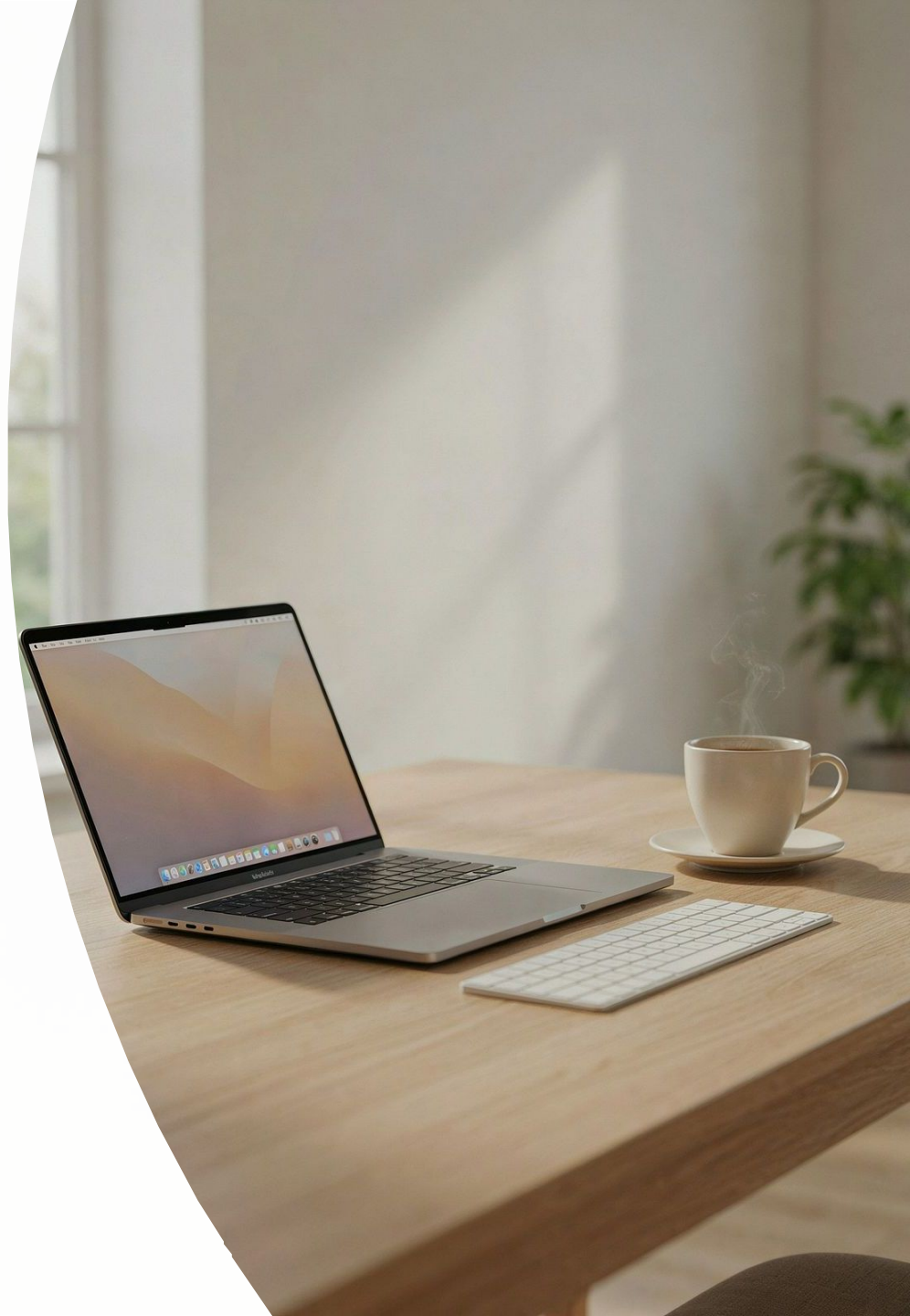
Ciberseguridad en el PC de la oficina

El ordenador de trabajo concentra buena parte de la actividad digital de una empresa: correo electrónico, aplicaciones corporativas, documentos, credenciales y servicios en la nube. Mantenerlo correctamente configurado, actualizado y gestionado refuerza la seguridad de toda la organización.

GUÍA PRÁCTICA

8 ASPECTOS CLAVE



Los errores más habituales

Muchos de los fallos de ciberseguridad en el PC de oficina son evitables mediante buenas prácticas, mantenimiento planificado y formación del equipo.

Contraseñas reutilizadas

Credenciales compartidas entre servicios multiplican el riesgo ante filtraciones.

Actualizaciones aplazadas

Dejar sin parchear el sistema operativo y las apps expone vulnerabilidades conocidas.

Phishing no detectado

No reconocer mensajes fraudulentos sigue siendo uno de los principales vectores de ataque.

