DigitAll

Formació en Competències Digitals

4

Seguretat

DigitAll

Formació en competències digitals

Seguretat

Nivell B2

ÍNDEX

DigitAll

Seguretat

4.1 PROTECCIÓ DE DISPOSITIUS

Seguretat

Nivell B2 4.1 Protecció de dispositius

Com implantar un SGSI: metodologies

Com implantar un SGSI: metodologies

Gestió de la seguretat de la informació

La gestió de la seguretat de la informació es refereix a la protecció dels actius d'informació d'una organització per garantir la seva confidencialitat, integritat i disponibilitat. Normalment consisteix en un conjunt de processos, polítiques, procediments i mesures tècniques dissenyades per identificar, avaluar i mitigar els riscos de seguretat de la informació.

GESTIÓ DE RISCOS: ACTIU, PROBABILITAT I IMPACTE

La gestió de riscos és el procés d'identificar, analitzar i avaluar els riscos potencials que poden afectar una organització i implementar les mesures preventives i de mitigació oportunes.

e.digitall.org.es/A4C41B1V02

SISTEMA DE GESTIÓ DE LA SEGURETAT DE LA INFORMACIÓ (SGSI): APLICANT CONTROLS ALS RISCOS

Aplicar controls als riscos suposa el següent pas a la gestió de riscos en el desenvolupament d'un sistema de gestió de seguretat de la informació.

e.digitall.org.es/A4C41B2V02

L'objectiu principal de la gestió de la seguretat de la informació és assegurar que la informació es mantingui segura i protegida contra amenaces internes i externes. Per facilitar el seu procés d'implementació en una organització és recomanable fer ús d'alguna de les metodologies existents.

NOTA

Metodologia de gestió de la seguretat de la informació: és un enfocament estructurat i sistemàtic utilitzat per planificar, implementar, controlar i millorar la seguretat de la informació en una organització.

Saber-ne més

La gestió de la seguretat de la informació és essencial en l'entorn actual, on la informació juga un paper crític en les operacions empresarials i en la confiança del client.

Metodologies de gestió de la seguretat de la informació

Existeixen diverses metodologies de gestió de la seguretat de la informació, cadascuna amb enfocaments i característiques específiques. L'elecció de l'una o l'altra depèn de les necessitats i requisits específics de cada organització, així com dels estàndards i regulacions que hagin de complir-se en la seva indústria.

Una de les característiques més valorades a l'hora de triar una metodologia és la possibilitat d'obtenir una certificació, ja que habitualment representa un valor afegit per a les organitzacions.

ISO 27001

La norma **ISO/IEC 27001** (*e.digitall.org.es/iso-27001*) és una norma internacionalment reconeguda que estableix els requisits per establir, implementar, mantenir i millorar un sistema de gestió de la seguretat de la informació (SGSI) en una organització. Va ser desenvolupada per l'Organització Internacional de Normalització (ISO) i la Comissió Electrotècnica Internacional (IEC).

Estableix un enfocament basat en el risc per a la gestió de la seguretat de la informació, la qual cosa implica identificar els riscos, avaluar el seu impacte i probabilitat, i prendre mesures per a mitigar-los.

Aquesta norma es basa en el cicle de millora continu conegut com a Cicle de Deming o cicle PDCA (Pla-Do-Check-Act) que segueix un enfocament iteratiu i cíclic.

Les principals fortaleses de l'ISO 27001 que la converteixen en una de les metodologies de gestió de seguretat de la informació més utilitzada són:

- **Reconeixement i confiança basada en la seva certificació:** obtenir la certificació demostra el compromís d'una organització amb la seguretat de la informació i brinda confiança als clients, socis comercials i parts interessades.

- **Enfocament integral:** aborda de manera integral la gestió de la seguretat de la informació en una organització, no es limita únicament a aspectes tècnics, sinó que també considera aspectes organitzatius, legals i humans.

- **Flexibilitat i adaptabilitat:** es pot adaptar a les necessitats i requisits específics de cada organització permetent establir controls i mesures de seguretat personalitzats, d'acord amb els riscos i el context particular de l'organització.

Un exemple de la importància que té l'ISO 27001 al nostre país és el fet que les administracions públiques espanyoles es basessin en aquesta metodologia, adaptant-la i complementant-la amb requisits i directrius addicionals específiques per a les administracions públiques a Espanya i donant lloc així a la creació de l'Esquema Nacional de Seguretat.

Saber-ne més

L'Esquema Nacional de Seguretat (ENS) és un marc de referència que estableix els principis i requisits mínims de seguretat de la informació per a les administracions públiques a Espanya.

Altres metodologies

Encara que l'ISO 27001 podem dir que és la metodologia més usada a escala global és important comentar altres existents.

NIST SP 800-53

El NIST SP 800-53 és un conjunt d'estàndards i guies desenvolupat per l'Institut Nacional d'Estàndards i Tecnologia (NIST) dels Estats Units. S'utilitza com a referència per a la gestió de la seguretat de la informació en sistemes federals d'informació d'agències governamentals als Estats Units.

El NIST SP 800-53 proporciona un ampli conjunt de controls i salvaguardes de seguretat i el seu enfocament es basa en la gestió de riscos i en l'adaptació dels controls a les necessitats i característiques de cada organització.

És important destacar que aquest conjunt d'estàndards ha d'entendre's com un conjunt de bones pràctiques i, per tant, no es correspon amb un marc de certificació.

COBIT

COBIT (*Control Objectives for Information and Related Technologies*) és un marc de referència desenvolupat per ISACA (*Information Systems Audit and Control Association*) que proporciona un conjunt de millors pràctiques per a la governança i gestió de tecnologies de la informació (TU) en les organitzacions, i dins d'aquest marc, la seguretat de la informació és un dels aspectes fonamentals.

Un dels principals objectius de COBIT és garantir el compliment dels requisits legals i reguladors.

Proporciona un marc estructurat, objectius de control i pràctiques recomanades per ajudar les organitzacions a establir i mantenir un nivell adequat de seguretat de la informació en el per mantenir les seves operacions i aconseguir els seus objectius estratègics.

Igual que la NIST SP 800-53 aquest marc de referència tampoc no és certificable.

Seguretat

Nivell B2 4.1 Protecció del dispositiu

Utilitats per xifrar la informació

Utilitats per xifrar la informació

En aquesta formació, ja s'han tractat els temes com el xifratge de la informació i, més detalladament, el xifratge d'arxius i dispositius. Xifrar la informació garanteix la protecció de la confidencialitat, per la qual cosa és essencial tenir a mà utilitats que ens permetin xifrar i desxifrar els nostres arxius i treballar de la manera més còmoda i segura possible. A continuació, veurem diferents utilitats per al xifratge de discs durs i per al xifratge d'arxius.

XIFRATGE D'ARXIUS I DISPOSITIUS

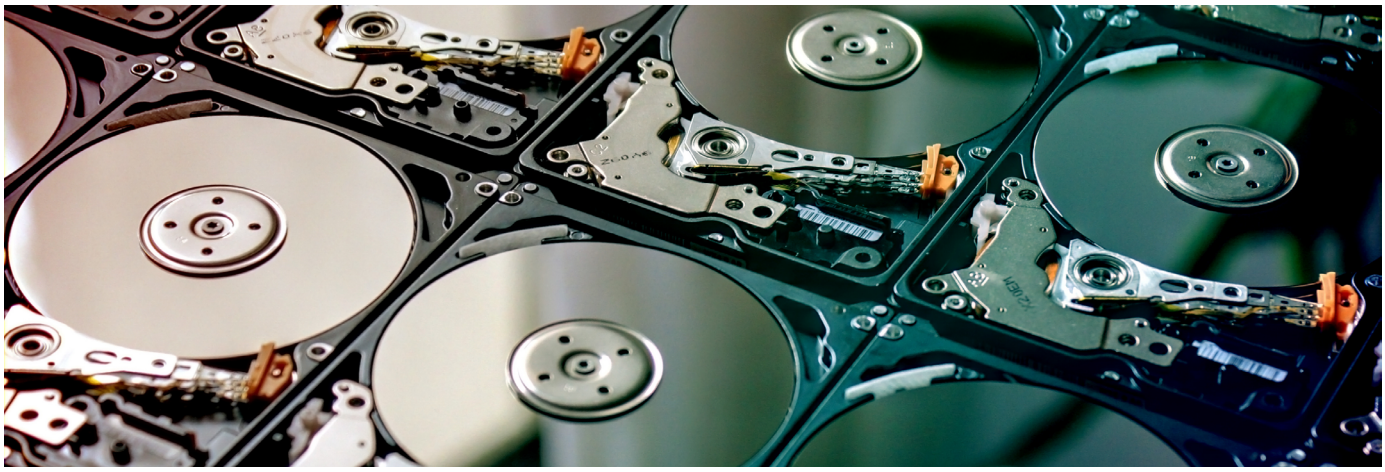
El xifratge d'arxius i dispositius garanteix la confidencialitat de la informació en repòs. Xifrar el disc dur del dispositiu protegeix tota la informació emmagatzemada, mentre que el xifratge d'arxius, protegeix els fitxers de manera independent.

e.digitall.org.es/A4C41B1V05

Xifrat de discs durs

La primera opció per xifrar la informació en repòs és xifrar el dispositiu. En concret, és possible xifrar el disc dur, que emmagatzema tota la informació, tant del sistema operatiu com la informació personal que gestioni l'usuari.

És important recordar que, per al xifratge de dispositius basat en contrasenya, si es perd la contrasenya, es perd accés a totes les dades xifrades.

