DigitAll

Gaitasun
digitaletan
prestakuntza

4

Segurtasuna

DigitAll

Gaitasun
digitaletan
prestakuntza

Segurtasuna

B2 maila

AURKIBIDEA

DigitAll

Segurtasuna

4.1
GAILUEN BABESA

Segurtasuna

B2 maila 4.1 Gailuen babesa

Nola ezarri SGSI bat: metodologiak

Nola ezarri SGSI bat: metodologiak

Informazioaren segurtasunaren kudeaketa

Informazioaren segurtasunaren kudeaketak erakunde baten informazio-aktiboak babesteari egiten dio erreferentzia, haien konfidentzialtasuna, osotasuna eta eskuragarritasuna bermatzeko. Oro har, informazioaren segurtasunaren arriskuak identifikatu, ebaluatu eta arintzeko diseinatutako prozesu, politika, prozedura eta neurri teknikoen multzoa da.

ARRISKUEN KUDEAKETA: AKTIBOA, PROBABILITATEA ETA INPAKTUA

Arriskuen kudeaketa erakunde bati eragin diezaioketen arrisku potentzialak identifikatu, aztertu eta ebaluatzeko eta prebentzio- eta arintze-neurri egokiak ezartzeko prozesua da.

e.digitall.org.es/A4C41B1V02

INFORMAZIOAREN SEGURTASUNAREN KUDEAKETA-SISTEMA (SGSI):ARRISKUEI KONTROLAK APLIKATZEN

Informazioaren segurtasunaren kudeaketa-sistema.baten garapenean, arriskuei kontrolak ezartzea arriskuen kudeaketaren ondorengo urratsa da.

e.digitall.org.es/A4C41B2V02

Informazioaren segurtasunaren kudeaketaren helburu nagusia informazioa seguru mantentzen dela ziurtatzea da, barneko eta kanpoko mehatxuetatik babestuta.
Erakunde batean hura ezartzea errazteko, komeni da gaur egungo metodologietako bat erabiltzea.

OHARRA

Informazioaren segurtasuna kudeatzeko metodologia erakunde batean informazioaren segurtasuna planifikatzeko, ezartzeko, kontrolatzeko eta hobetzeko erabilitako ikuspegi egituratua eta sistematikoa da.

Informazio gehiago

Informazioaren segurtasunaren kudeaketa funtsezkoa da gaur egungo ingurunean; izan ere, informazioak zeregin kritikoa du enpresa-eragiketetan eta bezeroaren konfiantzan.

Informazioaren segurtasuna kudeatzeko metodologiak

Informazioaren segurtasuna kudeatzeko hainbat metodologia daude, eta bakoitzak ikuspegi eta ezaugarri espezifikoak ditu. Bata edo bestea hautatzea erakunde bakoitzaren behar eta eskakizun espezifikoen mende dago, bai eta bere industrian bete beharreko estandar eta araudien mende ere.

Metodologia bat hautatzeko gehien baloratzen den ezaugarrietako bat ziurtagiri bat lortzeko aukera da, normalean erakundeei balio erantsia ematen baitie horrek.

ISO 27001

ISO/IEC 27001 araua (*e.digitall.org.es/iso-27001*) nazioartean onartutako araua da, eta erakunde batean informazioaren segurtasunaren kudeaketa-sistema (SGSI) bat ezartzeko, mantentzeko eta hobetzeko betekizunak ezartzen ditu. Normalizaziorako Nazioarteko Erakundeak (ISO) eta Nazioarteko Batzorde Elektroteknikoak (IEC) garatu zuten.

Informazioaren segurtasuna kudeatzeko arriskuan oinarritutako ikuspegia ezartzen du, eta horrek berekin dakar arriskuak identifikatzea, haien inpaktua eta probabilitatea ebaluatzea eta horiek arintzeko neurriak hartzea.

Arau hori Deming Zikloa edo PDCA zikloa (Plan-Do-Check-Act) izeneko etengabeko hobekuntzaren zikloan oinarritzen da, zeinak ikuspegi iteratibo eta ziklikoari jarraitzen baitio.

Hauek dira ISO 27001 arauaren indargune nagusiak, informazioaren segurtasuna kudeatzeko metodologia erabilienetako bat bihurtu dutenak:

- **Ziurtapenean oinarritutako aintzatespena eta konfiantza:** ziurtagiria lortzeak erakusten du erakunde batek informazioaren segurtasunarekin konpromisoa duela, eta konfiantza ematen die bezeroei, merkataritza-bazkideei eta alderdi interesdunei.
- **Ikuspegi integrala:** erakunde bateko informazioaren segurtasunaren kudeaketari modu integralean heltzen dio, ez da alderdi teknikoetara soilik mugatzen, eta antolamendu-alderdiak zein legalak eta humanoak ere kontuan hartzen ditu.

- **Malgutasuna eta moldagarritasuna:** erakunde bakoitzaren premia eta eskakizun espezifikoetara egokitu daiteke eta kontrol eta segurtasun-neurri pertsonalizatuak ezartzeko aukera ematen du, erakundearen arriskuen eta testuinguru bereziaren arabera.

ISO 27001 arauak gure estatuan duen garrantziaren adibideetako bat honako hau da: Espainiako administrazio publikoak metodologia horretan oinarritu dira, Espainiako administrazio publikoetarako berariazko betekizun eta jarraibide gehiagorekin egokitu eta osatu dute hura, eta, horrela, Espainiako Segurtasunaren Eskema sortu da.

Informazio gehiago

Espainiako Segurtasunaren Eskema (SEN) Espainiako administrazio publikoetarako informazioaren segurtasunerako gutxieneko printzipioak eta betekizunak ezartzen dituen erreferentzia-esparrua da.

Beste metodologia batzuk

ISO 27001 metodologia, oro har, gehien erabilitako metodologia den arren, beste batzuk daudela aipatzea garrantzitsua da.

NIST SP 800-53

NIST SP 800-53 Ameriketako Estatu Batuetako Estandarren eta Teknologiaren Institutu Nazionalak (NIST) garatutako estandar- eta gida-multzoa da. AEBetako gobernu-agentzien informazio-sistema federaletan, informazioaren segurtasuna kudeatzeko erreferentzia gisa erabiltzen da.

NIST SP 800-53k segurtasun-kontrol eta -babes ugari eskaintzen ditu, eta bere ikuspegia arriskuen kudeaketan oinarritzen da, baita kontrolak erakunde bakoitzaren premia eta ezaugarrietara egokitzean ere.
Garrantzitsua da nabarmentzea estandar-multzo hori jardunbide egokien multzo gisa ulertu behar dela, eta, beraz, ez datorrela bat inongo ziurtatze-esparrurekin.

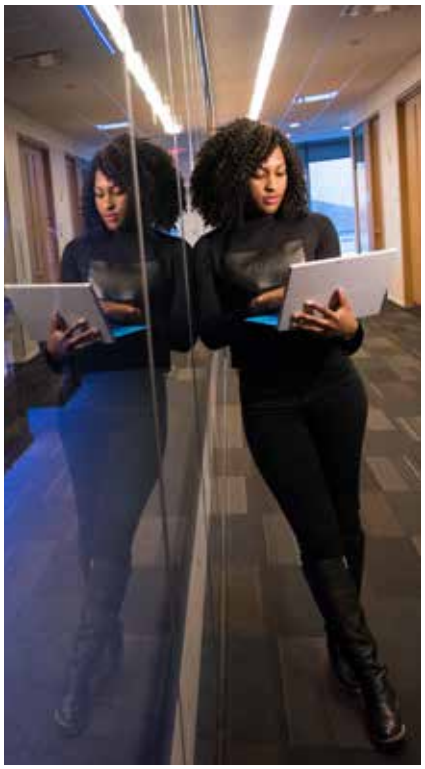
COBIT

COBIT (Control Objectives for Information and Related Technologies) ISACAk (Information Systems Audit and Control Association) garatutako erreferentzia-esparrua da. Erakundeetako informazio-teknologien (IT) gobernantzarako eta kudeaketarako jardunbide egokien multzo bat eskaintzen du, eta esparru horren barruan, informazioaren segurtasuna funtsezko alderdietako bat da.

COBITen helburu nagusietako bat lege- eta arau-baldintzak betetzen direla bermatzea da.

Esparru egituratua, kontrol-helburuak eta gomendatutako jardunbideak eskaintzen ditu, erakundeei laguntzeko informazioaren segurtasun-maila egokia ezartzen eta mantentzen, eragiketei eusteko eta helburu estrategikoak lortzeko asmoz.

NIST SP 800-53 bezala, erreferentzia-esparru hori ere ez dator bat inongo ziurtatze-esparrurekin.



Segurtasuna

B2 maila 4.1 Gailuen babesa

Informazioa zifratzeko utilitateak

Informazioa zifratzeko utilitateak

Prestakuntza honetan, informazioa zifratzea bezalako gaiak landu dira eta, zehatz-mehatz, fitxategiak eta gailuak zifratzea. Informazioa zifratzeak konfidentzialtasunaren babesa bermatzen du, eta, beraz, funtsezkoa da gure fitxategiak zifratzeko eta deszifratzeko eta ahalik eta erosoen eta seguruen lan egiteko aukera emango diguten utilitateak eskura izatea. Jarraian, disko gogorrak eta fitxategiak zifratzeko hainbat utilitate ikusiko ditugu.

