APLICACIONES PERMITIDAS

POLÍTICAS DE SEGURIDAD PARA LA PYME

Colección

PROTEGE TU EMPRESA

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. APLICACIONES PERMITIDAS

1.1 ANTECEDENTES

Las normas de protección de la **propiedad intelectual** [1] obligan a las empresas a usar en todo momento software original adquirido de manera legal. El uso de software pirata o adquirido de forma fraudulenta podría conllevar sanciones económicas y penales. Además, la instalación y uso de *software* ilegal en algún dispositivo incrementa los riesgos de infección por *malware* [2].

Por otra parte, para evitar **fugas de información y garantizar la privacidad** de los datos de carácter personal, la empresa debe determinar y controlar qué software está autorizado para el tratamiento de la información dentro de la empresa.

Cualquier incidente de seguridad puede repercutir en la imagen de la compañía.

Para hacer cumplir esta política la empresa debe contar con:

- Un listado de *software* autorizado.
- Un repositorio del *software* autorizado y un registro de licencias.
- Sanciones disciplinarias derivadas del incumplimiento de la política.

También se debe identificar a los responsables para realizar las actualizaciones del *software* y las auditorías.

1.2 OBJETIVOS

Controlar que siempre se usa ***software* autorizado** en la empresa, y que ha sido adquirido de forma legal.

1.3 CHECKLIST

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a **aplicaciones permitidas**.

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.

1.3 CHECKLIST

Nivel	Alcance	Control	
B	PRO	**Registro de licencias.** Mantienes un registro actualizado de las licencias disponibles del software autorizado.	☐
B	PRO/TEC	**Competencia para la instalación, actualización y borrado.** Nombras y autorizas al personal técnico que se encargará de la instalación, actualización y eliminación del *software* de los equipos de la empresa.	☐
B	PRO	**Sanciones por usos no autorizados.** Informas al personal de la empresa de las sanciones derivadas del uso no autorizado de *software*.	☐
B	PRO/TEC	**Repositorio de *software*.** Mantienes un repositorio donde se encuentra todo el *software* autorizado y sus correspondientes credenciales de instalación.	☐
A	PRO/TEC	**Auditoria de *software* instalado.** Analizas cada _____ que el *software* instalado en cada uno de los equipos de los usuarios está autorizado y tiene licencia.	☐
B	PER	**Autorización y licencia del *software*.** Garantizar que en todos los dispositivos que utilizas el *software* instalado es autorizado y que disponen de las correspondientes licencias de uso.	☐
B	PER	**Política de copias de *software*.** No realizas copias del *software* puesto a tu disposición sin el debido consentimiento.	☐