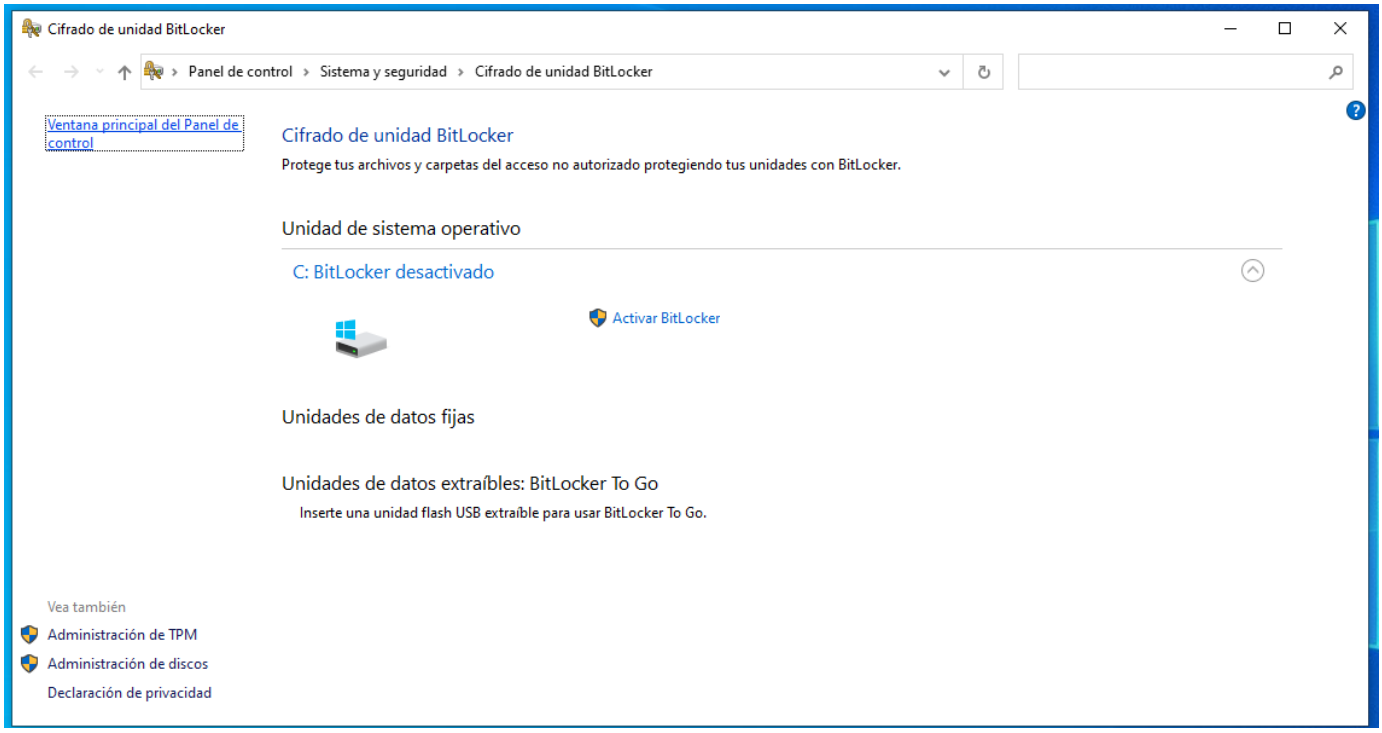


A Windows: BitLocker

L'opció per a sistemes operatius Windows més utilitzada és BitLocker, inclosa en el mateix sistema operatiu. D'aquesta manera, en iniciar Windows, BitLocker desxifrarà el disc dur per poder arrencar i permetre l'accés a la informació.

A més, permet la integració amb el xip Trusted-Platform-Moduli (TPM), que molts PCs moderns inclouen. D'aquesta manera, si es clona la informació o s'intenta accedir al disc dur, la informació estarà xifrada.

La configuració d'aquesta solució és molt senzilla. Si no es disposa d'un xip TPM, es pot establir una contrasenya d'accés, que haurà de ser introduïda en l'arrencada del dispositiu, abans d'iniciar Windows.



Imatge 1. Gestió del xifratge de disc amb Bitlocker.

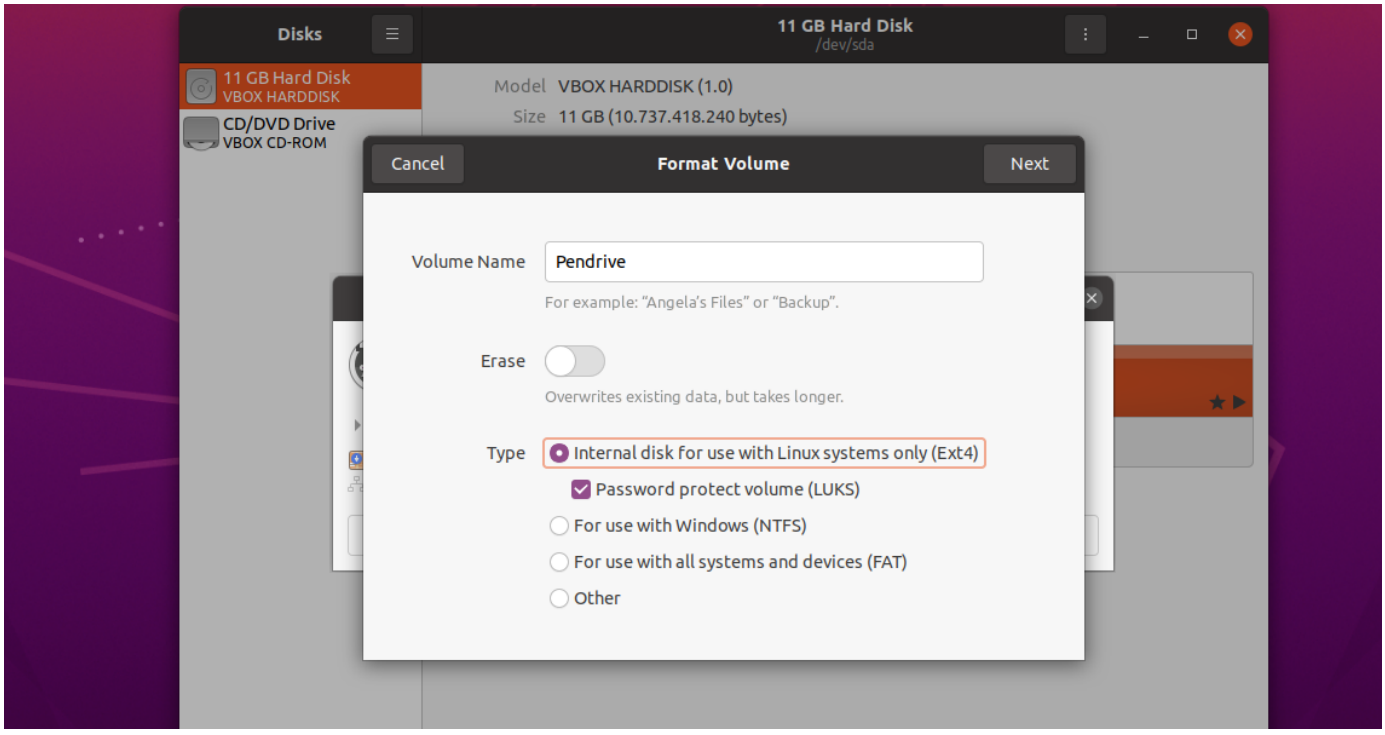
Saber-ne més

Pots consultar com activar el xifratge de dispositiu des de la pàgina de Suport de Microsoft: *e.digitall.org.es/activar-cifrado*

A Linux: LUKS

Igual que BitLocker per a Windows, LUKS permet xifrar discs durs en Linux. Aquesta solució s'utilitza majoritàriament utilitzant una contrasenya per xifrar un disc dur. És fàcil de configurar durant la instal·lació d'alguns sistemes operatius basats a Linux, com Ubuntu o Manjaro Linux.

A més, tenim l'opció de xifrar qualsevol mena d'unitat d'emmagatzematge. Per exemple, si tenim una memòria USB, podem xifrar-la amb l'ajuda del gestor de discs. D'aquesta manera, quan s'insereixi en l'equip, haurem de proporcionar la contrasenya de xifratge per poder accedir al contingut. És important recordar que aquesta opció no ofereix cap manera de recuperar-ho. Si oblides la contrasenya de xifratge, és possible que perdis accés a la informació.



Imatge 2. Xifratge d'una unitat extraible amb LUKS a Linux.

En macOS: FileVault

Si s'utilitza un dispositiu amb macOS, Apple proporciona en el seu sistema operatiu una solució integrada per al xifratge del disc dur. De la mateixa manera que Windows, aquesta opció es pot activar i desactivar en qualsevol moment. Pot requerir l'ús d'una contrasenya de xifratge, i ofereix alguna opció per a la recuperació en cas d'oblidar-se de la contrasenya de xifratge del dispositiu.

Imatge 3. Configuració de FileVault a macOS. (Font: *e.digitall.org.es/filevault*)

Saber-ne més

Pots consultar al web de Suport d'Apple com xifrar el disc d'arrencada a Mac: *e.digitall.org.es/filevault-mac*

Xifratge d'arxius

Pot ser que alguna de les opcions de xifratge de disc no s'adeqüi a algun dels dispositius o que l'usuari no vulgui xifrar tota la informació. Per això, existeixen altres eines que permeten el xifratge de part de la informació. A continuació, s'inclouen algunes de les més conegudes.

Veracrypt

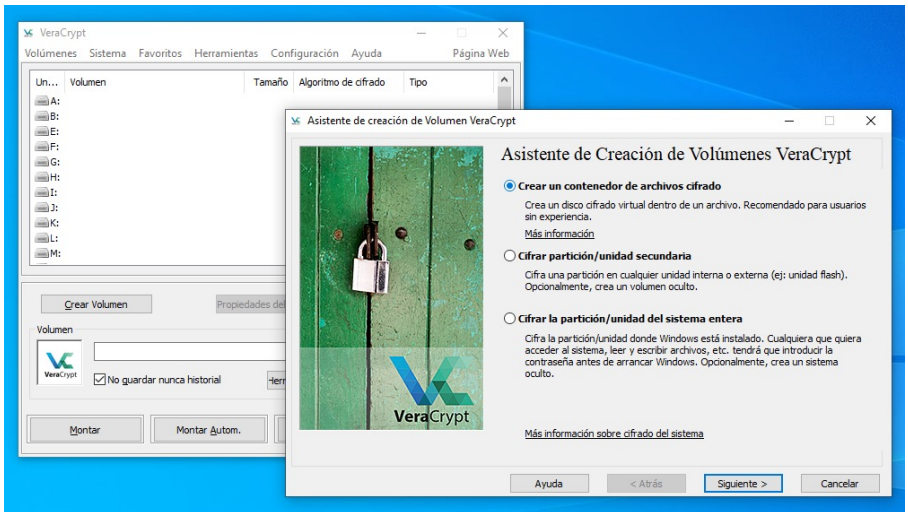
El programari Veracrypt és programari de codi obert que funciona a Windows, macOS i Linux. Permet xifrar uns certs arxius creant un "volum" virtual. D'aquesta manera, guarda un arxiu o volum xifrat, que només es pot accedir desxifrant-lo amb Veracrypt i una contrasenya de xifratge.