FITXATEGIAK ETA GAILUAK ZIFRATZEA

Fitxategiak eta gailuak zifratzeak erabiltzen ari ez den informazioaren konfidentzialtasuna bermatzen du. Gailuko disko gogorra zifratzeak biltegiratutako informazio guztia babesten du, eta fitxategiak zifratzeak, berriz, fitxategiak modu independentean babesten ditu.

e.digitall.org.es/A4C41B1V05

Disko gogorrak zifratzea

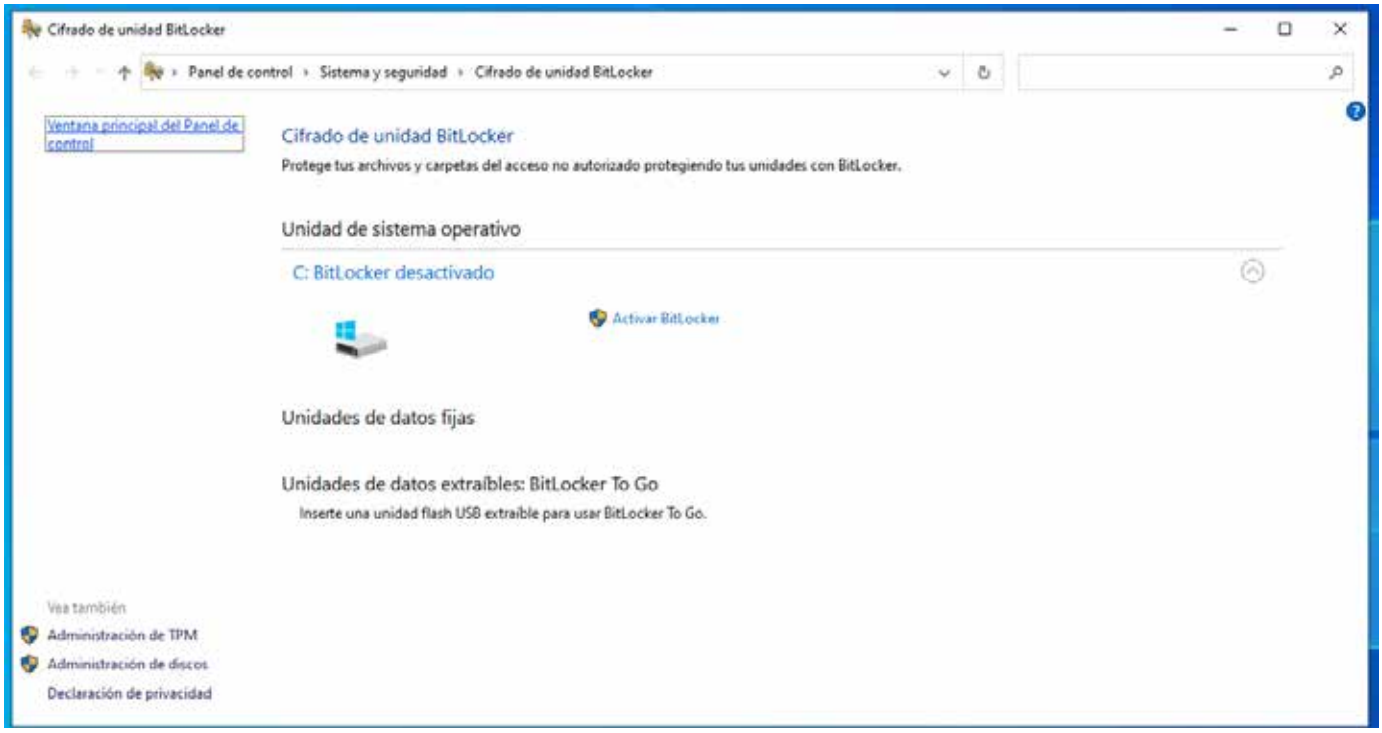
Erabiltzen ari ez den informazioa zifratzeko lehen aukera gailua zifratzea da. Zehazki, informazio guztia gordetzen duen disko gogorra zifratu daiteke (sistema eragilearen informazioa zein erabiltzaileak kudeatzen duen informazio pertsonala gordetzen ditu diskoak).

Garrantzitsua da gogoraraztea, gailuak pasahitzean oinarrituta zifratuz gero, hura galtzen bada, zifratutako datu guztietarako sarbidea galtzen dela.

Windowsen: BitLocker

Windows sistema eragileetarako gehien erabiltzen den aukera BitLocker da, sistema eragilean bertan sartuta dagoena. Horrela, Windows abiaraztean, Bitlockerek disko gogorra deszifratuko du, abian jarri eta informazioa eskuratu ahal izateko.

Gainera, PC moderno askok duten Trusted-Platform-Module (TPM) txiparekin integratzea ahalbidetzen du. Horrela, informazioa klonatzen bada edo inor disko gogorrera sartzen saiatzen bada, informazioa zifratuta egongo da.
Oso erraza da soluzio hori konfiguratzea. TPM txipik ez badago, sarbide-pasahitz bat ezar daiteke, gailua abiaraztean sartu beharko dena, Windows hasi aurretik.



1. irudia. Bitlocker bidez diskoa zifratzea kudeatzea.

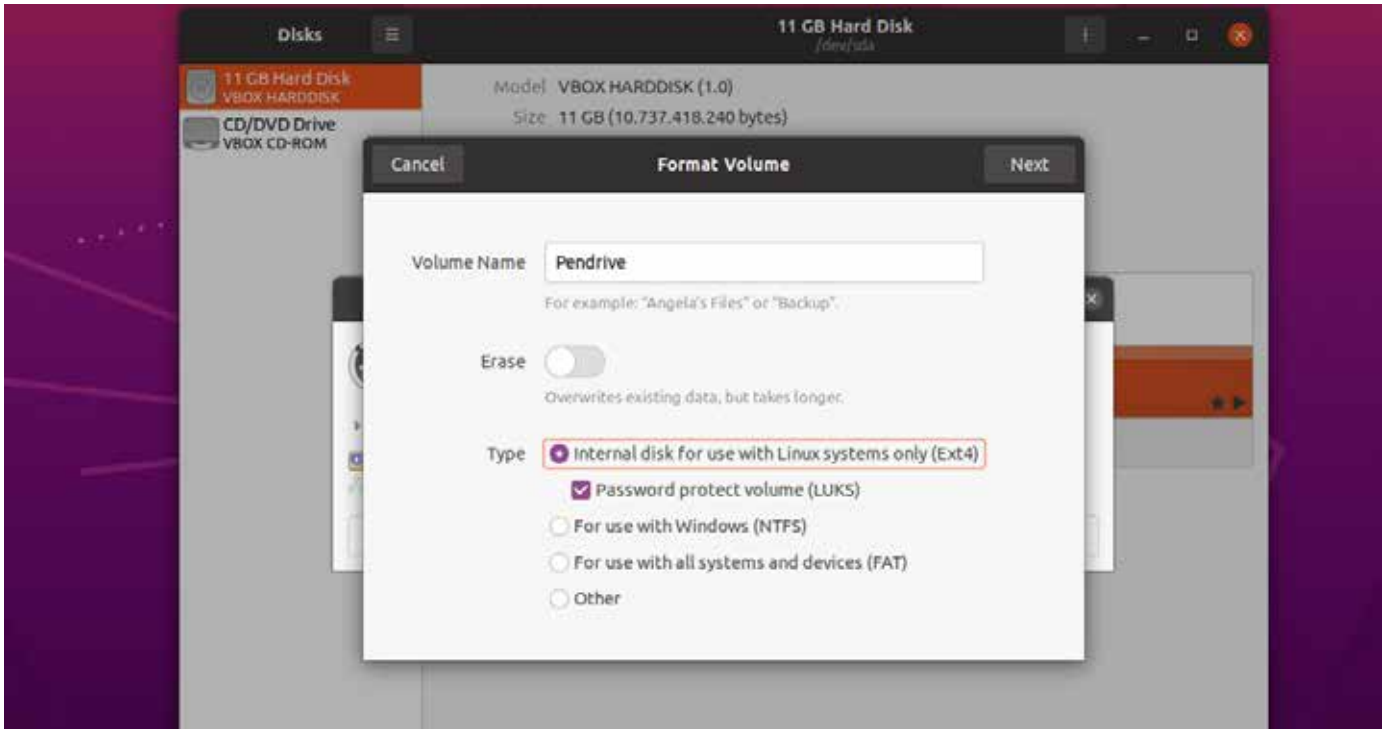
Informazio gehiago

Microsoften euskarri-orritik gailua zifratzea nola aktibatu kontsulta dezakezu: *e.digitall.org.es/activar-cifrado*

Linuxen: LUKS

Windowserako BitLockerek bezala, LUKSek Linuxen disko gogorrak zifratzeko aukera ematen du. Soluzio hori pasahitz bat erabiliz disko gogor bat zifratzeko erabiltzen da gehienbat. Erraz konfiguratzen da Linuxen oinarritutako zenbait sistema eragile instalatzean: Ubuntu edo Manjaro Linux, esaterako.

Gainera, edozein biltegiratze-unitate mota zifratzeko aukera dugu. Adibidez, USB memoria bat badugu, disko-kudeatzailearen laguntzarekin zifratu dezakegu. Horrela, ekipoan txertatzen denean, zifratze-pasahitza eman beharko dugu edukira sartu ahal izateko.
Garrantzitsua da gogoraraztea aukera horrek ez duela berreskuratzeko inolako modurik eskaintzen. Zifratze-pasahitza ahaztuz gero, baliteke informaziorako sarbidea galtzea.



2. irudia. Linuxen LUKS duen unitate ateragarri bat zifratzea.

MacOS: FileVault

MacOS duen gailu bat erabiliz gero, Applek disko gogorra zifratzeko soluzio integratua ematen du bere sistema eragilean. Windowsen bezala, aukera hori edozein unetan aktibatu eta desaktiba daiteke. Baliteke zifratze-pasahitza erabili behar izatea, eta berreskuratzeko aukeraren bat eskaintzen du, gailuaren zifratze-pasahitza ahaztuz gero.

3. irudia. MacOsen FileVault konfiguratzea. (Iturria: *e.digitall.org.es/filevault*)

Informazio gehiago

Mac-en abiarazte-diskoa nola zifratu kontsulta dezakezu Appleren euskarri-webgunean: *e.digitall.org.es / filevault-mac*

Fitxategiak zifratzea

Baliteke diskoa zifratzeko aukeretakoren bat gailuren batera ez egokitzea edo erabiltzaileak informazio guztia zifratu nahi ez izatea. Horretarako, informazioaren zati bat zifratzeko aukera ematen duten beste tresna batzuk daude. Hona hemen ezagunenetako batzuk:

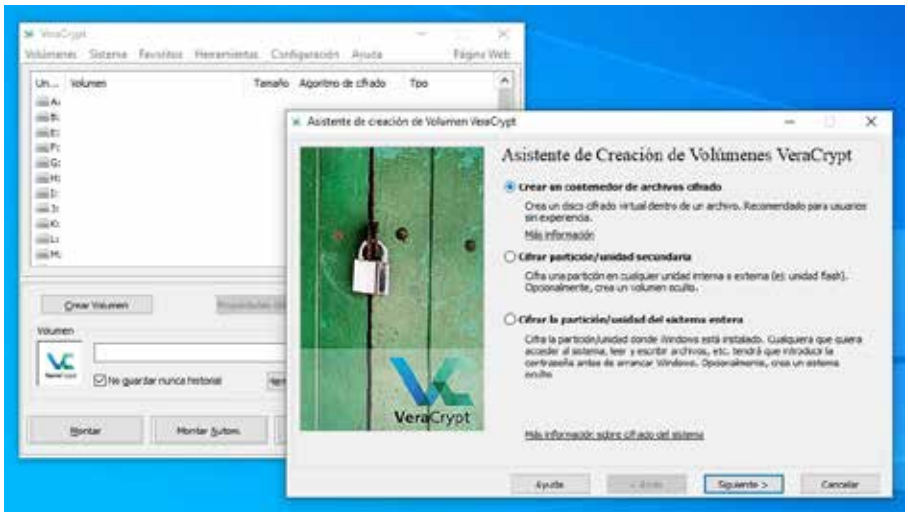
Veracrypt

Veracrypt Windowsen, MacOSen eta Linuxen funtzionatzen duen kode irekiko softwarea da. Fitxategi jakin batzuk zifratzeko aukera ematen du, "bolumen" birtual bat sortuz. Horrela, fitxategi edo bolumen zifratu bat gordetzen du, eta Veracryptekin deszifratuta eta zifratze-pasahitz bat erabiliz soilik sar daiteke bertara.

