DigitAll

Gaitasun
digitaletan
prestakuntza

4

Segurtasuna

DigitAll

Gaitasun
digitaletan
prestakuntza

Segurtasuna

B1 maila

AURKIBIDEA

DigitAll

Segurtasuna

4.1 GAILUEN BABESA

Segurtasuna

B1 maila 4.1 Gailuen babesa

Saioak eta web-autentifikazioa

Saioak eta web-autentifikazioa

Web-nabigazioak nola funtzionatzen duen ulertzea funtsezkoa da gure online-egunerokotasunerako. Erosketak egiteko, kudeaketak egiteko, informazioa bilatzeko edo film bat ikusteko erabiltzen dugu weba. Web-zerbitzuetako gure kontuak babesten laguntzeko, **web-autentifikazioak eta saioek nola funtzionatzen duten** ikusiko dugu jarraian.

Zerbitzariak eta nabigatzaileak

Aurreko mailetan ikasi dugun bezala, web-nabigazioak zerbitzariak eta nabigatzaileak erabiltzen ditu funtzionatzeko. Erabiltzen ditugun zerbitzu gehienek, web-orri estatikoak izan beharrean, zenbait funtzionalitate eskaintzen dituzte. Zerbitzu horiei "web-aplikazio" deritze.

Web-orri estatikoek zein web-aplikazioek **web-helbideak** edo URLak erabiltzen dituzte, DNSaren bidez IP helbide bihurtzen direnak. Horrela, gure nabigatzailea zerbitzarian ostatatutako baliabideetara sar daiteke. Zerbitzarian ostatatutako irudi, orri edo dokumentu bakoitzak URL desberdina du. Gure nabigatzaileak **eskabide bat egiten du edukiko, HTTP protokoloaren bidez.**

Web-saioetarako hurbilpena

Kasu batzuetan, zerbitzariak **gure identitatea ezagutu behar du eduki pertsonalizatua edo geuk bakarrik eskura dezakeguna eskaintzeko**. Adibidez, sare sozial bateko mezu pribatuak. Kasu horretan, sare sozialeko web-aplikazioak autentifikatu egin behar gaitu geure kontura sartzen garenean.

Web-saioak nabigatzailearen HTTP-eskaera bakoitza gurekin identifikatzeko erabiltzen dira. Aplikazioko geure kontura sartu ondoren, **zerbitzariak saio-identifikatzaile bat ematen digu**. Nabigatzaileak zerbitzariari egindako eskaera bakoitzean identifikatzaile hori sartuko du, geu garela eta kontura sartu garenean geure nortasuna egiaztatu dugula jakinarazteko.

Saio-identifikatzailea saio-cookieetan gordetzen da, nabigatzaileak nabigazioan gordetzen duen fitxategi txiki batean. Zerbitzariak HTTP-eskaera bat jasotzen duenean,

NABIGAZIOA WEB SEGURUA

Web-nabigazioa gure egunerokotasunaren parte da. Bideo honek URL bat zer den eta zerbitzariaren eta nabigatzailearen arteko komunikazioak nola funtzionatzen duen azaltzen digu.

e.digitall.org.es/A4C41A1V06

COOKIEAK, SAIOAK ETA PRIBATUTASUNA WEBEAN

Web-saioak web-eskaerak baimentzeko erabiltzen dira. Saio-cookieek informazio hori mantentzen dute. Hala ere, badira gure pribatutasunari eragin diezaioketen beste cookie batzuk.

e.digitall.org.es/A4C41C1V09

nabigatzaileak cookiea kontsultatu eta identifikatzailea bidaltzen du eskaeran. Horrela, geure kontura sartu garenez eta zerbitzariak identifikatzaile bat esleitu digunez, geure mezu pribatuak baino ez dira erakusten, eta ez beste pertsona batenak. **Nabigatzaileak saio-identifikatzaile horren arabera zer eduki erakutsi aukeratzen duenean ematen da baimena.**

Cookieek iraungitze-aldi desberdinak izaten dituzte, web-saioek bezala. Autentifikatzen gaituztenean eta zerbitzariak identifikatzailea esleitzen digunean definitzen da hori. Erasotzaile batek saio-identifikatzailea lapurtzen badigu, gu izango balitz bezala jardun dezake. Hala ere, iraungitze-epea laburra bada, erasotzaileak sarbidea luzaroan mantentzea saihesten du horrek.

Erregistroa, autentifikazioa eta saioak

Kontu batekin web-zerbitzuak erabiltzeko, lehenik eta behin zerbitzuan erregistratzen gara. Erabiltzaile-izenaz eta erregistrorako bererako behar diren datuez gain, autentifikazio-metodoa ere konfiguratzen dugu une horretan. Web-aplikazio gehienetan, lehenetsitako metodoa pasahitza da.

Puntu honetan, garrantzitsua da gogoratzea autentifikazioa eta baimena ez direla gauza bera. Autentifikazioak erabiltzailearen identitatea egiaztatzen du, pasahitzaren moduko metodoren bat erabiliz. Baimenak, aldiz, baliabideren bat erabiltzea ahalbidetu edo ukatzen du irizpideren baten arabera, hala nola erabiltzaile baten identitatea, saio-identifikatzailearen bidez. Zerbitzu bat lehen aldiz erabiltzen dugunean, honako hau egiten dugu:

1 | Erregistroa

- Kontu bat sortzeko, sartu beharreko datuak sartzen ditugu.
- **Autentifikazio-metodoa** ezartzen dugu; normalean, pasahitza.