Saber-ne més

Per obtenir Veracrypt, pots descarregar l'executable des de la pàgina de descàrregues de la pàgina oficial *e.digitall.org.es/veracrypt.*

Una vegada desxifrat, el volum es pot muntar i utilitzar com una carpeta normal del sistema de fitxers. En tancar-la amb Veracrypt, es torna a xifrar tota la informació. El volum xifrat de Veracrypt es pot copiar i compartir com un arxiu normal.

A més, Veracrypt també permet el xifratge de discs durs i unitats d'emmagatzematge extraïbles, de la mateixa manera que LUKS.



Imatge 4. Creació d'un volum o contenidor d'arxius xifrats a Veracrypt des de Windows.

Cryptomator

Similar a Veracrypt, Cryptomator permet crear “voltes” o contenidors xifrats. La interfície permet un ús molt senzill per a l’usuari. El codi de Cryptomator és obert, i la descàrrega des de la web permet el seu ús gratuït.

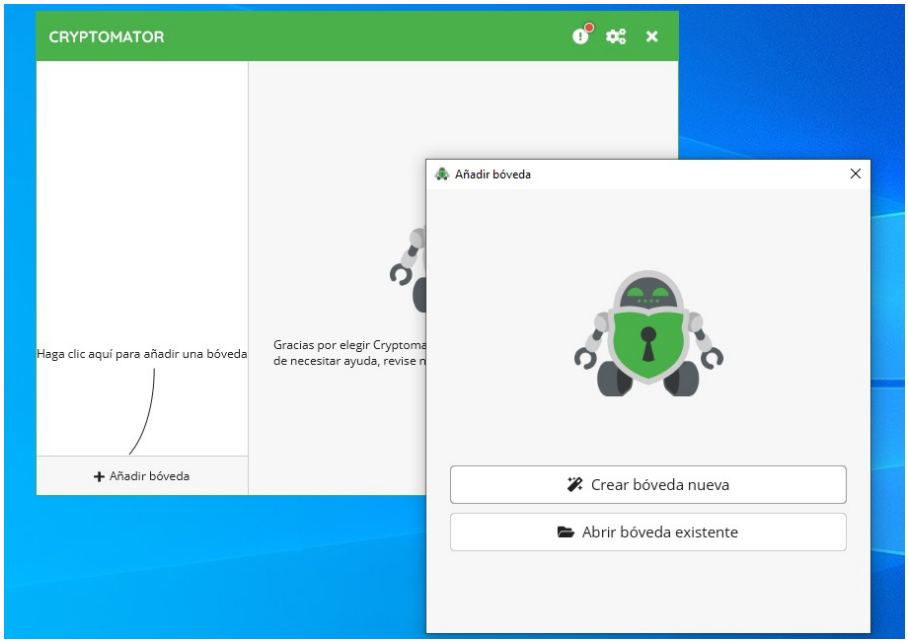


Imagen 5. Creació d’una bòveda o contenidor xifrat amb Cryptomator des de Windows.

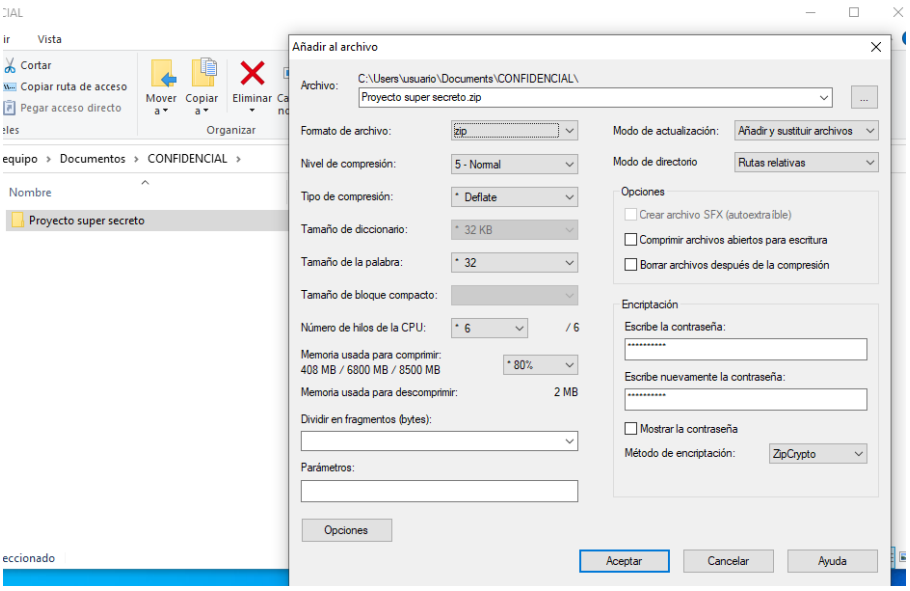
Saber-ne més

Per provar Cryptomator, pots descarregar-ho des de la seva pàgina web oficial: *cryptomator.org/downloads*

7-zip

Una de les opcions més versàtils per al xifratge d’arxius en qualsevol sistema operatiu és utilitzar 7-zip. Aquesta eina, encara que està pensada per a la compressió d’arxius, permet crear carpetes comprimides ZIP xifrades amb contrasenya. Així, es poden emmagatzemar o compartir arxius ZIP que requereixin una contrasenya per a ser desxifrats i descomprimits.

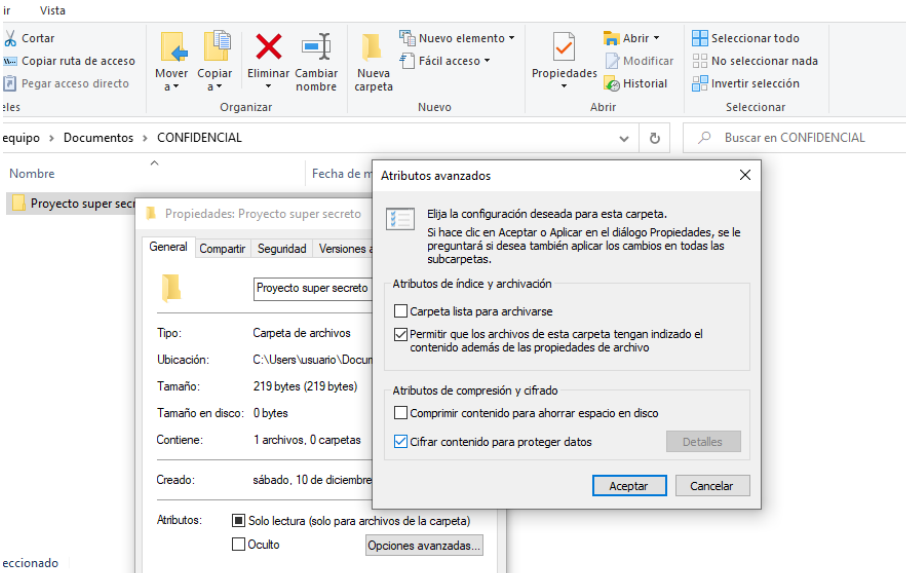
Quan no es coneix tal contrasenya, no es pot accedir al contingut dels arxius dins del ZIP.



Imatge 6. Xifratge i compressió d'una carpeta amb 7-zip des de Windows.

Windows EFS

Finalment, Windows ofereix la possibilitat de xifrar arxius des del mateix sistema operatiu. És important tenir en compte que aquests arxius només es podran desxifrar des del mateix dispositiu. Això pot ser útil per protegir uns certs arxius en el dispositiu, sense necessitar xifrar tot el disc dur.



Imatge 7. Xifratge d'una carpeta des de Windows amb EFS.

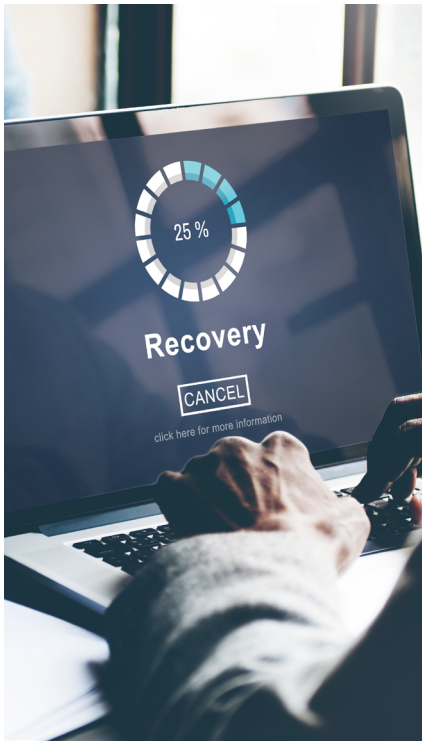
Seguretat

Nivell B2 4.1 Protecció de dispositius

Utilitats per fer còpies de seguretat

Utilitats per fer còpies de seguretat

Una còpia de seguretat és una còpia de les dades que es guarda en un lloc diferent de l'original. Les còpies de seguretat s'utilitzen per protegir les dades davant la pèrdua o el mal accidental. Per exemple, si s'esborra un arxiu per error, es pot restaurar des de la còpia de seguretat. O, si el disc dur d'un ordinador falla, es poden restaurar les dades des de la còpia de seguretat en un altre disc dur.



QUAN TOT FALLA: CÒPIES DE SEGURETAT

Les còpies de seguretat s'han de fer amb freqüència, en llocs diferents dels originals. Per a informació important, a més, s'ha de seguir el principi 3, 2 1: tres còpies, en dos llocs diferents i una desconnectada de la xarxa.

e.digitall.org.es/A4C41B1V09

Hi ha molts tipus diferents de còpies de seguretat, incloent-hi còpies de seguretat locals, còpies de seguretat en el núvol i còpies de seguretat híbrides. Les còpies de seguretat locals es guarden en un dispositiu local, com un disc dur extern o un USB. També existeix l'opció de desar les còpies de seguretat en un servei al núvol. A continuació, es detalla com fer còpies de seguretat depenent del sistema operatiu que utilitzes.

Còpia de seguretat a Windows

En un equip Windows, podem fer còpies de seguretat d'una manera molt senzilla utilitzant l'eina que porta integrada el sistema operatiu. Per exemple, els passos a Windows 11 són:

1 | Fem clic en el botó d'"Inici" i seleccionam "Configuració".
2 | Una vegada aquí, accedim a l'apartat "Actualització i seguretat" i després a "Còpia de seguretat".
3 | Seleccionam "Agregar una unitat de còpia de seguretat".
4 | Triam la unitat d'emmagatzematge en la qual desitgem desar la còpia de seguretat. Podem triar un disc extern o USB, o bé el servei del núvol com OneDrive.