> **Informazio gehiago**
>
> Veracrypt lortzeko, deskargatze-orri ofizialetik deskarga dezakezu exekutagarria: *e.digitall.org.es/veracrypt*

Behin deszifratuta, bolumena muntatu eta fitxategi-sistemaren karpeta arrunt gisa erabil daiteke. Veracryptekin ixtean, informazio guztia zifratzen da berriro ere. Veracryptekin zifratutako bolumena fitxategi normal gisa kopiatu eta parteka daiteke.

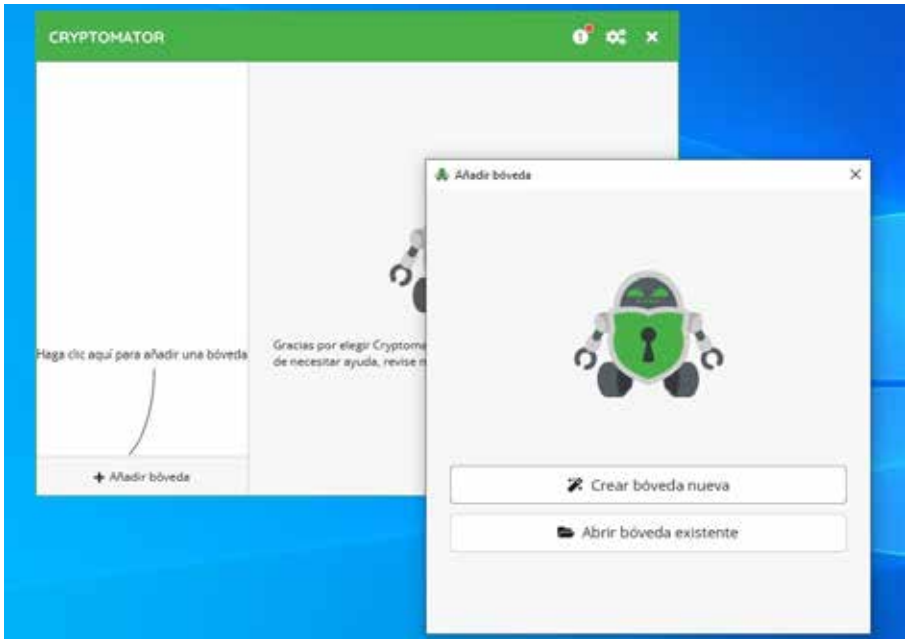
Gainera, Veracryptek disko gogorrak eta biltegiratze-unitate ateragarriak zifratzeko aukera ere ematen du, LUKSek bezala.



4. irudia. Windowsetik Veracrypten zifratutako fitxategi-bolumen edo -edukiontzi bat sortzea.

Cryptomator

Veracrypten antzekoa, Cryptomatorek "bobedak" edo edukiontzi zifratuak sortzeko aukera ematen du. Interfazeak oso erabilera erraza eskaintzen dio erabiltzaileari. Cryptomatoren kodea irekia da, eta webgunetik deskargatuz gero doan erabiltzeko aukera dago.



5. irudia. Windowsetik Cryptomatorekin bobeda edo edukiontzi zifratu bat sortzea.

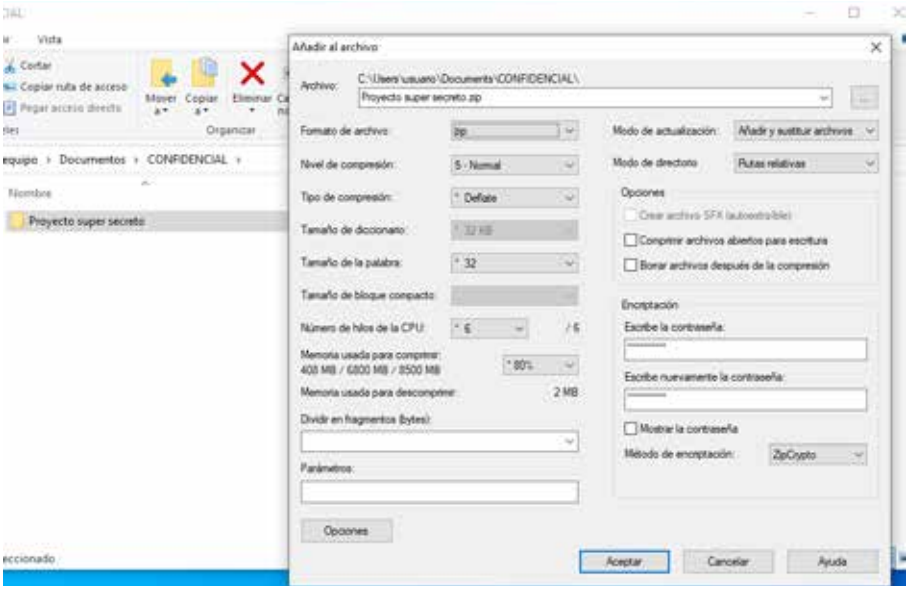
Informazio gehiago

Cryptomator probatzeko, haren webgune ofizialetik deskarga dezakezu: *cryptomator.org/downloads*

7-zip

Edozein sistema eragiletan fitxategiak zifratzeko aukera erabilgarrienetako bat 7-zip da. Tresna hori fitxategiak konprimatzeko pentsatuta badago ere, pasahitzez zifratutako ZIP karpeta konprimatuak sortzeko aukera ematen du. Horrela, deszifratzeko eta deskonprimatzeko pasahitza behar duten ZIP fitxategiak gorde edota parteka daitezke.

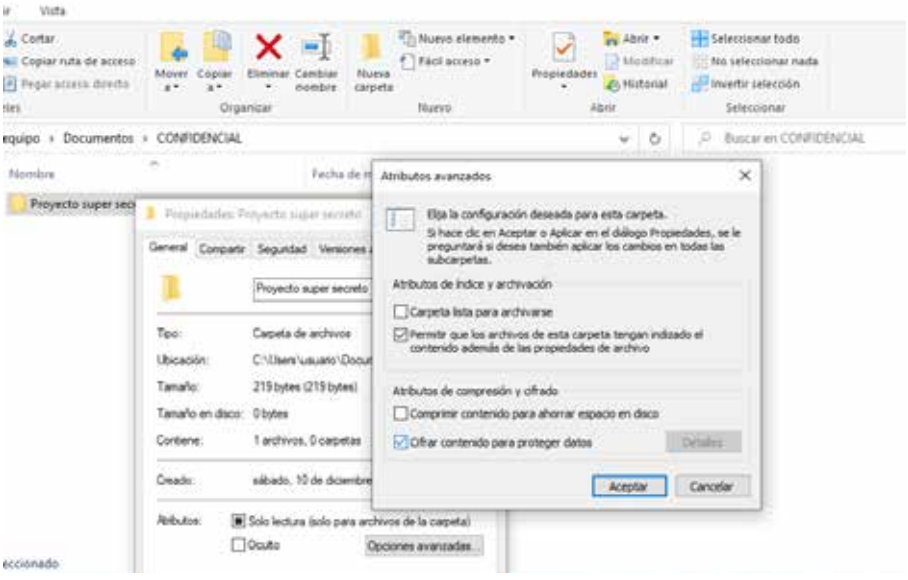
Pasahitz hori ezagutzen ez bada, ezin da ZIPeko fitxategien edukira sartu.



6. irudia. Windowsetik 7-zip duen karpeta bat zifratzea eta konprimatzea.

Windows EFS

Azkenik, Windowsek sistema eragiletik bertatik fitxategiak zifratzeko aukera ematen du. Garrantzitsua da kontuan hartzea fitxategi horiek gailu beretik bakarrik deszifratu ahal izango direla. Hori baliagarria izan daiteke gailuan fitxategi jakin batzuk babesteko, disko gogor osoa zifratu beharrik gabe.



7. irudia. Windowsetik EFS bidez karpeta bat zifratzea.

Segurtasuna

B2 maila 4.1 Gailuen babesa

Segurtasun-kopiak egiteko utilitateak

Segurtasun-kopiak egiteko utilitateak

Segurtasun-kopia bat datuen kopia bat da, jatorrizkoa ez den beste leku batean gordetzen dena. Segurtasun-kopiak datuak galtzetik edo ustekabeko kalteetatik babesteko erabiltzen dira. Adibidez, fitxategi bat errore baten ondorioz ezabatzen bada, segurtasun-kopiatik berrezar daiteke. Edo, ordenagailu baten disko gogorrak huts egiten badu, datuak segurtasun-kopiatik berrezar daitezke beste disko gogor batean.

DENAK HUTS EGITEN DUENEAN: SEGURTASUN-KOPIAK

Segurtasun-kopiak maiz egin behar dira, jatorrizkoak ez diren lekuetan. Informazio garrantzitsurako, gainera, 3 2 1 printzipioari jarraitu behar zaio; hau da, hiru kopia, bi toki eta saretik deskonektatutako bat.

e.digitall.org.es/A4C41B1V09

Segurtasun-kopia mota asko daude, hala nola segurtasun-kopia lokalak, hodeiko segurtasun-kopiak eta segurtasun-kopia hibridoak. Segurtasun-kopia lokalak gailu lokal batean gordetzen dira: kanpoko disko gogor batean edo USB batean, adibidez. Segurtasun-kopiak hodeiko zerbitzu batean gordetzeko aukera ere badago. Jarraian, erabiltzen duzun sistema eragilearen arabera segurtasun-kopiak nola egin zehaztuko da.

