**Actividad 1.2 Protección del Puesto de Trabajo**



Trabajo realizado por:

Samuel Romero de los Reyes

# **Índice**

[**Índice 2**](#_br70gdai3dpl)

[**1.- Antecedentes 3**](#_qmq0qcfxl4l0)

[**2.- Objetivos 4**](#_q0ceim8weo6f)

[**3.- Puntos clave 4**](#_ncnychmb3fh6)

[**4.- Checklist 5**](#_8mbi4zf4k1dz)

# 

# **1.- Antecedentes**

El uso de **ordenadores portátiles** se ha convertido en una herramienta esencial para el desarrollo de la actividad profesional, permitiendo el trabajo desde distintos lugares: oficina, domicilio, espacios compartidos o durante desplazamientos. Esta movilidad, sin embargo, amplía los riesgos asociados al manejo de información corporativa y requiere establecer medidas específicas de seguridad para su protección.

Los **portátiles** son equipos que contienen o pueden acceder a información sensible de la empresa y sus sistemas, por lo que su pérdida, robo o uso indebido puede tener consecuencias graves para la organización. Por ello, es imprescindible concienciar a los empleados y exigir el cumplimiento de unas normas mínimas de seguridad en el uso, transporte y almacenamiento de estos dispositivos.

Por una parte, el empleado debe conocer los **riesgos físicos y no tecnológicos**, entre los que se incluyen:

* Robo o extravío del equipo durante desplazamientos o en lugares públicos.
* Acceso visual no autorizado (“shoulder surfing”) por parte de terceros en lugares compartidos (cafeterías, transporte público, etc.).
* Falta de custodia adecuada del equipo o de la información en papel relacionada con él.
* Conexión a redes Wi-Fi públicas o no seguras que pueden comprometer la información transmitida.

Por otra parte, los **riesgos tecnológicos** también están presentes:

* Acceso no autorizado al portátil por contraseñas débiles o compartidas.
* Infecciones por malware o ransomware derivadas de la instalación de software no autorizado o del uso de dispositivos externos inseguros.
* Sincronización o copia de datos en servicios en la nube personales sin las debidas garantías.
* Robo o filtración de información a través de phishing o técnicas de ingeniería social.

Para garantizar un uso seguro y responsable de los portátiles corporativos, la organización debe implantar una **política de protección específica para dispositivos portátiles**, que incluya las obligaciones y buenas prácticas en materia de seguridad aplicables a estos equipos.

Dicha política debe abordar, entre otros aspectos:

* El cifrado obligatorio de los discos duros.
* El uso de contraseñas robustas y autenticación multifactor.
* La conexión exclusiva a redes seguras y autorizadas.
* La instalación y actualización periódica de medidas de seguridad (antivirus, cortafuegos, etc.).
* El reporte inmediato en caso de pérdida, robo o incidente de seguridad.

Esta normativa debe ser comunicada y firmada por todos los empleados que dispongan de un portátil corporativo, mantenerse accesible en todo momento y recordarse periódicamente para reforzar su cumplimiento.

# **2.- Objetivos**

El **Plan de Protección del Puesto de Trabajo para Portátiles** tiene como objetivo principal establecer las medidas necesarias para **proteger la información corporativa** y los recursos tecnológicos de la organización frente a los riesgos derivados del uso, transporte y almacenamiento de los equipos portátiles.

De manera específica, este plan persigue los siguientes objetivos:

1. **Garantizar la confidencialidad, integridad y disponibilidad** de la información almacenada o accesible desde los portátiles corporativos.
2. **Prevenir la pérdida, robo o uso indebido** de los equipos portátiles y de la información que contienen.
3. **Promover el uso seguro de los portátiles** tanto dentro como fuera de las instalaciones de la empresa, especialmente en entornos de movilidad o teletrabajo.
4. **Asegurar la correcta configuración y mantenimiento** de los equipos, incluyendo medidas de cifrado, actualización de software y protección antivirus.
5. **Regular las condiciones de conexión a redes externas**, garantizando que se utilicen únicamente canales seguros y autorizados por la organización.
6. **Concienciar y formar al personal** sobre las buenas prácticas en el uso de los portátiles, fomentando la responsabilidad individual en materia de seguridad.
7. **Definir los procedimientos de actuación ante incidentes**, como el extravío, robo o detección de accesos no autorizados, para minimizar el impacto y facilitar una respuesta rápida.
8. **Alinear la protección de los portátiles con las políticas generales de seguridad de la información** y los requisitos normativos o legales aplicables.