5 | En fer clic a "Següent", ens permet seleccionar els arxius i carpetes per incloure en la còpia de seguretat.
6 | Executam "Iniciar còpia de seguretat" i esperam.
7 | Finalment, verificam que els arxius estan disponibles a la ubicació que hem seleccionat.

A més, aquestes còpies de seguretat es poden programar perquè s'executin periòdicament. Per això, pots seleccionar "Programar" en el procés anterior. Per restaurar una còpia de seguretat, podem accedir al menú de "Còpia de seguretat" i seleccionar "Restaurar arxius a partir d'una còpia de seguretat".

Còpia de seguretat a macOS

En sistemes operatius macOS existeixen diferents alternatives. Usant l'eina integrada **Time Machine**. Per emprar-la, és necessari tenir un disc extern connectat o tenir un compte al núvol com iCloud. Els passos són molt senzills:

1 | Obrim l'aplicació "Time Machine" al Mac, des de la carpeta "Aplicacions".
2 | Seleccionam "Seleccionar disc de còpia de seguretat" i triam el dispositiu d'emmagatzematge que volem utilitzar per desar la còpia de seguretat.
3 | Esperam que faci el procés i verifiquem que els documents van ser copiats. Després d'aquest punt, Time Machine continuarà fent còpies de seguretat automàtiques de manera periòdica.

Utilitzant aquestes còpies de seguretat, és possible:

- **Restaurar un arxiu o carpeta.** Per això, pots accedir a "Time Machine" i cercar l'arxiu o carpeta per restaurar-lo.
- **Restaurar des del núvol.** Si has desat els teus arxius al núvol d'Apple, pots accedir-hi des d'iCloud Drive, descarregant l'arxiu o carpeta que vols recuperar.
- **Restaurar una còpia de tot l'ordinador.** Per això, hem d'apagar el dispositiu i encendre'l mantenint premudes les tecles "cmd + R". En la finestra d'"Utilitats de macOS" apareixerà un menú guiat "Restaurar des d'una còpia de seguretat de Time Machine".

Còpia de seguretat a Android

Els dispositius mòbils Android també permeten la configuració de còpies de seguretat. Els més actuals ja inclouen l'aplicació de Google One. Una vegada hem iniciat sessió a Google a aquesta aplicació:

1 | Seleccionam les dades que desitgem copiar, com a contactes, fotos, vídeos, calendaris, etc.
2 | Fem clic en "Còpia de seguretat" en la pàgina principal de l'aplicació.
3 | Una vegada seleccionat, fem clic en el botó "Crear còpia de seguretat ara".
4 | Quan acabi el procés, podem accedir a tot des del servei *one.google.com*

Per restaurar una còpia, en un dispositiu nou Android pots iniciar la sessió amb Google. De nou, en l'aplicació de Google One, podem accedir a "Còpia de seguretat" i a "Restaurar".

Còpia de seguretat en iOS

La còpia de seguretat en un mòbil iOS es pot fer de diverses formes. La més senzilla és emprar el núvol d'Apple, iCloud:

1 | Des de la "Configuració" de l'iPhone, accedim al primer apartat on apareix el nostre nom, i després a "iCloud".
2 | Seleccionam "Còpia en iCloud" i a continuació, "Fer còpia de seguretat ara".

Amb aquesta opció, es desaran totes les dades en iCloud. Si prefereixes utilitzar el teu ordinador, pots fer-ho. A Windows, has d'utilitzar l'aplicació iTunes:

1 | Connecta el teu iPhone a l'ordinador usant un cable USB.
2 | Obre "iTunes", o instal·la-ho des del web d'Apple.
3 | A la cantonada superior esquerra, fes clic a la icona d'iPhone.
4 | Selecciona "Resum" i "Fer una còpia de seguretat ara".

Si el teu ordinador és Mac:

1 | Connecta el teu iPhone a l'ordinador usant un cable USB.
2 | Obre "iTunes", o instal·la-ho des del web d'Apple.
3 | A la cantonada superior esquerra, fes clic a la icona d'iPhone.
4 | Selecciona "Resum" i "Fer una còpia de seguretat ara".

Depenent de quina estratègia hagis utilitzat, cadascuna de les eines permet restaurar de manera senzilla la còpia de seguretat. Per això, segueix el procés anterior, però selecciona l'opció de restauració.

Conclusió i recomanacions

Com hem vist, cada sistema operatiu té les seves eines pròpies. Aquí, hem tractat els passos a seguir amb les utilitats integrades en el sistema. No obstant això, existeixen moltes altres eines. És molt important recordar que hem d'utilitzar programari de còpia de seguretat de confiança, per evitar pèrdues de dades i garantir una recuperació eficient.

A més, és important realitzar les còpies de seguretat amb freqüència i emmagatzemar-les en llocs segurs. Idealment, utilitzar còpies de seguretat xifrades. Finalment, és una bona pràctica assegurar-se de la bona salut de la còpia de seguretat, provant de restaurar o comprovant la seva integritat.

DigitAll

Seguretat

4.2
PROTECCIÓ DE LES DADES PERSONALS I LA PRIVACITAT

Seguretat

Nivell B2 4.2 Protecció de les dades personals i la privacitat

Què és aquest correu electrònic?

Què és aquest correu electrònic?

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.

Què és aquest correu electrònic? Una comunicació d'una violació de la seguretat

Un dels deures del responsable del tractament de dades personals és garantir la seva seguretat, això és, en essència, garantir la confidencialitat, integritat, disponibilitat i resiliència permanents dels sistemes i serveis de tractament. Amb aquesta finalitat, ha d'adoptar les mesures tècniques i organitzatives apropiades.

No obstant això, a vegades, no s'implanten les mesures adequades o, malgrat això, no s'impedeix una vulneració d'aquesta seguretat. En particular, el creixement exponencial dels ciberatacs és alarmant.

En aquest context, el Reglament General de Protecció de Dades estableix que "quan sigui probable que la violació de la seguretat de les dades personals comporti un alt risc per als drets i llibertats de les persones físiques, el responsable del tractament la comunicarà a l'interessat". Aquest correu electrònic és un exemple d'una comunicació d'una violació de la seguretat.

La normativa exigeix que aquesta comunicació sigui feta sense dilació indeguda. El que es persegueix amb això és que l'afectat pugui adoptar les mesures oportunes al més aviat possible. Per ex., si han estat compromeses unes contrasenyes, que es canviïn immediatament; o si ha estat la numeració d'una targeta de crèdit, que es cancel·li. Observi's que en el cas el ciberatac s'ha produït l'11 d'abril, encara que el correu s'envia el dia 23, possiblement perquè no han estat afectades ni contrasenyes ni targetes bancàries –amb això no s'està dient que es comparteixi el criteri adoptat–, encara que sí números de compte bancari.

ATENCIÓ

L'interessat té dret al fet que el responsable del tractament l'informi de les violacions de seguretat de les dades personals que comportin un alt risc per als seus drets i llibertats.

ELS DEURES DELS SUBJECTES QUE MANEGEN DADES PERSONALS

e.digitall.org.es/A4C42A2V07

Contingut de la comunicació

El Reglament General de Protecció de Dades disposa que aquesta comunicació ha de tenir el següent contingut:

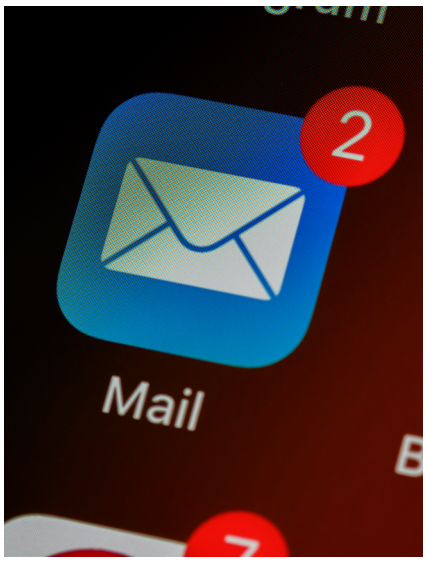
a) La descripció, amb llenguatge clar i senzill, de la naturalesa de la violació de la seguretat. En el cas s'explica que ha estat un ciberatac i en què ha consistit: "xifrar i fer inaccessibles els sistemes d'aquestes entitats amb la intenció d'impedir completament la seva activitat; així com a amenaçar de revelar dades dels interessats afectats" si no es paga un rescat. Resumidament, està descrivint un Ransomware amb robatori de dades personals. També s'informa que l'empresa no ha sofert pèrdua definitiva d'informació ni tampoc de cap dels seus aplicatius pel que els serveis no s'han vist afectats. O dit d'una altra manera, que hi havia una còpia de seguretat amb tota la informació que s'ha pogut restaurar.
b) El nom i les dades de contacte del delegat de protecció de dades o d'un altre punt de contacte en el qual pugui obtenir-se més informació. En el cas, es facilita informació genèrica sobre el Delegat de protecció de dades i es remet també a una pàgina web de preguntes i respostes sobre l'incident.
c) Les possibles conseqüències de la violació de la seguretat. En el cas, s'informa de dues qüestions:

- Que és possible que les dades personals s'hagin vist compromesos.
- Les dades potencialment afectades: nom, cognoms, adreça postal, telèfon, correu electrònic, DNI o equivalent, data de naixement, gènere, productes/serveis contractats, i número de compte bancari facilitat.

d) Les mesures adoptades o propostes pel responsable del tractament per posar remei a la violació i, si escau, per mitigar els possibles efectes negatius. En el cas es relaten les següents:

NOTA

Segons l'informe *Threat Landscape Report*, elaborat per S21sec, l'any 2022, Espanya ocupa el sisè lloc en el rànquing de les nacions que més ciberatacs sofreixen en el món. El 65% per ransomware



- Activació del pla d'actuació, amb la col·laboració d'una empresa externa experta en ciberseguretat.
- Notificació dels fets a l'Agència Espanyola de Protecció. Ha de tenir-se en compte que aquesta notificació és un deure per part del responsable del tractament, perquè la normativa prohibeix ocultar aquest tipus d'incidents.
- Denúncia davant el Cos Nacional de Policia, perquè aquest tipus de ciberatacs són constitutius de delicte.
- Rebuig del pagament del xantatge.

