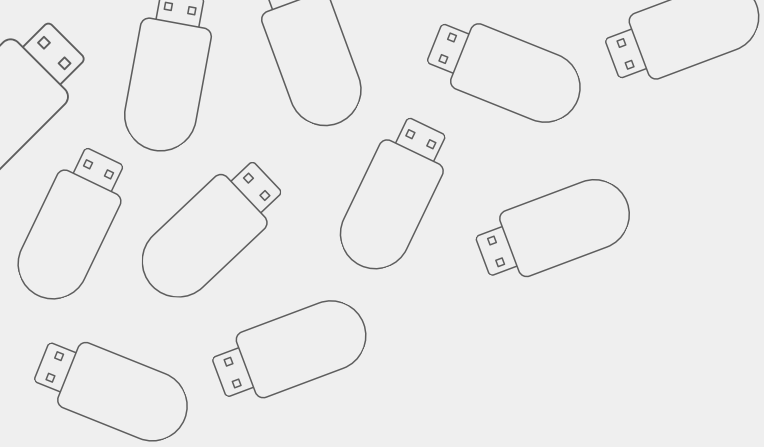
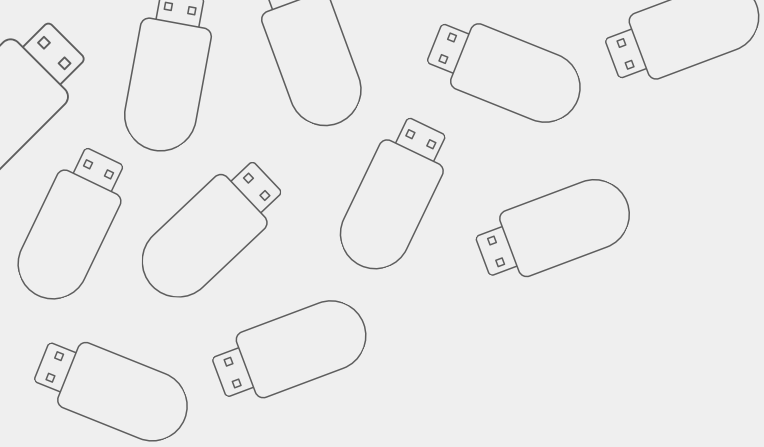
MANUAL DE BUENAS PRÁCTICAS SOBRE EL USO DE DISPOSITIVOS USB EN LA EMPRESA

ÍNDICE:



ÍNDICE:



ÍNDICE:

INTRODUCCIÓN

Objetivo del manual

La **ciberseguridad** es uno de los grandes retos para cualquier empresa. Los ataques informáticos evolucionan constantemente y los **dispositivos USB**, por su comodidad y portabilidad, se han convertido en una **puerta de entrada habitual para amenazas** como el *malware* o el robo de datos.

Como cada vez más empresas están revisando sus prácticas y reforzando sus medidas de seguridad, en este manual buscamos **ayudar a que el uso de USB en la empresa sea seguro y responsable**, evitando sustos innecesarios y protegiendo la información que mueve el día a día del negocio.

Por lo tanto, este manual tiene como propósito principal establecer una serie de **normas sobre el uso responsable de dispositivos USB dentro de la empresa**, para:

- **Garantizar la protección de la información corporativa.**
- **Evitar la introducción de malware mediante medios removibles.**
- **Prevenir la pérdida o fuga de datos sensibles.**
- **Establecer responsabilidades y procesos de control sobre estos dispositivos.**

Nuestro equipo de soporte ha elaborado una serie de directrices. Desde Cosmomedia esperamos que estas recomendaciones sean de interés para las empresas y ayuden a **reforzar su ciberseguridad**, protegiendo sus datos de posibles amenazas.

Ámbito de aplicación: Personal y dispositivos

PERSONAL. ¿PARA QUIÉN?

Este manual está enfocado a cualquiera que mantengan una relación laboral con la empresa, incluyendo:

- **Personal empleado** (permanente, temporal o en prácticas).
- **Personal externo** con acceso a equipos o redes corporativas.
- **Consultores, técnicos y proveedores** que interactúen con sistemas de información de la empresa.

De esta manera, se asegura que todos los usuarios comprendan y apliquen las mismas normas para proteger la información.