Windowseko segurtasun-kopia

Windows ekipo batean, oso erraz egin ditzakegu segurtasun-kopiak, sistema eragileak integratuta dakarren tresna erabiliz. Adibidez, hauek dira Windows 11ren urratsak:

1 | "Hasi" botoian klik egin eta "Konfigurazioa" hautatuko dugu.
2 | Hor gaudela, "Eguneratzea eta segurtasuna" atalera sartuko gara eta, ondoren, "Segurtasun-kopia"-ra.
3 | "Erantsi segurtasun-kopiaren unitate bat" hautatuko dugu.
4 | Segurtasun-kopia zer biltegiratze-unitatetan gorde nahi dugun aukeratuko dugu. Kanpoko disko bat edo USB bat aukera dezakegu, edo hodei-zerbitzua, hala nola OneDrive.

5 | "Hurrengoa" sakatzeak segurtasun-kopian sartu beharreko fitxategiak eta karpetak hautatzeko aukera ematen digu.
6 | "Hasi segurtasun-kopia" exekutatu eta itxaron egingo dugu.
7 | Azkenik, fitxategiak geuk aukeratu dugun kokalekuan eskuragarri daudela egiaztatuko dugu.

Gainera, segurtasun-kopia horiek programatu egin daitezke, aldizka exekuta daitezen. Horretarako, "Programatu" aukera dezakezu aurreko prozesuan. Segurtasun-kopia bat berrezartzeko, "Segurtasun-kopia" menura sartu eta "Segurtasun-kopia batetik fitxategiak berrezarri" aukeratu ahal izango dugu.

MacOSen segurtasun-kopia

MacOS sistema eragileetan hainbat aukera daude. **Time Machine** tresna integratua erabiliz. Erabiltzeko, kanpoko disko bat konektatuta eduki edo hodeian iCloud bezalako kontu bat izan behar da. Urratsak oso errazak dira:

1 | "Time Machine" aplikazioa irekiko dugu Macen, "Aplikazioak" karpetatik.
2 | "Hautatu segurtasun-kopiaren diskoa" aukeratu eta segurtasun-kopia gordetzeko erabili nahi dugun biltegiratze-gailua aukeratuko dugu.
3 | Prozesua egin arte itxarongo dugu, eta dokumentuak kopiatu zirela egiaztatuko dugu. Puntu horren ondoren, Time Machinek segurtasun-kopia automatikoak egiten jarraituko du aldizka.

Segurtasun-kopia horiek erabiliz, honako hau egin daiteke:

- **Fitxategi edo karpeta bat berrezarri.** Horretarako, "Time Machine"-ra jo dezakezu, eta fitxategia edo karpeta bilatu, hura berrezartzeko.
- **Hodeitik berrezarri.** Fitxategiak Appleren hodeian gorde badituzu, iCloud Drivetik sar zaitezke haietara, berreskuratu nahi duzun fitxategia edo karpeta deskargatzeko.
- **Ordenagailu osoaren kopia bat berrezarri.** Horretarako, gailua itzali eta, "cmd + R" teklak sakatuta, piztu egin behar dugu. "MacOSen utilitateak" leihoan "Time Machineren segurtasun-kopia batetik berrezarri" menu gidatua agertuko da.

Segurtasun-kopia Androiden

Android gailu mugikorrek ere aukera ematen dute segurtasun-kopiak konfiguratzeko. Berrienek **Google One** aplikazioa dute. Aplikazio horretan, Google-n saioa hasi ondoren:

1 | Kopiatu nahi ditugun datuak aukeratuko ditugu, hala nola kontaktuak, argazkiak, bideoak, egutegiak eta abar.
2 | "Segurtasun-kopia" klikatuko dugu aplikazioaren orri nagusian.
3 | Behin hautatuta, "Sortu segurtasun-kopia orain" botoian klik egingo dugu.
4 | Prozesua amaitzen denean, ***one.google.com*** zerbitzutik sartu ahal izango dugu guztietara.

Kopia bat berrezartzeko, Android-gailu berri batean, Googlerekin has dezakezu saioa. Berriz ere, Google One aplikazioan, "Segurtasun-kopia" eta "Berrezarri" ataletara sar gaitezke.

Segurtasun-kopia iOSen

iOS mugikor batean segurtasun-kopia hainbat modutan egin daiteke. Apple-ren hodeia erabiltzea da errazena**, iCloud**:

1 | iPhoneko "Ezarpenak" ataletik, gure izena agertzen den lehen atalera sartuko gara, eta gero "iCloud"-era.

2 | Hautatu "Kopia iClouden" eta, ondoren, "Segurtasun-kopia egin orain".

Aukera horrekin, datu guztiak iClouden gordeko dira. Ordenagailua erabili nahi baduzu, erabil dezakezu. Windowsen, iTunes aplikazioa erabili behar duzu:

1 | Konektatu zure iPhonea ordenagailura USB kable baten bidez.
2 | Ireki "iTunes", edo ezar ezazu Appleren webgunetik.
3 | Ezkerreko goiko ertzean, egin klik iPhonearen ikonoan.

4 | Hautatu "Laburpena" eta "Segurtasun-kopia egin orain".

Zure ordenagailua Mac bada:

1 | Konektatu zure iPhonea ordenagailura USB kable baten bidez.
2 | Ireki "iTunes", edo ezar ezazu Appleren webgunetik.
3 | Ezkerreko goiko ertzean, egin klik iPhonearen ikonoan.

4 | Hautatu "Laburpena" eta "Segurtasun-kopia egin orain".

Erabilitako estrategiaren arabera, tresna bakoitzak segurtasun-kopia erraz berrezartzeko aukera ematen du. Horretarako, jarraitu aurreko prozesuari, baina hauta ezazu berrezartzeko aukera.

Ondorioak eta gomendioak

Ikusi dugunez, sistema eragile bakoitzak bere tresnak ditu. Hemen, sisteman integratutako utilitateekin jarraitu beharreko urratsak landu ditugu. Hala ere, beste tresna asko daude. Oso garrantzitsua da gogoraraztea segurtasun-kopiaren software fidagarria erabili behar dugula, daturik ez galtzeko eta datuak eraginkortasunez berreskuratzea bermatzeko.

Gainera, garrantzitsua da segurtasun-kopiak maiz egitea eta leku seguruetan biltegiratzea. Ahal dela, segurtasun-kopia zifratuak erabili behar dira. Azkenik, jardunbide egokia da segurtasun-kopiaren osasun ona ziurtatzea, berrezarpenak probatuz edo haren osotasuna egiaztatuz.

DigitAll

Segurtasuna

4.2 DATU PERTSONALEN ETA PRIBATUTASUNAREN BABESA

Segurtasuna

B2 maila 4.2 Datu pertsonalen eta pribatutasunaren babesa

Zer esan nahi du jaso dudan mezu honek?

Zer esan nahi du jaso dudan mezu honek?

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=30d082d80b7c3016bc4a3e52eab19eb910622511614 6b02efea319ca35b418dafd151fadb767d5c30dd56dcb8b2e975195f91bb4736cfb86e9e615c41407e0a9)

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.

Zer da mezu elektroniko hau? Segurtasun-urraketa baten jakinarazpena

Datu pertsonalen tratamendu-arduradunaren betebeharretako bat haien segurtasuna bermatzea da; hau da, funtsean, tratamendu-sistemen eta -zerbitzuen konfidentzialtasun, osotasun, eskuragarritasun eta erresilientzia iraunkorra bermatzea. Helburu horrekin, hartu beharreko teknika- eta antolamendu-neurriak hartu behar ditu.

Dena dela, batzuetan, ez dira neurri egokiak ezartzen, edo, hori eginda ere, ez da segurtasun horren urraketa eragozten. Bereziki, zibererasoen hazkunde esponentziala kezkagarria da.

Testuinguru horretan, Datuak Babesteko Erregelamendu Orokorrak ezartzen duenez, "datu pertsonalen segurtasuna urratzeak arrisku handia ekar badiezaieke pertsona fisikoen eskubide eta askatasunei, tratamendu-arduradunak interesdunari jakinaraziko dio". Mezu elektroniko hori segurtasunaren urraketa baten jakinarazpenaren adibide bat da.

Araudiaren arabera, jakinarazpen hori bidegabeko atzerapenik gabe egin behar da. Horrekin, kaltetuak lehenbailehen hartu beharreko neurriak hartu ahal izatea lortu nahi da. Adibidez, pasahitz batzuk konprometitu badira, haiek berehala aldatzea edo, kreditu-txartel baten zenbakia izan bada, hura ezeztatzea. Kasu horretan, kontuan hartu zibererasoa apirilaren 11n gertatu zela, baina posta-mezua 23an bidali zela, ziurrenik ez zirelako kaltetu ez pasahitzak ez banku-txartelak— horrek ez du esan nahi bat egiten denik hartutako irizpidearekin —, baina, bai, banku-kontuen zenbakiak.

DATU PERTSONALAK ERABILTZEN DITUZTEN SUBJEKTUEN BETEBEHARRAK

e.digitall.org.es/A4C42A2V07

⚠ ADI

Interesdunak eskubidea du tratamendu-arduradunak bere eskubide eta askatasunetarako arrisku handia dakarten datu pertsonalen segurtasun-urraketen berri eman diezaion.

Komunikazioaren edukia

Datuak Babesteko Erregelamendu Orokorrak xedatutakoaren arabera, komunikazio horrek eduki hau izan behar du:

a) Segurtasun-urraketaren izaeraren deskribapena, hizkera argi eta errazean. Kasu horretan zibererasoa izan dela azaldu da, baita zer izan den ere: "erakunde horien sistemak zifratzea eta eskuragaitz bihurtzea, haien jarduera erabat eragozteko asmoz, eta kaltetutako interesdunen datuak jakinarazteko mehatxua egitea", erreskatea ordaintzen ez bada. Finean, datu pertsonalen lapurreta duen ransomware bat deskribatzen ari da. Halaber, jakinarazi da enpresak ez duela behin betiko informaziorik galdu, ezta aplikaziorik ere, eta, beraz, zerbitzuek ez dutela kalterik izan. Edo bestela esanda, informazio guztia zuen segurtasun-kopia bat zegoela eta hura berrezarri dela.

b) Datuak babesteko delegatuaren izena eta harekin harremanetan jartzeko datuak edo informazio gehiago lortzeko beste harreman-puntu batenak. Kasu horretan, datuak babesteko delegatuari buruzko informazio orokorra eman da, eta gorabeherari buruzko galderak eta erantzunak biltzen dituen web-orri bat ere helarazi da.

c) Segurtasun-urraketaren balizko ondorioak. Kasu horretan, bi gairen berri eman da:

- Baliteke datu pertsonalak konprometituta egotea.
- Kalteak izan ditzaketen datuak honako hauek dira: izena, abizenak, posta-helbidea, telefonoa, helbide elektronikoa, NANa (edo baliokidea), jaioteguna, generoa, kontratatutako produktu/zerbitzuak eta banku-kontuaren zenbakia.

d) Tratamendu-arduradunak urraketari aurre egiteko, eta hala badagokio, ondorio kaltegarriak arintzeko hartutako edo proposatutako neurrien deskripzioa. Kasu horretan honako hauek jaso dira:

- Jarduera-plana aktibatzea, zibersegurtasunean aditua den kanpoko enpresa baten laguntzarekin.