Suposats en els quals no és necessària aquesta comunicació

La normativa enumera una sèrie de supòsits en els quals no és necessari que l'entitat que sofreix una violació de seguretat la comuniqui als interessats:

a) El responsable del tractament ha adoptat mesures de protecció tècniques i organitzatives apropiades i aquestes mesures s'han aplicat a les dades personals afectades per la violació de la seguretat. En particular, es tracta d'aquelles mesures, com el xifratge, que facin inintel·ligibles les dades personals per a qualsevol persona no autoritzada.

b) S'han adoptat mesures ulteriors que garanteixin que no existeix probabilitat que es concreti el risc per als drets de l'interessat.

c) Suposi un esforç desproporcionat. En aquest cas, no es comunica a cada interessat (en el cas analitzat, era un correu electrònic dirigit a la concreta adreça de correu electrònic de cada potencial afectat), sinó que es fa una comunicació pública (premsa, Internet, televisió, etc.) en la qual s'informi també els interessats.

Saber-ne més

Grup de treball sobre protecció de dades de l'article 29. Directrius sobre la notificació de les violacions de la seguretat de les dades (WP 250). *e.digitall.org.es/articulo29*

DigitAll

Seguretat

4.3 PROTECCIÓ DE LA SALUT I EL BENESTAR

Seguretat

Nivell B2 4.3 Protecció de la salut i el benestar

Guia visual per fer un ús adequat del control parental

Guia visual per fer un ús adequat del control parental

En aquest document es pot consultar informació sobre què és i com es pot utilitzar el control parental. El control parental ofereix a les famílies amb nenes, nens i adolescents, nombrosos serveis com per exemple supervisar l'accés i l'ús que fan de la tecnologia. A més, en aquest document es pot observar un exemple de com configurar de manera àgil les principals utilitats del control parental a través de l'exemple de Maria i la seva família.

Control parental: generalitats

El control parental consisteix en un conjunt de mesures que permeten monitorar, restringir i limitar l'accés i la utilització d'Internet o de dispositius tecnològics, com a ordinadors, tauletes o mòbils.

Les eines de control parental es poden trobar en diferents serveis tecnològics per donar suport a la seguretat d'infants i adolescents quan utilitzen la tecnologia.

Aquestes eines poden ser útils per reduir riscos a mesura que els menors aprenen a desembolicar-se en Internet amb responsabilitat i autonomia. En cap cas substitueixen l'acompanyament o la supervisió que pot oferir una persona adulta, però poden constituir un suport en el seu procés d'aprenentatge digital.

⚠ ATENCIÓ

Les eines de control parental formen part de la mediació parental. No substitueixen la implicació i el diàleg quotidià amb els menors, sinó que donen suport a aquesta tasca de mediació parental. Perquè aquestes eines funcionin de manera reeixida, s'aconsella explicar als menors per què són necessàries. També és important adaptar les funcionalitats al seu nivell de desenvolupament i maduresa.

CONTROL PARENTAL

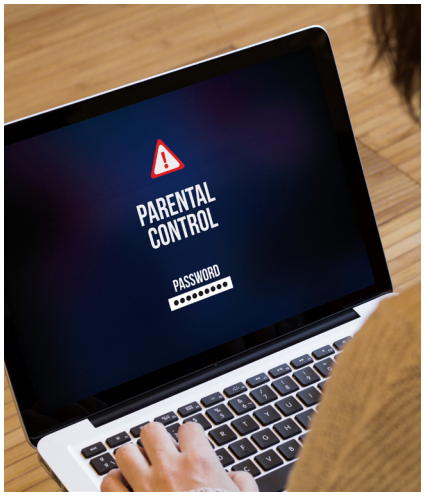
En aquest vídeo, s'introdueix el concepte de control parental i l'ús responsable d'aquestes eines en els dispositius mòbils d'infants i adolescents.

e.digitall.org.es/A4C43B2V03

S'identifiquen les següents funcions com a principals:

- **Filtratge de continguts:** serveix per bloquejar o restringir l'accés a uns certs continguts que es considerin inapropiats segons l'edat, generalment de caràcter sexual o violent. Aquesta funcionalitat pot incloure també la restricció de compres, el bloqueig de persones o el filtratge de llenguatge o paraules concretes.
- **Control de temps:** permet establir un horari específic o un temps màxim d'ús, per la qual cosa s'interromp la navegació i es bloqueja l'aplicació o el dispositiu en aconseguir determinada hora o límit de temps. També pot incloure l'emissió d'alarmes en cas d'ús excessiu de la tecnologia.
- **Supervisió d'activitat:** serveix per supervisar les pàgines que la/el menor ha visitat i les persones amb les quals ha contactat.
- **Geolocalització:** permet conèixer la posició en temps real i el recorregut previ del dispositiu.
- **Protecció de la configuració:** serveix per evitar canvis no desitjats en els mateixos ajustaments de control parental.

Les eines i funcions de control parental varien en cada país, i es poden trobar de manera general en els mateixos sistemes operatius d'ordinadors o dispositius mòbils, o de manera específica en determinades aplicacions, continguts digitals, jocs o xarxes socials. Així, alguns exemples que permeten funcionalitats de control parental són: sistemes operatius com Windows, iOS o Android; aplicacions específiques com Family Link (que s'explica a continuació); proveïdors de contingut com Netflix o YouTube; o xarxes socials com TikTok o Instagram.



CONTROL PARENTAL EN GRUP FAMILIAR

En aquest vídeo, s'amplia el concepte de control parental a un nivell més avançat. S'explica com controlar un grup familiar, mitjançant exemples en diferents dispositius per gestionar els continguts, les compres i el temps d'ús.

e.digitall.org.es/A4C43C1V04

Family Link: exemple de configuració bàsica d'eines de control parental

Com s'ha descrit en l'apartat anterior, les eines de control parental són nombroses i les podem trobar en diferents formats. La idea central d'aquest document és fer una aproximació a aquestes eines. Per això, es prendrà com a referència un exemple concret per conèixer les funcionalitats i la seva configuració; en aquest cas, Family Link de Google.

Family Link és una de les opcions d'eines de control parental que estan disponibles gratuïtament en el mercat tecnològic.

Figura 1. Font: Autoria pròpia.

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

L'enllaç anterior és la pàgina web oficial de Family Link de Google. Es pot trobar la informació completa sobre la plataforma i els enllaços que es necessiten per descarregar l'aplicació en els dispositius de la família.

Abans de la instal·lació de l'aplicació, és important assegurar-se que els dispositius que es configuraran són compatibles amb Family Link. Per això, podem consultar el sistema operatiu i la versió que tenen els mòbils, tant de la mare o del pare com dels menors.

⚠ ATENCIÓ

A la pàgina web de Family Link s'informa que és completament compatible amb versions iguals i superiors dels següents sistemes operatius, en funció del rol:

Dispositius per a infants: Android 7.0 i posteriors.
Dispositius per a pares i mares: Android 5.0 i posteriors; iOS 11 i posteriors; Chrome US 71 i posteriors.

Abans de començar amb les funcions del control parental, és important configurar aspectes generals perquè el programa entengui qui conforma la "família". A la Figura 1, s'observa una captura de Family Link i en la Figura 1, la configuració de "família".

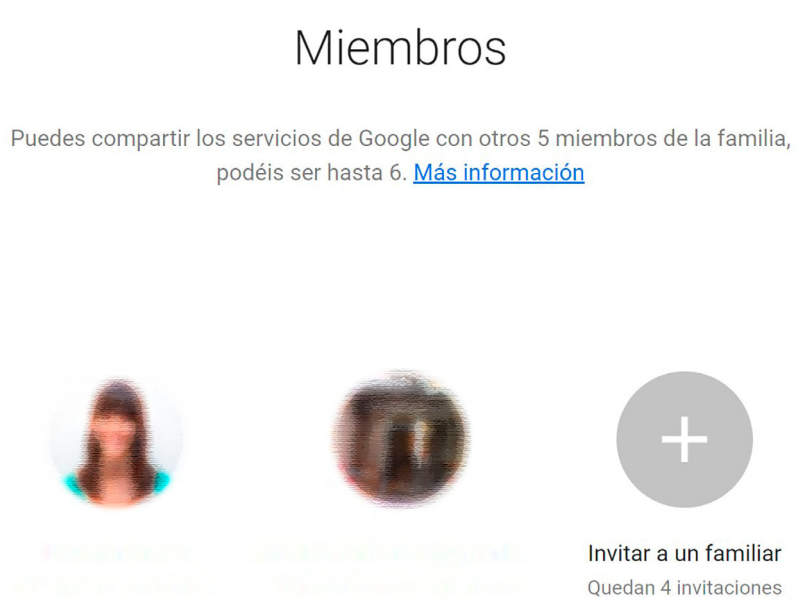


Figura 2. Font: Autoria pròpia.

La família d'aquest exemple es conforma pel pare i la mare d'una nina anomenada Maria. A la Figura 2, s'observa com es troba configurat el grup familiar, però sense la nina. A la Figura 3, s'ha afegit a Maria al grup familiar com un "membre de la família supervisat".

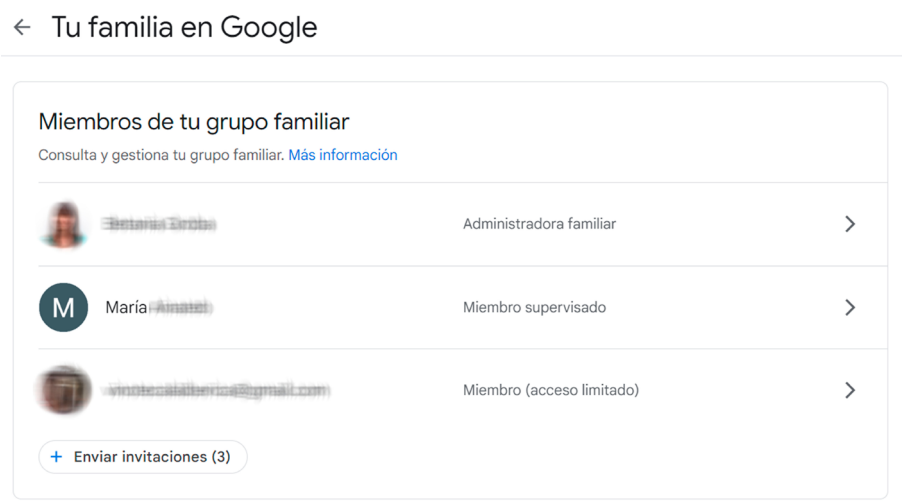


Figura 3. Font: Autoria pròpia.

Aquesta configuració de la "família" permet fer ús de Family Link i altres serveis de Google com: Google Calendar per a famílies, Keep per a famílies (notes i llistes), plans familiars de Youtube Premium, Biblioteca familiar de Google Play, Google Play Pass i Google One, entre altres.