2 | Autentifikazioa

- Kontura sartzeko, identifikatu egiten gara.
- Web-aplikazioak gure identitatea **egiaztatzen du**, erregistroan zehar aukeratutako metodoarekin.
- Zerbitzariak **saio-cookie bat** instalatzen du gure nabigatzailean.

BENETAN NOR ZAREN ESATEN DUZU?

Autentifikaziorako HURBILPENA

Autentifikazioa identitatea egiaztatzeko prozesua da. Hori mundu digitalean egiteko, hainbat metodo daude, denak hiru mota nagusietako batean oinarrituak: ni naizen zerbait, nik dakidan zerbait edo nik daukadan zerbait.

e.digitall.org.es/A4C41A2V06

3 | Web-baliabideetarako irispidea

- Geure kontura sartu ondoren, informazio pribatua kontsultatzen dugu. Adibidez, sare sozial bateko gure mezuak.
- Mezuetara sartzeko, nabigatzaileak **eskaera bidaltzen du saio-cookiearekin**.
- Zerbitzariak identifikatu egiten gaitu eta baliabide pribatura sartzeko eskaera **baimentzen du**: sare sozialeko gure mezuetara, alegia.

4 | Saioa itxi

- Zerbitzariak identifikatzailea ahaztu eta nabigatzaileak ezabatu egiten du.
- Eskaerarik eginez gero, zerbitzariak sarbidea ukatzen du eta berriro ere geure burua autentifikatzera behartzen gaitu.

Web-aplikazio gehienek prozesu hori partekatzen dute. Hala ere, kasu zehatzak daude horietako bakoitzean. Diferentzia nagusia erabilitako autentifikazio-metodoa da.

Gogoratuko duzunez, seguruena autentifikazio-metodo bat baino gehiago erabiltzea da. Zerbitzu askok **faktore anitzeko autentifikazioa** (MFA) edo **bigarren autentifikazio-faktore** bat (bi faseko autentifikazioa) erabiltzeko aukera ematen dute. Adibidez, pasahitzarekin batera, TOTP kodeak erabil ditzakegu aplikazio batean, kode-sorgailu batekin edo segurtasun-giltza batekin. Hartara, erasotzaile batek gure pasahitza lortzen badu, bigarren autentifikazio-faktorerako sarbidea ere lortu beharko du.

Azkenik, konturako sarbidea galtzen badugu, zerbitzuak **kontua berreskuratzeko** aukera eman ohi du erregistratu dugun helbidera mezu elektroniko bat bidalita. Beste aukera arrunt bat erabilera bakarreko kode batzuk deskargatzea da, **berreskuratze-kode** gisa ezagutzen direnak.

TOKENETAN OINARRITUTAKO AUTENTIFIKAZIOA: NIK DAUKADAN ZERBAIT

Faktore anitzeko autentifikazioa fisikoki daukagun zerbaitean oinarritu daiteke, token batean. Horren adibide dira segurtasun-giltzak, TOTP kodeak edo SMS kodeak. Horiek guztiek gure kontuen segurtasuna hobetzen dute beste metodo batekin batera erabiltzen direnean.

e.digitall.org.es/A4C41C1V07

⚠ ADI

Posta elektronikoko zeure kontua babestuta eduki! Erasotzaile batek hura eskuratzen badu, kontua berreskuratzeko funtzionalitatea erabil dezake beste zerbitzu batzuetarako sarbidea lortzeko.

Segurtasuna

B1 maila 4.1 Gailuen babesa

Cyber Kill Chain

Cyber Kill Chain

Gaur egun, gero eta ohikoagoak eta sofistikatuagoak dira zibererasoak. Gure burua haien aurka eraginkortasunez defendatu ahal izateko, funtsezkoa da sistemak konprometitzeko erasotzaileek erabiltzen duten prozesua ulertzea. Dokumentu honetan, xehetasunez azalduko da Cyber Kill Chain kontzeptua, eta adibide gisa eraso bat aztertuko dugu, faseak nola aplikatzen diren erakusteko.

2020an, SolarWinds enpresak oso zibereraso sofistikatua jasan zuen, eta horren ondorioz, erasotzaileek milaka erakundetako sistemetara jo zuten (mundu osoko gobernu-agentziak eta enpresa handiak barne). Cyber Kill Chainen zazpi faseei jarraikiz egin zen erasoa.

Cyber Kill Chainen faseak

Cyber Kill Chainek zazpi fase ditu. Lehenengo faseak erasotzailearen prestaketari dagozkio, eta azkenak, berriz, erasoaren ustiapenari eta azken helburuari.

> ***Informazio gehiago***
>
> Zibersegurtasunean espezializatutako hainbat organismotan Cyber Kill Chaini eta haren aplikazioei buruzko informazioa aurki dezakezu. Adibidez, INCIBEn: *e.digitall.org.es/fases-ciberataque*

1 | Azterketa

Lehenengo faseak erasoaren helburua aztertzea bilatzen du. Adibidean, erasotzaileek SolarWinds eta haren bezeroak ikertu zituzten hasieran. Online-ko bilaketa-teknikak erabili zituzten balizko kalteberatasunak eta helburuak identifikatzeko, eta SolarWinds sareari eta sistemei buruzko informazioa bildu zuten.