En conjunto, estos objetivos buscan reforzar la **cultura de seguridad corporativa**, garantizando que los portátiles por su carácter móvil y su acceso a información sensible sean utilizados de manera segura, controlada y conforme a los principios de protección de datos y seguridad de la información establecidos por la organización.

# **3.- Puntos clave**

Los puntos clave de esta política son:

* **Normativa de protección del puesto de trabajo.** La empresa debe contar con una normativa específica que recoja todas las medidas necesarias para proteger el puesto de trabajo, revisando periódicamente su cumplimiento y modificándola si hubiera cambios que la afecten por ejemplo si se cambian los equipos o los sistemas o se adoptan nuevos servicios.
  + También se dará a conocer a los empleados otras políticas relativas a los equipos o servicios que utilicen en su desempeño: correo electrónico, almacenamiento, etc.
* **Difusión de políticas complementarias.** El personal deberá conocer y cumplir las demás políticas relacionadas con el uso de equipos portátiles, tales como las de uso de correo electrónico, almacenamiento en la nube, acceso remoto, cifrado y contraseñas.
* **Bloqueo y cifrado de los equipos.** Todos los portátiles corporativos deberán:
  + disponer de **cifrado completo de disco** para proteger la información almacenada;
  + configurarse con **bloqueo automático de sesión** tras un periodo de inactividad;
  + requerir **autenticación mediante contraseña robusta** o autenticación multifactor (MFA).
* **Actualizaciones y protección antimalware.** El personal técnico aplicará las políticas de actualización y protección antimalware, garantizando que:
  + el sistema operativo y las aplicaciones estén actualizadas;
  + los antivirus estén activos y con bases de datos recientes;
  + se realicen revisiones periódicas para confirmar el correcto funcionamiento de las medidas de seguridad.
* **Conexión segura a redes.** Los empleados deben:
  + conectarse únicamente a redes Wi-Fi seguras y autorizadas;
  + utilizar **VPN corporativa** para acceder a recursos internos desde ubicaciones externas;
  + evitar el uso de redes públicas o abiertas sin protección adicional.
* **Protección física y custodia del equipo.** El empleado:
  + es responsable de la custodia de su portátil;
  + debe mantenerlo siempre bajo supervisión o guardarlo en un lugar seguro, especialmente en espacios públicos, transporte o alojamiento temporal;
  + en ningún caso debe dejarse el equipo visible en vehículos o lugares no vigilados.
* **Uso de dispositivos externos.** El uso de memorias USB, discos externos u otros dispositivos de almacenamiento deberá estar **autorizado por el departamento de TI**, y los puertos USB podrán estar deshabilitados por defecto. Cualquier soporte utilizado deberá contar con **cifrado y análisis antivirus previo**.
* **Prohibición de instalación de software no autorizado.** Los empleados no podrán modificar la configuración del equipo ni instalar programas sin la aprobación del área de sistemas. Toda necesidad de software adicional deberá solicitarse formalmente.

**Política de escritorio y entorno limpio.** Incluso en entornos de movilidad o teletrabajo, se deberá mantener el principio de **“mesa limpia”**:

* guardar documentos o dispositivos externos al finalizar la jornada;
* no dejar información sensible a la vista;
* evitar anotar contraseñas o datos críticos en papel.

**Uso responsable de Internet y correo electrónico.** Los usuarios deben respetar la normativa interna sobre uso de Internet y correo electrónico, evitando acceder a sitios web inseguros o abrir mensajes sospechosos.  
 Deberán verificar certificados y conexiones seguras (https://) cuando trabajen con información crítica.

**Cifrado de información confidencial.** Toda información sensible almacenada o transmitida desde el portátil deberá cifrarse conforme a la **Política de uso de tecnologías criptográficas** y la **Política de clasificación de información** de la empresa.

**Notificación de incidentes.** El empleado deberá comunicar de inmediato cualquier incidente relacionado con el portátil, tales como:

* pérdida, robo o extravío del equipo;
* detección de malware o alertas del antivirus;
* accesos no autorizados o sospechosos;
* uso indebido de credenciales o intento de phishing;
* fallos o comportamientos anómalos del sistema.

**Obligación de confidencialidad.** El personal con acceso a portátiles corporativos deberá firmar y cumplir un **compromiso de confidencialidad**, que seguirá vigente incluso tras la finalización de la relación laboral.

**Uso exclusivo para fines laborales.** El portátil corporativo debe utilizarse exclusivamente para tareas relacionadas con la actividad de la empresa, quedando prohibido su uso personal o el préstamo a terceros.

# **4.- Checklist**