DigitAll

Formación en
Competencias
Digitales

4
Seguridad

DigitAll

Formación en
Competencias
Digitales

Seguridad

Nivel B2

ÍNDICE

DigitAll

Seguridad

4.1 PROTECCIÓN DE DISPOSITIVOS

Seguridad

Nivel B2 4.1 Protección de dispositivos

Cómo implantar un SGSI: metodologías

Cómo implantar un SGSI: metodologías

Gestión de la seguridad de la información

La gestión de la seguridad de la información se refiere a la protección de los activos de información de una organización para garantizar su confidencialidad, integridad y disponibilidad. Normalmente consiste en un conjunto de procesos, políticas, procedimientos y medidas técnicas diseñadas para identificar, evaluar y mitigar los riesgos de seguridad de la información.

GESTIÓN DE RIESGOS: ACTIVO, PROBABILIDAD E IMPACTO

La gestión de riesgos es el proceso de identificar, analizar y evaluar los riesgos potenciales que pueden afectar a una organización e implementar las medidas preventivas y de mitigación oportunas.

e.digitall.org.es/A4C41B1V02

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI): APLICANDO CONTROLES A LOS RIESGOS

Aplicar controles a los riesgos supone el siguiente paso a la gestión de riesgos en el desarrollo de un sistema de gestión de seguridad de la información.

e.digitall.org.es/A4C41B2V02

El objetivo principal de la gestión de la seguridad de la información es asegurar que la información se mantenga segura y protegida contra amenazas internas y externas. Para facilitar su proceso de implementación en una organización es recomendable hacer uso de alguna de las metodologías existentes.

NOTA

Metodología de gestión de la seguridad de la información: es un enfoque estructurado y sistemático utilizado para planificar, implementar, controlar y mejorar la seguridad de la información en una organización.

Saber más

La gestión de la seguridad de la información es esencial en el entorno actual, donde la información juega un papel crítico en las operaciones empresariales y en la confianza del cliente.

Metodologías de gestión de la seguridad de la información

Existen varias metodologías de gestión de la seguridad de la información, cada una con enfoques y características específicas. La elección de una u otra depende de las necesidades y requisitos específicos de cada organización, así como de los estándares y regulaciones que deban cumplirse en su industria.

Una de las características más valoradas a lo hora de elegir una metodología es la posibilidad de obtener una certificación ya que habitualmente representa un valor añadido para las organizaciones.

ISO 27001

La norma **ISO/IEC 27001** (*e.digitall.org.es/iso-27001*) es una norma internacionalmente reconocida que establece los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) en una organización. Fue desarrollada por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC).

Establece un enfoque basado en el riesgo para la gestión de la seguridad de la información, lo que implica identificar los riesgos, evaluar su impacto y probabilidad, y tomar medidas para mitigarlos.

Esta norma se basa en el ciclo de mejora continuo conocido como Ciclo de Deming o ciclo PDCA (Plan-Do-Check-Act) que sigue un enfoque iterativo y cíclico.

Las principales fortalezas de la ISO 27001 que la convierten en una de las metodologías de gestión de seguridad de la información más utilizada son:

- **Reconocimiento y confianza basada en su certificación:** obtener la certificación demuestra el compromiso de una organización con la seguridad de la información y brinda confianza a los clientes, socios comerciales y partes interesadas.

- **Enfoque integral:** aborda de manera integral la gestión de la seguridad de la información en una organización, no se limita únicamente a aspectos técnicos, sino que también considera aspectos organizativos, legales y humanos

- **Flexibilidad y adaptabilidad:** se puede adaptar a las necesidades y requisitos específicos de cada organización permitiendo establecer controles y medidas de seguridad personalizados, de acuerdo con los riesgos y el contexto particular de la organización.

Un ejemplo de la importancia que tiene la ISO 27001 en nuestro país es el hecho de que las administraciones públicas españolas se basaran en esta metodología, adaptándola y complementándola con requisitos y directrices adicionales específicas para las administraciones públicas en España y dando lugar así a la creación del Esquema Nacional de Seguridad.

Saber más

El Esquema nacional de Seguridad (ENS) es un marco de referencia que establece los principios y requisitos mínimos de seguridad de la información para las administraciones públicas en España.

Otras metodologías

Aunque la ISO 27001 podemos decir que es la metodología más usada a nivel global es importante comentar otras existentes.

NIST SP 800-53

El NIST SP 800-53 es un conjunto de estándares y guías desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos. Se utiliza como referencia para la gestión de la seguridad de la información en sistemas federales de información de agencias gubernamentales en los Estados Unidos.

El NIST SP 800-53 proporciona un amplio conjunto de controles y salvaguardas de seguridad y su enfoque se basa en la gestión de riesgos y en la adaptación de los controles a las necesidades y características de cada organización.
Es importante destacar que este conjunto de estándares debe entenderse como un conjunto de buenas prácticas y por tanto no se corresponde con un marco de certificación.

COBIT

COBIT (Control Objectives for Information and Related Technologies) es un marco de referencia desarrollado por ISACA (Information Systems Audit and Control Association) que proporciona un conjunto de mejores prácticas para la gobernanza y gestión de tecnologías de la información (TI) en las organizaciones, y dentro de este marco, la seguridad de la información es uno de los aspectos fundamentales.

Uno de los principales objetivos de COBIT es garantizar el cumplimiento de los requisitos legales y regulatorios.

Proporciona un marco estructurado, objetivos de control y prácticas recomendadas para ayudar a las organizaciones a establecer y mantener un nivel adecuado de seguridad de la información en el para mantener sus operaciones y alcanzar sus objetivos estratégicos.

Al igual que la NIST SP 800-53 este marco de referencia tampoco es certificable.

Seguridad

Nivel B2 4.1 Protección de dispositivos

Utilidades para cifrar la información

Utilidades para cifrar la información

En esta formación, ya se han tratado los temas como el cifrado de la información y, más en detalle, el cifrado de archivos y dispositivos. Cifrar la información garantiza la protección de la confidencialidad, por lo que es esencial tener a mano utilidades que nos permitan cifrar y descifrar nuestros archivos y trabajar de la forma más cómoda y segura posible. A continuación, veremos diferentes utilidades para el cifrado de discos duros y para el cifrado de archivos.

CIFRADO DE ARCHIVOS Y DISPOSITIVOS

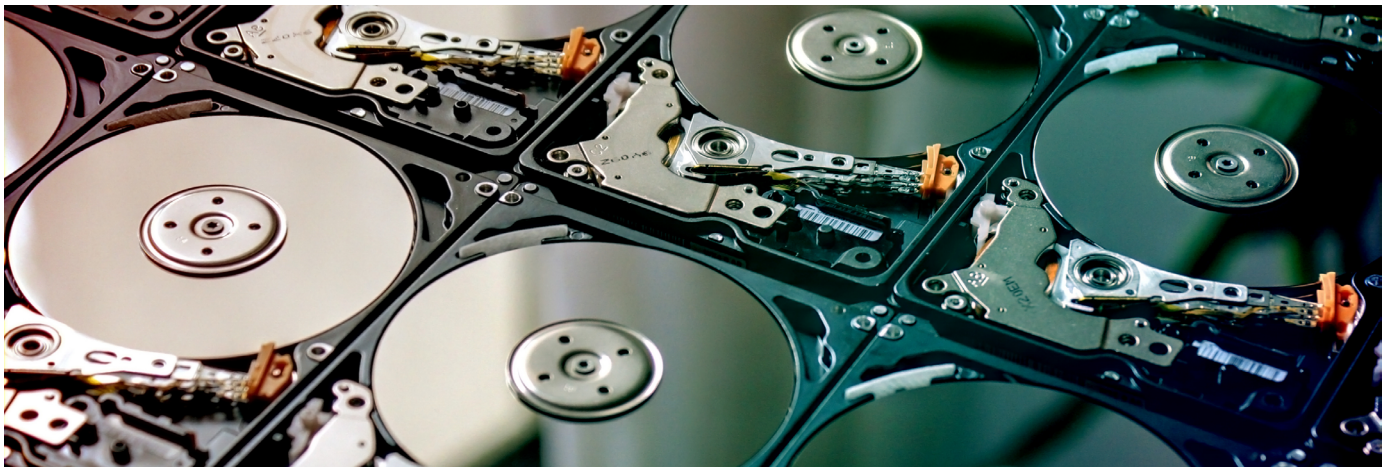
El cifrado de archivos y dispositivos garantiza la confidencialidad de la información en reposo. Cifrar el disco duro del dispositivo protege toda la información almacenada, mientras que el cifrado de archivos, protege a los ficheros de forma independiente.

e.digitall.org.es/A4C41B1V05

Cifrado de discos duros

La primera opción para cifrar la información en reposo es cifrar el dispositivo. En concreto, es posible cifrar el disco duro, que almacena toda la información, tanto del sistema operativo como la información personal que gestione el usuario.

Es importante recordar que, para el cifrado de dispositivos basado en contraseña, si se pierde la contraseña, se pierde acceso a todos los datos cifrados.



En Windows: BitLocker

La opción para sistemas operativos Windows más utilizada es BitLocker, incluida en el propio sistema operativo. De esta forma, al iniciar Windows, Bitlocker descifrará el disco duro para poder arrancar y permitir el acceso a la información.

Además, permite la integración con el chip Trusted-Platform-Module (TPM), que muchos PCs modernos incluyen. De esta forma, si se clona la información o se intenta acceder al disco duro, la información estará cifrada.
La configuración de esta solución es muy sencilla. Si no se dispone de un chip TPM, se puede establecer una contraseña de acceso, que deberá ser introducida en el arranque del dispositivo, antes de iniciar Windows.

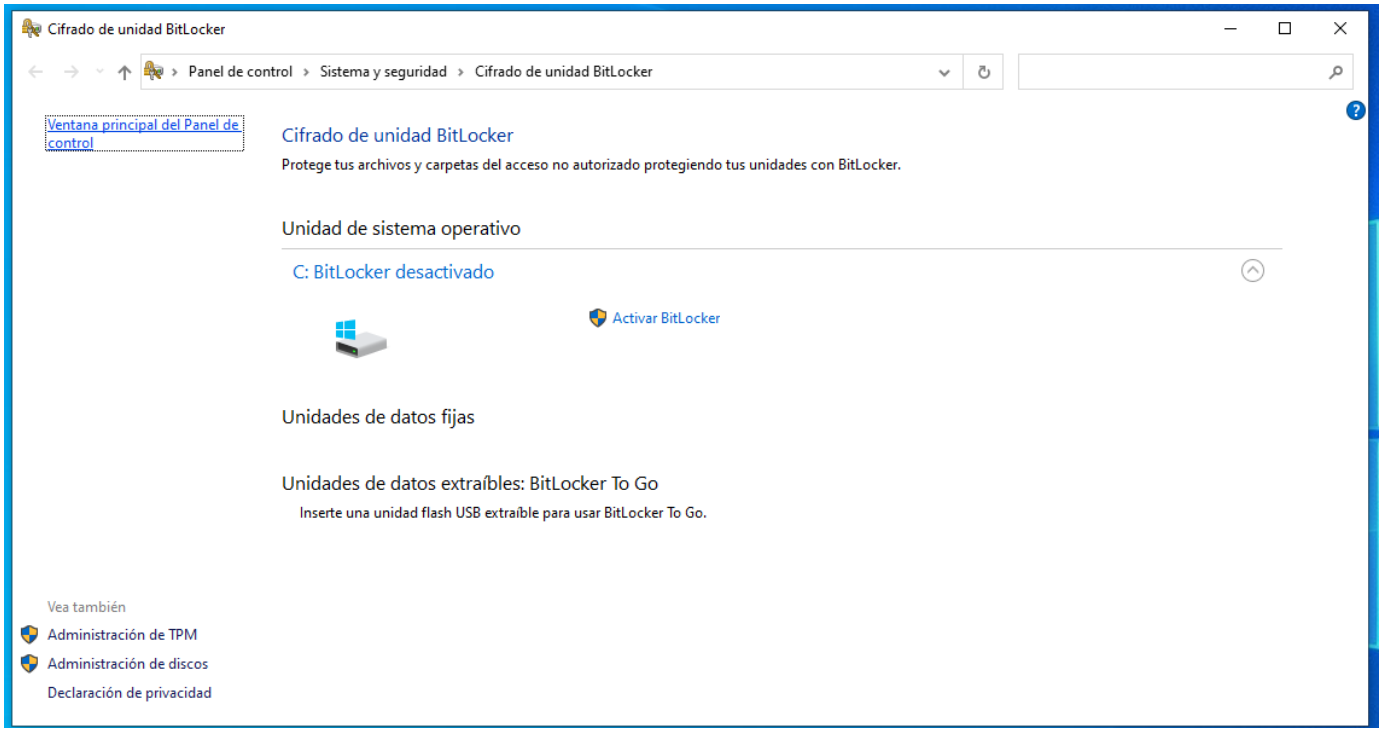


Imagen 1. Gestión del cifrado de disco con Bitlocker.

