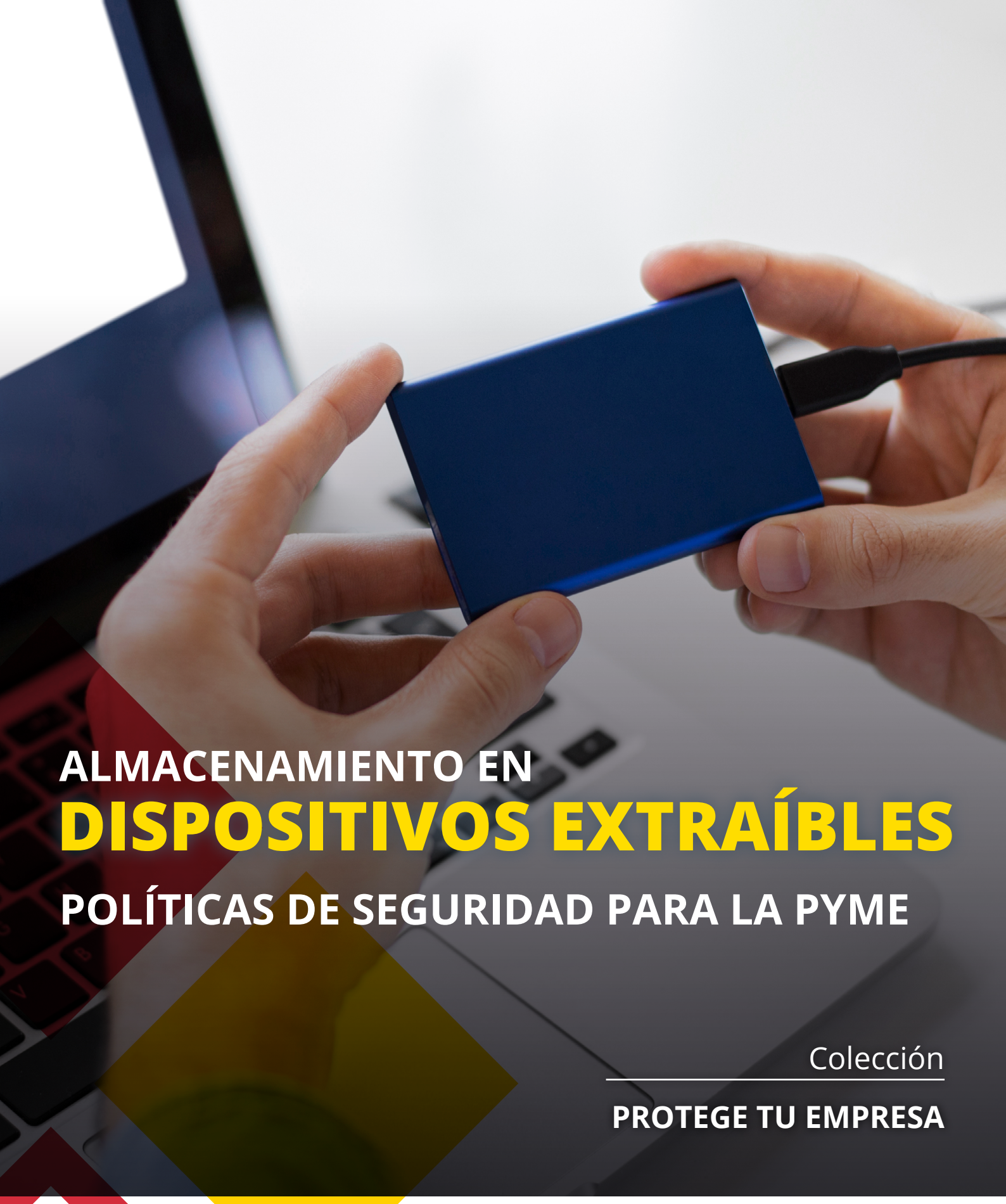


ALMACENAMIENTO EN DISPOSITIVOS EXTRAÍBLES

POLÍTICAS DE SEGURIDAD PARA LA PYME

Colección

PROTEGE TU EMPRESA

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. ALMACENAMIENTO EN DISPOSITIVOS EXTRAÍBLES

1.1 ANTECEDENTES

Los **dispositivos de almacenamiento extraíbles** (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 **BYOD** **[1]**, de sus siglas en inglés ***Bring Your Own Device***, (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. **[2]**