QUÉ DISPOSITIVOS

En cuanto a los dispositivos USB, el manual se centra en aquellos que pueden almacenar o transferir datos, como:

- **Memorias USB** o “pendrives”.
- **Discos duros externos** con interfaz USB.
- **Llavero USB** cifrado o con funciones de autenticación.
- **Adaptadores** Wi-Fi, Bluetooth o de red por USB.
- Cualquier otro tipo de **periférico USB que pueda interactuar con el sistema operativo o los datos.**

En este listado **quedan excluidos** los periféricos de entrada y salida comunes, como teclados o ratones, siempre que no tengan capacidad de almacenamiento.

Esta delimitación permite **enfocar las medidas de seguridad en los dispositivos que realmente representan un riesgo** para la empresa, facilitando un control más efectivo y adaptado a las necesidades reales del entorno laboral.

Este manual va dirigido a todo el personal laboral y no laboral que interactúe con la empresa. Se centra en USB con almacenamiento o transferencia de datos.

Riesgos asociados al uso del USB en las empresas

El uso de **dispositivos USB** mal gestionados representa múltiples riesgos para la seguridad de los datos de las empresas. **El puerto USB puede suponer un canal de entrada de múltiples amenazas**. A continuación, indicamos las más relevantes:

Malware y software malicioso

Los **dispositivos USB** pueden ser portadores de virus, que pueden afectar a tu equipo. Estos pueden ejecutarse automáticamente o al abrir archivos, comprometiendo así la seguridad de la red y de los sistemas.

Pérdida de datos

Debido a su pequeño tamaño y portabilidad, los dispositivos USB son propensos a perderse o ser robados. La pérdida de información sensible puede tener consecuencias legales, reputacionales y económicas.

Accesos no autorizados

Si un dispositivo no está cifrado o **protegido por contraseña**, cualquier persona que lo encuentre puede acceder a su contenido, exponiendo datos internos y confidenciales.

Filtración o robo de información

Un usuario malintencionado puede usar un USB para copiar datos de manera rápida y discreta, sin que el sistema lo registre o detecte fácilmente.

Daños a infraestructura

Algunos dispositivos USB pueden alterar las configuraciones del sistema, instalar controladores no autorizados o explotar vulnerabilidades del sistema operativo.

Entre los principales daños que puede causar un uso inadecuado del USB están el malware, la pérdida de datos, el acceso no autorizado a datos o daños en la infraestructura tecnológica.

Recomendaciones en el uso de dispositivos USB

Con el fin de reducir riesgos y asegurar una trazabilidad adecuada, **solo recomendamos utilizar dispositivos USB que hayan sido autorizados y registrados** por el departamento de IT. A continuación, se describen las condiciones que deben cumplir estos dispositivos:

Usar dispositivos USB con propiedad controlada

Los USB deben ser propiedad de la empresa o aprobados expresamente para uso laboral.

No se recomienda el uso de dispositivos personales, salvo en casos excepcionales justificados y autorizados. En ese caso, la empresa debería establecer un protocolo de autorización y revisión de esos dispositivos.

Registro de dispositivos USB en el inventario

Cada dispositivo aprobado debe estar inventariado con datos como: número de serie, marca, modelo, capacidad, responsable y fecha de entrega o registro.

Establecer un protocolo de cifrado de datos

Todos los dispositivos deben estar cifrados, especialmente si contienen información sensible o confidencial.

Se aceptan sistemas de cifrado como BitLocker, VeraCrypt u otros homologados por el área de seguridad.

Revisión antivirus previa

Antes de su primer uso y de forma periódica, los dispositivos USB deben ser escaneados con un antivirus actualizado.

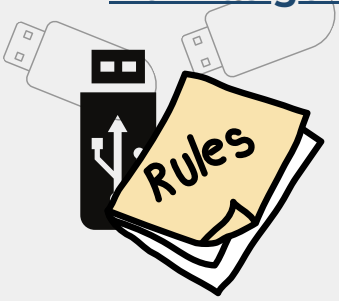
Cualquier hallazgo de malware será motivo para el bloqueo y aislamiento del dispositivo.

Cada USB tendrá un uso asignado

Cada dispositivo tendrá un responsable asignado. En caso de que el dispositivo sea compartido, deberá registrarse su préstamo en el sistema de IT de la empresa.

El control de los dispositivos comienza desde su entrada en la empresa hasta su retirada o destrucción. La empresa debe tener registrado el uso de éstos, durante toda su vida útil, hasta su reemplazo y destrucción.

Normas generales en el uso de USB



El uso adecuado de los dispositivos USB es **responsabilidad** del usuario autorizado, pero también de la empresa, que es la que marca las pautas a seguir y la que vigila y controla que se cumplan.

