

CIBERSEGURIDAD PARA EMPRESAS

10 CONTROLES QUE TU EMPRESA DEBERÍA REVISAR

Una lista corta y sin tecnicismos para saber dónde está tu empresa hoy. No sustituye a una auditoría, pero te ayuda a detectar los puntos débiles más habituales antes de que se conviertan en un incidente.

10

controles esenciales

30

comprobaciones para marcar

3

niveles de resultado para saber por dónde empezar

IDENTIDAD, COPIAS Y EQUIPOS

pág. 2

- 01** Doble factor en todas las cuentas
- 02** Copias que un ataque no pueda borrar
- 03** Actualizaciones al día
- 04** Protección avanzada en los equipos
- 05** Correo protegido

ACCESOS, RED Y PERSONAS

pág. 3

- 06** Cada persona, con lo justo
- 07** Inventario de equipos y programas
- 08** Red y acceso remoto seguros
- 09** Personas preparadas
- 10** Un plan por si algo pasa

1**Revisa en equipo**

Hazlo con la persona que lleva la tecnología de tu empresa.

2**Marca lo comprobado**

Solo las casillas que puedas verificar, no las que «creas» que están bien.

3**Mira tu resultado**

Cuenta los controles completos y consulta la escala de la página 4.

IDENTIDAD, COPIAS Y EQUIPOS

Los controles que más incidentes evitan.

1

DOBLE FACTOR EN TODAS LAS CUENTAS

Una contraseña robada no debería bastar para entrar en el correo ni en los sistemas de la empresa.

- ☐ El doble factor (MFA) está activado en el correo y en Microsoft 365 para todas las personas.
- ☐ También en la VPN, el acceso remoto y las cuentas de administración.
- ☐ Nadie usa la misma contraseña en el trabajo y en servicios personales.

2

COPIAS QUE UN ATAQUE NO PUEDA BORRAR

Ante un ransomware, la copia es lo que permite volver a trabajar sin pagar un rescate.

- ☐ Hay al menos una copia fuera de la red de la empresa o que no se puede modificar (inmutable).
- ☐ Se copian también Microsoft 365, el correo y los servidores, no solo los archivos.
- ☐ Se ha probado a recuperar algo de la copia en los últimos meses.

3

ACTUALIZACIONES AL DÍA

Muchos ataques aprovechan fallos ya conocidos y corregidos por el fabricante.

- ☐ Los equipos y servidores reciben los parches de seguridad de forma regular.
- ☐ El cortafuegos, la VPN y los equipos de red tienen soporte y están actualizados.
- ☐ No quedan equipos con sistemas sin soporte del fabricante.

4

PROTECCIÓN AVANZADA EN LOS EQUIPOS

Un antivirus tradicional no detecta muchos ataques actuales, que usan herramientas legítimas.

- ☐ Los equipos y servidores tienen una protección que detecta comportamientos sospechosos (EDR), no solo un antivirus.
- ☐ Alguien revisa las alertas, también fuera del horario de oficina.
- ☐ Los portátiles tienen el disco cifrado.

5

CORREO PROTEGIDO

El correo sigue siendo la puerta de entrada más habitual de los ataques.

- ☐ Hay filtros antiphishing y antispam más allá de los básicos.
- ☐ El dominio tiene configurados SPF, DKIM y DMARC para evitar suplantaciones.
- ☐ Se revisan las reglas que reenvían correo a direcciones externas.

ACCESOS, RED Y PERSONAS

Lo que limita el daño si algo falla.

6

CADA PERSONA, CON LO JUSTO

Cuantos menos permisos tenga una cuenta, menos daño puede hacer si alguien la roba.

- ☐ Las cuentas de administración están separadas de las de uso diario.
- ☐ Se revisa cada cierto tiempo quién tiene acceso a cada carpeta y aplicación.
- ☐ Cuando alguien deja la empresa, sus accesos se dan de baja ese mismo día.

7

INVENTARIO DE EQUIPOS Y PROGRAMAS

No se puede proteger lo que no se sabe que existe.

- ☐ Hay una lista actualizada de equipos, servidores y programas, con su responsable.
- ☐ Se sabe qué garantías y licencias vencen y cuándo.
- ☐ Los equipos personales que acceden a datos de la empresa están identificados y gestionados.

8

RED Y ACCESO REMOTO SEGUROS

Un acceso remoto mal configurado es una de las vías de entrada más aprovechadas.

- ☐ Ningún escritorio remoto (RDP) ni panel de gestión está expuesto directamente a internet.
- ☐ La red de invitados y los dispositivos conectados (cámaras, impresoras) están separados del resto.
- ☐ El cortafuegos tiene un responsable y sus reglas se revisan.

9

PERSONAS PREPARADAS

La mayoría de los incidentes empiezan con un clic de buena fe.

- ☐ El equipo ha recibido formación práctica o simulaciones de phishing en el último año.
- ☐ Todo el mundo sabe a quién avisar si ve algo raro, sin miedo a equivocarse.
- ☐ Los pagos y cambios de cuenta bancaria se confirman por un segundo canal.

10

UN PLAN POR SI ALGO PASA

Durante un incidente no es momento de improvisar quién hace qué.

- ☐ Hay un plan escrito: a quién llamar, qué aislar y cómo recuperar.
- ☐ Se sabe qué obligaciones hay de notificar (el RGPD exige comunicar a la autoridad las brechas de datos personales en 72 horas).
- ☐ Los contactos de proveedores y soporte están a mano fuera de los sistemas de la empresa.

¿CUÁNTOS CONTROLES TIENES COMPLETOS?

Cuenta solo los controles con sus tres casillas marcadas y apunta el resultado.

CONTROLES COMPLETOS	FECHA DE LA REVISIÓN	REVISADO POR
/ 10		

0	1	2	3	4	5	6	7	8	9	10
---	---	---	---	---	---	---	---	---	---	----

0 A 4 · EXPUESTA

Tu empresa tiene riesgos importantes. Conviene una revisión profesional cuanto antes y empezar por las medidas que menos cuestan y más protegen.

5 A 7 · CON HUECOS

Hay una base, pero quedan puntos débiles que un atacante puede aprovechar.

8 A 10 · BUENA BASE

Mantén revisiones periódicas y comprueba que todo sigue funcionando.

SI NO SABES POR DÓNDE EMPEZAR

01 · DOBLE FACTOR

Actívalo en el correo y en Microsoft 365. Es lo que más ataques frena con menos esfuerzo.

02 · COPIAS

Ten una copia fuera de la red o inmutable, y prueba a recuperar algo de ella.

03 · ACTUALIZACIONES

Pon al día equipos, servidores, cortafuegos y VPN.

¿PREFIERES QUE LO REVISEMOS CONTIGO?

Te ayudamos a comprobar estos controles en tu empresa y te decimos por dónde empezar, sin compromiso y sin tecnicismos.

Teléfono **944 362 257**

Email **info@olatic.es**

Web **olatic.es/contacto**

SI USAS MICROSOFT 365

MICROSOFT 365 SECURITY CHECK

Revisamos a fondo la seguridad de tu Microsoft 365 y te entregamos un informe con lo que corregir primero, en 1 a 2 semanas.

Desde **490 €** + IVA

Esta checklist es orientativa. Cada empresa tiene su contexto: tamaño, sector, normativa que le aplica (como NIS2 o el ENS) y herramientas que ya usa.