Saber más

Puedes consultar cómo activar el cifrado de dispositivo desde la página de Soporte de Microsoft: *e.digitall.org.es/activar-cifrado*

En Linux: LUKS

Igual que BitLocker para Windows, LUKS permite cifrar discos duros en Linux. Esta solución se utiliza mayoritariamente utilizando una contraseña para cifrar un disco duro. Es fácil de configurar durante la instalación de algunos sistemas operativos basados en Linux, como Ubuntu o Manjaro Linux.

Además, tenemos la opción de cifrar cualquier tipo de unidad de almacenamiento. Por ejemplo, si tenemos una memoria USB, podemos cifrarla con la ayuda del gestor de discos. De esta forma, cuando se inserte en el equipo, deberemos proporcionar la contraseña de cifrado para poder acceder al contenido. Es importante recordar que esta opción no ofrece ninguna forma de recuperación. Si olvidas la contraseña de cifrado, es posible que pierdas acceso a la información.

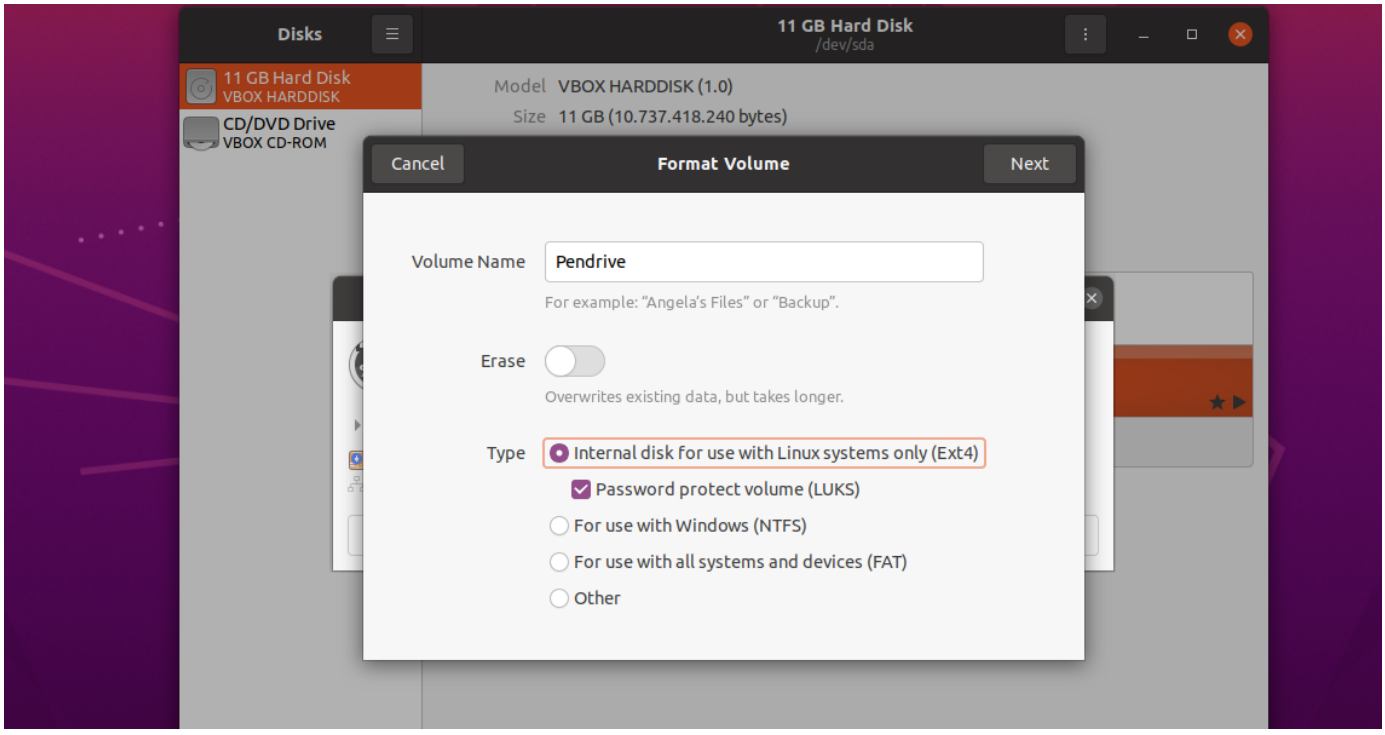


Imagen 2. Cifrado de una unidad extraíble con LUKS en Linux.

En macOS: FileVault

Si se utiliza un dispositivo con macOS, Apple proporciona en su sistema operativo una solución integrada para el cifrado del disco duro. De la misma forma que Windows, esta opción se puede activar y desactivar en cualquier momento. Puede requerir el uso de una contraseña de cifrado, y ofrece alguna opción para la recuperación en caso de olvidarse de la contraseña de cifrado del dispositivo.

Imagen 3. Configuración de FileVault en macOS. (Fuente: *e.digitall.org.es/filevault*)

Saber más

Puedes consultar en la web de Soporte de Apple cómo cifrar el disco de arranque en Mac: *e.digitall.org.es/filevault-mac*

Cifrado de archivos

Puede que alguna de las opciones de cifrado de disco no se adecúe a alguno de los dispositivos o que el usuario no quiera cifrar toda la información. Para esto, existen otras herramientas que permiten el cifrado de parte de la información. A continuación, se incluyen algunas de las más conocidas.

Veracrypt

El software Veracrypt es software de código abierto que funciona en Windows, macOS y Linux. Permite cifrar ciertos archivos creando un "volumen" virtual. De esta forma, guarda un archivo o volumen cifrado, que sólo se puede acceder descifrándolo con Veracrypt y una contraseña de cifrado.

Saber más

Para obtener Veracrypt, puedes descargar el ejecutable desde la página de descargas de la página oficial: *e.digitall.org.es/veracrypt*

Una vez descifrado, el volumen se puede montar y utilizar como una carpeta normal del sistema de ficheros. Al cerrarla con Veracrypt, se vuelve a cifrar toda la información. El volumen cifrado de Veracrypt se puede copiar y compartir como un archivo normal.

Además, Veracrypt también permite el cifrado de discos duros y unidades de almacenamiento extraíbles, de la misma forma que LUKS.

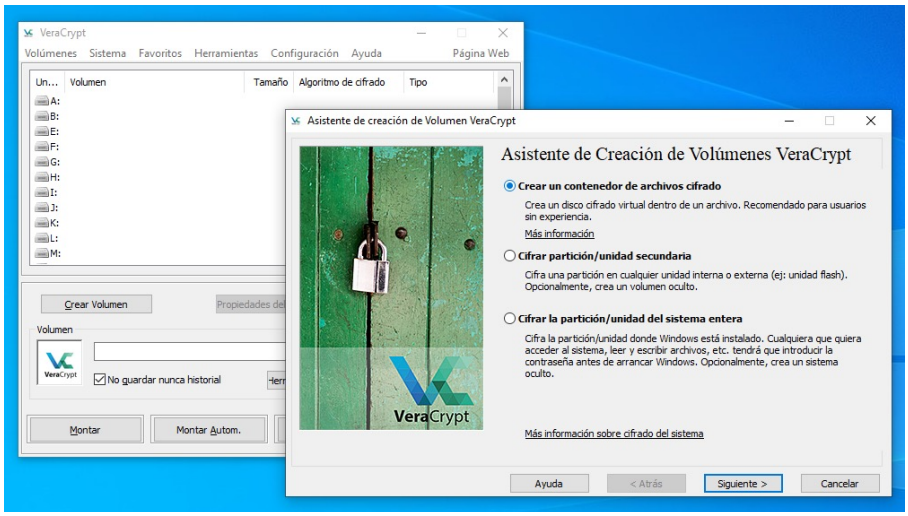


Imagen 4. Creación de un volumen o contenedor de archivos cifrados en Veracrypt desde Windows.

Cryptomator

Similar a Veracrypt, Cryptomator permite crear "bóvedas" o contenedores cifrados. La interfaz permite un uso muy sencillo para el usuario. El código de Cryptomator es abierto, y la descarga desde la web permite su uso gratuíto.

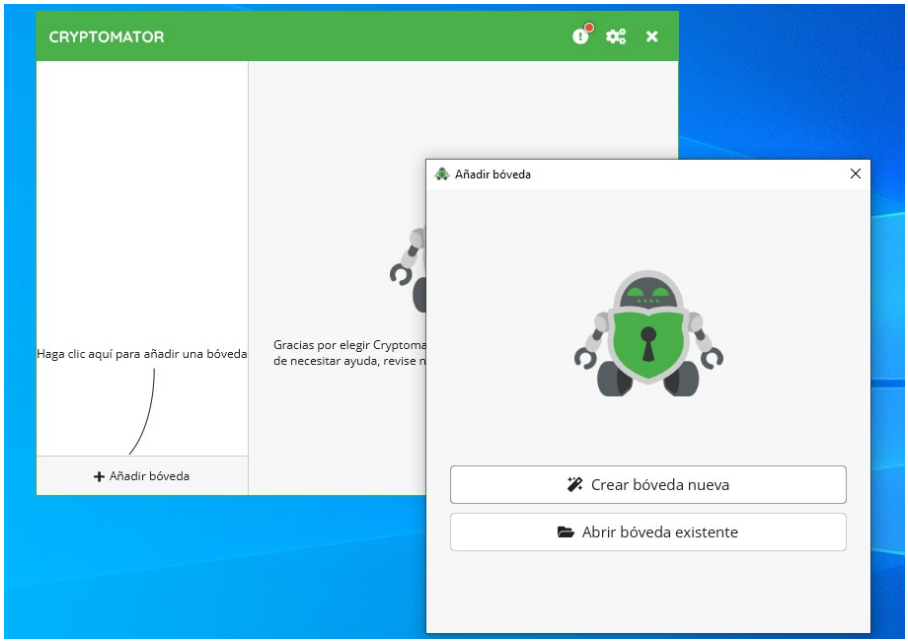


Imagen 5. Creación de una bóveda o contenedor cifrado con Cryptomator desde Windows.