A continuación, indicamos **algunas normas generales que pueden establecer las empresas**, para asegurar una utilización coherente de los USB.

1 - Conectar solo si es necesario

- No se debe conectar un dispositivo USB si no hay una necesidad clara y justificada.
- La conexión debe hacerse únicamente en los equipos corporativos y bajo contexto laboral.

2 - Evitar el uso de dispositivos personales

- Evitar o **prohibir expresamente el uso de dispositivos USB personales** en equipos de la empresa.
- En casos excepcionales, debe solicitarse **autorización por escrito** al departamento de IT.

3 - Evitar el uso compartido

- Los dispositivos USB asignados son de **uso individual**.
- Si se necesita compartir información, se debe utilizar **preferentemente un canal corporativo aprobado** (por ejemplo, almacenamiento en red o nube empresarial).

4 - No ejecutar software desde un USB

- Está **prohibido ejecutar aplicaciones desde el USB**, así como instaladores o archivos ejecutables directamente. En caso necesario, será el departamento de IT el encargado de gestionar esa instalación, de manera controlada y supervisada.

5 - Protección física de los USB corporativos

- El dispositivo USB debe **guardarse en un lugar seguro** cuando no se use.
- Se recomienda utilizar fundas, carcasas y evitar su exposición a ambientes con humedad, polvo o temperaturas extremas.

6 - Identificación visible de cada USB

- Los dispositivos USB deben estar **etiquetados** con nombre, departamento y número de inventario.

7 - Evitar dejar el USB conectado sin supervisión:

- No se debe dejar un dispositivo USB conectado a un equipo sin vigilancia, **especialmente en zonas comunes** o sin acceso restringido.

8 - Información sensible:

- **Nunca debe almacenarse información confidencial sin cifrado.**
- Se debe seguir la **política de clasificación de la información** para determinar el tipo de datos que pueden ser transportados.

Otros aspectos a considerar:

Establecer responsabilidades y advertencias

Para conseguir un correcto seguimiento de todas estas prácticas, es recomendable **establecer la responsabilidad por incumplimiento** deliberado de todas estas medidas de seguridad.

Procedimiento de autorización para el uso de USB

Para **garantizar un uso controlado y seguro** de los dispositivos USB dentro de la empresa, se recomienda seguir un procedimiento formal de autorización. Este procedimiento asegurará que **los dispositivos utilizados cumplen con los estándares de seguridad requeridos** y que su uso está justificado y documentado.

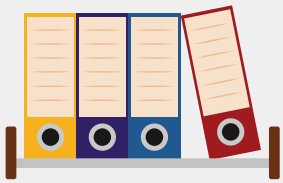
EJEMPLO DE PROCEDIMIENTO DE AUTORIZACIÓN

1. **Solicitud formal:**
   - El empleado interesado deberá realizar una solicitud a través del sistema oficial de tickets, email o formulario.
   - La solicitud debe incluir:
     - Justificación del uso.
     - Tipo de dispositivo.
     - Finalidad (ej. transporte de archivos, uso técnico).
     - Identificación del usuario responsable.
2. **Evaluación técnica inicial:**
   - El equipo de IT evaluará si existe una necesidad real de uso del dispositivo.
   - Se verificará que no existan alternativas más seguras (como almacenamiento en red, soluciones en la nube o canales cifrados internos).
3. **Análisis del dispositivo:**
   - El dispositivo USB será analizado antes de su aprobación:
     - Escaneo con herramientas antivirus y antimalware.
     - Verificación de integridad y funcionalidad.
     - Comprobación de características de cifrado (si procede).
4. **Registro en el inventario:**
   - Una vez aprobado, se registrará en el inventario de activos TI con:
     - Número de serie, marca, modelo.
     - Fecha de registro.
     - Usuario responsable.
     - Departamento al que pertenece.
5. **Notificación de aprobación:**
   - El solicitante recibirá una notificación formal de autorización.
   - Se le entregará una copia de las normas de uso y el compromiso de cumplimiento.

Renovación o baja de dispositivos de USB

- **Renovación**: Si se requiere seguir usando el mismo dispositivo tras un período prolongado (más de un año), debe renovarse la autorización y realizar un nuevo escaneo.
- **Retiro o baj**a: Cuando un dispositivo deje de usarse, deberá ser entregado a IT para su baja formal, destrucción segura o reciclaje.