OHARRA

S21sec-ek 2022an egindako *Threat Landscape Report* txostenaren arabera, Espainia seigarren postuan dago munduan zibererraso gehien jasaten dituzten estatuen rankingean. % 65 ransonware bidez.

- Gertakarien berri ematea Espainiako Babes Agentziari. Kontuan izan behar da jakinarazpen hori tratamendu-arduradunaren betebeharra dela, araudiak debekatu egiten baitu horrelako gorabeherak ezkutatzea.
- Salaketa Espainiako Polizia Nazionalaren aurrean, zibereraso horiek delitu baitira.
- Xantaia ordaintzeari uko egitea.

Komunikazio hori beharrezkoa ez duten kasuak

Araudiak zenbait kasu zerrendatzen ditu non ez den beharrezkoa segurtasun-urraketa bat jasaten duen erakundeak interesdunei jakinaraztea:

a) Tratamendu-arduradunak hartu beharreko babes-neurri teknikoak eta antolamendu-arlokoak hartu ditu, eta segurtasun-urraketak kaltetutako datu pertsonalei aplikatu zaizkie neurri horiek. Zehazki, datu pertsonalak baimendu gabeko edozein pertsonarentzat ulertezintzat bihurtzen dituzten neurriak dira, hala nola zifratzea.

b) Interesdunaren eskubideetarako arriskua gauzatzeko probabilitaterik ez dagoela bermatzen duten neurriak hartu dira ondoren.

c) Neurriz kanpoko ahalegina suposatzen du. Kasu horretan, interesdun bakoitzari jakinarazi ordez (aztertutako kasuan, kaltetua izan zitekeen bakoitzaren posta elektronikoko helbide zehatzera zuzendutako mezu elektroniko bat zen), komunikazio publiko bat egin da (prentsa, Internet, telebista eta abar), interesdunei ere jakinarazteko.

Informazio gehiago

29. artikuluko datuen babesari buruzko lantaldea. Datuen segurtasun-urraketen jakinarazpenari buruzko jarraibideak (WP 250). *e.digitall.org.es/articulo29*

DigitAll

Segurtasuna

4.3 OSASUNAREN ETA ONGIZATEAREN BABESA

Segurtasuna

B2 maila 4.3 Osasunaren eta ongizatearen babesa

Guraso-kontrola behar bezala erabiltzeko gida bisuala

Guraso-kontrola behar bezala erabiltzeko gida bisuala

Dokumentu honetan, guraso-kontrola zer den eta nola erabil daitekeen kontsulta daiteke. Guraso-kontrolak zerbitzu ugari eskaintzen dizkie haur eta nerabeak dituzten familiei, hala nola sarbidea eta teknologia-erabilera gainbegiratzea. Gainera, dokumentu honetan, Mariaren eta haren familiaren adibidearen bitartez guraso-kontrolaren utilitate nagusiak bizkor konfiguratzeko moduaren adibide bat ikus daiteke.

Guraso-kontrola: orokortasunak

Guraso-kontrola Interneterako edo gailu teknologikoetarako (ordenagailuak, tabletak edo mugikorrak) sarbidea eta erabilera monitorizatzeko eta mugatzeko aukera ematen duten neurrien multzoa da.

Guraso-kontrolerako tresnak hainbat zerbitzu teknologikotan aurki daitezke, haurrek eta nerabeek teknologia erabiltzen dutenean haien segurtasuna laguntzeko.

Tresna horiek baliagarriak izan daitezke arriskuak murrizteko, adingabeek Interneten arduraz eta autonomiaz jarduten ikasten duten heinean. Inola ere ez dute ordezkatzen pertsona heldu batek eskain dezakeen laguntza edo gainbegirada, baina lagungarriak izan daitezke ikaskuntza-prozesu digitalean.

⚠ ADI

Guraso-kontrolerako tresnak gurasoen bitartekotzaren parte dira. Ez dute ordezkatzen adingabeekiko eguneroko inplikazioa eta elkarrizketa: gurasoen bitartekotza-lan horretarako lagungarriak dira.
Tresna horiek arrakastaz funtziona dezaten, adingabeei zergatik diren beharrezkoak azaltzea komeni da. Halaber, garrantzitsua da funtzionalitateak haien garapen- eta heldutasun-mailara egokitzea.

GURASO-KONTROLA

Bideo honetan, guraso-kontrolaren kontzepturako eta haur eta nerabeen gailu mugikorretako tresna horien erabilera arduratsurako hurbilpena egingo da.

e.digitall.org.es/A4C43B2V03

Honako funtzio nagusi hauek identifikatzen dira:

- **Edukiak iragaztea:** adinaren arabera desegokitzat jotzen diren eduki jakin batzuetarako sarbidea blokeatzeko edo mugatzeko balio du (normalean sexu- edo indarkeria-izaerakoak). Funtzionalitate horretan, erosketak mugatzea, pertsonak blokeatzea edo hizkuntza edo hitz zehatzak iragaztea ere sar daitezke.
- **Denbora-kontrola:** ordutegi espezifiko bat edo gehieneko erabilera-denbora ezartzeko aukera ematen du, ordu edo denbora-muga jakin batera iristean nabigazioa etenda edo aplikazioa edo gailua blokeatuta. Era berean, alarmek ere jo dezakete, teknologia gehiegi erabiliz gero.
- **Jarduera gainbegiratzea:** adingabeak bisitatu dituen orriak eta harekin harremanetan jarri diren pertsonak gainbegiratzeko balio du.
- **Geolokalizazioa:** gailuaren kokapena, denbora errealean, eta aurretiko ibilbidea ezagutzeko aukera ematen du.
- **Konfigurazioaren babesa:** guraso-kontroleko doikuntzetan nahi ez diren aldaketak saihesteko balio du.

Guraso-kontrolerako tresnak eta funtzioak aldatu egiten dira herrialde batetik bestera, eta, oro har, ordenagailuen edo gailu mugikorren sistema eragileetan aurki daitezke, edo, bereziki, aplikazio, eduki digital, joko edo sare sozial jakin batzuetan. Hala, honako hauek dira guraso-kontroleko funtzionaltasunak ahalbidetzen dituzten adibide batzuk: Windows, iOS edo Android bezalako sistema eragileak; aplikazio espezifikoak, hala nola Family Link (jarraian azalduko da); eduki-hornitzaileak, hala nola Netflix edo YouTube, edo sare sozialak, hala nola TikTok edo Instagram.

GURASO-KONTROLA FAMILIA-TALDEAN

Bideo honetan, guraso-kontrolaren kontzeptua maila aurreratuago batera zabalduko da. Familia-talde bat nola kontrolatu azalduko da, edukiak, erosketak eta erabilera-denbora kudeatzeko hainbat gailuren adibideen bitartez.

e.digitall.org.es/A4C43C1V04

Family Link: guraso-kontrolerako tresnen oinarrizko konfigurazioaren adibidea

Aurreko atalean deskribatu den bezala, guraso-kontrolerako tresna ugari daude, eta hainbat formatutan aurki ditzakegu. Dokumentu honen ideia nagusia tresna horietarako hurbilpena egitea da. Horretarako, adibide zehatz bat hartuko da erreferentziatzat funtzionalitateak eta horien konfigurazioa ezagutzeko; kasu honetan, Googleren Family Link.

Family Link da merkatu teknologikoan doan eskura daitezkeen guraso-kontrolerako tresnetako bat.

1. irudia. Iturria: Sormen propioa.

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

Aurreko esteka Googleren Family Linken webgune ofiziala da. Plataformari eta aplikazioa familiaren gailuetan deskargatzeko behar diren estekei buruzko informazio osoa aurki daiteke.

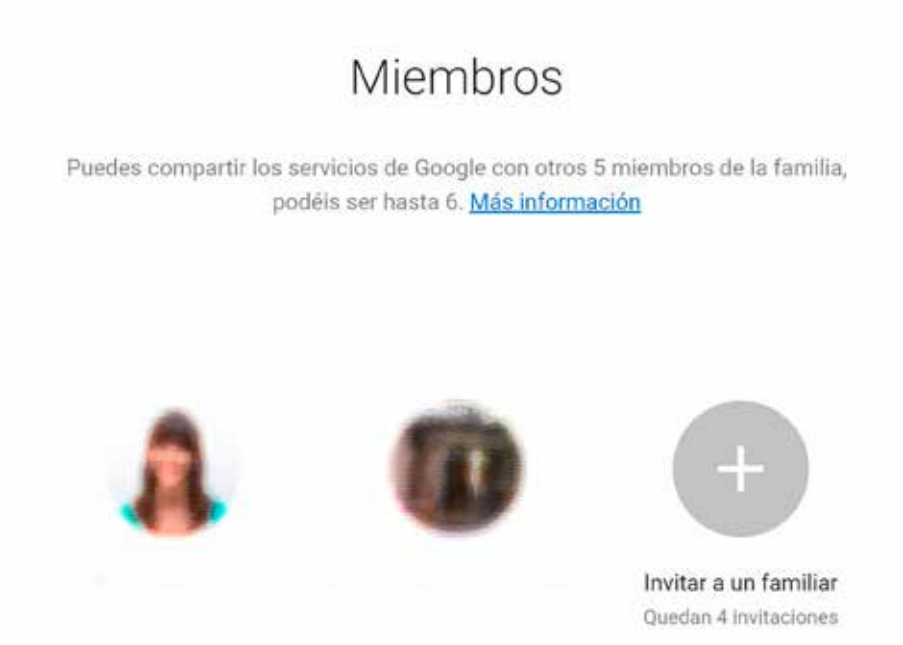
Aplikazioa instalatu aurretik, garrantzitsua da ziurtatzea konfiguratuko diren gailuak bateragarriak direla Family Linkekin. Horretarako, sistema eragilea eta mugikorren bertsioa kontsulta ditzakegu, bai amarenak edo aitarenak, bai adingabeenak.

