Autoevaluación de ciberseguridad

CyberScore: 

Fecha de generación del informe: **08/11/2026 20:16**

> Este informe es una simple autoevaluación de su nivel de seguridad informática, basada exclusivamente en sus respuestas al cuestionario diseñado por los expertos de Oxydian. En ningún caso constituye una auditoría técnica en profundidad. Aunque le ofrece una primera visión de sus fortalezas y vulnerabilidades en materia de ciberseguridad, no sustituye un análisis riguroso de sus infraestructuras y sistemas. Para ir más allá y beneficiarse de una auditoría técnica completa, no dude en ponerse en contacto con nosotros:
>
> contact@oxydian.fr

Resumen:

Su nivel de seguridad presenta debilidades significativas que merecen una atención inmediata. El riesgo de explotación de algunas vulnerabilidades es elevado, lo que podría comprometer la seguridad global de su organización. Recomendamos encarecidamente implantar medidas correctivas y le proponemos un acompañamiento especializado para realizar una auditoría en profundidad.

Detalle de las puntuaciones por categoría (40.0%)

Contraseñas



Seguridad de los datos



Supervisión y detección



Seguridad interna



Seguridad externa



Gestión de la seguridad



Identificación de riesgos



Seguridad física



Plan de acción personalizado:

Este plan de acción se basa en los resultados de su evaluación. Le recomendamos seguir estas indicaciones para mejorar su seguridad informática.

Almacenamiento seguro de las contraseñas
Asegúrese de que todas las contraseñas se guarden en un gestor de contraseñas seguro en lugar de en soportes no seguros.

Utilizar un antivirus
Asegúrese de que todos sus servidores y equipos cuenten con un antivirus actualizado para detectar y bloquear las amenazas.

Sustitución de los equipos obsoletos
Sustituya o migre los equipos obsoletos (Windows XP, Vista, 7, 8 o Windows Server 2003 / 2008 / 2012) para reducir el riesgo de vulnerabilidades sin corregir.

Separar los derechos de usuario y de administrador
Esta práctica consiste en asignar cuentas distintas para las tareas diarias y para las tareas de administración. Reduce considerablemente los riesgos de compromiso, ya que limita el acceso a los privilegios elevados únicamente a las operaciones concretas que requieren una gestión administrativa.

Implantación de una política de contraseñas
Implante una política de contraseñas rigurosa para garantizar que las contraseñas sean seguras, complejas y se renueven con regularidad.

Protección del correo electrónico con 2FA
Active la autenticación en dos factores (2FA) en todas las cuentas de correo electrónico de la empresa (Microsoft 365, Google Workspace...). El compromiso del correo electrónico es el vector de ataque más frecuente contra las pymes y la 2FA bloquea la gran mayoría de estos ataques.

Análisis periódico de las contraseñas
Encargue periódicamente a un profesional o a su departamento de TI un análisis de sus contraseñas para detectar contraseñas débiles y reutilizadas, y reforzar así la seguridad.

Implantación del cifrado de disco
Se recomienda encarecidamente activar el cifrado de disco en todos los ordenadores y servidores, utilizando soluciones como BitLocker para Windows o LUKS para Linux, con el fin de proteger sus datos sensibles frente a accesos no autorizados.

Pruebas de restauración de las copias de seguridad
Planifique pruebas de restauración periódicas (al menos una vez por trimestre) para comprobar que sus copias de seguridad son realmente utilizables y medir el tiempo necesario para reanudar su actividad.

Elaboración de un inventario de los activos externos
Actualice y complete periódicamente el inventario de sus activos expuestos en internet para mejorar la gestión de la seguridad.

Implantación de la 2FA en la VPN
Active la autenticación en dos factores (2FA) en todos los accesos VPN para reforzar la seguridad de las conexiones remotas.

Procedimiento de respuesta a incidentes
Formalice un procedimiento de respuesta a incidentes: primeras acciones que deben llevarse a cabo, lista de contactos de emergencia (proveedor especializado, aseguradora, autoridad de protección de datos en caso de fuga de datos) y funciones internas. Pruébelo al menos una vez al año mediante un ejercicio de simulación de mesa.

Implantación de la autenticación en dos factores
Active la autenticación en dos factores (2FA) en todas sus cuentas y servicios críticos para añadir una capa adicional de seguridad.

Redundancia de las copias de seguridad
Se recomienda encarecidamente almacenar sus copias de seguridad en varias ubicaciones distintas para reducir el riesgo de pérdida de datos en caso de siniestro.

Evolución hacia un EDR
Sustituya o complemente su antivirus tradicional con una solución EDR (Endpoint Detection and Response), capaz de detectar comportamientos maliciosos y de aislar los equipos comprometidos frente a ataques modernos como el ransomware.

Centralización de los registros
Centralice los registros de sus servidores y equipos críticos en un espacio de almacenamiento dedicado y consérvelos durante varios meses (se recomiendan de 6 a 12 meses). Esto permite detectar los incidentes y analizarlos aunque el atacante borre los rastros locales.

Elaboración de un inventario de los activos internos
Actualice y complete periódicamente el inventario de sus activos internos para mejorar la gestión de la seguridad.

Segmentación de la red Wi-Fi
Implemente varias redes Wi-Fi para separar los accesos públicos de los internos y reforzar así la seguridad, ofreciendo al mismo tiempo una red Wi-Fi pública solo para el acceso a internet.

Implantación de una política de actualización externa
Adopte una política de actualización estricta para todos sus activos externos con el fin de minimizar los riesgos relacionados con las vulnerabilidades.

Implantación de una política de uso de los sistemas informáticos
Asegúrese de que todos los empleados firmen una política de uso de los sistemas informáticos que defina las normas y buenas prácticas de seguridad, haciendo hincapié en la protección de los datos personales para cumplir los requisitos del RGPD.

Simulaciones de phishing periódicas
Organice campañas de phishing simulado al menos una vez al año para medir los reflejos de sus empleados en condiciones reales y orientar la concienciación hacia los puntos débiles detectados.

Control de los accesos de proveedores
Controle los accesos de sus proveedores: cuentas nominativas dedicadas, derechos limitados a lo estrictamente necesario, desactivación sistemática al finalizar la intervención o el contrato, y trazabilidad de las conexiones.

Control de acceso a la sala de servidores
Implante un control estricto del acceso a la sala de servidores para evitar manipulaciones no autorizadas.

Implantación de un protocolo de incorporación y salida
Defina un protocolo claro para la incorporación y la salida de los empleados, que incluya la eliminación de las cuentas y los accesos, para proteger a la empresa frente a los riesgos de seguridad.

Leyenda:

INFORMACIÓN

Riesgo global nulo, se trata simplemente de observaciones detectadas durante la auditoría.

MENOR

Riesgo global bajo que no requiere acciones importantes.

MODERADO

Riesgo global moderado que requiere acciones a medio plazo.

MAYOR

Riesgo global importante que requiere acciones a corto plazo.

CRÍTICO

Riesgo global crítico que requiere acciones inmediatas.