Por otro lado, será muy importante hacer **copias de seguridad de la información almacenada**, así como establecer un sistema de prevención de pérdida datos (DLP). Todo ello con la finalidad de proteger la información contenida en los dispositivos.

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 sobreescritura **[3]**, 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.

1.2 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.

1.3 CHECKLIST

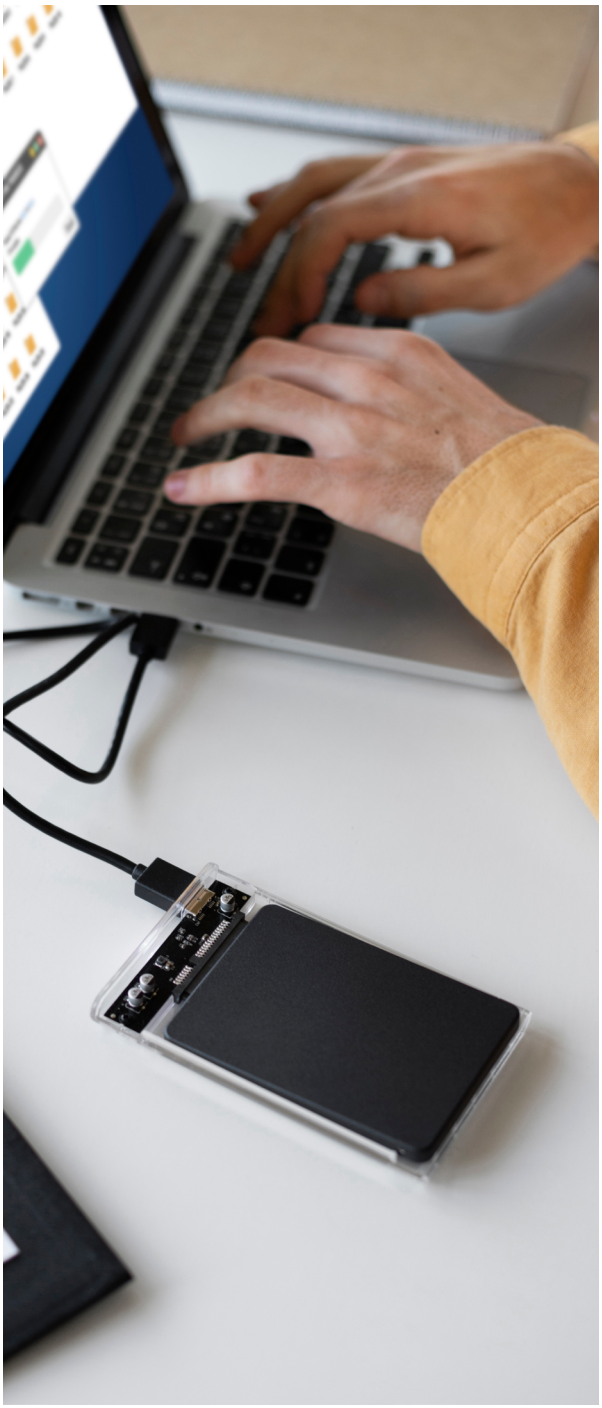
A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a **almacenamiento en dispositivos extraíbles**.