Configuració del dispositiu de l'infant o adolescent

La configuració del dispositiu de l'infant o adolescent és senzilla i intuïtiva. Family Link ofereix instruccions detallades per guiar en el procés de configuració. En les següents pàgines s'ofereix una guia amb els aspectes més rellevants de la configuració.

El dispositiu utilitzat com a exemple és una tauleta amb sistema operatiu Android, per la qual cosa la configuració del control parental es fa a través d'"Ajustaments", tal com es mostra en la Figura 4; sent la seqüència de passos: (1) Fer clic a Configuració; (2) Fer clic a Google i (3) Fer clic a Controls parentals.

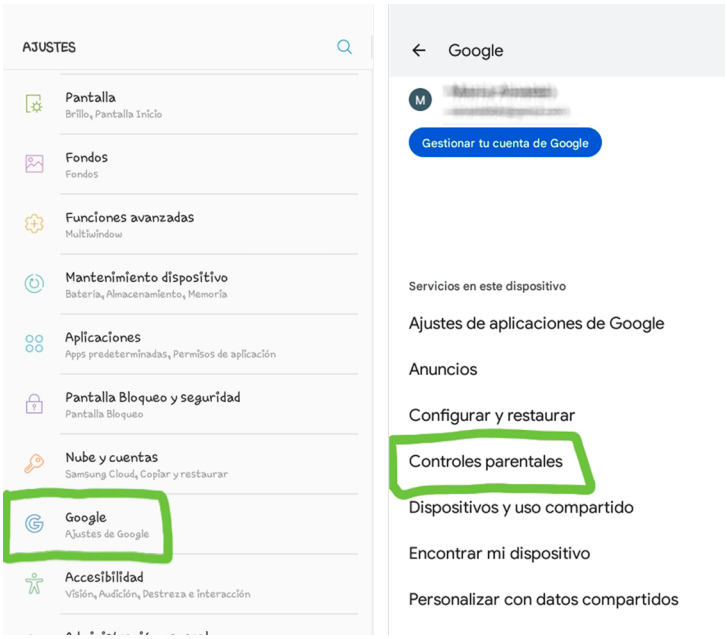


Figura 4. Font: Autoria pròpia.

Al dispositiu es van configurant diferents aspectes que augmenten la seguretat de Maria enemprar la seva tauleta:

- **Vincular el compte de Google de l'infant o adolescent amb la del pare o mare en un grup família.**

La clau per poder accedir a totes les opcions és fer de manera correcta la vinculació de l'infant o adolescent al grup familiar (tal com es mostrava en la Figura 3) i vincular el compte de correu electrònic de Maria amb les de la seva mare i el seu pare (Figura 5).

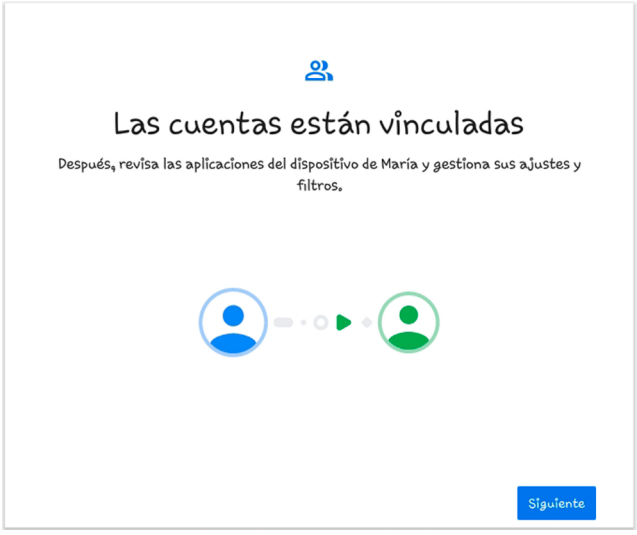


Figura 5. Font: Autoria pròpia.

- **Triar a quines aplicacions pot accedir l'infant o adolescent**

El dispositiu de Maria conté un nombre elevat d'aplicacions. Encara que la major part de les aplicacions han estat instal·lades perquè Maria pugui utilitzar-les, la seva mare i el seu pare poden decidir aquelles a les quals li volen donar accés. A la Figura 6, es mostra com es poden anar habilitant o bloquejant les aplicacions.

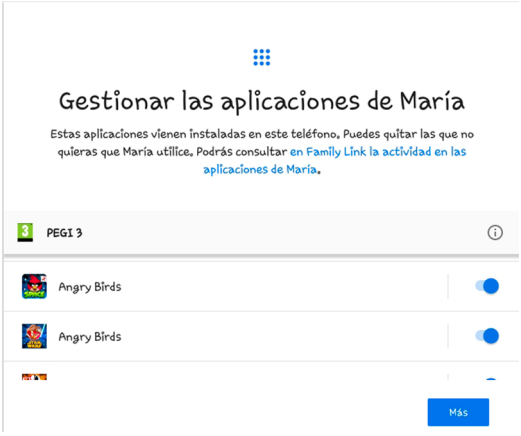


Figura 6. Font: Autoria pròpia.

A la Figura 7, es troben dos exemples de com el control parental classifica de manera automàtica les aplicacions i recomana el seu ús o no en funció de la classificació coneguda com a PEGI. Encara que aquestes recomanacions són útils, és important que mares i pares analitzin les aplicacions detalladament.

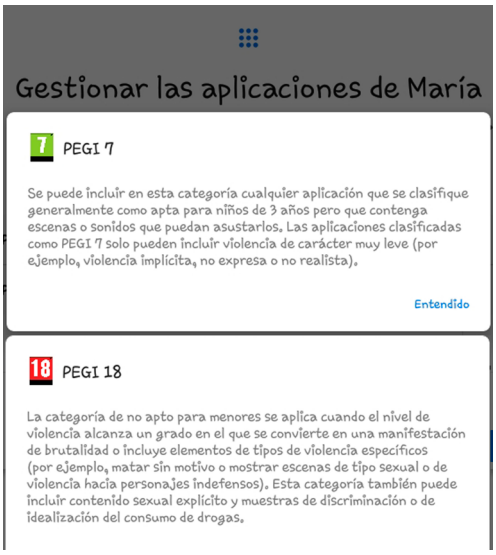


Figura 7. Font: Autoria pròpia.

- **Establir límits de temps i crear rutines de temps màxim**

La limitació en el temps depèn de l'edat de cada menor i de les circumstàncies familiars. De manera general, es poden seguir les recomanacions de l'American Academy of Pediatrics (2016).

⚠ ATENCIÓ

L'*American Academy of Pediatrics* dona recomanacions sobre el temps d'ús màxim de pantalles al qual s'haurien d'exposar infants i adolescents en funció de la seva edat: Menors de 18 o 24 mesos: evitar l'ús de mitjans digitals.

Menors entre 2 i 5 anys: màxim 1 hora d'exposició al dia i com menys temps, millor.
Menors entre 7 i 12 anys: màxim 1 hora, en companyia d'una persona adulta.
Menors entre 12 i 15 anys: màxim 1 hora i mitja, amb especial atenció a les xarxes socials.
Més de 16 anys: màxim 2 hores, evitant pantalles a les habitacions.

A través del control parental, es poden ajustar aquests temps màxims d'ús en funció del dia de la setmana i, fins i tot, es pot ajustar el temps màxim per aplicació concreta.

- Controlar els ajustaments d'ubicació.
- Definir filtres i controls en Google Chrome, la Cerca, Play i YouTube.

Entre les opcions de configuració, destaquen els filtres per cercar informació i per comprar a Internet. A la Figura 8, els pares de na Maria configuren les opcions per permetre o bloquejar els llocs web als quals pot tenir accés. A la Figura 9, configuren les opcions de compra d'aplicacions a Google Play.

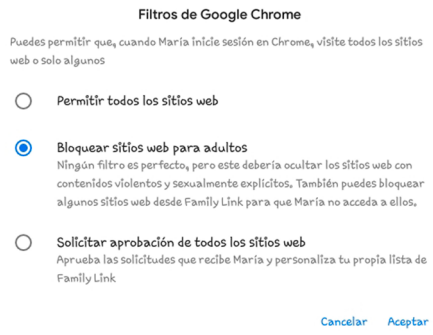


Figura 8. Font: Autoria pròpia.

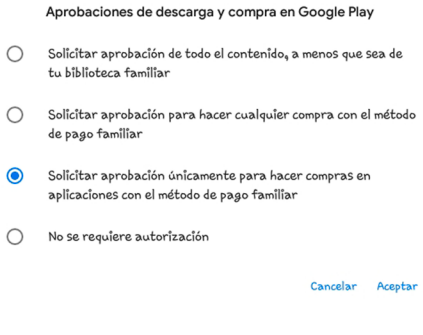


Figura 9. Font: Autoria pròpia.

Si s'han seguit tots els passos, es durà a terme la instal·lació de l'aplicació en el dispositiu de l'infant i en el dispositiu del pare o mare (Figura 10). A la Figura 11, es mostra la informació sobre la tauleta de na Maria i la configuració de manera correcta per poder ser supervisada a través de les eines de control parental.

Figura 10. Font: Autoria pròpia.

Figura 11. Font: Autoria pròpia.

Configuració del dispositiu de la mare o pare

En el dispositiu de la mare o del pare és necessari instal·lar l'aplicació disponible de Family Link.

Aquesta aplicació permet la configuració i ajust de totes les funcionalitats anteriorment configurades en el dispositiu de Maria. A més, l'aplicació permet fer el seguiment de l'activitat de la nena. La Figura 12 (a la dreta) és una captura de les funcions que la família de Maria pot consultar en remot sobre el dispositiu i l'ús d'aquest per part de Maria.

Així mateix, si és necessari canviar la configuració d'algun aspecte, es pot fer a través d'aquesta aplicació. Per exemple, es poden configurar o modificar els temps d'ús o l'hora d'apagada del dispositiu o crear rutines en funció dels dies de la setmana (Figura 13). També es pot configurar el límit de temps sobre la base de les aplicacions específiques; a la Figura 14, la família de na Maria li atorga un límit màxim de 30 minuts per utilitzar l'aplicació Bona nit.

