servicio, contraseñas en fichas.

05 · Contraseñas y bloqueo

18 controles · **1 crítico**

Política real, longitud, caducidad, bloqueo por intentos y cuentas exentas.

06 · Políticas del sistema

19 controles · **2 críticos**

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

07 · Servicios y tareas

9 controles · **1 crítico**

Servicios con cuentas privilegiadas, permisos sobre binarios, tareas con credenciales.

08 · Estado de parcheo

9 controles

Actualizaciones pendientes, WSUS inaccesible, actualizaciones que fallan repetidamente.

09 · Red

15 controles · **1 crítico**

Servicios expuestos a internet, DNS correcto, salida sin restricción, firewall de Windows.

10 · Cifrado de disco

7 controles

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

11 · Registro y auditoría

12 controles

Si el sistema anota quién entra, quién falla y quién modifica cuentas: para reconstruir incidentes.

12 · Acceso remoto

9 controles · **1 crítico**

Escritorio remoto publicado en internet (principal vía de ransomware en PYME) y herramientas olvidadas.

13 · Recursos compartidos

8 controles · **1 crítico**

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

14 · Verificación perímetro

6 controles

Comprueba de verdad si la red bloquea amenazas (EICAR, tráfico cifrado). Con autorización firmada.

21 · Salud del directorio

11 controles · **4 críticos**

Servicios críticos del controlador, FSMO, replicación, SYSVOL/NETLOGON, DNS del dominio.

BLOQUES REVISADOS EN SERVIDORES LINUX.

47 controles específicos de Linux, más el bloque de cifrado (compartido con Windows).

15 · SSH

11 controles · **1 crítico**

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

16 · Privilegios y sudo

6 controles · **1 crítico**

Cuentas con UID de superusuario ocultas, elevación sin contraseña, registro de comandos ejecutados.

17 · Cuentas y contraseñas

10 controles · **1 crítico**

Cuentas sin contraseña, contraseñas mal protegidas, caducidad no aplicada.

18 · Servicios y cortafuegos

7 controles

Cortafuegos activo, política por defecto adecuada, parámetros de red correctos.

19 · Registro y auditoría

5 controles

Sistema de auditoría, retención de registros, envío externo para su conservación segura.

20 · Endurecimiento base

7 controles

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

10 · Cifrado de disco (comp.)

7 controles

Compartido con Windows: si los discos están cifrados y si la clave de recuperación está bien custodiada.

Cinco controles (verificación de perímetro y control remoto) son comprobaciones activas — se ejecutan solo con autorización explícita y por escrito. Más detalle en la slide 09.

HALLAZGOS EN LENGUAJE DE NEGOCIO, NO TÉCNICO.

Textos literales de la herramienta. El riesgo se explica por su consecuencia, no por su jerga.

ANTIVIRUS Y EDR

« 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. »

COPIAS DE SEGURIDAD

« 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. »

ACTIVE DIRECTORY

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

ACCESO REMOTO

« Escritorio remoto publicado a internet: es hoy la principal vía de entrada del ransomware en pequeñas y medianas empresas. »

CIFRADO DE DISCO

« 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. »

REGISTRO Y AUDITORÍA

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

QUÉ NO HACEMOS.

La honestidad es un argumento comercial. Esto es lo que dcsaudit NO hace, en ningún caso.

NO INSTALAMOS NADA ✓

El colector se ejecuta una vez y se va. No queda ningún programa, servicio ni agente residente en los equipos del cliente.

NO MODIFICAMOS NADA ✓

La auditoría solo lee. No cambia absolutamente nada en los sistemas: ni configuraciones, ni políticas, ni permisos.

NO ACCEDEMOS A CONTRASEÑAS ✓

Aunque se detectan contraseñas mal guardadas, el informe cita la cuenta o el equipo afectado — nunca el valor. No viajan al servidor ni se almacenan.

NO HACEMOS FUERZA BRUTA NI ATAQUES ✓

No se prueban credenciales, no se explotan fallos, no hay pentesting. Es una revisión de configuración, no una prueba ofensiva.

NO DEJAMOS DATOS EXPUESTOS ✓

La evidencia se cifra. Los datos de empresas sin contrato tienen una frontera de privacidad estricta, y se eliminan si no continúa con nosotros.

NADA INTRUSIVO OCURRE
SIN PERMISO EXPRESO Y POR ESCRITO.

SOLO

5

CONTROLES ACTIVOS

De 243 en total — el resto es lectura pasiva.

Se ejecutan solo si el cliente marca una casilla de autorización explícita en el documento firmado.

QUÉ HACEN ESTOS CINCO CONTROLES

WIN-NET-008

Verificación real de perímetro con fichero EICAR (inofensivo y reconocido por todos los antivirus).

WIN-RMT-003

Detección de herramientas de control remoto olvidadas o sin autorización en los equipos.

WIN-ACT-001

Comprobación de inspección de tráfico cifrado en el filtrado perimetral.

WIN-ACT-002

Comprobación de protección antisuplantación en la navegación.