Revisado por: _____ **Fecha:** _____

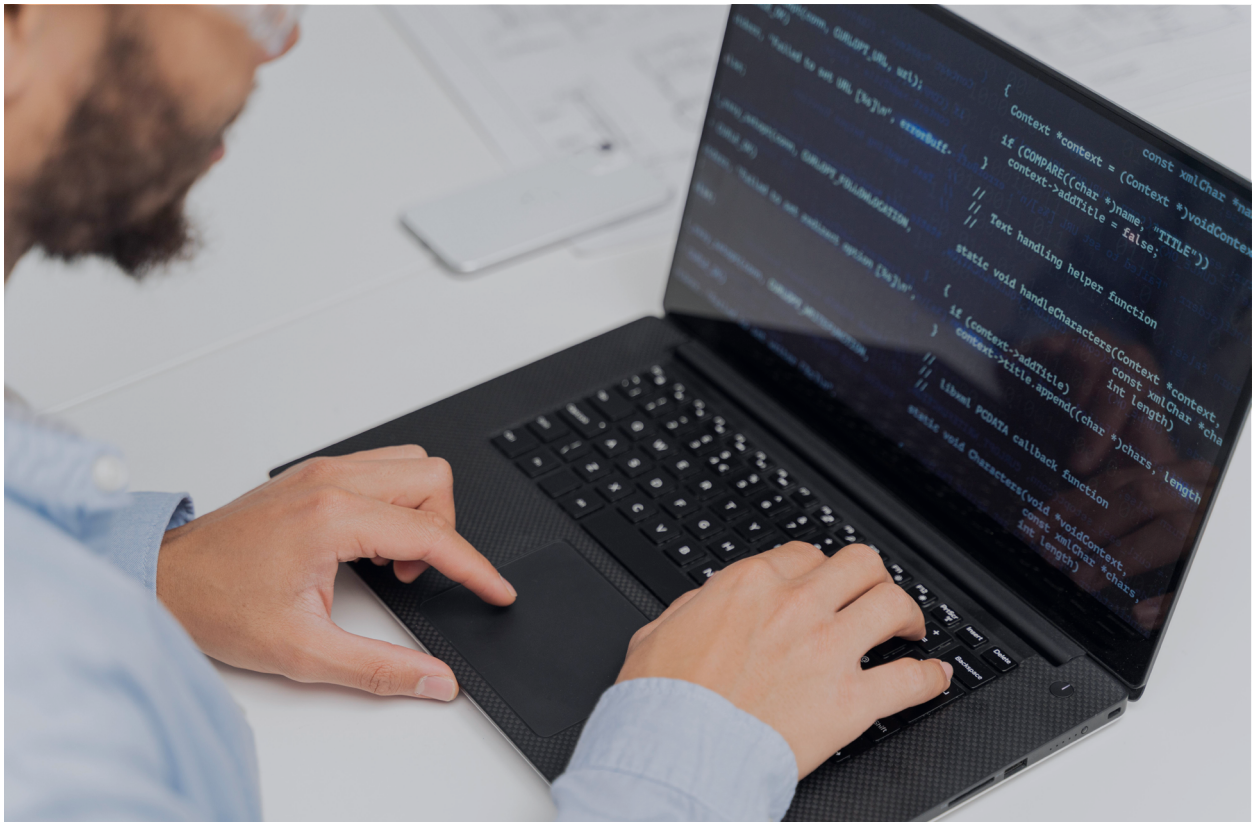
1.4 PUNTOS CLAVE

Los puntos clave de esta política son:

- **Inventario de la información.** Si queremos saber de qué *software* dispone la organización conviene tener un registro actualizado de licencias. En dicho registro se almacenará al menos la siguiente información:
  - Nombre y versión del producto.
  - Autor.
  - Fecha de adquisición.
  - Vigencia de la licencia.
  - Tipo de licencia.
  - Número de usuarios permitidos por licencia.
  - Número de licencias adquiridas por cada *software*.
  - Facturas o comprobantes de compra.
  - Ubicación física del producto.
- **Competencia para la instalación, actualización y borrado.** Para asegurarnos una configuración óptima en nuestros equipos es aconsejable que únicamente el personal técnico indicado pueda instalar, actualizar y eliminar *software*. En los casos en los que no se disponga de dicho personal técnico o este sea externo, se debe documentar y notificar la autorización y la operativa para instalar, actualizar, revisar y eliminar *software* legal de forma autónoma. Para ello, se deberá utilizar una cuenta de administrador diferente a la del usuario habitual. En ningún caso debe permitirse la instalación ni la actualización de *software* a través de enlaces de webs o correos cuyo origen no sea completamente seguro. Por último, remarcar que además de ser legal, el *software* instalado en los equipos debe estar correctamente actualizado **[3]**.
- **Sanciones por uso de software no autorizado.** Es importante documentar y dar a conocer las posibles sanciones disciplinarias por el uso de *software* ilegal o no autorizado, y concienciar a los empleados de la importancia del cumplimiento legal de la empresa **[4]**. Además, se notificará la posibilidad de acarrear con responsabilidades civiles y penales según la legislación vigente en cada momento en materia de protección de la propiedad intelectual. Con esta medida conseguimos concienciar a la plantilla sobre las consecuencias de utilizar *software* ilegal.

1.4 PUNTOS CLAVE

- **Repositorio de *software*.** Para poder instalar el *software* de forma rápida y eficaz se deben determinar las ubicaciones donde localizarlo, así como sus credenciales de activación, números de serie, licencias, etc. Además, puede ser conveniente registrar metódicamente quién accede a dichos repositorios.
- **Auditoría de *software* instalado.** La organización debe reservarse el derecho de auditar o inspeccionar en cualquier momento los equipos de los usuarios para verificar que se cumple esta política.
- **Autorización y licencia del *software*.** Debemos garantizar en todo momento que los programas instalados en cualquier dispositivo corporativo **[5]** (se incluyen los dispositivos BYOD **[6]** están debidamente autorizados y que disponen de las licencias necesarias. Además, es aconsejable que los empleados lean y comprendan los términos y condiciones de uso de dichas licencias, de este modo podremos cumplir con la Ley de Propiedad Intelectual.
- **Política de copias de *software*.** Para garantizar lo especificado en las licencias de uso, no se debe permitir que los empleados realicen copias del *software* disponible sin el debido consentimiento.



2. REFERENCIAS

[1] BOE – Texto refundido de la Ley de Propiedad Intelectual – https://www.boe.es/buscar/act.php?id=BOE-A-1996-8930

[2] INCIBE – Empresas – Blog – TemáTICas: te infectan, mutan y se extienden; hablemos del malware – https://www.incibe.es/empresas/blog/tematicas-te-infectan-mutan-y-se-extienden-hablemos-del-malware

[3] INCIBE – Empresas – Herramientas – Políticas de seguridad para la pyme – Actualizaciones de software – https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/actualizaciones-software.pdf

[4] INCIBE – Empresas – ¿Qué te interesa? –Cumplimiento legal – https://www.incibe.es/empresas/que-te-interesa/cumplimiento-legal

[5] INCIBE – Empresas – Herramientas – Políticas de seguridad para la pyme – Uso dispositivos móviles corporativos – https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-dispositivos-moviles-corporativos.pdf

[6] INCIBE – Empresas – TemáTICas - BYOD – https://www.incibe.es/empresas/tematicas/byod

Financiado por
la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

INSTITUTO NACIONAL DE CIBERSEGURIDAD