Saber más

Para probar Cryptomator, puedes descargarlo desde su página web oficial: *cryptomator.org/downloads*

7-zip

Una de las opciones más versátiles para el cifrado de archivos en cualquier sistema operativo es utilizar 7-zip. Esta herramienta, aunque está pensada para la compresión de archivos, permite crear carpetas comprimidas ZIP cifradas con contraseña. Así, se pueden almacenar y/o compartir archivos ZIP que requieran una contraseña para ser descifrados y descomprimidos.

Cuando no se conoce tal contraseña, no se puede acceder al contenido de los archivos dentro del ZIP.

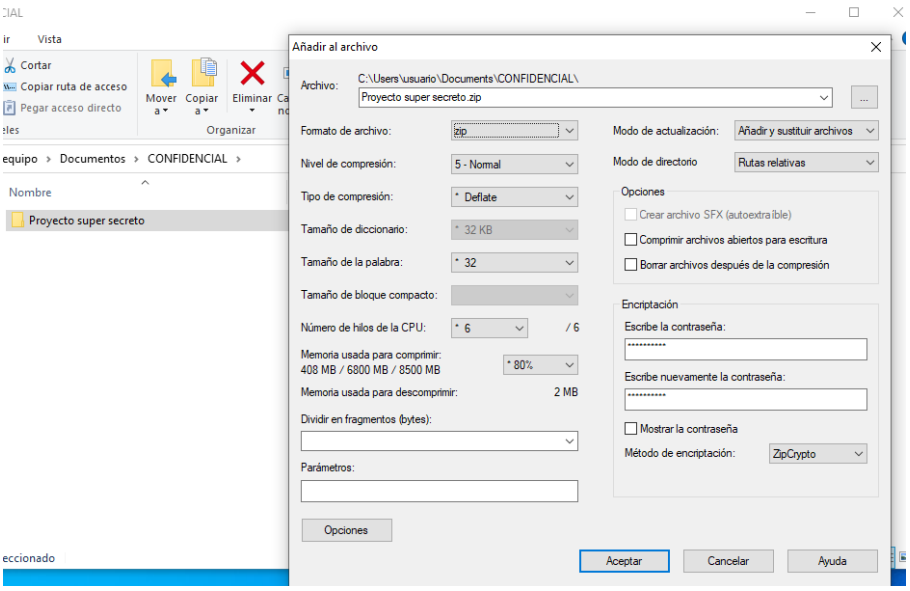


Imagen 6. Cifrado y compresión de una carpeta con 7-zip desde Windows.

Windows EFS

Por último, Windows ofrece la posibilidad de cifrar archivos desde el propio sistema operativo. Es importante tener en cuenta que estos archivos sólo se podrán descifrar desde el mismo dispositivo. Esto puede ser útil para proteger ciertos archivos en el dispositivo, sin necesitar cifrar todo el disco duro.

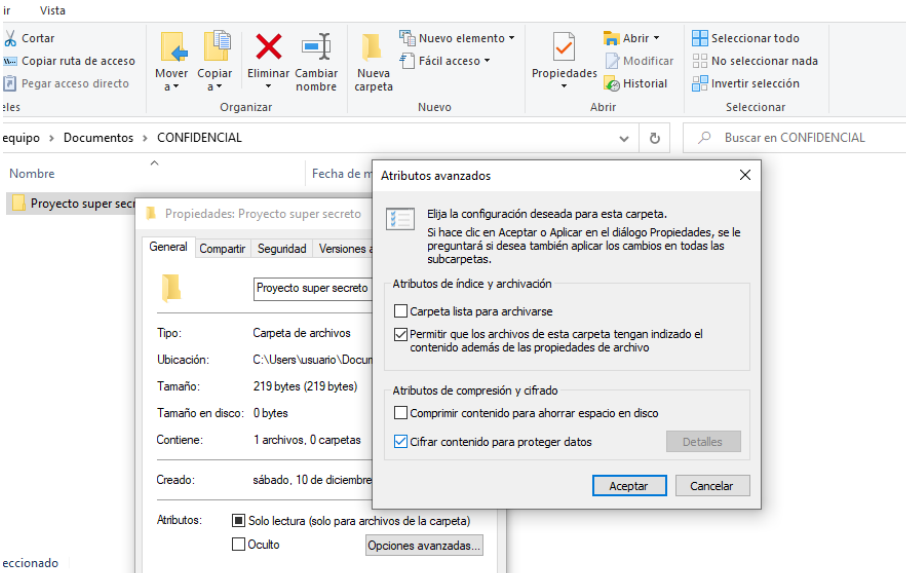


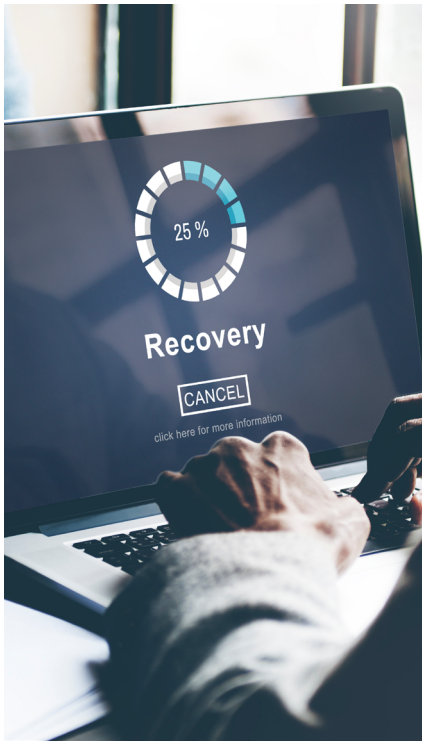
Imagen 7. Cifrado de una carpeta desde Windows con EFS.

Seguridad

Nivel B2 4.1 Protección de dispositivos

Utilidades para realizar copias de seguridad

Utilidades para realizar copias de seguridad



Una copia de seguridad es una copia de los datos que se guarda en un lugar diferente al original. Las copias de seguridad se utilizan para proteger los datos ante la pérdida o el daño accidental. Por ejemplo, si se borra un archivo por error, se puede restaurar desde la copia de seguridad. O, si el disco duro de un ordenador falla, se pueden restaurar los datos desde la copia de seguridad en otro disco duro.

CUANDO TODO FALLA: COPIAS DE SEGURIDAD

Las copias de seguridad se deben realizar con frecuencia, en lugares distintos a los originales. Para información importante, además, se debe seguir el principio 3, 2 1: tres copias, en dos lugares diferentes y una desconectada de la red.

e.digitall.org.es/A4C41B1V09

Hay muchos tipos diferentes de copias de seguridad, incluyendo copias de seguridad locales, copias de seguridad en la nube y copias de seguridad híbridas. Las copias de seguridad locales se guardan en un dispositivo local, como un disco duro externo o un USB. También existe la opción de guardar las copias de seguridad en un servicio en la nube. A continuación, se detalla cómo realizar copias de seguridad dependiendo del sistema operativo que utilizas.

Copia de seguridad en Windows

En un equipo Windows, podemos realizar copias de seguridad de una forma muy sencilla utilizando la herramienta que trae integrada el sistema operativo. Por ejemplo, los pasos en Windows 11 son:

1 | Hacemos click en el botón de “Inicio” y seleccionamos “Configuración”.
2 | Una vez aquí, accedemos al apartado “Actualización y seguridad” y después a “Copia de seguridad”.
3 | Seleccionamos “Agregar una unidad de copia de seguridad”.

4 | Elegimos la unidad de almacenamiento en la que deseamos guardar la copia de seguridad. Podemos elegir un disco externo o USB, o bien el servicio de la nube como OneDrive.
5 | Al pulsar "Siguiente", nos permite seleccionar los archivos y carpetas que incluir en la copia de seguridad.
6 | Ejecutamos "Iniciar copia de seguridad" y esperamos.
7 | Por último, verificamos que los archivos están disponibles en la ubicación que hemos seleccionado.

Además, estas copias de seguridad se pueden programar para que se ejecuten periódicamente. Para ello, puedes seleccionar "Programar" en el proceso anterior. Para restaurar una copia de seguridad, podemos acceder al menú de "Copia de seguridad" y seleccionar "Restaurar archivos a partir de una copia de seguridad".

Copia de seguridad en macOS

En sistemas operativos macOS existen diferentes alternativas. Usando la herramienta integrada **Time Machine**. Para usarla, es necesario tener un disco externo conectado o tener una cuenta en la nube como iCloud. Los pasos son muy sencillos:

1 | Abrimos la aplicación "**Time Machine**" en el Mac, desde la carpeta "Aplicaciones".
2 | Seleccionamos "Seleccionar disco de copia de seguridad" y elegimos el dispositivo de almacenamiento que deseamos utilizar para guardar la copia de seguridad.
3 | Esperamos a que realice el proceso y verificamos que los documentos fueron copiados. Después de este punto, Time Machine seguirá haciendo copias de seguridad automáticas de forma periódica.

Utilizando estas copias de seguridad, es posible:

- **Restaurar un archivo o carpeta.** Para ello, puedes acceder a "Time Machine" y buscar el archivo o carpeta para restaurarlo.
- **Restaurar desde la nube.** Si has guardado tus archivos en la nube de Apple, puedes acceder a ellos desde iCloud Drive, descargando el archivo o carpeta que deseas recuperar.

- **Restaurar una copia de todo el ordenador.** Para ello, debemos apagar el dispositivo y encenderlo manteniendo pulsadas las teclas “cmd + R”. En la ventana de “Utilidades de macOS” aparecerá un menú guiado “Restaurar desde una copia de seguridad de Time Machine”.

Copia de seguridad en Android

Los dispositivos móviles Android también permiten la configuración de copias de seguridad. Los más actuales ya incluyen la aplicación de **Google One**. Una vez hemos iniciado sesión en Google en esta aplicación:

1 | Seleccionamos los datos que deseamos copiar, como contactos, fotos, vídeos, calendarios, etc.
2 | Hacemos click en “Copia de Seguridad” en la página principal de la aplicación.
3 | Una vez seleccionado, hacemos click en el botón “Crear copia de seguridad ahora”.
4 | Cuando termine el proceso, podemos acceder a todo desde el servicio *one.google.com*

Para restaurar una copia, en un dispositivo nuevo Android puedes iniciar la sesión con Google. De nuevo, en la aplicación de Google One, podemos acceder a “Copia de seguridad” y a “Restaurar”.

Copia de seguridad en iOS

La copia de seguridad en un móvil iOS se puede hacer de diversas formas. La más sencilla es usar la nube de Apple, **iCloud**:

1 | Desde los “Ajustes” del iPhone, accedemos al primer apartado donde aparece nuestro nombre, y luego en “iCloud”.
2 | Seleccionamos “Copia en iCloud” y a continuación, “Realizar copia de seguridad ahora”.

Con esta opción, se guardarán todos los datos en iCloud. Si prefieres utilizar tu ordenador, puedes hacerlo. En Windows, debes utilizar la aplicación iTunes:

1 | Conecta tu iPhone al ordenador usando un cable USB.
2 | Abre “iTunes”, o instálalo desde la web de Apple.

3 | En la esquina superior izquierda, haz click en el icono de iPhone.
4 | Selecciona “Resumen” y “Hacer una copia de seguridad ahora”.

Si tu ordenador es Mac:

1 | Conecta tu iPhone al ordenador usando un cable USB.
2 | Abre “iTunes”, o instálalo desde la web de Apple.
3 | En la esquina superior izquierda, haz click en el icono de iPhone.
4 | Selecciona “Resumen” y “Hacer una copia de seguridad ahora”.

Dependiendo de qué estrategia hayas utilizado, cada una de las herramientas permite restaurar de forma sencilla la copia de seguridad. Para ello, sigue el proceso anterior, pero selecciona la opción de restauración.