2 | Prestaketa

Jarraian, erasorako beharrezkoak diren armak edo malwarea sortzen dira. Adibidean, erasotzaileek malware pertsonalizatu bat sortu zuten, SUNBURST izenekoa, SolarWindsen softwarearen eguneraketa batean integratu zena. Eguneraketa horren helburua zen SolarWindseko bezeroei banatu eta erasotzaileei haien sistemetara baimenik gabe sartzen uztea.

3 | Entrega

Arma sortu ondoren, eraso-bektorea bilatzeko eta malwarea entregatzeko unea da. Adibidean, erasotzaileek "supply chain attack" izeneko teknika erabili zuten haiek sortutako malwarea banatzeko. Biktimei zuzenean eraso beharrean, erasotzaileek konfiantzazko software-hornitzaile bat konprometitu zuten (kasu honetan, SolarWinds) eta malwarea banatu zuten haren software-eguneraketen bidez.

4 | Ustiapena

Erasotzaileek lehen fasean aurkitutako kalteberatasunak fase horretan ustiatzen dira. Adibidean, malwarea SolarWindseko bezeroen sistemetan behin instalatuta, erasotzaileak sistemen kalteberatasunak ustiatzen hasi ziren, erabateko kontrola lortzeko. Engainu-teknikak erabili zituzten saioa hasteari buruzko informazioa eta langileen kredentzialak lortzeko, baita barne-sarera sartzeko tresnak ere.

SISTEMA INFORMATIKOAK EZ DIRA PERFEKTUAK: KALTEBERATASUNAK

Erasotzaileek ustia ditzaketen sistema informatikoen akatsak dira kalteberatasunak. Kalteberatasun bat aurkitzen bada, "0-day" esaten zaio. Horiek konpontzeko, fabrikatzaileek adabakiak diseinatu eta eguneraketa gisa aplikatzen dituzte.
e.digitall.org.es/A4C41B1V04

5 | Komandoa eta kontrola

Sistema biktimarako sarbidea behin lortuta, erasotzaileek ez dute beren armaren kontrola galtzen. Fase horretan, infektatutako biktimarekin komunikatzen dira, "Command & Control" (C2) izeneko zerbitzariak erabiliz. Adibide horretan, erasotzaileek tresna gehigarriak ezarri zituzten epe luzerako sarbidea eta konprometitutako sistemen gaineko kontrola mantentzeko. Ihes egiteko teknikak ere erabili zituzten, beren jarduera ezkutatzeko eta segurtasun-sistemek ez detektatzeko.

6 | Helburuen gaineko ekintza
Azkenik, erasoa egiten da, erasotzaileen helburu nagusiarekin bat. Adibidean, erasotzaileen azken helburua informazio konfidentziala ateratzea zen. Konprometitutako sistemetarako sarbidea izan zutenean, erasotzaileek datu kalteberak deskargatu eta atera zituzten, gobernuaren eta enpresen informazioa barne.

Zertarako erabiltzen da Cyber Kill Chain?

SolarWindsen kontrako zibererasoa Cyber Kill Chainen faseak jarraitzen dituen eraso zibernetiko baten adibide oso sofistikatua izan zen. Erasoak agerian utzi zuen garrantzitsua dela segurtasun-jarrera sendoa izatea eta online egon daitezkeen mehatxuen aurrean adi egotea. Gainera, nabarmendu zuen garrantzitsua dela hornidura-katea indartzea eta softwarearen eta zerbitzuen hornitzaile guztietan kontrol zorrotzak ere egin behar direla zibererasoen arriskuak arintzeko.

Cyber Kill Chain kontzeptua esparru baliagarria da ulertzeko erasotzaileek nola konprometitu ditzaketen sistemak eta zer neurri har ditzakegun geure burua defendatzeko. Garrantzitsua da kontuan hartzea eraso bakoitza bakarra dela, eta fase bakoitzak garrantzi handiagoa edo txikiagoa izan dezakeela egoeraren arabera. Cyber Kill Chainek nola funtzionatzen duen ulertuta, onlineko segurtasun-jarrera hobetu dezakegu, eta hobeto prestatuta egon gaitezke zibererasoak detektatzeko eta haiei erantzuteko.

Segurtasuna

B1 maila 4.1 Gailuen babesa

Algoritmoak sare sozialetan

Algoritmoak sare sozialetan

Aro digitalean, sare sozialek aldatu egin dute harremanak izateko, komunikatzeko eta informazioa kontsumitzeko modua. Iraultza teknologiko horren atzean algoritmoak daude: eduki pertsonalizatua eskaintzeko, datu kopuru handiak prozesatzen eta aztertzen dituzten sistema adimendunak.

Hala ere, algoritmo horiek erabiltzaileengan eta informazioaren kudeaketan duten eraginak **erronkak eta kezkak planteatzen ditu pribatutasunari, isuriei eta manipulazioari buruz**.

Ikusi ditugu jada pribatutasunarekin eta sare sozialetako informazioaren kudeaketarekin lotutako zenbait arazo, hala nola aztarna digitala, ospea eta iturri irekietako informaziorako sarbidea (OSINT). Jarraian, sare sozialetako algoritmoak azalduko dira, baita algoritmo horiek zer eragin duten erabiltzaileengan eta informazioa nola kudeatzen duten ere.

