Autoavaluació de ciberseguretat

CyberScore: 

Data de generació de l'informe: **08/11/2026 20:16**

> Aquest informe és una simple autoavaluació del seu nivell de seguretat informàtica, basada exclusivament en les seves respostes al qüestionari dissenyat pels experts d'Oxydian. En cap cas no constitueix una auditoria tècnica en profunditat. Tot i que li ofereix una primera visió dels seus punts forts i de les seves vulnerabilitats en ciberseguretat, no substitueix una anàlisi rigorosa de les seves infraestructures i sistemes. Per anar més enllà i beneficiar-se d'una auditoria tècnica completa, no dubti a posar-se en contacte amb nosaltres:
>
> contact@oxydian.fr

Resum:

El seu nivell de seguretat presenta debilitats importants que mereixen una atenció immediata. El risc que s'explotin algunes vulnerabilitats és elevat, cosa que podria comprometre la seguretat global de la seva organització. Li recomanem fermament implantar mesures correctives i considerar un acompanyament especialitzat per dur a terme una auditoria en profunditat.

Detall de les puntuacions per categoria (40.0%)

Contrasenyes



Seguretat de les dades



Supervisió i detecció



Seguretat interna



Seguretat externa



Gestió de la seguretat



Identificació de riscos



Seguretat física



Pla d'acció personalitzat:

Aquest pla d'acció es basa en els resultats de la seva avaluació. Li recomanem que segueixi aquests consells per millorar la seva seguretat informàtica.

Emmagatzematge segur de les contrasenyes
Asseguri's que totes les contrasenyes es guarden en un gestor de contrasenyes segur i no en suports no segurs.

Utilitzar un antivirus
Asseguri's que tots els seus servidors i equips disposen d'un antivirus actualitzat per detectar i bloquejar les amenaces.

Substitució dels equips obsolets
Substitueixi o migri els equips obsolets (Windows XP, Vista, 7, 8 o Windows Server 2003 / 2008 / 2012) per reduir el risc de vulnerabilitats sense corregir.

Separar els drets d'usuari i d'administrador
Aquesta pràctica consisteix a assignar comptes diferents per a les tasques quotidianes i per a les tasques d'administració. Redueix considerablement el risc de compromís de la seguretat, ja que limita l'accés als privilegis elevats només a les operacions concretes que requereixen una gestió administrativa.

Implantació d'una política de contrasenyes
Estableixi una política de contrasenyes rigorosa per garantir que les contrasenyes siguin segures, complexes i es renovin periòdicament.

Protecció del correu electrònic amb 2FA
Activi l'autenticació de dos factors (2FA) en tots els comptes de correu electrònic de l'empresa (Microsoft 365, Google Workspace...). El compromís del correu electrònic és el vector d'atac més freqüent contra les pimes i la 2FA bloqueja la gran majoria d'aquests atacs.

Anàlisi periòdica de les contrasenyes
Encarregui periòdicament a un professional o al seu departament d'informàtica una anàlisi de les contrasenyes per detectar contrasenyes febles i reutilitzacions, i reforçar així la seguretat.

Implantació del xifratge de disc
Es recomana fermament activar el xifratge de disc en tots els ordinadors i servidors, amb solucions com BitLocker per a Windows o LUKS per a Linux, per protegir les seves dades sensibles contra els accessos no autoritzats.

Proves de restauració de les còpies de seguretat
Planifiqui proves de restauració periòdiques (com a mínim un cop per trimestre) per verificar que les seves còpies de seguretat són realment utilitzables i mesurar el temps necessari per reprendre l'activitat.

Elaboració d'un inventari dels actius externs
Actualitzi i completi periòdicament l'inventari dels seus actius exposats a internet per millorar la gestió de la seguretat.

Implantació de la 2FA per a la VPN
Activi l'autenticació de dos factors (2FA) per a tots els accessos VPN per reforçar la seguretat de les connexions remotes.

Procediment de resposta a incidents
Formalitzi un procediment de resposta a incidents: primeres accions que cal dur a terme, llista de contactes d'emergència (proveïdor especialitzat, asseguradora, autoritat de protecció de dades en cas de fuga de dades) i rols interns. Posi'l a prova com a mínim un cop l'any amb un exercici de simulació.

Implantació de l'autenticació de dos factors
Activi l'autenticació de dos factors (2FA) en tots els seus comptes i serveis crítics per afegir una capa addicional de seguretat.

Redundància de les còpies de seguretat
Es recomana fermament guardar les còpies de seguretat en diverses ubicacions diferents per reduir el risc de pèrdua de dades en cas de sinistre.

Evolució cap a un EDR
Substitueixi o complementi el seu antivirus convencional amb una solució EDR (Endpoint Detection and Response), capaç de detectar comportaments maliciosos i d'aïllar els equips compromesos davant d'atacs moderns com els ransomwares.

Centralització dels registres
Centralitzi els registres dels seus servidors i equips crítics en un espai d'emmagatzematge dedicat i conservi'ls durant diversos mesos (es recomanen de 6 a 12 mesos). Així podrà detectar i analitzar els incidents encara que l'atacant esborri els rastres locals.

Elaboració d'un inventari dels actius interns
Actualitzi i completi periòdicament l'inventari dels seus actius interns per millorar la gestió de la seguretat.

Segmentació de la xarxa wifi
Implanti diverses xarxes wifi per separar els accessos públics dels interns i reforçar així la seguretat, tot oferint una wifi pública només per accedir a internet.

Implantació d'una política d'actualització externa
Adopti una política d'actualització estricta per a tots els seus actius externs per minimitzar els riscos associats a les vulnerabilitats.

Implantació d'una política d'ús dels recursos informàtics
Asseguri's que tots els treballadors signin una política d'ús dels recursos informàtics que defineixi les normes i bones pràctiques de seguretat, posant l'accent en la protecció de les dades personals per complir els requisits del RGPD.

Simulacres de phishing periòdics
Organitzi campanyes de phishing simulat com a mínim un cop l'any per mesurar els reflexos dels seus col·laboradors en condicions reals i orientar la conscienciació cap als punts febles detectats.

Regulació dels accessos dels proveïdors
Reguli els accessos dels seus proveïdors: comptes nominatius dedicats, drets limitats al mínim necessari, desactivació sistemàtica en acabar la intervenció o el contracte, i traçabilitat de les connexions.

Control d'accés a la sala de servidors
Implanti un control estricte de l'accés a la sala de servidors per evitar manipulacions no autoritzades.

Implantació d'un protocol d'incorporació i sortida
Defineixi un protocol clar per a la incorporació i la sortida dels col·laboradors, que inclogui la supressió dels comptes i dels accessos, per protegir l'empresa contra els riscos de seguretat.

Llegenda:

INFORMACIÓ

Risc global nul, es tracta simplement d'observacions detectades durant l'auditoria.

MENOR

Risc global baix que no requereix accions importants.

MODERAT

Risc global moderat que requereix accions a mitjà termini.

GREU

Risc global greu que requereix accions a curt termini.

CRÍTIC

Risc global crític que requereix accions immediates.