WIN-ACT-004

Verificación activa de la salida a internet sin restricciones indebidas.

ALINEADOS CON ESTÁNDARES,
Y CON LO QUE LOS ESTÁNDARES NO COMPRUEBAN.

ESQUEMA NACIONAL DE SEGURIDAD (ENS)

243 / 243

Los 243 controles están mapeados al Esquema Nacional de Seguridad. Nivel objetivo de la herramienta: ENS categoría media.

CIS BENCHMARKS

96 verificados

96 controles con referencia CIS verificada. CIS es un benchmark de configuración del sistema operativo, publicado por el Center for Internet Security.

147 controles son de criterio propio (gestión, estado operativo, infraestructura).
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.

HONESTIDAD TÉCNICA: 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.

SEIS PASOS, SIN INTERRUMPIR EL TRABAJO.

01 VISITA

Se ejecuta un colector — un único programa que no se instala — en los equipos y servidores a auditar. Windows y Linux.

02 RECOGIDA Y SALIDA

El colector recoge datos y se va. No deja rastro, no modifica nada, no guarda contraseñas.

03 EVALUACIÓN

El servidor de DCSeguridad evalúa los datos recogidos contra los 243 controles del catálogo.

04 INFORME

Se genera un informe con los hallazgos ordenados por gravedad, cada uno con explicación en lenguaje de negocio y solución concreta.

05 REVISIÓN HUMANA

Flujo borrador → revisado → entregado. Una persona lo revisa antes de entregarlo. Nunca se entrega automático.

06 ENTREGA Y CONVERSACIÓN

El informe es del cliente. Puede resolverlo con quien quiera, incluido su proveedor actual.

QUÉ NO ES.

Somos claros con lo que dcsaudit NO cubre — para dimensionar bien lo que aporta.

✗ NO ES CONFORMIDAD NI CERTIFICACIÓN

Evalúa medidas técnicas verificables de forma automática. La conformidad con ENS o ISO 27001 incluye además procedimientos, documentación y análisis de riesgos que ninguna herramienta puede comprobar.

✗ NO ES UN TEST DE INTRUSIÓN

No se intenta acceder a ningún sistema ni explotar ninguna vulnerabilidad. Es una revisión de configuración, no una prueba ofensiva.

✗ NO SUSTITUYE LA SUPERVISIÓN CONTINUA

Es una fotografía del estado actual. Para vigilar de forma continua se necesita un servicio de monitorización activo, no una auditoría puntual.

✗ NO ENTREGA CVE POR EQUIPO

Damos la señal de parcheo (sistemas fuera de soporte, actualizaciones pendientes, software abandonado, parches que fallan) — fiable y defendible. El detalle CVE por equipo es un servicio de gestión continua posterior.

PREGUNTAS FRECUENTES.

? ¿Interrumpe el trabajo?

No. El colector se ejecuta en segundo plano y no requiere reiniciar ni cerrar programas. Algunas comprobaciones activas pueden generar avisos en el antivirus; se acuerdan previamente y se avisa antes de realizarlas.

? ¿Qué información se llevan?

Configuración de seguridad, inventario de programas y relación de usuarios y permisos. No se accede al contenido de sus archivos, ni al correo, ni a bases de datos.

? ¿Necesitan la contraseña de administrador?

No necesariamente. Con permisos limitados se obtiene menos información y el informe lo indica expresamente. Si desea una revisión completa, puede introducir usted mismo las credenciales o crear una cuenta temporal de solo lectura que se deshabilita al terminar. Las credenciales no se almacenan ni se transmiten.

? ¿Y si el informe sale mal?

Es lo habitual, y no es un juicio sobre su empresa. Prácticamente todas las auditorías iniciales encuentran puntos críticos, porque son configuraciones que se acumulan durante años. El valor está en saberlo.

VALOR DE MERCADO
DE UNA AUDITORÍA DE ESTE ALCANCE.

EQUIVALENTE EN EL MERCADO ESPAÑOL 2026

1.800 € – 3.500 €

dcsaudit se ofrece a **0 €**, sin compromiso, como primer paso.

RANGOS DE MERCADO EN PYME 20-50 EMPLEADOS

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 €

42.000 €

COSTE MEDIO DE RECUPERACIÓN TRAS UN CIBERATAQUE EN PYME ESPAÑOLA.
Sistemas sin actualizar (~78 %) · contraseñas débiles (~65 %) · copias no funcionales (~52 %) · accesos de ex-empleados sin revocar (~44 %): los problemas más frecuentes son los que más detecta dcsaudit.

DCSaudit

SOLICITE HOY
SU AUDITORÍA GRATUITA.

30 minutos sin compromiso · informe escrito · **si no continúa, sus datos se eliminan.**

EMAIL

hola@dcseguridad.es

TELÉFONO

910 053 662

WEB

https://dcseguridad.es

Avenida de la Rioja 28 · 28691 Villanueva de la Cañada, Madrid | Horario: L-V 9:00 – 18:00