Algoritmoek erabiltzaileengan duten eragina

Sare sozialen testuinguruan, algoritmoak funtsezkoak dira erabiltzaileak ikus dezakeen informazio kopuru handia kudeatzeko. Algoritmo horiek erabiltzaile bakoitzari erakusten zaion edukia pertsonalizatzeko gaitasuna dute, eduki hori haren interes eta lehentasunetara egokituta.

Hala ere, pertsonalizazio horren ondorioz, **informazio-burbuilak** sor daitezke, zeinetan erabiltzaileek beraienen moduko informazioa eta iritziak baino ez dituzten jasotzen. Informazio-burbuilek polarizazioa susta dezakete eta ikuspegi-aniztasuna mugatu.

Informazio gehiago

Algoritmoek eta informazio-isuriek sare sozialetan duten eragina eztabaida publikoan dago. ***Sare sozialen dilema*** dokumentalak (thesocialdilemma.com) informazio-isuri horiek gizartean duten eragina erakusten du.

OSINT: ITURRI IREKIETAKO INFORMAZIOA

Erreferentzia-dokumentua: ***A4C41A2D01***

PRIBATUTASUNA, AZTARNA DIGITALA ETA ONLINE-OSPEA

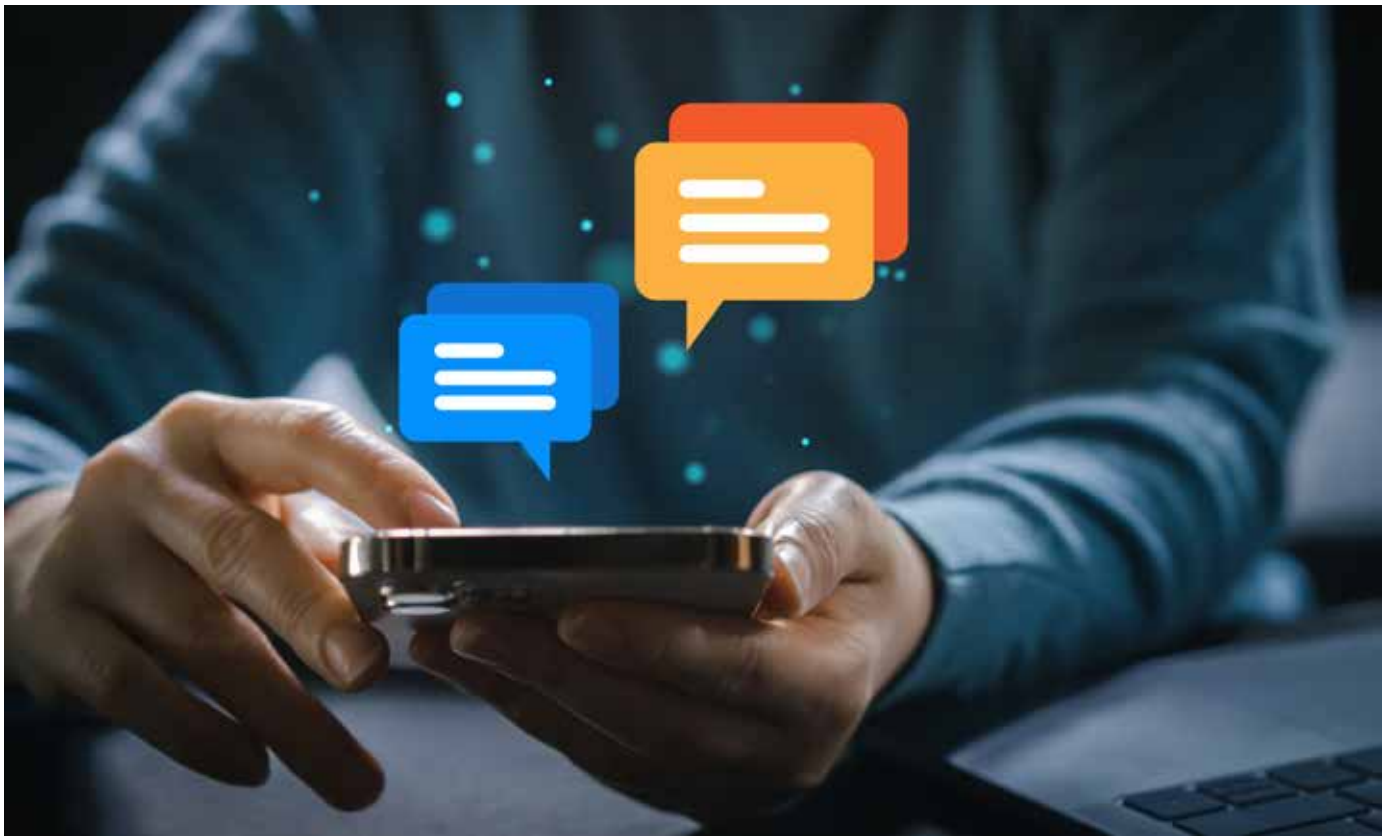
Erreferentzia-dokumentua: ***A4C41A2D02***

Algoritmoen boterearen eta informazioaren segmentazioaren adierazpen nagusietako bat masa-manipulazioa edo kanpaina politiko oso pertsonalizatuak dira. **Cambridge Analytica kasua da ziurrenik ezagunena, Ameriketako Estatu Batuetako 2016ko hauteskunde presidentzialen testuinguruan gertatua.** Kanpaina politikoetan aritzen den enpresa horrek Facebookek bildutako datuak eskuratu zituen baimen egokirik gabe. Informazio horri esker, profil psikologiko zehatzak erabili zituen informazio partziala eta kanpaina politikoko informazio oso pertsonalizatua helarazteko.