Documentación que toda empresa debería disponer para controlar el uso adecuado de dispositivos USB



- Formulario de solicitud de dispositivo USB.
- Registro de dispositivos autorizados.
- Acta de entrega y compromiso de buen uso.

Prácticas seguras en el uso de dispositivos USB

Para reducir al máximo los riesgos que implica el uso de dispositivos USB, es importante que el personal adopte una serie de **prácticas seguras** y las convierta en parte de su rutina diaria.

Estas recomendaciones no solo ayudan a **proteger la información de la empresa**, sino que también **evitan problemas técnicos y posibles brechas de seguridad** que pueden afectar a todos.

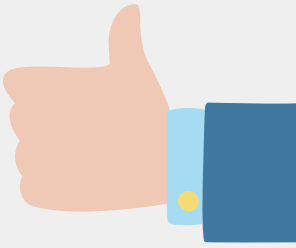
Mantener una **actitud preventiva** y responsable frente al uso de estos dispositivos es fundamental para garantizar un entorno de trabajo más seguro y confiable.

A continuación, exponemos algunas de esas **prácticas seguras en el uso de dispositivos USB**:

Uso de cifrado

Todo dispositivo que almacene información sensible debe utilizar cifrado robusto.
Herramientas recomendadas:

- BitLocker (Windows Pro o Enterprise): Ideal para entornos corporativos.
- VeraCrypt: Software libre multiplataforma.



- El cifrado evita que la información sea legible si el dispositivo se extravía o cae en manos no autorizadas.

Copias de seguridad

- No se debe almacenar la única copia de un archivo importante en un USB.
- Toda la información de valor debe tener una copia de respaldo en:
  - Un servidor interno.
  - Un almacenamiento en la nube corporativa.
  - Un sistema de backup autorizado por la empresa.

Etiquetado e identificación

- Cada dispositivo debe estar claramente etiquetado con:
  - Nombre del responsable.
  - Departamento.
  - Código de inventario.
- Esto facilita su identificación en caso de pérdida o en auditorías.

Revisión periódica con antivirus

- Antes de abrir el contenido de un USB, debe ser analizado con antivirus corporativo.
- La revisión debe realizarse:
  - Tras su autorización inicial.
  - Cada vez que se use en un equipo ajeno al entorno corporativo.
  - Periódicamente, al menos una vez al mes.

Expulsión segura de dispositivos USB

- Siempre se debe expulsar el dispositivo de forma segura antes de retirarlo físicamente del puerto USB.
- Esto evita:
  - Corrupción de datos.
  - Posibles daños al dispositivo o al sistema operativo.

Buenas prácticas adicionales para tener en cuenta:

- No utilizar dispositivos USB en ordenadores públicos o no corporativos.
- No usar dispositivos antiguos o dañados.
- Evitar la conexión en puertos expuestos en lugares públicos.
  - Evitar copiar archivos no relacionados con la actividad profesional

Formación y concienciación sobre ciberseguridad y uso de USB

La concienciación sobre los **riesgos y buenas prácticas en el uso de dispositivos USB** es una herramienta fundamental para **prevenir incidentes de seguridad.**

La tecnología más segura puede verse comprometida si los usuarios no están informados y formados en esta materia.

Con **manuales de uso** como éste, las empresas pueden tener una guía clara sobre cómo usar los USB y establecer protocolos de uso, registro o eliminación.

Cómo desarrollar la formación en el uso de USB

- Establecer una **formación periódica** sobre:
  - Riesgos asociados a dispositivos extraíbles.
  - Uso responsable y seguro.
  - Protocolos de autorización, uso y respuesta ante incidentes.

Contenidos clave de la formación

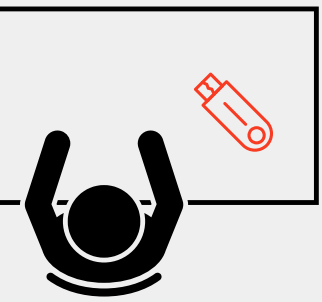
Los temas que deberían cubrirse en las sesiones incluyen:

- Tipos de dispositivos USB y sus usos comunes.
- Amenazas de malware y ataques por USB (BadUSB, keyloggers, etc.).
- Consecuencias legales y empresariales de una pérdida de datos.
- Procedimiento de solicitud y retirada de dispositivos.
- Cifrado y herramientas recomendadas.
- Políticas internas y sanciones en caso de incumplimiento.

