1. Antecedentes

Los dispositivos de almacenamiento extraíble (memorias USB, discos duros portátiles, tarjetas de memoria, CD, etc.) permiten una transferencia rápida y directa de información. Hoy en día son imprescindibles y muy utilizados. Debemos aplicar las medidas de seguridad que este tipo de dispositivos requieren por su susceptibilidad al robo, manipulación, extravío e infección por virus.

La empresa debe decidir si se permite el uso de dispositivos de almacenamiento externo, y de ser así, debe disponer de una normativa que contemple en qué situaciones pueden utilizarse y qué tipo de información se permite guardar en ellos.

Si se necesita almacenar información sensible o confidencial se utilizarán dispositivos externos corporativos debidamente protegidos, se almacenarán en lugares seguros y se informará al responsable si ocurre algún incidente (robo, pérdida, infección del dispositivo, etc.).

En el caso de que se permita el uso de dispositivos personales (dispositivos extraíbles propiedad del empleado) se aplicarán las normas de seguridad recogidas en la política correspondiente.

Para asegurar la información contenida en los dispositivos extraíbles tendremos que aplicar medidas de seguridad como: cifrar los datos almacenados, establecer permisos de acceso, cambiar periódicamente la contraseña, etc.

Otro de los aspectos importantes a tener en cuenta es la eliminación de la información almacenada. Para asegurar que estos datos no volverán a ser accesibles, debemos utilizar los métodos de borrado seguro: destrucción física del dispositivo, desmagnetización o sobre-escritura [2], según convenga en cada caso.
En definitiva, debemos aplicar las medidas de seguridad que este tipo de dispositivos requieren, así como concienciar a los empleados para su buen uso. De esta forma protegeremos tanto la información contenida en ellos como la de los dispositivos a los que se conectan.

2. Objetivos

Establecer unas normas de uso de los dispositivos extraíbles que garanticen la seguridad de la información corporativa que almacenan y la de los equipos a los que se conectan.

3. Checklist

A continuación se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a borrado seguro y gestión de soportes.

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	**Normativa de almacenamiento en dispositivos extraíbles.** Elaboras una normativa específica para el uso de dispositivos extraíbles (dispositivos autorizados, condiciones de uso, cómo se accede a la información, configuraciones de seguridad, etc.)	☐
B	PRO	**Concienciación de los empleados** Involucras a los usuarios en la protección de estos dispositivos y los datos que contienen.	☐
B	PRO/TEC	**Alternativas a los medios de Almacenamiento extraíble.** Implementas alternativas para evitar la necesidad de utilizar dispositivos de almacenamiento externo (repositorios comunes, clouds autorizados, etc.).	☐
B	TEC	**Registro de usuarios y dispositivos.** Mantienes un registro actualizado con usuarios, dispositivos y privilegios de acceso	☐
B	TEC	**Aplicar medidas técnicas para garantizar un almacenamiento seguro de la información en el dispositivo extraíble.** Aplicas medidas para el almacenamiento seguro de la información en el dispositivo extraíble (cifrado de datos, autenticación, cambio periódico de contraseñas, etc.)	☐
B	TEC	**Aplicar medidas técnicas para garantizar un almacenamiento seguro de la información en los dispositivos a los que se conecta.** Aplicas medidas para el almacenamiento seguro de la información en los dispositivos a	☐

		los que se conecta (autenticación, bloqueo de dispositivos no autorizados, deshabilitar puertos USB, deshabilitar Autoarranque desde USB, etc.)	
B	TEC	**Aplicar medidas técnicas para garantizar un almacenamiento seguro de la información sobre los documentos.** Aplicas medidas para el almacenamiento seguro de la información en los documentos que se transfieren (control de accesos, cifrado, etc.)	☐
B	PER	**Cumplimiento de la normativa.** Conoces y aceptas la normativa corporativa vigente para el uso de dispositivos extraíbles en actividades de la empresa.	☐

	ELABORADO POR:	REVISADO POR:	APROBADO POR:
CARGO:	Consultor	Gerencia	Gerencia
NOMBRE:	Ing. Enith E. Gustin	Diego Córdoba	Diego Córdoba
Fecha:	2024-01-27	2024-01-28	2024-02-01

CONTROL DE CAMBIOS		
VERSIÓN No.	**FECHA DE APROBACIÓN**	**DESCRIPCIÓN DEL CAMBIO**
1	2024-02-01	Creación del documento