Gorabehera hark eztabaida handia eragin zuen sare sozialetako datuen pribatutasunari buruz, eta kezkak sortu zituen informazioaren manipulazioari eta algoritmo-isuriei buruz.

Informazio gehiago

Jehane Noujaim eta Karim Amer-en "The Great Hack" dokumentalak (2019an estreinatu zen) Facebook eta Cambridge Analyticaren kasua jorratzen du.



Sare sozialek informazioa nola kudeatzen duten

Algoritmoek erabiltzaileei buruz biltzen dituzten datu ugariek ahalbidetzen dute haien eragina. Hori sare sozialen negozio-ereduaren ondorio da, publizitate-enpresak baitira bezeroak, eta produktua, zuzendutako publizitate-plataforma bera da: sare soziala.

Besteak beste, erabiltzaileei buruz bildutako informazioa honelakoa izan daiteke:

- **Datu demografikoak:** algoritmoek erabiltzailearen adina, generoa, kokapen geografikoa, hizkuntza eta lanbidea bezalako informazioa eskura dezakete.
- **Sare sozialeko portaera:** algoritmoek erabiltzaileak plataforman duen jarduera erregistratzen dute: bisitatutako profilak, klik egindako argitalpenak, emandako "atsegin dut" horiek eta egindako iruzkinak, adibidez.
- **Elkarreragin sozialak:** algoritmoek erabiltzailearen konexio sozialak aztertzen dituzte, hala nola lagunak, jarraitzaileak eta zein pertsonarekin duen elkarreragina maiztasun handienaz.
- **Nabigazio-historiala:** kasu batzuetan, algoritmoek erabiltzailearen nabigazio-historiala araka dezakete sare sozialen plataformaren barruan eta kanpoan, hirugarrenen cookieak erabiliz, adibidez.
- **Gailuei buruzko datuak:** algoritmoek plataformara sartzeko erabilitako gailuari buruzko informazioa ere bil dezakete, hala nola gailu mota, sistema eragilea eta pantailaren bereizmena.

Oso garrantzitsua da kontuan hartzea zenbat informazio biltzen duten sare sozialek erabiltzaileei buruz eta horretaz jabetzea. Mugatu behar dugu zer partekatzen dugun sare sozialetan, nola erabiltzen ditugun haiek, eta aldian behin pribatutasun-konfigurazioak berrikusi behar ditugu, funtsezkoak baitira konfigurazio horiek sareak behar bezala erabiltzeko eta algoritmoen eragin-gaitasuna minimizatzeko.

Segurtasuna

B1 maila 4.1 Gailuen babesa

Arriskuak kudeatzeko metodologiak

Arriskuak kudeatzeko metodologiak

Arriskuak kudeatzeko metodologiak

Ezaugarri nagusiak

Lortu nahi diren helburuak lortzeko berme handiagoaz arriskuak kudeatzeko prozesua gidatzen laguntzeko, hainbat metodologia daude.

OHARRA

Arriskuak kudeatzeko metodologia: erakunde edo proiektu bati eragin diezaioketen arriskuak identifikatu, ebaluatu eta arintzeko erabiltzen diren prozesu eta tekniken multzoa.

Informazio gehiago

Arriskuak kudeatzeko metodologia funtsezkoa da erakundearen eragiketaren jarraitutasuna bermatzeko eta arrakastarako eta helburuak lortzeko probabilitatea maximizatzeko

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

Arriskuak kudeatzeko metodologia guztiek, aipatutako faseez gain (arriskuak identifikatzea, baloratzea eta lehenestea), honako hauek ere jaso beharko lituzkete: erantzuna planifikatzea eta ezartzea, arriskuen bilakaera etengabe monitorizatzea eta interesdun guztiei jakinaraztea.

Kontuan izan behar da arriskuak kudeatzeko metodologia desberdinak daudela eta horietako bakoitza egokiagoa izan daitekeela industria jakin batzuetarako edo hainbat arrisku-tipologiatarako, hala nola arrisku finantzarioetarako, operazionaletarako, estrategikoetarako, legaletarako eta abarrerako.

Prestakuntza horrekin lotutako gaia informazioaren segurtasuna denez, esparru horretan erabiltzen diren metodologia hauek berrikusiko dira:

- ***ISO 27005*** (e.digitall.org.es/iso27005)
- ***Magerit*** (e.digitall.org.es/magerit)
- ***OCTAVE*** (e.digitall.org.es/octave)
- ***NIST SP 800-30*** (e.digitall.org.es/nistsp800-30)
- ***FAIR*** (fairinstitute.org/learn-fair)

ISO 27005

ISO 27005 Normalizaziorako Nazioarteko Erakundeak (ISO) garatutako nazioarteko arau bat da, 2018an azkenekoz berrikusia.

ISO 27005 arauaren ezaugarri nagusiak hauek dira: arriskuan oinarritutako ikuspegia, hainbat erakunde motatara egokitzeko aukera, egitura argia eta jarraitzeko erraza, eta informazioaren beste segurtasun-arau batzuekin (ISO 27001) integratzeko gaitasuna.

