Almacenamiento en los equipos de trabajo

Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. ALMACENAMIENTO EN LOS EQUIPOS DE TRABAJO

1.1. Antecedentes

En el puesto de trabajo los empleados utilizan como herramienta equipos informáticos: ordenadores, tabletas, teléfonos móviles, etc. También generan y transmiten información necesaria para el desempeño de sus funciones. Esta información a veces se almacena de manera local en los discos duros de estos equipos, por lo que surge la necesidad de disponer de una política que regule cómo hacerlo de forma segura. Igualmente deben regularse en forma de políticas el almacenamiento en dispositivos extraíbles [1], en la nube [9] y en la red corporativa [7].

La empresa dispondrá de una Política de clasificación de la información [8]. Junto con esta clasificación se elaborará una normativa para el tratamiento de la información crítica y sensible (según el RGPD [2]), que indicará cuando debe ir cifrada, cuando se ha de controlar el acceso a la misma y otras medidas de seguridad a llevar a cabo como las copias de seguridad o la destrucción de la información.

1.2. Objetivos

Mantener de modo seguro la información almacenada de forma local, especificando reglas, criterios y procedimientos que deben seguir todos los empleados.

1.3. Checklist

A continuación se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a **almacenamiento en los equipos 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	
B	PRO	**Qué se puede almacenar en los equipos corporativos.** Elaboras una normativa que regula el almacenamiento de información personal en los equipos corporativos.	☐
B	PRO	**Dónde guardar la información.** Informas a los empleados sobre dónde guardar la información generada en su trabajo dentro del árbol de directorios del equipo.	☐
B	PRO	**Conservación de la información en discos locales.** El tiempo de conservación de la información de forma local es de _____. Después se transferirá a los servidores o se eliminará.	☐
A	PRO/TEC	**Permanencia de la información en discos locales una vez transferida a los servidores.** El tiempo de permanencia de la información en local una vez transmitida a los servidores corporativos es de _____. Después será eliminada.	☐
A	TEC/PER	**Cifrado de la información.** Cifras la información crítica y sensible antes de guardarla localmente.	☐
B	PER	**Conocimiento y aplicación de la normativa.** Conoces y aplicas la normativa establecida.	☐

Revisado por: _____ **Fecha:** _____

1.4. Puntos clave

Los puntos clave de esta política son:

- **Qué se puede almacenar en los equipos corporativos.** Los empleados deben conocer qué tipo de información se puede almacenar en los equipos locales [3]. Para ello redactaremos una normativa que regule el almacenamiento de información en los equipos locales, indicando la información que no debe almacenarse (documentos personales, archivos de música, fotografías, etc.).
  Se debe prestar especial atención a los archivos descargados que posean derechos de autor [4]. Los empleados no almacenarán información que no haya sido aprobada por la organización.
- **Dónde guardar la información.** La normativa debe detallar dónde guardar la información derivada del trabajo dentro del árbol de directorios del equipo. Esta medida facilita la migración de esta información a servidores.
- **Conservación de la información en discos locales.** Para evitar problemas de espacio en los discos duros estableceremos un periodo de tiempo de conservación de la información. Transcurrido este tiempo, según la información en cuestión, tendremos que decidir si se transfiere a los servidores empresariales o si se elimina definitivamente.
- **Permanencia de la información en discos locales una vez transferida a los servidores** [5]**.** Si la información ya se ha transferido a los servidores corporativos, tendremos que establecer un periodo de permanencia en local para no almacenar por duplicado la información. Después de este periodo de tiempo establecido, la información se borrará del disco duro del equipo.
- **Cifrado de la información.** El empleado debe conocer cuándo y cómo utilizar el cifrado de documentación, según la Política de uso de técnicas criptográficas [6]. Esta medida es útil en caso de fuga de información o acceso no autorizado.
- **Conocimiento y aplicación de la normativa.** Los empleados deben conocer y aplicar la normativa relativa al almacenamiento en local en sus equipos de trabajo y otras políticas relacionadas [1, 7, 8 y 9].

2. REFERENCIAS

[1]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Almacenamiento en dispositivos extraíbles https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[2]. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo · https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=es

[3]. Incibe – Protege tu empresa – ¿Qué te interesa? – Protección de la información https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-informacion

[4]. Incibe – Protege tu empresa – Blog – ¿Quieres tener el control de lo que publicas? Usa la licencia adecuada · https://www.incibe.es/protege-tu-empresa/blog/licencias-publicaciones-empresas

[5]. Incibe – Protege tu empresa – Guías – Almacenamiento seguro de la información: una guía de aproximación para el empresario · https://www.incibe.es/protege-tu-empresa/guias/almacenamiento-seguro-informacion-guia-aproximacion-el-empresario

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

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

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

[9]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Almacenamiento en la nube https://www.incibe.es/protege-tu-empresa/herramientas/politicas

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

INSTITUTO NACIONAL DE CIBERSEGURIDAD