Conclusión y recomendaciones

Como hemos visto, cada sistema operativo tiene sus herramientas propias. Aquí, hemos tratado los pasos a seguir con las utilidades integradas en el sistema. Sin embargo, existen muchas otras herramientas. Es muy importante recordar que debemos utilizar software de copia de seguridad confiable, para evitar pérdidas de datos y garantizar una recuperación eficiente.

Además, es importante realizar las copias de seguridad con frecuencia y almacenarlas en lugares seguros. Idealmente, utilizar copias de seguridad cifradas. Por último, es buena práctica asegurarse de la buena salud de la copia de seguridad, probando a restaurar o comprobando su integridad.

DigitAll

Seguridad

4.2 PROTECCIÓN DE LOS DATOS PERSONALES Y LA PRIVACIDAD

Seguridad

Nivel B2 4.2 Protección de los datos personales y la privacidad

¿Qué significa este correo que he recibido?

¿Qué significa este correo que he recibido?

Asunto: Comunicado de seguridad
De: "Phone House" <Newsletter@t.phonehouse.es>
Fecha: 23/04/2021 18:37
Para: < >

() ()

Phone House

Hola !

Como sabes, en Phone House estamos comprometidos con nuestros valores, con el servicio a nuestros clientes y con la privacidad y seguridad de tus datos.

Hoy, lamentablemente, te escribimos para informarte respecto al ciberataque que sufrimos el pasado domingo día 11 de abril de 2021. A pesar de todas las medidas de seguridad con las que contamos, en esta ocasión no ha sido posible evitar el ciberataque, y queremos trasladarte con detalle, exactitud y total transparencia lo ocurrido.

Desde el primer momento, nuestros equipos internos, junto con la compañía líder nacional y referente mundial en servicios de ciberseguridad, activaron el correspondiente plan de actuación y adoptaron las medidas más contundentes posibles para limitar el alcance de dicho ciberataque.

Como no podía ser de otra forma, Phone House ha notificado los hechos a la Agencia Española de Protección de Datos, estando en contacto desde el primer momento, con la Brigada Central de Investigación Tecnológica (BCIT) de la Policía Nacional, ante la que se ha presentado la correspondiente denuncia.

Desgraciadamente y, a pesar de que en muchos casos no llegan a trascender, los ataques cibernéticos son cada vez más habituales y, como sabes, están afectando a todo tipo de entidades, tanto del sector público como del sector privado.

Se trata de ataques planificados y perpetrados por redes internacionales que pretenden lucrarse por medio del chantaje. Su modus operandi consiste en cifrar y hacer inaccesibles los sistemas de dichas entidades con la intención de impedir completamente su actividad; así como en amenazar con revelar datos de los interesados afectados, sin importar el daño que pudieran ocasionar.

En Phone House queremos estar a la altura de lo que esperas de nosotros por lo que, en ningún momento, hemos accedido al chantaje. Hacerlo, sería contribuir a que, con dichos fondos, estos grupos criminales pudieran financiar otro ciberataque más, a otra compañía distinta de la nuestra, ocasionando así un nuevo daño a sus trabajadores y a sus clientes, entre los que posiblemente, podrías estar tú.

A pesar de que en Phone House contamos con todas las medidas de seguridad requeridas por la normativa de protección de datos, así como con aquellas definidas por los principales estándares internacionales, los atacantes han logrado acceder a información almacenada en nuestros sistemas. En base a las investigaciones realizadas hasta la fecha, la descarga de dicha información sería parcial y no afectaría a la totalidad de los datos tratados por parte de Phone House, pero **es posible que algunos de tus datos se hayan visto comprometidos.**

Los datos potencialmente afectados serían: nombre, apellidos, dirección postal, teléfono, correo electrónico, DNI (o equivalente), fecha de nacimiento, género, productos/servicios contratados, y, en caso de que nos lo hayas proporcionado, tu número de cuenta bancaria. Gracias al cumplimiento estricto por parte de Phone House, de la normativa de servicios de pago y tratamiento de datos de tarjetas, **en ningún momento los datos de tus tarjetas bancarias se han visto comprometidos, en caso de que nos la hubieras facilitado, ya que no almacenamos este tipo de información. Tampoco se han puesto en riesgo ningún tipo de contraseñas.**

Aun así, queremos transmitirte también que cualquiera que pudiera, como consecuencia de este ciberataque, conseguir acceso a dichos datos y los revelara a cualquier tercero, estaría actuando al margen de la Ley y, muy posiblemente, incurriendo en la comisión de un delito.

Por otro lado, queremos comunicarte que Phone House no ha sufrido pérdida definitiva de información, ni tampoco de ninguno de sus aplicativos por lo que los servicios que te prestamos no se han visto afectados en modo alguno. Asimismo, nuestra red de tiendas ha permanecido abierta sin que la operativa se haya visto interrumpida, así como nuestra web y nuestros servicios de soporte telefónico y digital, que están activos y funcionando con garantías de seguridad.

Lamentamos enormemente este incidente y condenamos enérgicamente este tipo de actividad criminal de la que hemos sido víctimas.

En Phone House continuamos trabajando día y noche en reforzar nuestros protocolos de seguridad para garantizar que disponemos en todo momento de las máximas medidas de protección disponibles.

Hemos habilitado una página de preguntas y respuestas relacionadas con el incidente que esperamos resuelvan tus principales dudas y que iremos actualizando si se produjese cualquier novedad al respecto: preguntas frecuentes. (https://click.e.phonehouse.es /?qs=30d082d80b7c3016bc4a3e52eab19eb9106225116146b02efea319ca35b418dafd151fadb767d5c30dd56dcb8b2e975195f91bb4736cfb86e9e615c41407e0a9)

Para solventar cualquier duda que pueda surgirte al respecto, te recordamos que nuestro Delegado de Protección de Datos está a tu disposición, al que puedes acceder desde nuestra web www.phonehouse.es, en el apartado Política de Privacidad.

Muchas gracias por tu comprensión MANUEL,

Con afecto,

El equipo Phone House.

¿Qué es este correo electrónico? Una comunicación de una violación de la seguridad

Uno de los deberes del responsable del tratamiento de datos personales es garantizar su seguridad, esto es, en esencia, garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento. Con esa finalidad, debe adoptar las medidas técnicas y organizativas apropiadas.

Sin embargo, en ocasiones, no se implantan las medidas adecuadas o, a pesar de ello, no se impide una vulneración de esa seguridad. En particular, el crecimiento exponencial de los ciberataques es alarmante.

En este contexto, el Reglamento General de Protección de Datos establece que "cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado". Este correo electrónico es un ejemplo de una comunicación de una violación de la seguridad.

La normativa exige que esa comunicación sea realizada sin dilación indebida. Lo que se persigue con ello es que el afectado pueda adoptar las medidas oportunas a la mayor brevedad. Por ej., si han sido comprometidas unas contraseñas, que se cambien inmediatamente; o si ha sido la numeración de una tarjeta de crédito, que se cancele. Obsérvese que en el caso el ciberataque se ha producido el 11 de abril, aunque el correo se envía el día 23, posiblemente porque no han sido afectadas ni contraseñas ni tarjetas bancarias -con ello no se está diciendo que se comparta el criterio adoptado-, aunque sí números de cuenta bancaria.

⚠ ATENCIÓN

El interesado tiene derecho a que el responsable del tratamiento le informe de las violaciones de seguridad de los datos personales que entrañen un alto riesgo para sus derechos y libertades.

LOS DEBERES DE LOS SUJETOS QUE MANEJAN DATOS PERSONALES
e.digitall.org.es/A4C42A2V07

Contenido de la comunicación

El Reglamento General de Protección de Datos dispone que esa comunicación debe tener el siguiente contenido:

a) La descripción, con lenguaje claro y sencillo, de la naturaleza de la violación de la seguridad. En el caso se explica que ha sido un ciberataque y en qué ha consistido: "cifrar y hacer inaccesibles los sistemas de dichas entidades con la intención de impedir completamente su actividad; así como en amenazar con revelar datos de los interesados afectados" si no se paga un rescate. En fin, está describiendo un Ransomware con robo de datos personales. También se informa que la empresa no ha sufrido pérdida definitiva de información ni tampoco de ninguno de sus aplicativos por lo que los servicios no se han visto afectados. O dicho de otra manera, que había una copia de respaldo con toda la información que se ha podido restaurar.

b) El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información. En el caso, se facilita información genérica sobre el Delegado de protección de datos y se remite también a una página web de preguntas y respuestas sobre el incidente.

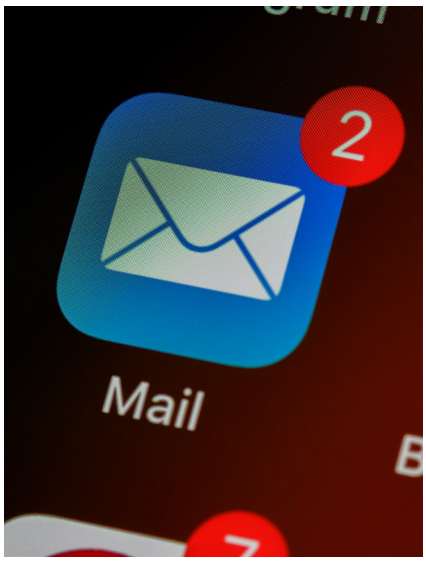
c) Las posibles consecuencias de la violación de la seguridad. En el caso, se informa de dos cuestiones:

- Que es posible que los datos personales se hayan visto comprometidos.
- Los datos potencialmente afectados: nombre, apellidos, dirección postal, teléfono, correo electrónico, DNI o equivalente, fecha de nacimiento, género, productos/servicios contratados, y número de cuenta bancaria facilitada.

d) Las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación y, si procede, para mitigar los posibles efectos negativos. En el caso se relatan las siguientes:

NOTA

Según el informe *Threat Landscape Report*, elaborado por S21sec, en el año 2022, España ocupa el sexto lugar en el ranking de las naciones que más ciberataques sufren en el mundo. El 65 % por *ransonware*.



- Activación del plan de actuación, con la colaboración de una empresa externa experta en ciberseguridad
- Notificación de los hechos a la Agencia Española de Protección. Debe tenerse en cuenta que esta notificación es un deber por parte del responsable del tratamiento, pues la normativa prohíbe ocultar este tipo de incidentes.
- Denuncia ante el Cuerpo Nacional de Policía, pues este tipo de ciberataques son constitutivos de delito.
- Rechazo del pago del chantaje.

Supuestos en los que no es necesaria esta comunicación

La normativa enumera una serie de supuestos en los que no es necesario que la entidad que sufre una violación de seguridad la comunique a los interesados:

a) El responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad. En particular, se trata de aquellas medidas, como el cifrado, que hagan ininteligibles los datos personales para cualquier persona no autorizada.

b) Se han adoptado medidas ulteriores que garanticen que no existe probabilidad de que se concrete el riesgo para los derechos del interesado.

c) Suponga un esfuerzo desproporcionado. En este caso, no se comunica a cada interesado (en el caso analizado, era un correo electrónico dirigido a la concreta dirección de correo electrónico de cada potencial afectado), sino que se hace una comunicación pública (prensa, internet, televisión, etc.) en la que se informe también a los interesados.

Saber más

Grupo de trabajo sobre protección de datos del artículo 29. Directrices sobre la notificación de las violaciones de la seguridad de los datos (WP 250). *e.digitall.org.es/articulo29*

DigitAll

Seguridad

4.3 PROTECCIÓN DE LA SALUD Y EL BIENESTAR

Seguridad

Nivel B2 4.3 Protección de la salud y el bienestar

Guía visual para hacer un uso adecuado del control parental

Guía visual para hacer un uso adecuado del control parental

En este documento se puede consultar información sobre qué es y cómo se puede utilizar el control parental. El control parental ofrece a las familias con niñas, niños y adolescentes, numerosos servicios como por ejemplo supervisar el acceso y el uso que hacen de la tecnología. Además, en este documento se puede observar un ejemplo de cómo configurar de forma ágil las principales utilidades del control parental a través del ejemplo de María y su familia.

