**Actividad 1.2 Protección del Puesto de Trabajo**



Trabajo realizado por:

Samuel Romero de los Reyes

# **Índice**

[**Índice 2**](#_rn22sorsfyex)

[**1.- Antecedentes 3**](#_vjxpnqeh5lz4)

[**2.- Objetivos 4**](#_de0hu4aoc5l0)

[**3.- Puntos clave 4**](#_i5p69odwhd5)

[**4.- Checklist 5**](#_ngy0r8xi9zht)

# 

# **1.- Antecedentes**

1.- Pandemia -> teletrabajo

2.- Robo/manipulación dispositivos exterior y obtención de datos

3.- Conexión a redes inseguras

# **2.- Objetivos**

1.- Empleados que trabajen sin incidentes desde su domicilio

2.- Mantener la integridad de los datos cifrados de la empresa

3.- Proteger los dispositivos de accesos externos a través de conexiones inseguras

# **3.- Puntos clave**

Los puntos clave de esta política son: A PRO

* **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.
* **Cifrado de la información sensible contenida en el dispositivo. B TEC**
* **Aplicación de protección de dispositivos. A TEC**
* **Política de control de acceso a los sistemas remotos.**
* **Sistema de copias de seguridad del dispositivo automático.**
* **Ley de cumplimiento de protección de datos. B PER**
* **Configuración de la red doméstica.** De no saber, la empresa te asignará un técnico para su configuración.
* **No trastear con los portátiles.** Abrir los portátiles para arreglar algo.
* **Eliminación de los datos locales. B TEC**
* **Control del uso del portátil de la empresa y llevar un seguimiento de quién lo usó antes.**
* **Bloqueo de sesión automático. B TEC**
* **Actualizaciones y protección antimalware. B TEC** 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. B PER** 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. B PER** 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. B GTEC** 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. B PER** 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. B PER** 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**

A continuación se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a protección del puesto de trabajo.

Los controles se clasificarán en dos niveles de complejidad:

* Básico (B): el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.
* Avanzado (A): el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente alcance:

* Procesos (PRO): aplica a la dirección o al personal de gestión.
* Tecnología (TEC): aplica al personal técnico especializado.
* Personas (PER): aplica a todo el personal.

| **Nivel** | **Alcance** | **Control** | |
| --- | --- | --- | --- |
| A | PRO | **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. | ☐ |
| B | TEC |  | ☐ |
|  |  |  | ☐ |
|  |  |  | ☐ |
|  |  |  | ☐ |
|  |  |  | ☐ |
|  |  |  | ☐ |
|  |  |  | ☐ |
|  |  |  | ☐ |
|  |  |  | ☐ |