Sin copias de seguridad

La ausencia de backups verificados impide recuperarse ante ransomware o fallos de hardware.

Permisos innecesarios

Accesos que no se revisan acumulan privilegios que ya no corresponden a la función real.

Equipos sin soporte

Sistemas operativos al final de su ciclo dejan de recibir correcciones de seguridad.

1. Contraseñas: la primera línea de defensa

Reutilizar contraseñas en diferentes servicios es uno de los errores más extendidos. Si esas credenciales quedan expuestas en una filtración, un atacante puede intentar acceder a otros servicios corporativos.

Contraseña única por cuenta

Nunca reutilizar claves entre servicios distintos.

Claves largas y robustas

Difíciles de predecir y gestionadas con un gestor corporativo.

Autenticación multifactor (MFA)

Activarla siempre que el servicio lo permita. No compartir credenciales entre compañeros.

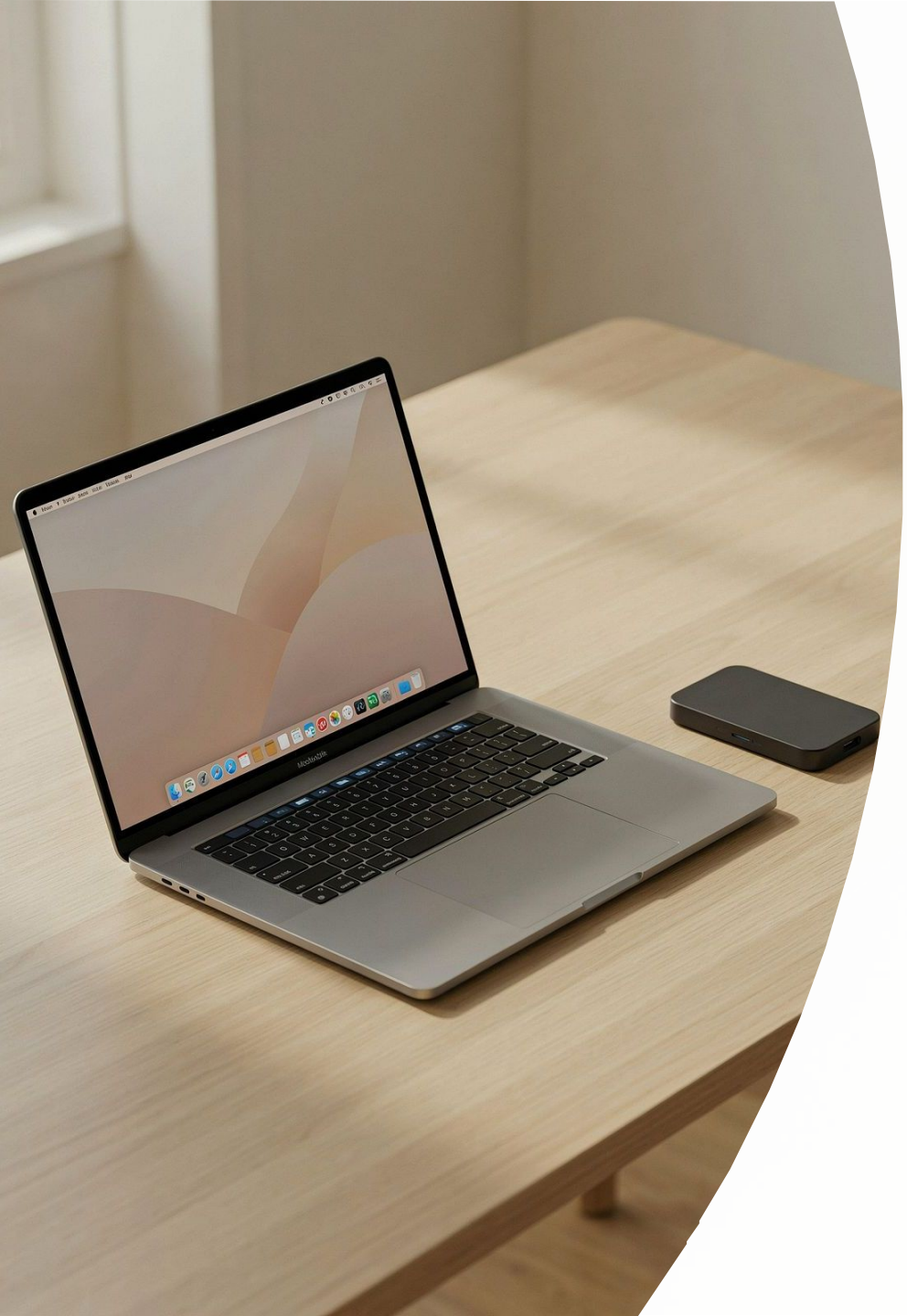
2 y 3. Actualizaciones y protección frente al phishing

Mantener el software actualizado

Las actualizaciones incluyen correcciones para vulnerabilidades detectadas. Se recomienda activar las actualizaciones automáticas, establecer una política centralizada para todo el parque y mantener un inventario del software instalado, comprobando que las aplicaciones siguen teniendo soporte activo del fabricante.