Hainbat tresna barne hartzen ditu, hala nola arrisku-matrizeak, kontrol-zerrendak, adituekin egindako elkarrizketak eta analisi estatistikoak.

Magerit

MAGERITv3 Espainian erabilitako metodologia bat da, Espainiako Administrazio Elektronikoaren Kontseilu Goren zaharrak garatua.

MAGERIT metodologiaren indargune gisa, haren elementu-katalogoa nabarmendu dezakegu, zeinak jarraibideak ezartzen baititu aktibo motei, balorazio-dimentsioei, balorazio-irizpideei, mehatxu tipikoei eta babesei dagokienez. Nabarmendu behar da, halaber, arriskuen analisi- eta kudeaketa-proiektuak gauzatzeko orientabidea ematen duen haren teknika-gida.

Octave

Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation) Carnegie Mellon Unibertsitateko Software Engineering Institute (SEI) delakoaren metodologia bat da. Eskura dagoen azken bertsioa Octave Allegro da, 2012an kaleratu zutena.

Octaveren metodologiaren indarguneak honako hauek dira: erakundearen negozio-prozesuetan eta haietan informazioa erabiltzeko moduan oinarritutako ikuspegia; prozesu egituratua, taldearen ikuspegi kolaboratiboa eta pertsonalizazio-maila handia.

Arriskuak kudeatzeko prozesua errazteko tresna espezializatuak daude, hala nola SEIk garatutako OCTAVE Allegro softwarea.

NIST SP 800-30

NIST SP 800-30 Ameriketako Estatu Batuetako National Institute of Standards and Technology (NIST) delakoak garatutako gida bat da, eta azken berrikuspena 2021eko irailean egin zen.

NIST SP 800-30en funtsezko ezaugarriak edo indarguneak honako hauek dira: lau faseko egitura (prestatzea, ebaluatzea, arintzea eta komunikatzea), edozein erakunderen behar espezifikoetara egokitzeko gaitasuna eta industriaren estandarretan eta jardunbide onenetan oinarritutako haren jatorria.

Garrantzitsua da nabarmentzea NIST SP 800-30 arriskuak kudeatzeko gida bat dela, eta ez duela hura ezartzeko tresna espezifikorik preskribatzen.

FAIR

FAIR (Factor Analysis of Information Risk) Open Groupek 2006an garatutako eredua da. Gaur egungo berrikuspena 2019ko apirilean argitaratutako 3.0a da.

Eredu kuantitatiboa da, informazioaren segurtasun-arrisku baten probabilitatea eta finantza-inpaktua neurtzeko datuen analisi- eta estatistika-teknikak erabiltzen dituena. FAIRek bottom-up ikuspegia du oinarri eta informazio-aktibo espezifikoen mailan arriskuaren ebaluazio zehatza eta objektiboa ahalbidetzen du. Garrantzitsua da nabarmentzea erraz integratzen dela zibersegurtasuneko beste metodologia eta esparru batzuekin, hala nola NIST edo ISOrekin.

FAIR ezartzeko, informazioaren segurtasun-arriskuen ebaluazio kuantitatiboa egiteko aukera ematen duten hainbat tresna daude, hala nola RiskLens, FAIR-U eta Open Fair.

PILAR

Atal berezi bat eskainiko zaio ***Plataforma Integrada de Análisis y Gestión de Riesgos (PILAR)*** **(*e.digitall.org.es/pilar*)tresnari, Espainiako Zentro Kriptologikoak (CCN) garatutakoari.**

Doako tresna da, sarbide mugatua duena, eta aldez aurretik eskatu egin behar da eta CCN-CERTek baimendu egin behar du.

PILAR erakundeei informazioaren segurtasun-arriskuak eraginkortasunez identifikatzen, ebaluatzen eta kudeatzen laguntzeko dago diseinatuta, MAGERIT zein ISO metodologiei jarraikiz. Tresna horren ezaugarri nagusien artean honako hauek daude: arriskuen ebaluazio kualitatiboak eta kuantitatiboak egiteko gaitasuna, hainbat erakunde motatara egokitzeko malgutasuna eta ebaluazioen emaitzei buruzko txosten xehatuak egiteko gaitasuna.

Tresna hori Espainian informazioaren segurtasun-arriskuak kudeatzeko gehien erabilitako bat da, eta oso ezaguna da arriskuen ebaluazioan duen fidagarritasunagatik eta zehaztasunagatik.

DigitAll

Segurtasuna

4.2

DATU PERTSONALEN ETA PRIBATUTASUNAREN BABESA

Segurtasuna

B1 maila 4.2 Datu pertsonalen eta pribatutasunaren babesa

Pribatutasunaren aurkako erasoak: *Phisinga*

Pribatutasunaren aurkako erasoak: Phishinga eta Smishinga

Agian, identitate digitalaren kontrako mehatxu nagusietako bat "Phishing" izenez ezagutzen den zibereraso-modalitatea da. Zibergaizkileen helburua da gure datu pertsonalak eta banku-datuak lortzea, gure identitate digitala ordezteko. Horrela, dirua lapurtu diezagukete, edo besteek gu ikusten gaituzten moduan ere eragin dezakete, gure izenean iruzkinak argitaratuz. Eraso mota hori ez da berria, aspalditik ari da gertatzen. Hala ere, teknologia digital berriekin, izugarri handitu dira biktimen kopurua eta eraso horiek gauzatzeko moduak.