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

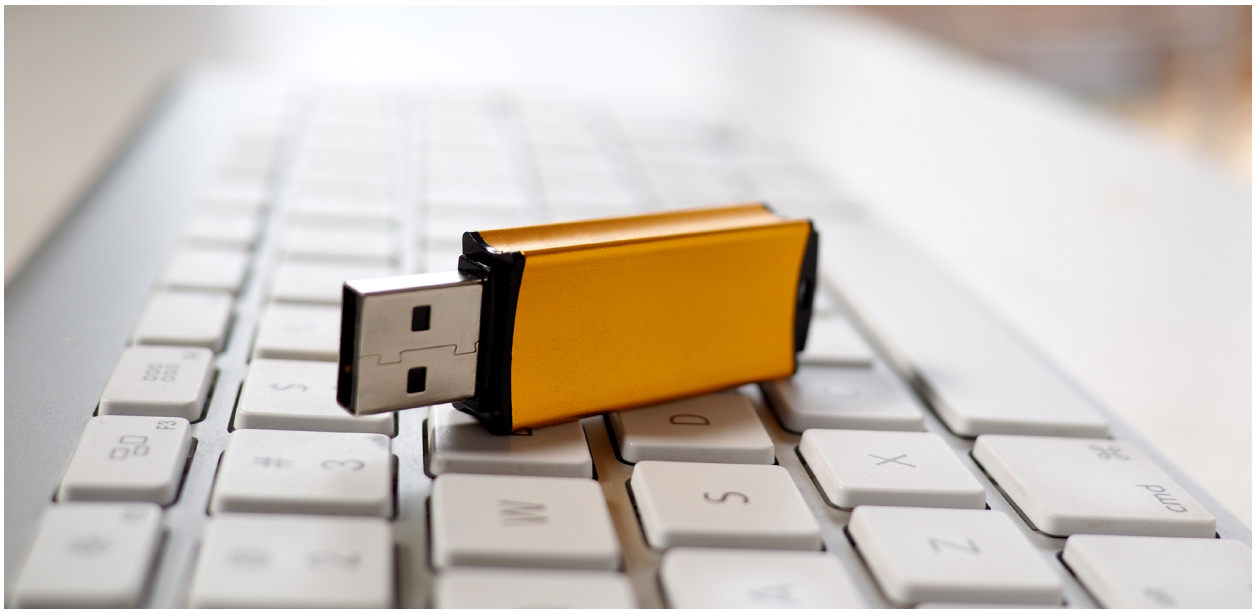
Nivel	Alcance	Control	
B	PRO	**Normativa de almacenamiento en dispositivos extraíbles.** Elaboras una normativa específica para el uso de dispositivos extraíbles (dispositivos autorizados, condiciones de uso, cómo se accede a la información, configuraciones de seguridad, etc.).	☐
B	PRO	**Concienciación 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 Utilizas herramientas *software* de gestión de dispositivos.	☐
B	TEC	**Aplicar medidas técnicas para garantizar un almacenamiento seguro de la información.** Aplicas medidas para el almacenamiento seguro de la información en el dispositivo extraíble (cifrado de datos, autenticación, cambio periódico de contraseñas, etc.). 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, análisis de los dispositivos previo a su ejecución, etc.). 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.	☐
B	TEC	**Auditorías.** Realizas auditorías periódicamente para la evaluación de los controles.	☐

Revisado por: _____ **Fecha:** _____

1.4 PUNTOS CLAVE

Los puntos clave de esta política son:

- **Normativa de almacenamiento en dispositivos extraíbles.** Si no disponemos aún de ella tendremos que elaborar una normativa que regule el uso de dispositivos extraíbles que incluya:
  - Llevar un registro de los dispositivos autorizados.
  - Definir en qué condiciones o casos se permite su uso.
  - Definir cómo se accede y si la información debe ir cifrada.
  - Establecer las configuraciones de seguridad necesarias para poder utilizarlos, etc.
  - Para la elaboración de la normativa de almacenamiento podemos basarnos en normativas de cumplimiento opcional, tales como la ISO/IEC 27001.
- **Concienciación de los empleados.** El robo o extravío, la manipulación, y la infección por virus de los dispositivos extraíbles son las causas más frecuentes por las que puede perderse la información contenida en ellos. Por eso es importante involucrar a los usuarios en la protección, vigilancia y buen uso de estos dispositivos, concienciándolos **[4]** de la trascendencia del cuidado de los mismos y de los datos que contienen.
- **Alternativas a los medios de almacenamiento extraíble.** Para evitar la necesidad del uso de estos soportes pueden implantarse las siguientes alternativas:
  - Utilizar repositorios comunes para el intercambio de información **[5]**.
  - Implantar la posibilidad de acceso remoto para poder trabajar desde fuera de la oficina.
  - Usar los servicios de almacenamiento en la nube autorizados por la organización **[6]**.