⚠ ADI

Family Linken webgunean jakinarazten dute guztiz bateragarria dela sistema eragile hauen bertsio berberekin eta hobeekin, rolaren arabera:

Haurrentzako gailuak: Android 7.0 edo berriagoak.
Gurasoentzako gailuak: Android 5.0 edo berriagoak; iOS 11 eta berriagoak; Chrome OS 71 eta berriagoak.

Guraso-kontrolaren funtzioekin hasi aurretik, garrantzitsua da alderdi orokorrak konfiguratzea, programak uler dezan nork osatzen duen "familia". 1. irudian, Family Linken irudi bat ikusten da, eta 2. irudian, berriz, "familia" konfigurazioa.



2. irudia. Iturria: Sormen propioa.

Adibide horretako familia Maria izeneko neska baten aitak eta amak osatzen dute. 2. irudian ikusten da nola dagoen eratuta familia-taldea, baina neskatorik gabe. 3. irudian, Maria familia-taldean sartu da, "gainbegiratutako familia-kide" gisa.

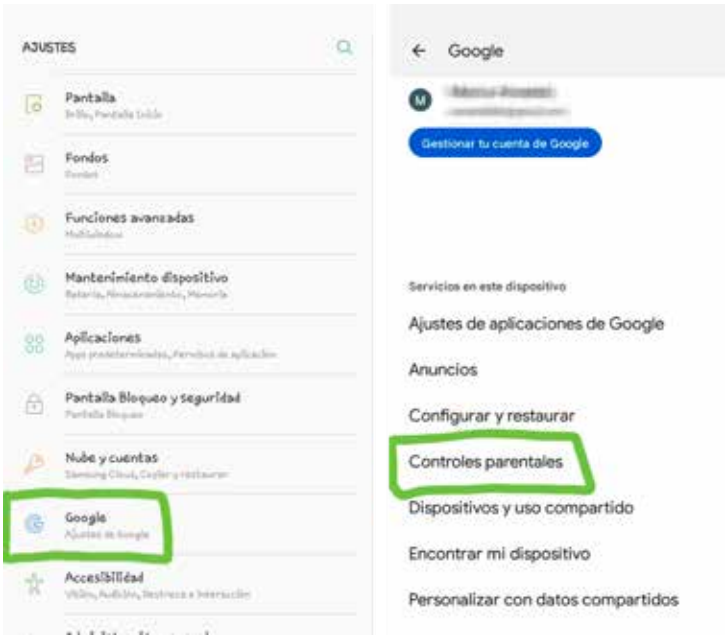
3. irudia. Iturria: Sormen propioa.

"Familia" konfigurazio horri esker, Family Link eta Googleren beste zerbitzu batzuk erabil daitezke, hala nola familientzako Google Calendar, familientzako Keep (oharrak eta zerrendak), Youtube Premiumen familia-planak, Google Playren familia-liburutegia, Google Play Pass edo Google One, besteak beste.

Haurraren edo nerabearen gailuaren konfigurazioa

Haurraren edo nerabearen gailuaren konfigurazioa erraza eta intuitiboa da. Family Linkek konfigurazio-prozesua gidatzeko jarraibide zehatzak eskaintzen ditu. Hurrengo orrialdeetan, konfigurazioaren alderdi garrantzitsuenen gida bat eskainiko da.

Adibide gisa erabilitako gailua Android sistema eragilea duen tableta bat da, eta, beraz, guraso-kontrola "Ezarpenak" atalaren bidez konfiguratzen da, 4. irudian ikus daitekeen bezala. Hona hemen urratsen segida: (1) Sakatu “Ezarpenak”, 2) sakatu “Google” eta (3) sakatu “Guraso-kontrolak”.



4. irudia. Iturria: Sormen propioa.

Tableta erabiltzen duenean Mariaren segurtasuna areagotzen duten hainbat alderdi konfiguratzen dira gailuan:

- **haurraren edo nerabearen Googleko kontua aitaren edo amaren kontuarekin lotzea familia-talde batean.**

Aukera guztiak baliatu ahal izateko gakoa da haurra edo nerabea familia-taldearekin behar bezala lotzea (3. irudian ikus daitekeen bezala) eta Mariaren posta elektronikoko kontua ama eta aitarenekin lotzea (5. irudia).

5. irudia. Iturria: Sormen propioa.

- **Haurra edo nerabea zer aplikaziotan sar daitekeen aukeratzea.**

Mariaren gailuak aplikazio ugari ditu. Aplikazio gehienak Mariak erabili ahal izateko instalatu badira ere, amak eta aitak zein aplikaziotarako sarbidea eman erabaki dezakete. 6. irudian, aplikazioak nola gaitu edo blokeatu daitezkeen erakusten da.

6. irudia. Iturria: Sormen propioa.

7. irudian, guraso-kontrolak aplikazioak automatikoki nola sailkatzen dituen eta, PEGI izenaz ezagutzen den sailkapenaren arabera, horiek erabiltzea nola gomendatzen duen ala ez azaltzen duten bi adibide daude. Gomendio horiek baliagarriak badira ere, garrantzitsua da gurasoek aplikazioak xehetasunez aztertzea.

7. irudia. Iturria: Sormen propioa.

- **Denbora-mugak ezartzea eta gehieneko denbora-errutinak sortzea**

Denbora-muga adingabe bakoitzaren adinaren eta familia-zirkunstantzien araberakoa da. Oro har, American Academy of Pediatrics (2016) erakundearen gomendioak jarrai daitezke.

⚠ ADI

American Academy of Pediatrics erakundeak gomendioak ematen ditu haurrek eta nerabeek, adinaren arabera, pantailak erabiltzen pasatu beharko luketen gehieneko denboraz:

18 eta 24 hilabete bitarteko adingabeak: bitarteko digitalen erabilera saihestu behar da.
2 eta 5 urte bitarteko adingabeak: egunean gehienez ere ordubetez egon daitezke eraginpean, eta zenbat eta denbora gutxiagoan, orduan eta hobeto.
7 eta 12 urte bitarteko adingabeak: gehienez ere ordubetez, pertsona heldu batek lagunduta.

12 eta 15 urte bitarteko adingabeak: gehienez ere ordu eta erdiz, eta bereziki sare sozialei arreta berezia jarrita.

16 urte baino gehiago: gehienez ere bi orduz, geletan pantailak saihestuta.

Guraso-kontrolaren bidez, gehieneko erabilera-denbora horiek asteko egunaren arabera doitu daitezke, eta aplikazio bakoitzaren gehieneko denbora ere doitu daiteke.

- Kokapen-doikuntzak kontrolatzea.
- Google Chrome, Bilaketa, Play eta Youtuben iragazkiak eta kontrolak definitzea.

Konfigurazio-aukeren artean, Interneten informazioa bilatzeko eta erosketak egiteko iragazkiak nabarmentzen dira. 8. irudian, Mariaren gurasoak neskak eskura ditzakeen webguneak baimentzeko edo blokeatzeko aukerak konfiguratzen ari dira. 9. irudian, Google Playn aplikazioak erosteko aukerak konfiguratzen ari dira.

8. irudia. Iturria: Sormen propioa.

9. irudia. Iturria: Sormen propioa.

Urrats guztiak egin badira, aplikazioa haurraren gailuan eta aitaren edo amarenean instalatuko da (10. irudia). 11. irudian, Mariaren tabletari buruzko informazioa agertzen da, bai eta guraso-kontrolerako tresnen bidez hura gainbegiratu ahal izateko konfigurazio zuzena ere.

10. irudia. Iturria: Sormen propioa.

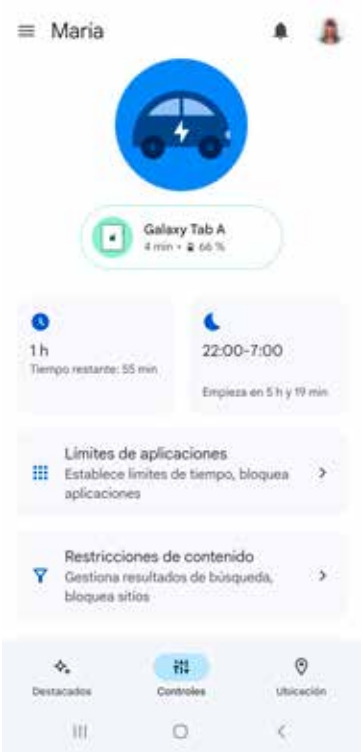
11. irudia. Iturria: Sormen propioa.

Amaren edo aitaren gailuaren konfigurazioa

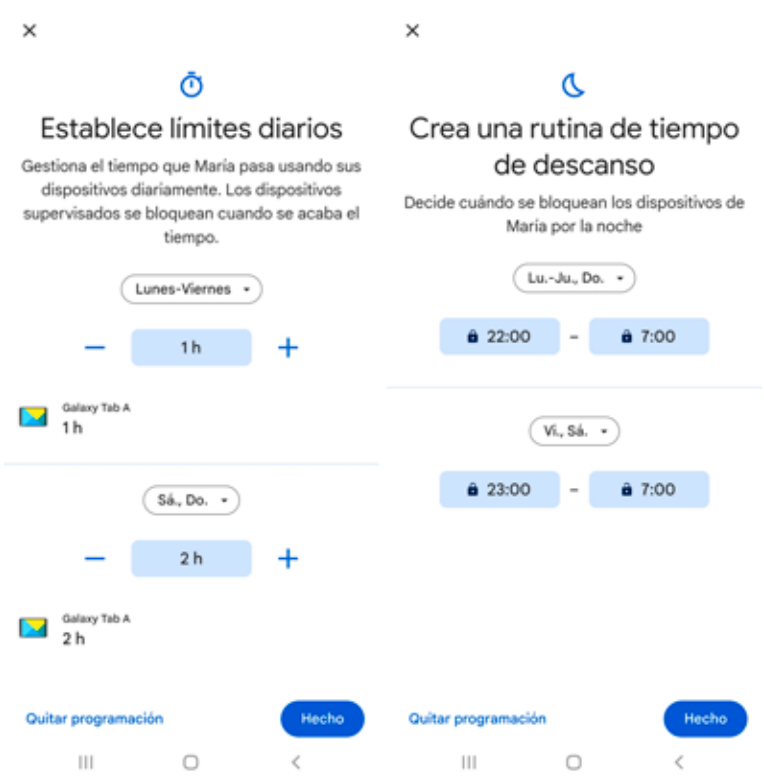
Amaren edo aitaren gailuan Family Link aplikazioa instalatu behar da.