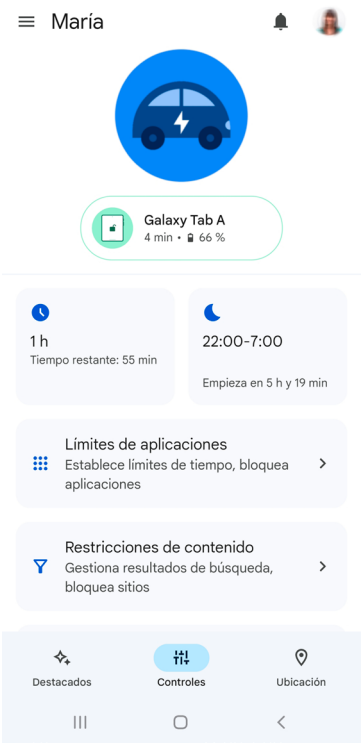


Figura 12. Font: Autoria pròpia.

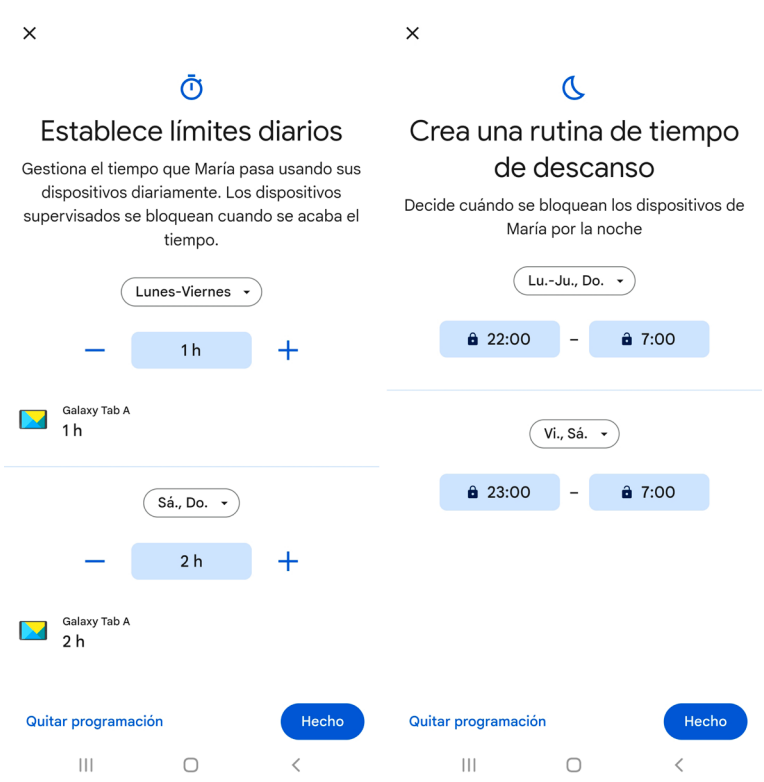


Figura 13. Font: Autoria pròpia.

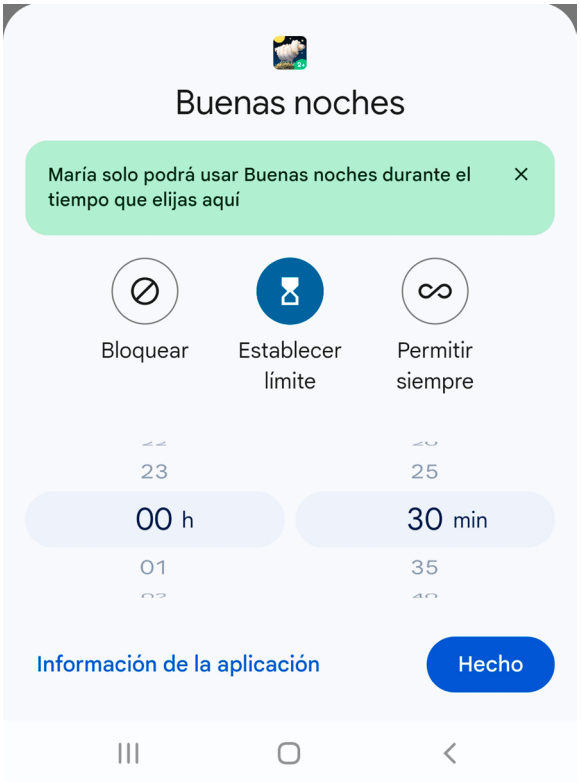


Figura 14. Font: Autoria pròpia.

Una altra de les utilitats de les eines de control parental que ofereix un major interès quan no estam amb els menors, és la geolocalització. A la Figura 15, en el seu lateral esquerre, s'observa la pantalla en la qual es configuren els ajustaments de la ubicació i en el lateral dret, com es visualitza la ubicació en temps real del dispositiu.

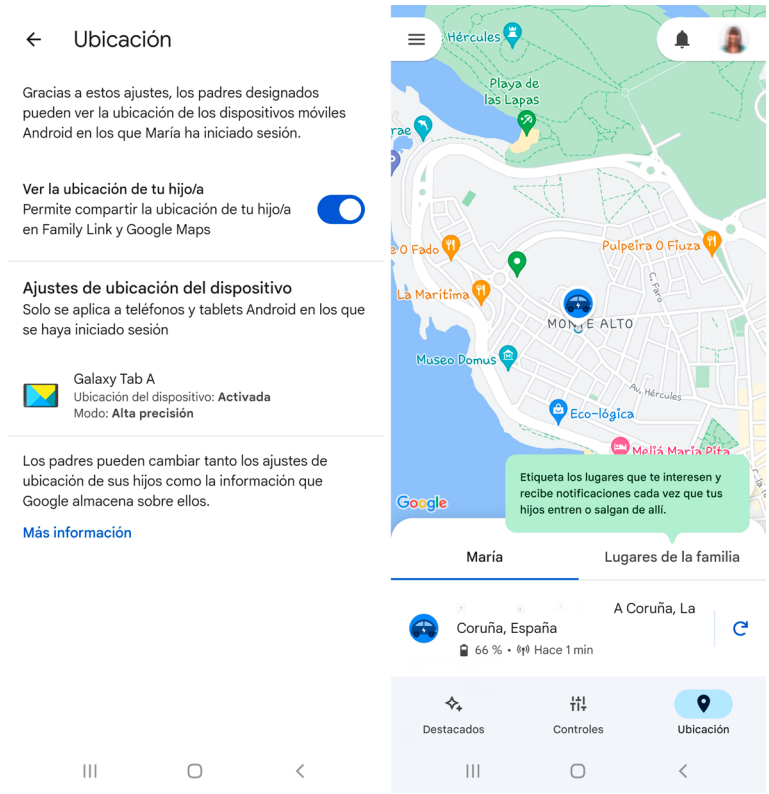


Figura 15. Font: Autoria pròpia.

Finalment, és essencial recordar que el control parental de les aplicacions no substitueix a l'acompanyament i supervisió de les persones adultes de la família. De fet, Family Link aconsella que la configuració i els termes d'ús es facin en conjunt entre els menors i els parents com a manera respectuosa de criança.

Exemples de pactes familiars per a emprar tecnologia:
e.digitall.org.es/pactos-familiares

En la pàgina web es poden consultar i descarregar exemples concrets de pactes familiars per fer un ús adequat de la tecnologia (xarxes socials, videoconsoles, tauleta, mòbil, entre altres opcions).

Saber-ne més

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

Guia de ferramentes de control parental. Institut Nacional de Ciberseguretat (INCIBE). e.digitall.org.es/guia-control-parental

Guia de mediació parental per a un ús segur i responsable dInternet per part dels menors. Institut Nacional de Ciberseguretat (INCIBE). e.digitall.org.es/mediacion-parental

Eines de control parental. Cerca de ferramentes de control. Institut Nacional de Ciberseguretat (INCIBE). e.digitall.org.es/control-parental

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

Pactes familiars pel bon ús de dispositius. Institut Nacional de Ciberseguretat (INCIBE). e.digital.org.es/pactos-familiares-incibe

DigitAll

Seguretat

4.4
PROTECCIÓ DEL MEDI AMBIENT

Seguretat

Nivell B2 4.4 Protecció del medi ambient

De les 3 R a l'economia circular

De les 3 R a l'economia circular

Introducció

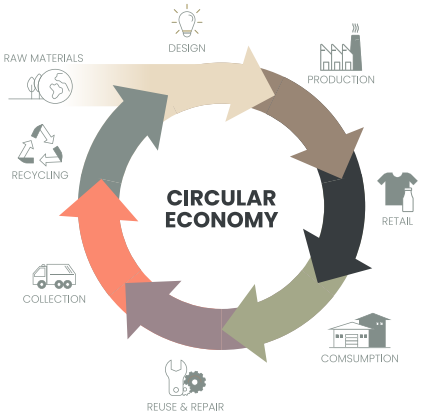
En aquest document es tractaran de manera més detallada conceptes que s'han inclòs en els vídeos del nivell, com les diferents "erres" que amplien la visió clàssica del "reduir, reutilitzar, reciclar" com a proposta clàssica de l'ambientalisme.

Veurem com l'ampliació conceptual lligada a les noves "erres" a través de termes com Reavaluar, Reparar, Reestructurar, Redistribuir o relocalitzar està relacionada amb les propostes teòriques que es vinculen amb el concepte de "decreixement", com una alternativa d'aproximació a les problemàtiques ambientals actuals lligades al model de producció i consum.

I precisament com a proposta de model econòmic alternatiu que cerca augmentar els nivells de sostenibilitat social i ambiental, ens aproximarem a l'economia circular. Aquesta proposta es tracta d'implementar una nova economia, basada en el principi de tancar el cicle de vida dels productes, els serveis, els residus, els materials, l'aigua i l'energia.

A més de presentar els fonaments de l'economia circular, presentarem exemples concrets de productes i serveis relacionats amb les tecnologies digitals que s'acullen a una reconceptualització que parteix del seu propi disseny, per minimitzar els seus impactes ambientals i socials.

Més enllà de les 3R: les propostes decrecentistes



A nivells anteriors hem analitzat com per aconseguir disminuir els impactes ambientals i socials de la tecnologia digital és necessari replantejar el model econòmic, orientant-lo cap a una reducció del consum i de la producció amb la finalitat d'augmentar el benestar humà i les condicions ambientals en el planeta.
A partir d'aquesta idea, és important aprofundir en les vies per a aconseguir-ho. Per començar, podem partir de les "3

R" clàssiques de l'ambientalisme: reduir, reutilitzar i reciclar. Com ja hem vist, en els vídeos d'aquesta sèrie "**Opcions de consum responsable de tecnologia mòbil"** (v.5) i "**Sumant erres a la sostenibilitat: l'economia circular**" (v.4), necessitem reduir el nostre consum de productes i dispositius tecnològics atenent necessitats reals i estant alerta a les estratègies d'obsolescència; reutilitzar, en la mesura del possible, aparells i components que encara puguin tenir una vida útil que eviti exhaurir nous recursos naturals; i, finalment, optimitzar els processos de reciclatge d'elements necessaris per al funcionament del sector tecnològic, indispensables per al manteniment de les cadenes de subministrament i cada vegada més costosos d'extreure, tant ambientalment com socialment.