Control parental: generalidades

El control parental consiste en un conjunto de medidas que permiten monitorizar, restringir y limitar el acceso y la utilización de Internet o de dispositivos tecnológicos, como ordenadores, tablets o móviles.

Las herramientas de control parental se pueden encontrar en diferentes servicios tecnológicos para apoyar la seguridad de niñas, niños y adolescentes cuando utilizan la tecnología.

Estas herramientas pueden ser útiles para reducir riesgos a medida que las/os menores aprenden a desenvolverse en Internet con responsabilidad y autonomía. En ningún caso sustituyen el acompañamiento o la supervisión que puede ofrecer una persona adulta, pero pueden constituir un apoyo en su proceso de aprendizaje digital.

⚠ ATENCIÓN

Las herramientas de control parental forman parte de la mediación parental. No sustituyen la implicación y el diálogo cotidiano con las/os menores, sino que apoyan esta labor de mediación parental.
Para que estas herramientas funcionen de forma exitosa, se aconseja explicarle a las/os menores por qué son necesarias. También es importante adaptar las funcionalidades a su nivel de desarrollo y madurez.

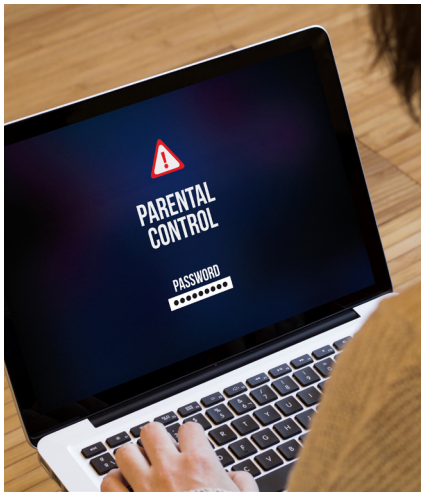
CONTROL PARENTAL

En este vídeo, se introduce el concepto de control parental y el uso responsable de estas herramientas en los dispositivos móviles de niñas/os y adolescentes.

e.digitall.org.es/A4C43B2V03

Se identifican las siguientes funciones como principales:

- **Filtrado de contenidos:** sirve para bloquear o restringir el acceso a ciertos contenidos que se consideren inapropiados según la edad, generalmente de carácter sexual o violento. Esta funcionalidad puede incluir también la restricción de compras, el bloqueo de personas o el filtrado de lenguaje o palabras concretas.
- **Control de tiempo:** permite establecer un horario específico o un tiempo máximo de uso, interrumpiéndose la navegación o bloqueándose la aplicación o el dispositivo al alcanzar determinada hora o límite de tiempo. También puede incluir la emisión de alarmas en caso de uso excesivo de la tecnología.
- **Supervisión de actividad:** sirve para supervisar las páginas que la/el menor ha visitado y las personas con las que ha contactado.
- **Geolocalización:** permite conocer la posición en tiempo real y el recorrido previo del dispositivo.
- **Protección de la configuración:** sirve para evitar cambios no deseados en los propios ajustes de control parental.



Las herramientas y funciones de control parental varían en cada país, y se pueden encontrar de forma general en los propios sistemas operativos de ordenadores o dispositivos móviles, o de manera específica en determinadas aplicaciones, contenidos digitales, juegos o redes sociales. Así, algunos ejemplos que permiten funcionalidades de control parental son: sistemas operativos como Windows, iOS o Android; aplicaciones específicas como Family Link (que se explica a continuación); proveedores de contenido como Netflix o YouTube; o redes sociales como TikTok o Instagram.

CONTROL PARENTAL EN GRUPO FAMILIAR

En este vídeo, se amplía el concepto de control parental a un nivel más avanzado. Se explica cómo controlar un grupo familiar, mediante ejemplos en diferentes dispositivos para gestionar los contenidos, las compras y el tiempo de uso.

e.digitall.org.es/A4C43C1V04

Family Link: ejemplo de configuración básica de herramientas de control parental

Como se ha descrito en el apartado anterior, las herramientas de control parental son numerosas y las podemos encontrar en diferentes formatos. La idea central de este documento es hacer una aproximación a estas herramientas. Para ello, se tomará como referencia un ejemplo concreto para conocer las funcionalidades y su configuración; en este caso, Family Link de Google.

Family Link es una de las opciones de herramientas de control parental que están disponibles gratuitamente en el mercado tecnológico.

Figura 1. Fuente: Autoría propia.

Family Link: *e.digitall.org.es/familylink*

El enlace anterior es la página web oficial de Family Link de Google. Se puede encontrar la información completa sobre la plataforma y los enlaces que se necesitan para descargar la aplicación en los dispositivos de la familia.

Antes de la instalación de la aplicación, es importante asegurarse de que los dispositivos que se van a configurar son compatibles con Family Link. Para ello, podemos consultar el sistema operativo y la versión que tienen los móviles, tanto de la madre o del padre como de los/as menores.

⚠ ATENCIÓN

En la página web de Family Link se informa que es completamente compatible con versiones iguales y superiores de los siguientes sistemas operativos, en función del rol:

Dispositivos para niños y niñas: Android 7.0 y posteriores.
Dispositivos para padres y madres: Android 5.0 y posteriores; iOS 11 y posteriores; Chrome OS 71 y posteriores.

Antes de comenzar con las funciones del control parental, es importante configurar aspectos generales para que el programa entienda quién conforma la "familia". En la Figura 1, se observa una captura de Family Link y en la Figura 1, la configuración de "familia".

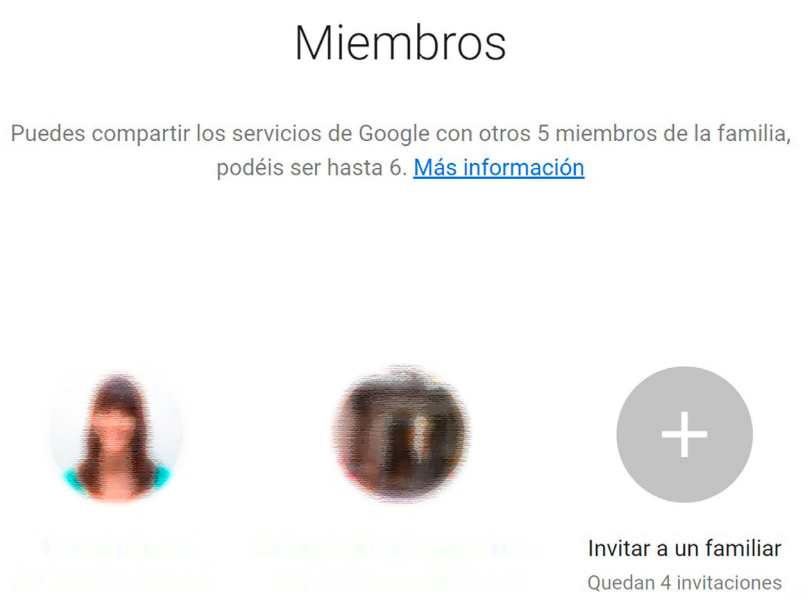


Figura 2. Fuente: Autoría propia.

La familia de este ejemplo se conforma por el padre y la madre de una niña llamada María. En la Figura 2, se observa cómo está el grupo familiar configurado, pero sin la niña. En la Figura 3, se ha añadido a María al grupo familiar como un "miembro de la familia supervisado".

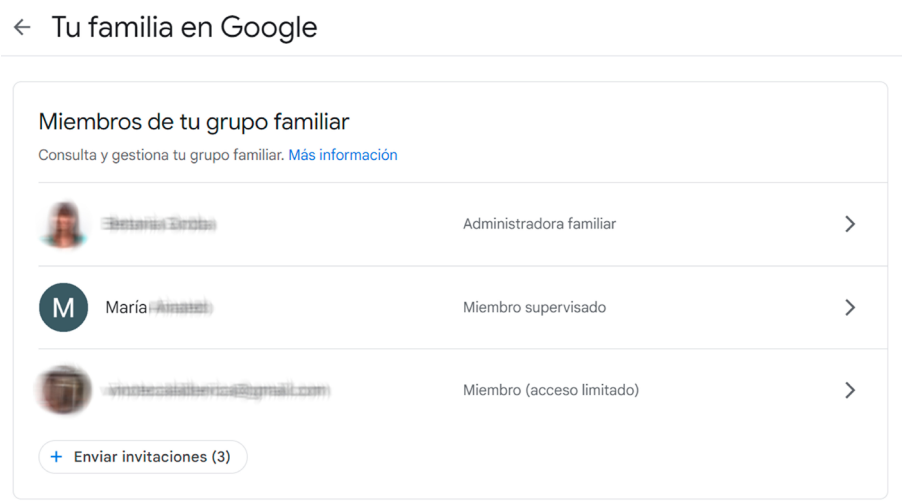


Figura 3. Fuente: Autoría propia.

Esta configuración de la "familia" permite hacer uso de Family Link y otros servicios de Google como: Google Calendar para familias, Keep para familias (notas y listas), planes familiares de Youtube Premium, Biblioteca familiar de Google Play, Google Play Pass o Google One, entre otros.

Configuración del dispositivo del niño, niña o adolescente

La configuración del dispositivo del niño, niña o adolescente es sencilla e intuitiva. Family Link ofrece instrucciones detalladas para guiar en el proceso de configuración. En las siguientes páginas se ofrece una guía con los aspectos más relevantes de la configuración.

El dispositivo utilizado como ejemplo es una tablet con sistema operativo Android, por lo que la configuración del control parental se hace a través de "Ajustes", tal y como se muestra en la Figura 4; siendo la secuencia de pasos: (1) Pulsar en Ajustes; (2) Pulsar en Google y (3) Pulsar en Controles parentales.

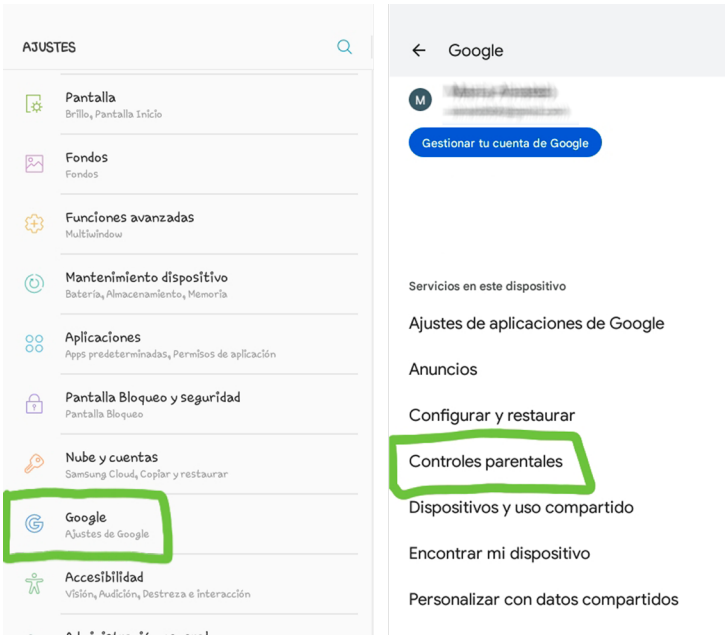


Figura 4. Fuente: Autoría propia.