1.4 PUNTOS CLAVE

- **Registro de usuarios y dispositivos.** Tenemos que mantener un inventario que incluya un identificador para cada dispositivo y, además, detallando los privilegios de acceso asignados a cada usuario que los necesite.
  - Utilizar herramientas que faciliten la gestión de los dispositivos inventariados de manera centralizada. Estas soluciones permiten la monitorización y administración de los dispositivos.
- **Aplicar medidas técnicas para garantizar un almacenamiento seguro de la información.** Estas medidas podrán aplicarse tanto sobre el dispositivo extraíble como sobre los dispositivos a los que se conecta o sobre los documentos. Por ejemplo:
  - **Sobre el dispositivo extraíble:**
    - Programar cambios periódicos de contraseña de acceso al dispositivo.
  - **Sobre los dispositivos a los que se conectan:**
    - Implementar mecanismos de autenticación de usuarios.
    - Evitar que dispositivos no registrados puedan conectarse a cualquier equipo de la organización.
    - Desactivar la opción de autoarranque en los equipos para no permitir posibles ejecuciones automáticas no deseadas cuando los dispositivos extraíbles son enchufados.
    - Deshabilitar por defecto los puertos USB y habilitarlos para el personal que necesite dicha funcionalidad de manera periódica o gestione ficheros de gran tamaño.
    - Realizar un análisis de los dispositivos USB previo a su ejecución.
  - **Sobre los documentos que se transfieren:**
    - Establecer control de accesos con permisos de lectura, escritura y ejecución.
    - Implementar mecanismos de cifrado de la documentación **[7]**.
- **Cumplimiento de la normativa.** Tendremos que comunicar esta normativa y asegurarnos de que los empleados la conocen y se comprometen a cumplirla antes de utilizar dispositivos extraíbles en el entorno de trabajo. De esta forma, aseguraremos que todos los empleados conocen, entienden y acatan las normas y medidas de protección.
- **Auditorías.** Realizas auditorías con regularidad para evaluar la efectividad de los controles técnicos. Este proceso se debe realizar de manera periódica para garantizar que se cumplen las medidas tomadas de manera satisfactoria, o en su defecto, tomar las medidas oportunas para corregir o mitigar los riesgos.

2. REFERENCIAS

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

[2] INCIBE – Empresas – Blog – ¡La seguridad en movimiento! Protege tus dispositivos extraíbles - https://www.incibe.es/protege-tu-empresa/blog/seguridad-movimiento-protege-dispositivos-extraibles-empresas

[3] INCIBE – Empresas – Guía – Borrado seguro y gestión de soportes - https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/2024/Borrado_seguro_Pol%C3%ADtica%20de%20seguridad_2024.pdf

[4] INCIBE – Empresas – Formación - https://www.incibe.es/empresas/formacion

[5] INCIBE – Empresas – Herramientas – Políticas de seguridad para la pyme – Almacenamiento en la red corporativa - https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/almacenamiento-red-corporativa.pdf

[6] INCIBE – Empresas – Herramientas – Políticas de seguridad para la pyme – Almacenamiento en la nube - https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/almacenamiento-nube.pdf

[7] INCIBE – Empresas – Herramientas – Políticas de seguridad para la pyme – Uso de técnicas criptográficas - https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-_tecnicas-criptograficas.pdf


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


incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD


protege
tuempresa