SUMANT ERRES A LA SOSTENIBILITAT: L'ECONOMIA CIRCULAR

Explorar les propostes de l'economia circular per al consum tecnològic basades en el "redisseny" de processos amb criteris sostenibles. Donarem exemples dels dissenys "del bressol al bressol"

e.digitall.org.es/A4C44B2V04

OPCIONS DE CONSUM RESPONSABLE DE TECNOLOGIA MÒBIL

Es mostren un nivell més concret diferents alternatives de consum responsable i sostenible de tecnologia mòbil, des de tallers d'acte-reparació al Fairphone o "telèfon just".

e.digitall.org.es/A4C44B2V05

Però és molt possible que amb això no sigui suficient. Per aconseguir canvis estructurals en el nostre model de producció i consum, necessitarem una altra mena de propostes que aportin alternatives a un nivell més profund, ja que s'ha demostrat que les 3 R han estat interioritzades com a part del sistema econòmic actual, de manera que aconsegueixen "posar pegats" d'alguna manera les problemàtiques socioambientals sense realment contribuir a la transformació de les seves causes.

És aquí on entren en joc altres propostes alternatives com les que presentarem en aquest document. En primer lloc, ens centrarem en un concepte que està guanyant popularitat en el context internacional en els darrers anys: el decreixement.

El decreixement és un moviment filosòfic i activista amb origen a França, on la proposta de la *décroissance* es pot assenyalar com l'origen dels altres moviments decadentistes. El fundador de la décroissance és l'economista i filòsof francès Serge Latouche. En diverses de les seves obres, entre les quals es poden destacar "Petit tractat del decreixement serè" (2009); L'hora del decreixement" (2012); o el recent "Introducció al decreixement" (2022), Latouche proposa diferents camins i possibles aproximacions a un sistema econòmic que no tengui com a objectiu fonamental el creixement continuat.

⚠ ATENCIÓ

Entrant detalladament, la seva proposta es basa a ampliar les conegudes tres "R" a les vuit "R" com a pilars del decreixement: Revaluar, reconceptualitzar, reestructurar, relocalitzar, Redistribuir, Reduir, Reutilitzar i Reciclar (Latouche, 2009).

A més de les propostes ja conegudes sobre la necessitat de Reduir, Reutilitzar i Reciclar en el sector digital, una aplicació de les 5 R restants es podria exemplificar de la manera següent:

1 | **Reavaluar**,en referència a donar un nou valor al cost de la producció dels dispositius digitals. Hem de saber que no paguem el cost real de la producció si tenim en compte la deslocalització de la producció o els costos ambientals d'aquesta.

2 | **Reparar**. S'ha de fer incidència en què els productes han d'estar dissenyats per facilitar la seva reparació i evitar que es rebutgin abans d'hora. Per això, és indispensable comptar amb una normativa que ho faciliti i doni suport, amb l'objectiu d'evitar les estratègies d'obsolescència tan comunes en el sector de la tecnologia.

3 | Reestructurar els models de producció i comercialització dels dispositius digitals, tenint en compte a tots els actors que intervenen en el procés productiu, així com el seu impacte en l'entorn.

4 | Relocalitzar els processos productius amb la idea d'afavorir el producte local, ja que tindrà un impacte menor en el mitjà i contribuirà en grau més alt a millorar l'economia de proximitat. Aquesta filosofia és difícil d'aplicar en el sector digital, ja que les cadenes de producció i subministrament estan molt localitzades, però és un desafiament que hem d'abordar com a societat.

5 | Redistribuir els costs i beneficis del model de producció i consum de tecnologia digital, amb la idea que, si tothom consumís de la mateixa manera que es fa als països industrialitzats, aquest model seria totalment inviable.

Una aproximació a l'economia circular

En línia amb les propostes decadentistes, l'economia circular emergeix com una proposta de transformació del model de producció i consum que implica compartir, llogar, reutilitzar, reparar, renovar i reciclar materials i productes existents el màxim possible, d'aquesta manera limitar l'esgotament de recursos i els impactes ambientals del procés.

Si la proposta del decreixement parteix de cercles acadèmics i activistes, l'economia circular ha estat acollida per diverses institucions com una aposta ferma en l'àmbit polític. Per exemple, la Unió Europea i les institucions comunitàries treballen en la reforma del marc legislatiu per promoure un canvi del model de gestió de residus actual, que té un caràcter lineal, per una veritable "economia circular".

L'economia circular cerca, en essència, que el cicle de vida dels productes s'estengui. Això, en la pràctica, implica reduir els residus al mínim, però també els impactes ambientals i socials del model productiu. Sota aquest prisma, el sector tecnològic seria un dels quals es veurien més beneficiats amb la transformació del model productiu.

En l'actualitat, quan un producte arriba al final de la seva vida, els seus materials es mantenen dins de l'economia sempre que sigui possible gràcies al reciclatge. Aquests poden ser productivament utilitzats una vegada i una altra, creant així un valor addicional que té a veure amb l'aprofitament del recurs en si mateix, però també amb el fet que no s'estan explotant més reserves de recursos que són limitats.

De fet, un dels motius principals per a avançar cap a una economia circular és l'augment de la demanda de matèries primeres i l'escassetat de recursos. Diverses matèries primeres crucials són finites i, com la població mundial creix, la demanda també augmenta.

La consolidació del model de l'economia circular contrastaria amb el model econòmic lineal tradicional, basat principalment en el concepte "emprar i tirar", que requereix grans quantitats de materials i energia barats i de fàcil accés. Per al sector de les tecnologies digitals, ja hem vist en nivells anteriors els conflictes socials i ambientals associats als processos extractius.

També vàrem veure com els impactes ambientals no es redueixen simplement a l'extracció i esgotament de recursos. Un altre benefici de l'economia circular és la reducció de les emissions anuals totals de gasos d'efecte d'hivernacle.

NOTA

Segons l'Agència Europea de Medi Ambient, els processos industrials i l'ús de productes són responsables del 9,10% de les emissions de gasos d'efecte d'hivernacle a la UE, mentre que la gestió de residus representa el 3,32% (Parlament Europeu, 2023).

A més, crear productes més sostenibles des del seu disseny, adoptant els principis i les premisses de l'eco-disseny o de la perspectiva "del bressol al bressol", també ajudaria a reduir el consum d'energia i recursos, ja que es calcula que més del 80% de l'impacte ambiental d'un producte es determina durant la fase de disseny.

Per si tot això no fos suficient, hi ha estudis que calculen que la transició cap a una economia més circular podria augmentar la competitivitat, estimular la innovació, impulsar el creixement econòmic i crear ocupació. Segons dades del Parlament Europeu (2023), es preveu que es puguin crear almenys 700.000 llocs de treball sol a la Unió Europea per a 2030, gràcies als processos de transformació del model productiu.

Per tant, el redissenyo de materials i productes per a una nova economia circular també impulsaria la innovació en diferents sectors de l'economia.

Finalment, cal destacar que perquè l'aposta per l'economia circular sigui realment efectiva, es necessita un suport institucional real en l'àmbit normatiu. Si bé és cert que a escala planetària aquest procés encara dista molt de ser una realitat, en el context europeu sí que es pot afirmar que l'aposta per l'economia circular és bastant ferma.

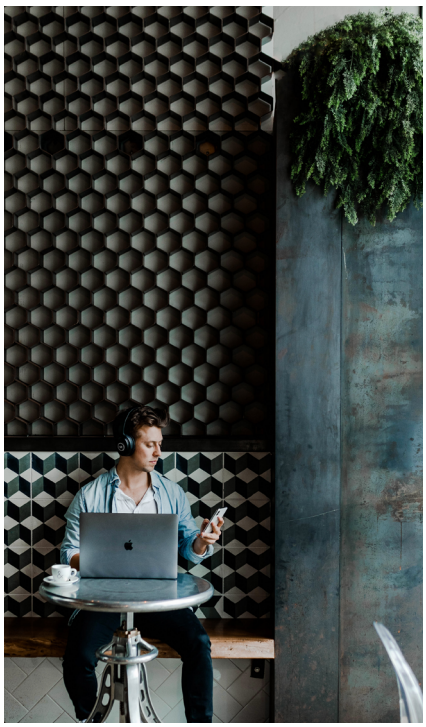
Per exemple, la Comissió Europea va presentar el març de 2020 el pla d'acció per a l'Economia Circular que a més de promoure el disseny de productes més sostenibles i la reducció de residu, potència els processos de participació i apoderament dels ciutadans a través d'iniciatives com el "dret a reparar". En aquesta normativa, com no podia ser d'una altra forma, es presta especial atenció als sectors intensius en recursos, com l'electrònica i les TIC.

Com a continuació, el febrer de 2021 es va votar en el Parlament Europeu el pla d'acció sobre economia circular i va demandar mesures addicionals per a promulgar lleis més efectives sobre reciclatge i la formulació d'objectius vinculants per a la reducció de la petjada ecològica per l'ús i consum de materials, que afectarien de manera directa al sector digital.

NOTA

L'any 2022, la Comissió va donar a conèixer el primer paquet de mesures per a accelerar la transició cap a una economia circular, a més de proposar noves normes sobre envasos per a tota la Unió Europea, que es basen en propostes d'eco-disseny. A més, des de la Comissió es proposa també la transició a elements de base biològica i biodegradables, com els bioplàstics.

Així que, com veiem, l'economia circular és una proposta transformadora amb una base molt real, ja que el suport institucional i normatiu a escala europea garanteix una base sòlida per iniciar el canvi de model productiu, que per descomptat haurà de veure's referendada en els casos particulars de cada país i els comportaments socials per garantir la transició a un model més sostenible.



Saber-ne més

Comissió Europea (2023) Pla d'Acció d'Economia Circular. *e.digitall.org.es/economia-circular*

Latouche, Serge (2009) Petit tractat del decreixement serè. Icaria. *e.digitall.org.es/icaria*

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

Parlament Europeu (2023) Economia circular: definició, importància i beneficis. *e.digitall.org.es/beneficions-economiacircular*

Parlament Europeu (2022). Dret a reparar: el PE vol productes més fàcils de reparar. *e.digitall.org.es/derecho-reparar*

Research & Degrowth (Investigació i Decreixement) (2023). *degrowth.org*

DigitAll

Formació en
Competències
Digitals

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