En el dispositivo se van configurando diferentes aspectos que aumentan la seguridad de María al usar su tablet:

- **Vincular la cuenta de Google del niño, niña o adolescente con la del padre o madre en un grupo familia.**

La clave para poder acceder a todas las opciones es realizar de forma correcta la vinculación del niño, niña o adolescente al grupo familiar (tal como se mostraba en la Figura 3) y vincular la cuenta de correo electrónico de María con las de su madre y su padre (Figura 5).

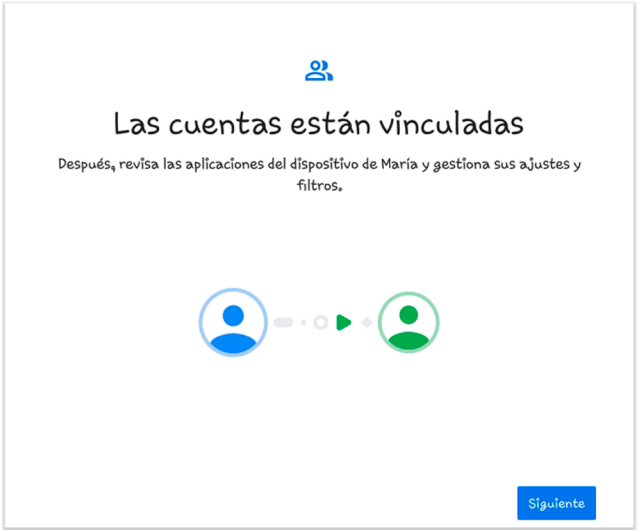


Figura 5. Fuente: Autoría propia.

- **Elegir a qué aplicaciones puede acceder el niño, niña o adolescente.**

El dispositivo de María contiene un número elevado de aplicaciones. Aunque la mayor parte de las aplicaciones han sido instaladas para que María pueda utilizarlas, su madre y su padre pueden decidir aquellas a las que le quieren dar acceso. En la Figura 6, se muestra cómo se pueden ir habilitando o bloqueando las aplicaciones.

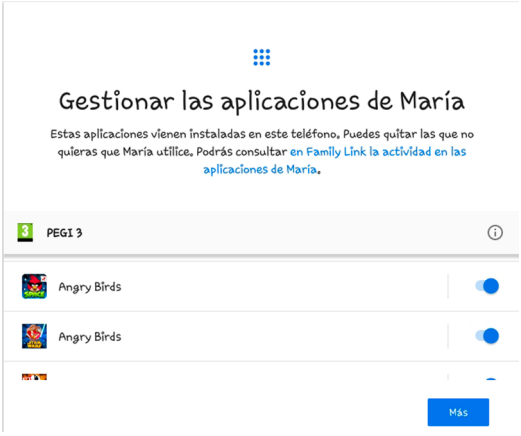


Figura 6. Fuente: Autoría propia.

En la Figura 7, se encuentran dos ejemplos de cómo el control parental clasifica de forma automática las aplicaciones y recomienda su uso o no en función de la clasificación conocida como PEGI. Aunque estas recomendaciones son útiles, es importante que madres y padres analicen las aplicaciones en detalle.

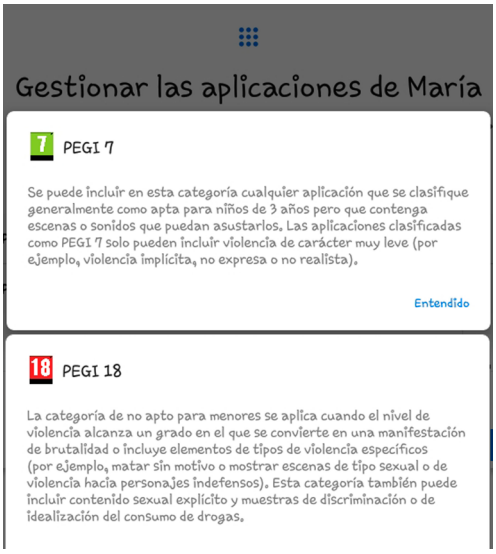


Figura 7. Fuente: Autoría propia.

- **Establecer límites de tiempo y crear rutinas de tiempo máximo**

La limitación en el tiempo depende de la edad de cada menor y de las circunstancias familiares. De forma general, se pueden seguir las recomendaciones de la American Academy of Pediatrics (2016).

⚠ ATENCIÓN

La American Academy of Pediatrics, realiza recomendaciones sobre el tiempo de uso máximo de pantallas al que se deberían exponer niños, niñas y adolescentes en función de su edad:

Menores de 18 o 24 meses: evitar el uso de medios digitales.
Menores entre 2 y 5 años: máximo 1 hora de exposición al día y cuanto menos tiempo, mejor.
Menores entre 7 y 12 años: máximo 1 hora, en compañía de una persona adulta.
Menores entre 12 y 15 años: máximo 1 hora y media, con especial atención a las redes sociales.
Más de 16 años: máximo 2 horas, evitando pantallas en las habitaciones.

A través del control parental, se pueden ajustar estos tiempos máximos de uso en función del día de la semana e, incluso, se puede ajustar el tiempo máximo por aplicación concreta.

- Controlar los ajustes de ubicación.
- Definir filtros y controles en Google Chrome, la Búsqueda, Play y Youtube.

Entre las opciones de configuración, destacan los filtros para buscar información y para comprar en Internet. En la Figura 8, los padres de María están configurando las opciones para permitir o bloquear los sitios web a los que la niña puede tener acceso. En la Figura 9, se están configurando las opciones de compra de aplicaciones en Google Play.

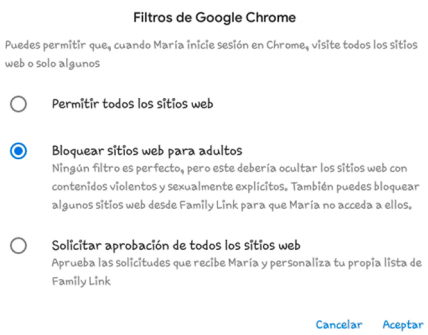


Figura 8. Fuente: Autoría propia.

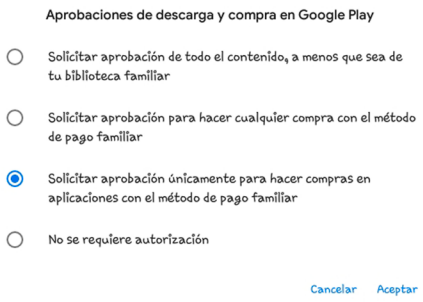


Figura 9. Fuente: Autoría propia.

Si se han realizado todos los pasos, se procederá a realizar la instalación de la aplicación en el dispositivo del niño o niña y en el dispositivo del padre o madre (Figura 10). En la Figura 11, se muestra la información sobre la tablet de María y la configuración de forma correcta para poder ser supervisada a través de las herramientas de control parental.

Figura 10. Fuente: Autoría propia.

Figura 11. Fuente: Autoría propia.

Configuración del dispositivo de la madre o padre

En el dispositivo de la madre o del padre es necesario instalar la aplicación disponible de Family Link.

Esta aplicación permite la configuración y ajuste de todas las funcionalidades anteriormente configuradas en el dispositivo de María. Además, la aplicación permite realizar el seguimiento de la actividad de la niña. La Figura 12 (a la derecha) es una captura de las funciones que la familia de María puede consultar en remoto sobre el dispositivo y el uso de este por parte de María.

Asimismo, si es necesario cambiar la configuración de algún aspecto se puede hacer a través de esta aplicación. Por ejemplo, se pueden configurar o modificar los tiempos de uso o la hora de apagado del dispositivo o crear rutinas en función de los días de la semana (Figura 13). También se puede configurar el límite de tiempo en base a las aplicaciones específicas; en la Figura 14, la familia de María le otorga un límite máximo de 30 minutos para utilizar la aplicación Buenas noches.

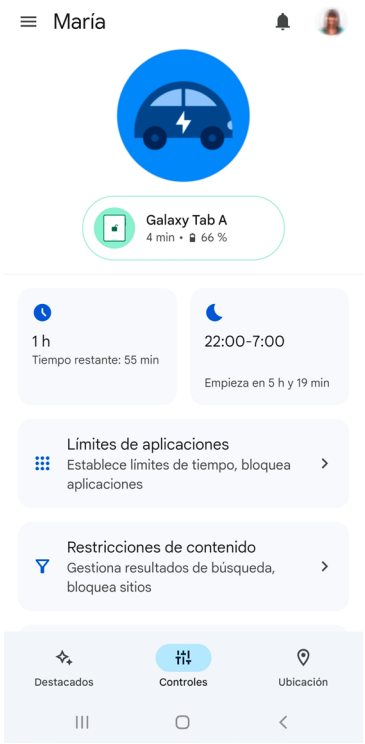


Figura 12. Fuente: Autoría propia.

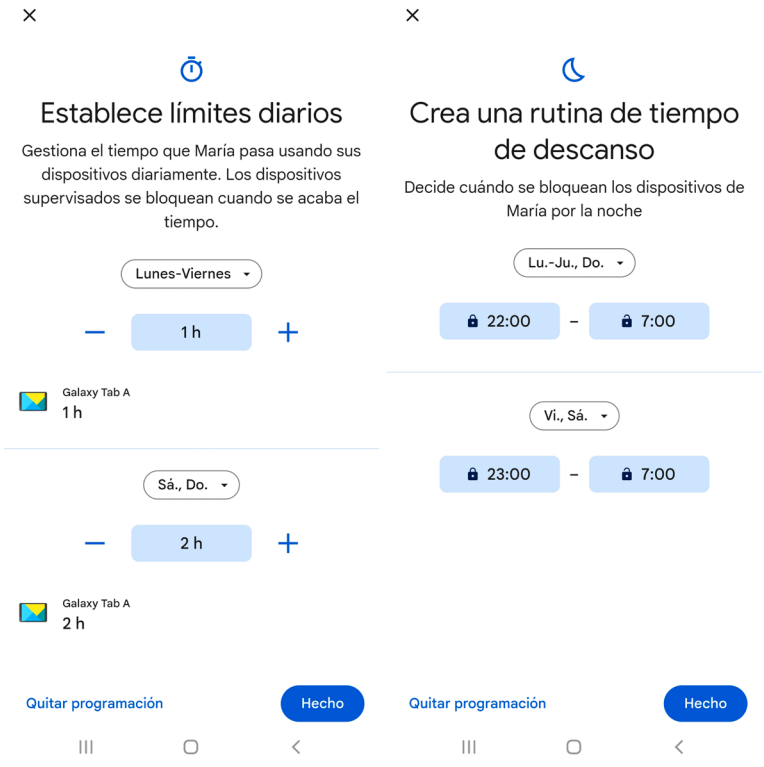


Figura 13. Fuente: Autoría propia.

Figura 14. Fuente: Autoría propia.

Otra de las utilidades de las herramientas de control parental que ofrece un mayor interés cuando no estamos con las/os menores, es la geolocalización. En la Figura 15, en su lateral izquierdo, se observa la pantalla en la que se configuran los ajustes de la ubicación y en el lateral derecho, cómo se visualiza la ubicación en tiempo real del dispositivo.