Cómo identificar el phishing

Según el **ENISA Threat Landscape 2025**, el phishing sigue siendo uno de los principales vectores de acceso inicial en la UE. Antes de interactuar con un mensaje dudoso: revisar la dirección real del remitente, comprobar el destino del enlace, desconfiar de solicitudes urgentes de credenciales y comunicar cualquier sospecha al departamento de TI.



4. Cifrado y copias de seguridad

Los ordenadores corporativos almacenan documentación comercial, financiera y datos de clientes. El cifrado protege esa información ante pérdida o sustracción. Las copias de seguridad permiten recuperar la actividad ante fallos de hardware, errores humanos o ataques de ransomware. El **INCIBE** recomienda verificar periódicamente que las copias pueden restaurarse correctamente.

Copias periódicas

Con almacenamiento independiente del equipo original.

Control de acceso

A los sistemas de backup para evitar compromisos.

Pruebas de restauración

Verificar regularmente que la copia funciona cuando se necesita.

Procedimientos documentados

Protocolos claros de recuperación ante incidentes.

5 y 6. Software autorizado y ciclo de vida de los dispositivos

Uso del PC corporativo

Una política clara debe determinar qué aplicaciones pueden instalarse, qué dispositivos externos pueden conectarse, qué usos están permitidos y cómo se gestionan las licencias. Mantener el PC corporativo separado del uso personal facilita el mantenimiento y contribuye a una configuración más segura.

Gestión del ciclo de vida

Windows 10 alcanzó el final de su soporte general el 14 de octubre de 2025. Microsoft ofrece programas ESU como medida de transición, pero no como solución definitiva. Un inventario actualizado permite conocer qué equipos tienen soporte activo, cuáles están próximos al fin de soporte y cuáles necesitan renovación planificada.

7. Revisar y actualizar los permisos de acceso

Los permisos deben evolucionar al mismo tiempo que las responsabilidades de cada persona. El **principio de mínimo privilegio** establece que cada usuario debe disponer únicamente de los permisos necesarios para su función.

1

Incorporación

Asignar solo los accesos necesarios para el puesto desde el primer día.

2

Cambio de puesto

Actualizar permisos ante cualquier cambio de función o responsabilidades.

3

Revisión periódica

Auditar accesos activos como parte de las revisiones de seguridad regulares.

4

Baja

Revocar todos los accesos de inmediato al finalizar la relación laboral.

8. Formar al equipo: la mejor inversión en ciberseguridad

Un empleado que conoce las políticas de seguridad y sabe cómo actuar ante situaciones poco habituales es una capa de protección adicional. La concienciación periódica, adaptada a las amenazas reales del momento, resulta más efectiva que una sesión puntual durante la incorporación.

Identificar el phishing

Reconocer mensajes fraudulentos antes de interactuar con ellos.

Gestión de contraseñas

Entender por qué las claves únicas y el MFA son esenciales.

Comunicar incidencias

Saber a quién y cuándo reportar un mensaje o archivo sospechoso.

Tabla resumen: aspectos clave

Aspecto	Acción clave
Contraseñas	Claves únicas por servicio y autenticación multifactor (MFA) activada.
Actualizaciones	Mantener sistema operativo y aplicaciones siempre al día.
Phishing	Formar al equipo para identificar y gestionar mensajes fraudulentos.
Cifrado y copias	Proteger la información y verificar la restauración periódicamente.
Software autorizado	Definir qué aplicaciones pueden instalarse en los equipos corporativos.
Ciclo de vida	Controlar qué equipos tienen soporte activo y planificar su renovación.
Permisos de acceso	Revisarlos ante cada incorporación, baja o cambio de responsabilidades.
Formación del equipo	La concienciación periódica convierte a cada persona en una capa de protección real.

La ciberseguridad también depende del estado de tus dispositivos

Un PC de oficina bien mantenido, actualizado y con soporte del fabricante vigente es la base de cualquier estrategia de ciberseguridad. El estado técnico de los dispositivos y su seguridad van de la mano.

IT Asset Management

Un inventario actualizado permite anticipar finales de soporte, planificar el mantenimiento y decidir con criterio cuándo reparar o renovar un equipo.

Eficiencia y economía circular

Este enfoque integra eficiencia tecnológica y economía circular dentro de una misma visión del parque tecnológico corporativo.

¿Tienes dudas sobre el estado de soporte de tus equipos? Un inventario actualizado es el primer paso para tomar decisiones informadas.