Campañas de concienciación

La empresa también puede desarrollar campañas de concienciación en el uso de dispositivos de almacenamiento USB, con **carteles, correos electrónicos, infografías o boletines internos.**
Estas campañas ayudan a mantener la atención activa sobre el uso adecuado de los dispositivos removibles.
Este manual forma parte una campaña de concienciación que, desde Cosmomedia desarrollamos para fomentar el uso adecuado de los USB dentro de las empresas.

Simulacros y pruebas



- Sería conveniente que, de cara a verificar que los protocolos y pautas se siguen, la empresa pueda realizar simulacros de incidentes o pruebas de concienciación, por ejemplo:
  - Dejar intencionadamente un USB “olvidado” para medir si alguien lo conecta o si informa de ello.
  - Pruebas con archivos señuelo para detectar accesos indebidos.

- Es importante señalar que **el objetivo de estas acciones es el de medir el nivel de concienciación y ajustar las formaciones si es necesario**, en ningún caso sancionador, sino instructivo y práctico, para mejorar los protocolos de trabajo.

Prohibiciones y respuesta ante incidentes con dispositivos USB

Para garantizar la integridad de la red corporativa y la protección de los datos, existen ciertas acciones que están expresamente prohibidas en relación con el uso de dispositivos USB.

Además, se establece un protocolo claro de actuación en caso de incidentes relacionados con estos dispositivos.

Acciones NO recomendadas:

- **Conectar dispositivos no autorizados:**
  - En ninguna circunstancia debe conectarse a un equipo corporativo un USB personal o no registrado.
- **Ejecutar software portable desde el USB:**
  - No se debe ejecutar ninguna aplicación, instalador, script o archivo ejecutable desde un USB sin validación técnica.
- **Instalar sistemas operativos desde USB:**
  - Solo el departamento técnico está autorizado a realizar tareas de arranque desde USB por motivos de instalación o recuperación.

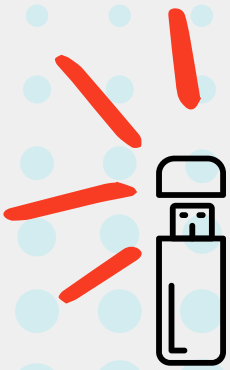
Acciones NO recomendadas:

- **Copiar información confidencial sin cifrado**
  - Todo archivo sensible debe ser cifrado si se transporta en un dispositivo USB.
- **Utilizar dispositivos de origen desconocido o regalados**
  - Está prohibido conectar a equipos de la empresa dispositivos encontrados, de promoción o sin procedencia comprobable.
- **Manipulación de registros o etiquetas:**
  - No se debe alterar, borrar o falsificar etiquetas de identificación ni modificar el estado del registro en el inventario.

Trasladar estas prácticas NO recomendadas a los empleados puede evitar consecuencias irreparables en las empresas, como la pérdida de datos, su uso fraudulento o brechas de seguridad que ponen en riesgo extremo la seguridad del negocio.

Respuesta ante incidentes con dispositivos USB

Si se sospecha que un dispositivo USB ha causado o podría causar un incidente de seguridad, se debe actuar de inmediato siguiendo estos pasos:



- **Notificación inmediata**
  - El usuario debe comunicar la situación al equipo de IT o Seguridad de la Información tan pronto como detecte un comportamiento anómalo (por ejemplo, aparición de archivos desconocidos, lentitud inusual, alertas del antivirus, etc.).
- **No manipular el dispositivo**
  - No debe abrirse, desconectarse ni examinarse el contenido del dispositivo sin indicaciones del personal técnico. Manipularlo puede alterar o destruir evidencias útiles para el análisis.

- **Aislamiento del equipo afectado**
  - Si se sospecha infección, el equipo afectado debe desconectarse de la red para evitar propagación.

- **Entrega y análisis del dispositivo**
  - El dispositivo será recogido por el personal de IT para su análisis forense si fuera necesario.
  - Se registrará el incidente en la base de datos interna.

- **Medidas correctivas**
  - Según el análisis del incidente, se podrán aplicar medidas como
    - Bloqueo de dispositivos USB temporalmente.
    - Reentrenamiento del usuario.
    - Revisión de otras estaciones de trabajo.
    - Actualización de políticas o controles técnicos
  - Base de datos o archivo actualizado con todos los dispositivos registrados y su situación actual.

Te ayudamos a gestionar la ciberseguridad de tu empresa

hola@cosmomedia.es

cosmomedia.
marketing digital para tu negocio