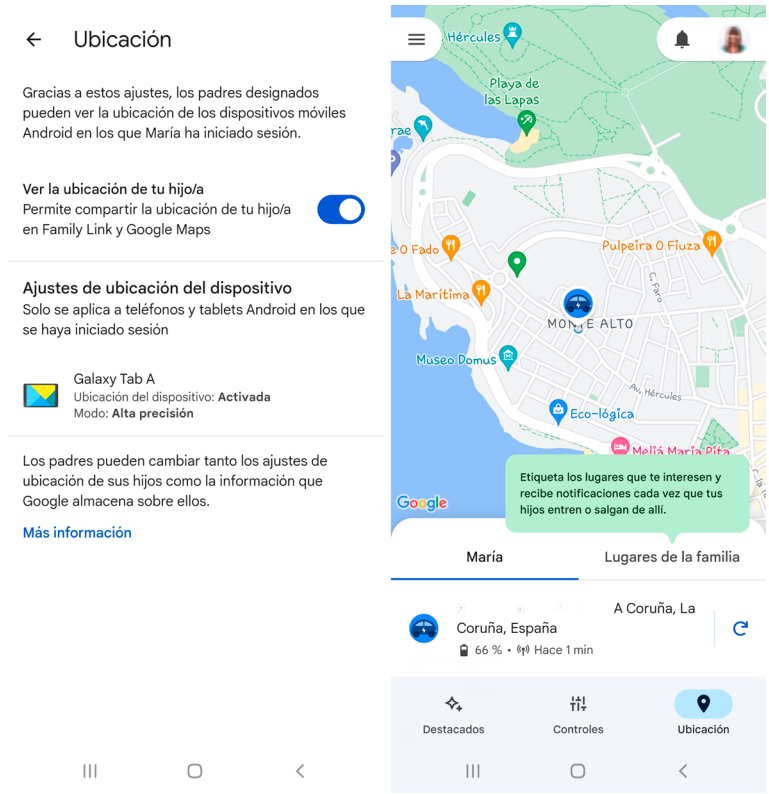


Figura 15. Fuente: Autoría propia.

Finalmente, es esencial recordar que el control parental de las aplicaciones no sustituye al acompañamiento y supervisión de las personas adultas de la familia. De hecho, Family Link aconseja que la configuración y los términos de uso se realicen en conjunto entre los menores y sus padres/madres como forma respetuosa de crianza.

Ejemplos de pactos familiares para usar tecnología:
e.digitall.org.es/pactos-familiares

En la página web se pueden consultar y descargar ejemplos concretos de pactos familiares para hacer un uso adecuado de la tecnología (redes sociales, videoconsolas, tablet, móvil, entre otras opciones).

Saber más

Family Link. Google. e.dgitall.org.es/familiylink

Guía de herramientas de control parental. Instituto Nacional de Ciberseguridad (INCIBE). e.digitall.org.es/guia-control-parental

Guía de mediación parental para un uso seguro y responsable de Internet por parte de los menores. Instituto Nacional de Ciberseguridad (INCIBE). e.digitall.org.es/mediacion-parental

Herramientas de control parental. Búsqueda de herramientas de control. Instituto Nacional de Ciberseguridad (INCIBE). e.digitall.org.es/control-parental

Media and Young Minds. American Academy of Pediatrics. e.digital.org.es/media-young

Pactos familiares para el buen uso de dispositivos. Instituto Nacional de Ciberseguridad (INCIBE). e.digital.org.es/pactos-familiares-incibe

DigitAll

Seguridad

4.4
PROTECCIÓN DEL MEDIO AMBIENTE

Seguridad

Nivel B2 4.4 Protección del medio ambiente

De las 3 Rs a la economía circular

De las 3 Rs a la economía circular

Introducción

En este documento se van a tratar de forma más detallada conceptos que se han incluido en los videos del nivel, como las distintas "erres" que amplían la visión clásica del "reducir, reutilizar, reciclar" como propuesta clásica del ambientalismo.

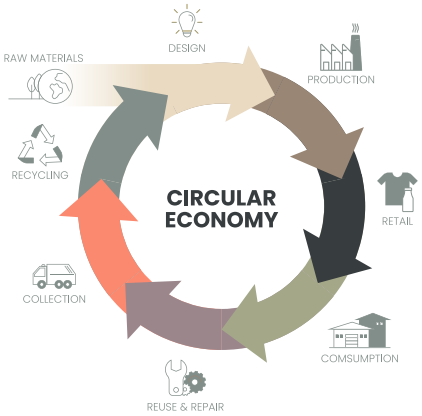
Veremos cómo la ampliación conceptual ligada a las nuevas "erres" a través de términos como Reevaluar, Reparar, Reestructurar, Redistribuir o Relocalizar está relacionada con las propuestas teóricas que se vinculan con el concepto de "decrecimiento", como una alternativa de aproximación a las problemáticas ambientales actuales ligadas al modelo de producción y consumo.

Y precisamente como propuesta de modelo económico alternativo que busca aumentar los niveles de sostenibilidad social y ambiental, nos aproximaremos a la economía circular. Esta propuesta se trata de implementar una nueva economía, basada en el principio de cerrar el ciclo de vida de los productos, los servicios, los residuos, los materiales, el agua y la energía.

Además de presentar los fundamentos de la economía circular, presentaremos ejemplos concretos de productos y servicios relacionados con las tecnologías digitales que se acogen a una reconceptualización que parte de su propio diseño, para minimizar sus impactos ambientales y sociales.

Más allá de las 3Rs: las propuestas decrecentistas

En niveles anteriores hemos analizado cómo para conseguir disminuir los impactos ambientales y sociales de la tecnología digital es necesario replantear el modelo económico, orientándolo hacia una reducción del consumo y de la producción con el fin de aumentar el bienestar humano y las condiciones ambientales en el planeta.



A partir de esta idea, es importante profundizar en las vías para conseguirlo. Para empezar, podemos partir de las "3 Rs" clásicas del ambientalismo: reducir, reutilizar y reciclar. Como ya hemos visto, en los videos de esta serie **"Opciones de consumo responsable de tecnología móvil"** (v.5) y **"Sumando erres a la sostenibilidad: la economía circular"** (v.4), necesitamos reducir nuestro consumo de productos y dispositivos tecnológicos atendiendo a necesidades reales y estando alerta a las estrategias de obsolescencia; reutilizar, en la medida de los posible, aparatos y componentes que todavía puedan tener una vida útil que evite esquilmar nuevos recursos naturales; y, por último, optimizar los procesos de reciclaje de elementos necesarios para el funcionamiento del sector tecnológico, indispensables para el mantenimiento de las cadenas de suministro y cada vez más costosos de extraer, tanto ambiental como socialmente.

SUMANDO ERRES A LA SOSTENIBILIDAD: LA ECONOMÍA CIRCULAR

Explorar las propuestas de la economía circular para el consumo tecnológico basadas en el "rediseño" de procesos con criterios sostenibles. Daremos ejemplos de los diseños "de la cuna a la cuna".

e.digitall.org.es/A4C44B2V04

OPCIONES DE CONSUMO RESPONSABLE DE TECNOLOGÍA MÓVIL

Se muestran a un nivel más concreto diferentes alternativas de consumo responsable y sostenible de tecnología móvil, desde talleres de auto-reparación al Fairphone o "teléfono justo".

e.digitall.org.es/A4C44B2V05

Pero es muy posible que con esto no sea suficiente. Para conseguir cambios estructurales en nuestro modelo de producción y consumo, vamos a necesitar de otro tipo de propuestas que aporten alternativas a un nivel más profundo, ya que se ha demostrado que las 3 Rs han sido interiorizadas como parte del sistema económico actual, de forma que consiguen "parchear" de alguna manera las problemáticas socioambientales sin realmente contribuir a la transformación de sus causas.

Es aquí donde entran en juego otras propuestas alternativas como las que vamos a presentar en este documento. En primer lugar, nos vamos a centrar en un concepto que está ganando popularidad en el contexto internacional en los últimos años: el decrecimiento.

El decrecimiento es un movimiento filosófico y activista con origen en Francia, donde la propuesta de la *décroissance* se puede señalar como el origen de los demás movimientos decrecentistas. El fundador de la *décroissance* es el economista y filósofo francés Serge Latouche. En varias de sus obras, entre las que se pueden destacar "Pequeño tratado del decrecimiento sereno"(2009); La hora del decrecimiento" (2012); o el reciente "Introducción al decrecimiento" (2022), Latouche propone distintos caminos y posibles aproximaciones a un sistema económico que no tenga como objetivo fundamental el crecimiento continuado.

⚠ ATENCIÓN

Entrando en detalle, su propuesta se basa en ampliar las conocidas tres "Rs" a las ocho "Rs" como pilares del decrecimiento: Revaluar, Reconceptualizar, Reestructurar, Relocalizar, Redistribuir, Reducir, Reutilizar y Reciclar (Latouche, 2009).

Además de las propuestas ya conocidas sobre la necesidad de Reducir, Reutilizar y Reciclar en el sector digital, una aplicación de las 5 Rs restantes se podría ejemplificar de la siguiente manera:

1 | **Revaluar**, en referencia a dar un nuevo valor al coste de la producción de los dispositivos digitales. Debemos saber que no pagamos el coste real de la producción si tenemos en cuenta la deslocalización de la producción o los costes ambientales de la misma.

2 | **Reparar**. Se debe hacer incidencia en que los productos deben estar diseñados para facilitar su reparación y evitar que se desechen antes de tiempo. Para ello, es indispensable contar con una normativa que lo facilite y lo respalde, con el objetivo de evitar las estrategias de obsolescencia tan comunes en el sector de la tecnología.

3 | Reestructurar los modelos de producción y comercialización de los dispositivos digitales, teniendo en cuenta a todos los actores que intervienen en el proceso productivo, así como su impacto en el entorno.

4 | Relocalizar los procesos productivos con la idea de poner en valor el producto local ya que tendrá un impacto menor en el medio y contribuirá en mayor medida a mejorar la economía de cercanía. Esta filosofía es difícil de aplicar en el sector digital ya que las cadenas de producción y suministro están muy localizadas, pero es un desafío que debemos abordar como sociedad.

5 | Redistribuir los costes y beneficios del modelo de producción y consumo de tecnología digital, con la idea de que, si todo el mundo consumiera del mismo modo que se hace en los países industrializados, ese modelo sería totalmente inviable.

Una aproximación a la economía circular

En línea con las propuestas decrecentistas, la economía circular emerge como una propuesta de transformación del modelo de producción y consumo que implica compartir, alquilar, reutilizar, reparar, renovar y reciclar materiales y productos existentes lo máximo posible, para de esta forma limitar el agotamiento de recursos y los impactos ambientales del proceso.

Si la propuesta del decrecimiento parte de círculos académicos y activistas, la economía circular ha sido acogida por diversas instituciones como una apuesta firme a nivel político. Por ejemplo, la Unión Europea y las instituciones comunitarias trabajan en la reforma del marco legislativo para promover un cambio del modelo de gestión de residuos actual, que tiene un carácter lineal, por una verdadera "economía circular".

La economía circular busca, en esencia, que el ciclo de vida de los productos se extienda. Eso, en la práctica, implica reducir los residuos al mínimo, pero también los impactos ambientales y sociales del modelo productivo. Bajo este prisma, el sector tecnológico sería uno de los que se verían más beneficiados con la transformación del modelo productivo.

En la actualidad, cuando un producto llega al final de su vida, sus materiales se mantienen dentro de la economía siempre que sea posible gracias al reciclaje. Estos pueden ser productivamente utilizados una y otra vez, creando así un valor adicional que tiene que ver con el aprovechamiento del recurso en sí mismo, pero también con el hecho de que no se están explotando más reservas de recursos que son limitados.

De hecho, uno de los motivos principales para avanzar hacia una economía circular es el aumento de la demanda de materias primas y la escasez de recursos. Varias materias primas cruciales son finitas y, como la población mundial crece, la demanda también aumenta.