Aplikazio horren bidez, Mariaren gailuan aldez aurretik konfiguratutako funtzionalitate guztiak konfiguratu eta doitu daitezke. Gainera, aplikazioak neskaren jardueraren jarraipena egiteko aukera ematen du. 12. irudia (eskuinean) Mariaren familiak urrutitik Mariaren gailuari eta haren erabilerari buruz kontsulta ditzakeen funtzioen irudi bat da.

Era berean, alderdiren baten konfigurazioa aldatu behar bada, aplikazio horren bidez egin daiteke. Adibidez, erabilera-denborak edo gailua itzaltzeko ordua konfiguratu edo alda daitezke, edo errutinak sor daitezke asteko egunen arabera (13. irudia). Denbora-muga aplikazio espezifikoen arabera ere konfigura daiteke; 14. irudian, Mariaren familiak 30 minutuko gehieneko muga eman dio Buenas Noches aplikazioa erabiltzeko.



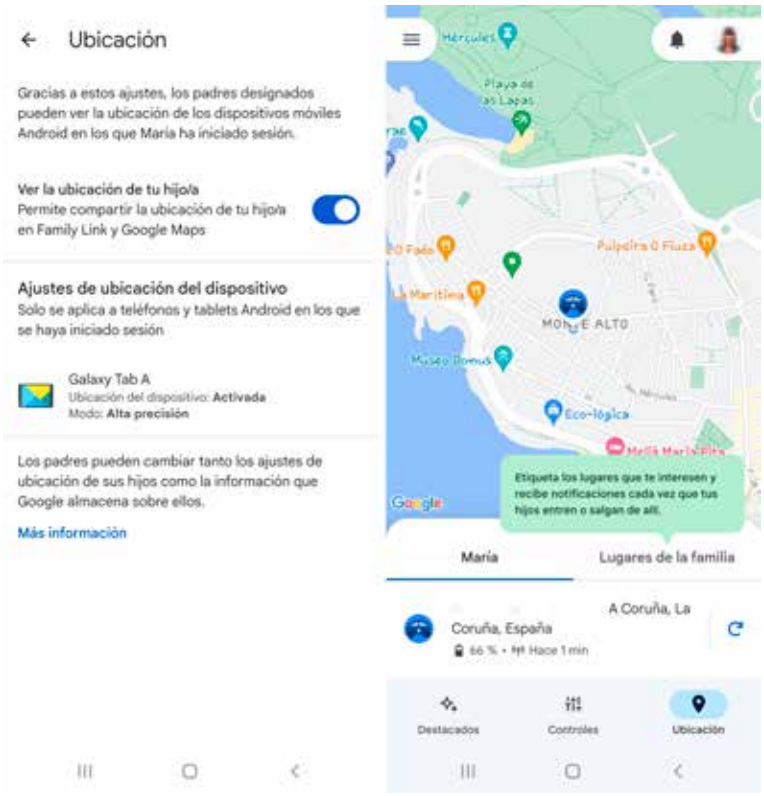
12. irudia. Iturria: Sormen propioa.



13. irudia. Iturria: Sormen propioa.

14. irudia. Iturria: Sormen propioa.

Adingabeekin ez gaudenerako guraso-kontrolerako tresnen beste utilitate interesgarrienetako bat geolokalizazioa da. 15. irudian, ezkerreko aldean, kokapenaren doikuntzak konfiguratzeko pantaila ikusten da, eta eskuineko aldean, nola bistaratzen den gailuaren kokapena denbora errealean.



15. irudia. Iturria: Sormen propioa.

Azkenik, funtsezkoa da gogoraraztea aplikazioen guraso-kontrolak ez dituela ordezkatzen familiako helduen laguntza eta gainbegirada. Hain zuzen, Family Linkek gomendatzen du konfigurazioa eta erabilera-terminoak adingabeek eta gurasoek batera egitea, errespetuzko hazkuntza-modu gisa.

Teknologia erabiltzeko familia-itunen adibideak:
e.digitall.org.es /pactos-familiares

Webgunean, teknologia behar bezala erabiltzeko familia-itunen adibide zehatzak kontsultatu eta deskarga daitezke (sare sozialak, bideokontsolak, tableta eta mugikorra, besteak beste).

Informazio gehiago

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

Guraso-kontrolerako tresnen gida. Zibersegurtasunaren Estatuko Institutua (INCIBE). *e.digitall.org.es/guia-control-parental*
Adingabeek Internet modu seguruan eta arduratsuan erabiltzeko guraso-bitartekotzarako gida. Zibersegurtasunaren Estatuko Institutua (INCIBE). *e.digitall.org.es/mediacion-parental*

Guraso-kontrolerako tresnak. Kontrol-tresnak bilatzea. Zibersegurtasunaren Estatuko Institutua (INCIBE). *e.digitall.org.es/control-parental*

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

Gailuak behar bezala erabiltzeko familia-itunak. Zibersegurtasunaren Estatuko Institutua (INCIBE). *e.digital.org.es/pactos-familiares-incibe*

DigitAll

Segurtasuna

4.4 INGURUMENAREN BABESA

B2 maila 4.4 Ingurumenaren babesa

Hiru ingurumen-ardatzetatik ekonomia zirkularrera

Hiru ingurumen-ardatzetatik ekonomia zirkularrera

Sarrera

Dokumentu honetan xehetasun handiagoz landuko dira mailako bideoetan txertatu diren kontzeptuak, hala nola "murriztu, berrerabili, birziklatu" ingurumen-proposamen klasikoaren ikuspegia zabaltzen duten ardatzak.

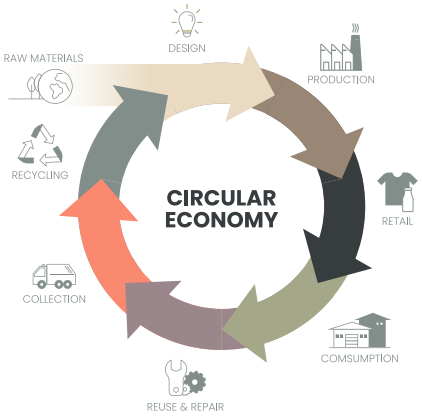
Ikusiko dugu ardatz berriei lotutako kontzeptu-zabalkuntza, Berrebaluatu, Konpondu, Berregituratu, Birbanatu edo Birkokatu terminoen bidez, lotuta dagoela "deshazkunde" kontzeptuari atxikitzen zaizkion proposamen teorikoekin, ekoizpen- eta kontsumo- ereduari lotutako gaur egungo ingurumen-arazoetara hurbiltzeko alternatiba gisa.

Eta, hain zuzen ere, gizarte- eta ingurumen-jasangarritasunaren mailak handitzea bilatzen duen eredu ekonomiko alternatiboaren proposamena baita, ekonomia zirkularrera hurbilduko gara. Proposamen horren helburua da ekonomia berri bat ezartzea, produktuen, zerbitzuen, hondakinen, materialen, uraren eta energiaren bizi-zikloa ixteko printzipioan oinarrituta.

Ekonomia zirkularraren oinarriak aurkezteaz gain, teknologia digitalekin lotutako produktu eta zerbitzuen adibide zehatzak aurkeztuko ditugu. Produktu eta zerbitzu horiek beren diseinutik bertatik abiatutako birkontzeptualizazio bati heltzen diote, ingurumenean eta gizartean dituzten inpaktuak minimizatzeko.

Hiru ardatzetatik harago: desazkunde-proposamenak

Aurreko mailetan aztertu dugu nola, teknologia digitalaren ingurumen- eta gizarte-inpaktuak murrizteko, eredu ekonomikoa birplanteatu behar den, kontsumoa eta ekoizpena murriztera bideratuta, giza ongizatea eta planetako ingurumen-baldintzak hobetzeko.



Ideia horretatik abiatuta, garrantzitsua da hori lortzeko bideetan sakontzea. Lehenik, hiru ingurumen-ardatz klasikoak erabil ditzakegu: murriztea, berrerabiltzea eta birziklatzea. Sail honetako **"Teknologia mugikorraren kontsumo arduratsurako aukerak"** (v.5) eta **"Jasangarritasunari ardatzak gehitzen: ekonomia zirkularra"** (v.4) bideoetan ikusi dugun bezala, produktu eta gailu teknologikoen kontsumoa murriztu behar dugu, benetako premiak kontuan hartuta eta zaharkitze-estrategiei adi gaudela; ahal den neurrian, oraindik ere bizitza erabilgarria izan dezaketen aparatu eta osagaiak berrerabili behar ditugu baliabide natural berriak galtzea saihesteko, eta azkenik, sektore teknologikoaren funtzionamendurako beharrezkoak diren elementuak birziklatzeko prozesuak optimizatu behar ditugu, elementu horiek ezinbestekoak baitira hornidura-kateak mantentzeko eta gero eta garestiagoa baita haien erauzketa ingurumen- zein gizarte-aldetik.

JASANGARRITASUNARI ARDATZAK GEHITZEN: EKONOMIA ZIRKULARRA

Ekonomia zirkularrak kontsumo teknologikorako dituen proposamenak aztertzea, prozesuak irizpide jasangarriekin "birdiseinatzean" oinarrituak. "Sehaskatik sehaskara" diseinuen adibideak emango ditugu.

e.digitall.org.es/A4C44B2V04

TEKNOLOGIA MUGIKORRAREN KONTSUMO ARDURATSURAKO AUKERAK

Zehaztasun handiagoz erakusten dira teknologia mugikorraren kontsumo arduratsu eta jasangarrirako hainbat aukera, hala nola autokonponketa-tailerrak eta Fairphone edo "bidezko telefonoa".

e.digitall.org.es/A4C44B2V05

Baina oso litekeena da horrekin nahikoa ez izatea. Gure ekoizpen- eta kontsumo-ereduan egiturazko aldaketak lortzeko, beste proposamen mota batzuk beharko ditugu, maila sakonagoan alternatibak ekarriko dituztenak; izan ere, frogatuta geratu da hiru ardatzak gaur egungo sistema ekonomikoaren zati gisa barneratu direla eta hartara, gizarte- eta ingurumen-arazoetan nolabait adabakiak jartzea lortzen dutela, baina zergatiak benetan aldatzen lagundu gabe.