Dokumentu honetan azalduko da zer den Phishing-erasoa, zer modalitate izan ditzakeen, nola identifika dezakegun eraso egiten ari direla eta nola babes dezakegun geure burua.

Zer esan nahi du Phishingak?

Espainiako Hizkuntzaren Errege Akademiaren hiztegian ez dago “Phishing” terminoaren definiziorik. Hala ere, oro har onartzen da honako honi egiten diola erreferentzia: biktimak manipulatzeko eta haiek informazio pertsonal konfidentziala ezagutaraztea lortzeko asmoz gaizkileek iruzur eta engainuaren bidez erabilitako teknika eta metodoen multzoa. Azken helburua hau da: informazio pribatu hori biktimaren identitate digitala asmo gaiztoekin ordezteko erabiltzea.

Gaizkile horiek lortu nahi duten informazioa askotarikoa izan daiteke; adibidez, gure seme-alaben izena, Gizarte Segurantzako gure zenbakia edo banku-datuak, hala nola gure kreditu-txartelaren zenbakia. Arazoa da askotan zaila dela jakitea zer ondorio gaizto izan dezakeen datu pertsonal jakin bat ezagutarazteak.

“Phishing” terminoa ingelesezko "fishing" hitzetik sortua da, “arrantza” esan nahi baitu. Arrain batek (biktima) amua irensteko eta harrapatua izateko beita erabiltzearen metafora gisa erabiltzen da terminoa. Era berean, horrelako erasoak erabiltzen dituzten gaizkileei "phishers" esaten zaie.

“Phishing” terminoak arrantza-jarduerari egiten dio erreferentzia ("fishing" ingelesez).

Phishingaren funtzionamendua

Agian, eraso mota hori prebenitzeko modurik onena nola funtzionatzen duen jakitea da. Erabilitako teknika zehatza gorabehera, Phishing-erasoek eredu berari jarraitzen diote:

1 | Erasotzaileak biktimarekiko komunikazioa hasten du, biktima horren konfiantzazko erakunde edo pertsona baten identitatea ordeztuz. Adibidez, norberaren bankua, zerga-agentzia, lagun bat eta abar.

2 | Komunikazio horretan, erasotzaileak amua botatzen du. Adibidez, "xxxxx txartelaren informazioa eguneratu behar duzu", "yyyyy matrikula duen zeure autoaren isun bat duzu ordaintzeke" edo "sari bat egokitu zaizu".

3 | Biktimak amua irentsi eta informazio konfidentzialen bat ematen du, zuzen jokatzen ari dela sinetsita. Adibidez, pasahitz bat ematen du, kontu-zenbaki bat eta abar.

Internet aurreko garaian, komunikazioa hasteko modu nagusiak telefono-dei bat, gutun bat edo etxean bisita bat egitea ziren. Dena dela, gaur egun, aro digitalean, erasotzaileek hainbat modutan has dezakete komunikazio hori. Agian ezagunenak posta elektroniko bat edo mugikorreko testu-mezu bat dira.

Erasotzaileek ingeniaritza sozial gisa ezagutzen diren teknikak erabiltzen dituzte: zibergaizkileek erabiltzailearen konfiantza irabazteko eta, horrela, amu erakargarria eraikitzeko erabilitako tekniken multzoa dira (*e.digitall.org.es/ingenierial-social*). Nahi baino gehiagotan, biktimak berak ematen du amu erakargarri hori eraikitzeko behar den guztia, informazio pribatu gehiegi argitaratu baitu, adibidez, sare sozial bateko egoeretan.

Informazio gehiago

Bideoa ikustea gomendagarria da (*e.digitall.org.es/experimento-social*) jakiteko zenbat informazio pribatu argitaratzen den Interneten eta nola "phisherrek" amu erakargarriak egiteko erabil dezaketen hori.

Phishingaren ondorioak

Phishingaren biktima izateak oso ondorio txarrak izan ditzake. Bankura sartzeko biktimaren pasahitza eskuratu duen erasotzaileak transferentziak agindu ditzake. Pasahitza biktimak sare sozial batean duen profilarena bada, haren identitate digitalari eragin diezaioke horrek, iruzkinak egin baitaitezke haren izena zikintzeko edo bigarren biktima bati eraso egiteko oinarri gisa ere erabil baitaiteke.

FAKTORE ANITZEKO AUTENTIFIKAZIOA

Zenbait teknika daude, hala nola faktore anitzeko identifikazioa, nork bere burua babesteko aukera ematen dutenak, baita pasahitz-lapurreta baten biktima izanez gero ere.
e.digitall.org.es/A4C41A2V07

Biktima enpresa edo erakunde publiko bat bada, Phishingaren ondorioak are larriagoak izan daitezke, langileen, bezeroen edo erabiltzaileen datu pribatuen ihes masiboa eragin baitezake erasoak. Askotan, egoera are okerragoa da, jasandako erasoa ez delako publiko egiten, eta horrek eragotzi egiten dielako alboko biktimei haien burua babesteko neurriak hartzea, hala nola pasahitza aldatzea.