La consolidación del modelo de la economía circular contrastaría con el modelo económico lineal tradicional, basado principalmente en el concepto "usar y tirar", que requiere de grandes cantidades de materiales y energía baratos y de fácil acceso. Para el sector de las tecnologías digitales, ya hemos visto en niveles anteriores los conflictos sociales y ambientales asociados a los procesos extractivos.

También vimos cómo los impactos ambientales no se reducen simplemente a la extracción y agotamiento de recursos. Otro beneficio de la economía circular es la reducción de las emisiones anuales totales de gases de efecto invernadero.

NOTA

Según la Agencia Europea de Medio Ambiente, los procesos industriales y el uso de productos son responsables del 9,10% de las emisiones de gases de efecto invernadero en la UE, mientras que la gestión de residuos representa el 3,32% (Parlamento Europeo, 2023).

Además, crear productos más sostenibles desde su propio diseño, adoptando los principios y las premisas del eco-diseño o de la perspectiva "de la cuna a la cuna", también ayudaría a reducir el consumo de energía y recursos, ya que se calcula que más del 80% del impacto ambiental de un producto se determina durante la fase de diseño.

Por si todo esto no fuera suficiente, hay estudios que calculan que la transición hacia una economía más circular podría aumentar la competitividad, estimular la innovación, impulsar el crecimiento económico y crear empleo. Según datos del Parlamento Europeo (2023), se prevé que se puedan crear al

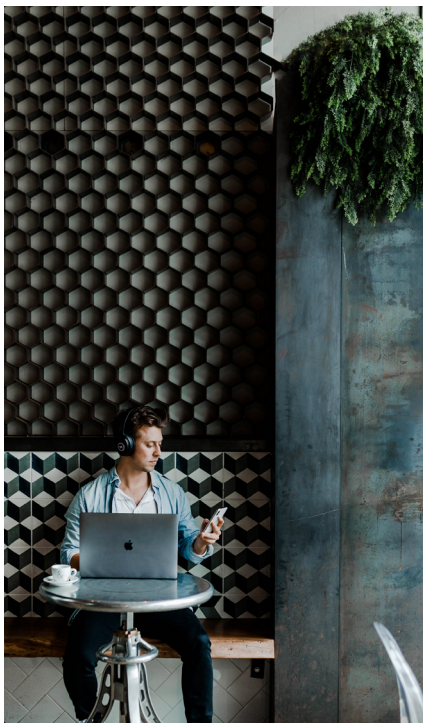
menos 700.000 puestos de trabajo solo en la Unión Europea para 2030, gracias a los procesos de transformación del modelo productivo.

Por tanto, el rediseño de materiales y productos para una nueva economía circular también impulsaría la innovación en diferentes sectores de la economía.

Por último, cabe destacar que para que la apuesta por la economía circular sea realmente efectiva, se necesita de un respaldo institucional real a nivel normativo. Si bien es cierto que a nivel planetario ese proceso todavía dista mucho de ser una realidad, en el contexto europeo sí se puede afirmar que la apuesta por la economía circular es bastante firme.

Por ejemplo, la Comisión Europea presentó en marzo de 2020 el plan de acción para la Economía Circular que además de promover el diseño de productos más sostenibles y la reducción de residuo, potencia los procesos de participación y empoderamiento de los ciudadanos a través de iniciativas como el "derecho a reparar". En esta normativa, como no podía ser de otra forma, se presta especial atención a los sectores intensivos en recursos, como la electrónica y las TIC.

Como continuación, en febrero de 2021 se votó en el Parlamento Europeo el plan de acción sobre economía circular y demandó medidas adicionales para promulgar leyes más efectivas sobre reciclaje y la formulación de objetivos vinculantes para la reducción de la huella ecológica por el uso y consumo de materiales, que afectarían de manera directa al sector digital.



NOTA

En el año 2022, la Comisión dio a conocer el primer paquete de medidas para acelerar la transición hacia una economía circular, además de proponer nuevas normas sobre envases para toda la Unión Europea, que se basan en propuestas de eco-diseño. Además, desde la Comisión se propone también la transición a elementos de base biológica y biodegradables, como los bio-plásticos.

Así que, como vemos, la economía circular es una propuesta transformadora con una base muy real, ya que el apoyo institucional y normativo a nivel europeo garantiza una base sólida para iniciar el cambio de modelo productivo, que por supuesto deberá verse refrendada en los casos particulares de cada país y los comportamientos sociales para garantizar la transición a un modelo más sostenible.

Saber más

Comisión Europea (2023) Plan de Acción de Economía Circular. *e.digitall.org.es/economia-circular*

Latouche, Serge (2009) Pequeño tratado del decrecimiento sereno. Icaria. *e.digitall.org.es/icaria*

Latouche, Serge (2022) Introducción al decrecimiento. Popular. *e.digitall.org.es/decrecimiento*

Parlamento Europeo (2023) Economía circular: definición, importancia y beneficios. *e.digitall.org.es/beneficions-economiacircular*

Parlamento Europeo (2022). Derecho a reparar: el PE quiere productos más duraderos y fáciles de reparar. *e.digitall.org.es/derecho-reparar*

Research & Degrowth (Investigación y Decrecimiento) (2023). *degrowth.org*

DigitAll

Formación en
Competencias
Digitales

https://www.digitall.org.es/

DigitAll

Coordinación General

Universidad de Castilla-La Mancha
Carlos González Morcillo
Francisco Parreño Torres

Coordinadores de área

Área 1. Búsqueda y gestión de información y datos

Universidad de Zaragoza
Francisco Javier Fabra Caro

Área 2. Comunicación y colaboración

Universidad de Sevilla
Francisco Javier Fabra Caro
Francisco de Asís Gómez Rodríguez
José Mariano González Romano
Juan Ramón Lacalle Remigio
Julio Cabero Almenara
María Ángeles Borrueco Rosa

Área 3. Creación de contenidos digitales

Universidad de Castilla-La Mancha
David Vallejo Fernández
Javier Alonso Albusac Jiménez
José Jesús Castro Sánchez

Área 4. Seguridad

Universidade da Coruña
Ana M. Peña Cabanas
José Antonio García Naya
Manuel García Torre

Área 5. Resolución de problemas

UNED
Jesús González Boticario

Coordinadores de nivel

Nivel A1

Universidad de Zaragoza
Ana Lucía Esteban Sánchez
Francisco Javier Fabra Caro

Nivel A2

Universidad de Córdoba
Juan Antonio Romero del Castillo
Sebastián Rubio García

Nivel B1

Universidad de Sevilla
Francisco de Asís Gómez Rodríguez
José Mariano González Romano
Juan Ramón Lacalle Remigio
Montserrat Argandoña Bertran

Nivel B2

Universidad de Castilla-La Mancha
María del Carmen Carrión Espinosa
Rafael Casado González
Víctor Manuel Ruiz Penichet

Nivel C1

UNED
Antonio Galisteo del Valle

Nivel C2

UNED
Antonio Galisteo del Valle

Maquetación

Universidad de Salamanca
Fernando De la Prieta Pintado
Pilar Vega Pérez
Sara Alejandra Labrador Martín

Creadores de contenido

Área 1. Búsqueda y gestión de información y datos

1.1 Navegar, buscar y filtrar datos, información y contenidos digitales

Universidad de Huelva
Ana Duarte Hueros (coord.)
Arantxa Vizcaíno Verdú
Carmen González Castillo
Dieter R. Fuentes Cancell
Elisabetta Brandi
José Antonio Alfonso Sánchez
José Ignacio Aguaded
Mónica Bonilla del Río
Odiel Estrada Molina
Tomás de J. Mateo Sanguino (coord.)

1.2 Evaluar datos, información y contenidos digitales

Universidad de Zaragoza
Ana Belén Martínez Martínez
Ana María López Torres
Francisco Javier Fabra Caro
José Antonio Simón Lázaro
Laura Bordonaba Plou
María Sol Arqued Ribes
Raquel Trillo Lado

1.3 Gestión de datos, información y contenidos digitales

Universidad de Zaragoza
Ana Belén Martínez Martínez
Francisco Javier Fabra Caro
Gregorio de Miguel Casado
Sergio Ilarri Artigas

Área 2. Comunicación y colaboración

2.1 Interactuar a través de tecnología digitales

Iseazy

2.2 Compartir a través de tecnologías digitales

Universidad de Sevilla
Alién García Hernández
Daniel Agüera García
Jonatan Castaño Muñoz
José Candón Mena
José Luis Guisado Lizar

2.3 Participación ciudadana a través de las tecnologías digitales

Universidad de Sevilla
Ana Mancera Rueda
Félix Biscarri Triviño
Francisco de Asís Gómez Rodríguez
Jorge Ruiz Morales
José Manuel Sánchez García
Juan Pablo Mora Gutiérrez
Manuel Ortigueira Sánchez
Raúl Gómez Bizcocho

2.4 Colaboración a través de las tecnologías digitales

Universidad de Sevilla
Belén Vega Márquez
David Vila Viñas
Francisco de Asís Gómez Rodríguez
Julio Barroso Osuna
María Puig Gutiérrez
Miguel Ángel Olivero González
Óscar Manuel Gallego Pérez
Paula Marcelo Martínez

2.5 Comportamiento en la red

Universidad de Sevilla
Ana Mancera Rueda
Eva Mateos Núñez
Juan Pablo Mora Gutiérrez
Óscar Manuel Gallego Pérez

2.6 Gestión de la identidad digital

Iseazy

Área 3. Creación de contenidos digitales

3.1 Desarrollo de contenidos

Universidad de Castilla-La Mancha
Carlos Alberto Castillo Sarmiento
Diego Cordero Contreras
Inmaculada Ballesteros Yáñez
José Ramón Rodríguez Rodríguez
Rubén Grande Muñoz

3.2 Integración y reelaboración de contenido digital

Universidad de Castilla-La Mancha
José Ángel Martín Baos
Julio Alberto López Gómez
Ricardo García Ródenas

3.3 Derechos de autor (copyright) y licencias de propiedad intelectual

Universidad de Castilla-La Mancha
Gabriela Raquel Gallicchio Platino
Gerardo Alain Marquet García

3.4 Programación

Universidad de Castilla-La Mancha
Carmen Lacave Rodero
David Vallejo Fernández
Javier Alonso Albusac Jiménez
Jesús Serrano Guerrero
Santiago Sánchez Sobrino
Vanesa Herrera Tirado

Área 4. Seguridad

4.1 Protección de dispositivos

Universidade da Coruña
Antonio Daniel López Rivas
José Manuel Vázquez Naya
Martiño Rivera Dourado
Rubén Pérez Jove

4.2 Protección de datos personales y privacidad

Universidad de Córdoba
Aida Gema de Haro García
Ezequiel Herruzo Gómez
Francisco José Madrid Cuevas
José Manuel Palomares Muñoz
Juan Antonio Romero del Castillo
Manuel Izquierdo Carrasco

4.3 Protección de la salud y del bienestar

Universidade da Coruña
Javier Pereira Loureiro
Laura Nieto Riveiro
Laura Rodríguez Gesto
Manuel Lagos Rodríguez
María Betania Groba González
María del Carmen Miranda Duro
Nereida María Canosa Domínguez
Patricia Concheiro Moscoso
Thais Pousada García

4.4 Protección medioambiental

Universidad de Córdoba
Alberto Membrillo del Pozo
Alicia Jurado López
Luis Sánchez Vázquez
María Victoria Gil Cerezo

Área 5. Resolución de problemas

5.1 Resolución de problemas técnicos

Iseazy

5.2 Identificación de necesidades y respuestas tecnológicas

Iseazy

5.3 Uso creativo de la tecnología digital

Iseazy

5.4 Identificar lagunas en las competencias digitales

Iseazy

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia