Aplicaciones permitidas

Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

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 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;
- las sanciones disciplinarias derivadas del incumplimiento de la política.

Y 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.

NIVEL	ALCANCE	CONTROL	
B	PRO	**Registro de licencias** Mantienes un registro actualizado de las licencias disponibles del software autorizado.	☐
B	PRO	**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** Utilizas en todos los dispositivos que utilizas software autorizado y que dispone 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:

- **Registro de licencias.** 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. 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 [1]. Con esta medida conseguimos concienciar a la plantilla sobre las consecuencias de utilizar software ilegal.
- **Repositorio de software.** Para poder instalar el software rápidamente se debe determinar las localizaciones donde estará ubicado, así como sus claves de activación, números de serie, licencias, etc. Además, puede ser conveniente registrar metódicamente quien accede a dichos repositorios.
- **Auditoria 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 (se incluyen los dispositivos BYOD [4]) están debidamente autorizados y que disponen de las licencias necesarias. Es aconsejable además 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 [1].
- **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, Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia https://www.boe.es/buscar/act.php?id=BOE-A-1996-8930

[2]. Incibe – Protege tu empresa – Blog – Descubre los diferentes tipos de malware que pueden afectar a tu pyme https://www.incibe.es/protege-tu-empresa/blog/descubre-tipos-malware

[3]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Actualizaciones de software https://www.incibe.es/protege-tu-empresa/que-te-interesa

[4]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Uso de dispositivos móviles no corporativos https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[5]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Protección del puesto de trabajo https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[6]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Uso dispositivos móviles corporativos https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[7]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Cumplimiento legal https://www.incibe.es/protege-tu-empresa/herramientas/politicas

INSTITUTO NACIONAL DE CIBERSEGURIDAD