Hor sartzen dira jokoan beste proposamen alternatibo batzuk, hala nola dokumentu honetan aurkeztuko ditugunak. Lehenik eta behin, azken urteotan nazioarteko testuinguruan ospea hartzen ari den kontzeptu batean jarriko dugu arreta: deshazkundea.

Deshazkundea mugimendu filosofiko eta aktibista bat da, jatorria Frantzian duena: bertako *décroissance* proposamena deshazkundearen aldeko gainerako mugimenduen jatorri gisa har dezakegu. Serge Latouche ekonomialari eta filosofo frantsesa da *décroissance* proposamenaren sortzailea. Latouchek hazkunde etengabea helburu nagusi ez duen sistema ekonomiko baterako hainbat bide eta balizko hurbilketa proposatu ditu zenbait lanetan: besteak beste, "Deshazkunde lasaiaren tratatu txikia" (2009), "Deshazkundearen ordua" (2012) edo oraintsuko "Deshazkunderako hurbilketa" (2022) lanak nabarmen daitezke.

⚠ ADI

Xehetasunei helduta, bere proposamena hiru ardatzak zortzira zabaltzean oinarritzen da, deshazkundearen zutabe gisa: Berrebaluatu, Birkontzeptualizatu, Berregituratu, Birkokatu, Birbanatu, Murriztu, Berrerabili eta Birziklatu (Latouche, 2009).

Sektore digitalean murriztu, berrerabili eta birziklatzeko beharrari buruz jada ezagunak diren proposamenez gain, gainerako bosten aplikazio bat honela eman liteke, adibidez:

1 | **Berrebaluatzea**, gailu digitalen ekoizpenaren kostuari balio berri bat emateko. Jakin behar dugu ez dugula ekoizpenaren benetako kostua ordaintzen, kontuan hartzen baditugu ekoizpenaren deslokalizazioa edo ingurumen-kostuak.

2 | **Konpontzea.** Nabarmendu behar da produktuek konponketa errazteko diseinatuta egon behar dutela, eta ez direla behar baino lehen bota behar. Horretarako, ezinbestekoa da hori erraztu eta babestuko duen araudia izatea, teknologiaren sektorean hain ohikoak diren zaharkitze-estrategiak saihesteko.

3 | Berregituratzea gailu digitalen ekoizpen- eta merkaturatze-ereduak, produkzio-prozesuan esku hartzen duten eragile guztiak eta ingurunean haiek duten eragina kontuan hartuta.

4 | Birkokatzea produkzio-prozesuak, tokiko produktuari balioa emateko; izan ere, eragin txikiagoa izango du ingurunean, eta gehiago lagunduko du hurbileko ekonomia hobetzen. Filosofia hori sektore digitalean aplikatzea zaila da, ekoizpen- eta hornidura-kateak oso lokalizatuta baitaude, baina erronka horri aurre egin behar diogu gizarte gisa.

5 | Birbanatzea teknologia digitalaren ekoizpen- eta kontsumo-ereduaren kostuak eta onurak, honako ideia honekin: mundu guztiak herrialde industrializatuetan bezala kontsumituko balu eredu hori guztiz bideraezina izango litzateke.

Ekonomia zirkularrerako hurbilketa

Deshazkunde-proposamenen ildotik, ekonomia zirkularra ekoizpen- eta kontsumo-eredua eraldatzeko proposamen gisa agertzen da, materialak eta produktuak ahalik eta gehien partekatzea, alokatzea, berrerabiltzea, konpontzea, berritzea eta birziklatzea dakarrena, horrela baliabideak agortzea eta prozesuaren ingurumen-inpaktuak mugatzeko.

Deshazkundearen proposamena zirkulu akademikoetatik eta aktibistetatik abiatu da, baina hainbat erakundek ekonomia zirkularra maila politikoko apustu sendo gisa hartu dute. Adibidez, Europar Batasuna eta Europar Batasuneko erakundeak lege-esparruaren erreforman ari dira lanean, hondakinen gaur egungo kudeaketa-ereduaren aldaketa sustatzeko, zeina lineala baita, benetako "ekonomia zirkular" baten alde egiteko.

Ekonomia zirkularraren helburua, funtsean, produktuen bizi-zikloa luzatzea da. Horrek esan nahi du, praktikan, hondakinak zein ekoizpen-ereduaren ingurumen- eta gizarte-inpaktuak ere ahalik eta gehien murriztea. Ikuspegi horretatik, sektore teknologikoa izango litzateke ekoizpen-ereduaren eraldaketarekin onura gehien izango luketenetako bat.

Gaur egun, produktu bat bere bizitzaren amaierara iristen denean, materialak ekonomiaren barruan mantentzen dira, ahal den guztietan, birziklatzeari esker. Horiek behin eta berriz erabil daitezke, eta, horrela, balio gehigarri bat sortzen da, baliabidearen beraren aprobetxamenduarekin zerikusia duena, baina baita baliabide-erreserba gehiago (mugatuak dira) ez ustiatzearekin ere.

Izan ere, ekonomia zirkular baterantz aurrera egiteko arrazoi nagusietako bat lehengaien gero eta eskari handiagoa eta baliabide-eskasia da. Funtsezko lehengai batzuk mugatuak dira, eta munduko biztanleria hazten ari denez, eskariak ere gora egiten du.

Ekonomia zirkularraren eredua egonkortzeak kontrastea ekarriko luke eredu ekonomiko lineal tradizionalarekin, hura, batez ere, "erabili eta bota" kontzeptuan oinarritzen baita eta material eta energia merke eta eskuragarri asko eskatzen baititu. Teknologia digitalen sektoreari dagokionez, aurreko mailetan ikusi ditugu erauzketa-prozesuekin lotutako gizarte- eta ingurumen-gatazkak.

Era berean, ikusi genuen ingurumen-inpaktuak ez direla baliabideak erauztera eta agortzera mugatzen. Ekonomia zirkularraren beste onura bat berotegi-efektuko gasen urteko emisio orokorrak murriztea da.

OHARRA

Europako Ingurumen Agentziaren arabera, prozesu industrialek eta produktuen erabilerak EBko berotegi-efektuko gasen emisioen % 9, 10 eragiten dute, eta hondakinen kudeaketak, % 3,32 (Europako Parlamentua, 2023).

Gainera, diseinutik bertatik produktu jasangarriagoak sortzeak, ekodiseinuaren edo "sehaskatik sehaskara" ikuspegiaren printzipioak eta premisak betez, energia- eta baliabide-kontsumoa murrizten ere lagunduko luke; izan ere, kalkulatu da produktu baten ingurumen-inpaktuaren % 80 baino gehiago diseinu-fasean zehazten dela.

Hori guztia nahikoa izango ez balitz, azterlan batzuek kalkulatu dute ekonomia zirkularrago baterako trantsizioak lehiakortasuna areagotu, berrikuntza sustatu, hazkunde ekonomikoa bultzatu eta enplegua sor lezakeela. Europako Parlamentuaren datuen arabera (2023), 2030erako gutxienez 700.000 lanpostu sortu ahal izango dira Europar Batasunean, ekoizpen-eredua eraldatzeko prozesuei esker.

Beraz, ekonomia zirkular berri baterako materialak eta produktuak birdiseinatzeak ekonomiaren hainbat sektoretako berrikuntza ere bultzatuko luke.

Azkenik, nabarmendu behar da ekonomia zirkularraren aldeko apustua benetan eraginkorra izan dadin, erakundeek araudi mailan babestu behar dutela. Egia da planeta mailan prozesu hori errealitate izatetik urrun dagoela oraindik, baina Europako testuinguruan baiezta daiteke ekonomia zirkularraren aldeko apustua nahiko irmoa dela.

Adibidez, Europako Batzordeak Ekonomia Zirkularrerako Ekintza Plana aurkeztu zuen 2020ko martxoan. Plan horrek, produktu jasangarriagoen diseinua eta hondakinen murrizketa sustatzeaz gain, herritarren partaidetza- eta ahalduntze-prozesuak ere bultzatzen ditu, "konpontzeko eskubidea" bezalako ekimenen bidez. Araudi horretan, jakina, arreta berezia jartzen da baliabideetan intentsiboak diren sektoreetan, hala nola elektronikan eta IKTetan.

Ondoren, 2021eko otsailean, Europako Parlamentuan ekonomia zirkularrari buruzko ekintza-plana bozkatu zen, eta birziklatzeari buruzko lege eraginkorragoak promulgatzeko neurri gehiago eskatu ziren, baita material-erabileraren eta -kontsumoaren ondoriozko aztarna ekologikoa murrizteko helburu lotesleak formulatzea ere, sektore digitalari zuzenean eragingo lioketenak.

OHARRA

2022. urtean, ekonomia zirkular baterako trantsizioa bizkortzeko lehen neurri sorta ezagutarazi zuen Batzordeak, eta bilgarriei buruzko arau berriak proposatu zituen Europar Batasun osorako, ekodiseinu-proposamenetan oinarrituak. Gainera, Batzordeak oinarri biologikoa duten elementuetarako eta biodegradagarrietarako trantsizioa proposatu du, hala nola elementu bio-plastikoetarakoa.

Beraz, ikusten ari garen bezala, ekonomia zirkularra oso oinarri erreala duen proposamen eraldatzailea da; izan ere, Europa mailako erakundeen eta arauen babesak produkzio-eredua aldatzen hasteko oinarri sendoa bermatzen du, eta, jakina, eredu hori berretsi egin beharko da herrialde bakoitzaren kasu berezien eta gizarte-portaeren arabera, eredu jasangarriago baterako trantsizioa bermatzeko.

Informazio gehiago

Europako Batzordea (2023) Ekonomia Zirkularrerako Ekintza Plana. *e.digitall.org.es/economia-circular*

Latouche, Serge (2009) "Deshazkunde lasaiaren tratatu txikia". Icaria. *e.digitall.org.es/icaria*

Latouche, Serge (2022) "Deshazkunderako hurbilketa". Popular. *e.digitall.org.es/decrecimiento*

Europako Parlamentua (2023) Ekonomia zirkularra: definizioa, garrantzia eta onurak. *e.digitall.org.es/beneficions-economiacircular*

Europako Parlamentua (2022). Konpontzeko eskubidea: Europako Parlamentuak produktu iraunkorragoak eta konpontzen errazagoak nahi ditu. *e.digitall.org.es/derecho-reparar*

Research & Degrowth (Ikerkuntza eta Deshazkundea) (2023). *degrowth.org*

DigitAll

Gaitasun
digitaletan
prestakuntza

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