AUTENTIFIKAZIOA: PASAHITZEN KUDEAKETA

Enpresa edo erakunde bati egindako erasoan alboko biktima izatearen arazoa saihesteko, enpresa edo erakunde bakoitzerako, non norbera erregistratuta dagoen, pasahitz seguru desberdina erabiltzea da gomendagarria.
e.digitall.org.es/A4C41B1V08

Phishing digital motak

Esan bezala, Internet izan aurretik erabilitako teknika bat da Phishinga. Internet eta teknologia digitalak iritsi ondoren, teknologia horiek erabiltzen dituzten Phishing-modalitate berriak agertu dira.

Dokumentu honek teknologia digitalen bat erabiltzen duten eta modu generikoan “Phishing digital” izena hartzen duten Phishing-modalitateei helduko die.

Posta elektroniko bidezko Phishinga

Beharbada, Phishing digitalaren modalitaterik ohikoena da. Mezu elektronikoak erabiltzen dira biktimei amua botatzeko. Mezu horiek webgune gaiztoetara edo programa gaiztoekin infektatutako fitxategi erantsietara daramaten estekak izaten dituzte ("malware" esaten zaie).

Mezu elektroniko bat bidaltzearen kostua zero izan ohi denez, ohikoena mezu bera erabiltzea da, milaka erabiltzaileri masiboki bidaltzen zaiena. Hor amua zakarra izaten da, baina biktimen ehuneko txiki batek hura irenstea da erasotzailearen itxaropena.

Beste batzuetan, erasoa espezializatuagoa izaten da, enpresa baten publizitate-kanpainaren bat edo bezero guztiei bidalitako mezu berriren bat aprobetxatuta. Kasu horretan, aurreko mezuaren kopia bat bidaltzen da, aldatuta, esteka gaiztoekin. Modalitate horretan zailagoa da erasoa dela antzematea.

Web bidezko Phishinga

Modalitate horretan, erasotzaileak webgune baten kopia zehatza sortzen du. Horrela, biktima kopia maltzurrera sartzen denean, konfiantza hartzen du eta hark nahi duen informazio pribatua ematen dio erasotzaileari, normalean autentifikatzeko pasahitza.

Gaizkileek erabil dezaketen beste teknika bat webgune batean kode gaiztoa injektatzea da. Hartara, biktima webgune legitimora sartzen denean, erasotzaileek aldatuta dagoenez, berriz ere informazio pribatua eman dezake, jakin gabe. Duela gutxiko adibide bat saioa hasteko kredentzialak sartzeko leiho emergenteak izan dira.

Beste teknika bat ere ezaguna da: erasotzaileek web-orriak sortzen dituzte, eta produktu oso merkeak iragartzen dituzte haietan. Horren ondorioz, web-bilatzaileek balizko biktimak orri horietara bideratzen dituzte, eta, logikoa denez, haietan, informazio konfidentzial asko eman beharko dute ustezko erosketa egiteko. Horren adibide izan dira banku faltsuen orriak, interes txikiko maileguen edo komisiorik gabeko kreditu-txartelen publizitatea egiten zutenak.

Vishinga

Modalitate horretan, erasotzaileak telefono-dei bat erabiltzen du. “Vishing” terminoa "voice phishing" terminoetatik dator. Horrelako erasoetan, gaizkilea enpresa edo erakunde ospetsu bateko langile gisa kamuflatu ohi da. Ez da arraroa biktimen sare sozialen profilak ere aztertu izana, deian zehar ustez pribatua den informazioa emateko. Horren ondorioz, biktimak alerta-maila jaitsi eta konfiantza hartzen du. Ondoren, gaizkileak benetan nahi duen informazio pribatua eskatuko dio.

Smishinga

Modalitate horretan, erasotzaileak SMS mezu bat erabiltzen du. "Smishing" terminoa "sms phishing" terminoen laburketatik dator. Eraso-modalitate hori posta elektroniko bidezkoaren antzekoa da. Normalean, biktimak testu-mezu bat jasotzen du, esteka batean klik egiteko edo aplikazio bat deskargatzeko eskatuz. Hala ere, hori egiten duenean, engainatu egiten dute, haren informazio pertsonala jaso dezakeen eta erasotzaileari bidal diezaiokeen app gaizto bat deskarga dezan. Beste behin ere, oso ohikoa da horrelako erasoak kanpaina orokorrekin batera gertatzea, hala nola Zerga Agentziari pertsona fisikoen errentaren gaineko aitorpena egiteko kanpainekin batera.

Sare sozialen bidezko Phishinga

Modalitate horretan, gaizkileek sare sozialetan argitaratzen den informazio pribatu guztia erabiltzen dute biktimaren profila bahitzen saiatzeko eta lagunei esteka gaiztoak bidaltzera behartzeko. Horrela, lagunak ere biktima bihurtzen dira. Beste gaizkile batzuek profil faltsuak sortzen dituzte, beste pertsona batzuk direla simulatuz, eta biktimak engainatzeko erabiltzen dituzte, haiengan eragiten saiatzeko.

Phishingaren biktima izatea prebenitzeko gomendio nagusiak

Phishing digitalaren modalitate nagusiak erakutsi direnez, hori prebenitzeko jarraibide batzuk emateko garaia da.

Phishingaren biktima izatea prebenitzeko jarraibideak.

1 | Informazioa bila ezazu. Horixe egiten ari zara dokumentu hau irakurrita. Internautaren Segurtasun Bulegoa (*incibe.es/ciudadanía*) iturri ona da prestakuntza zabaltzeko eta ezagutzen diren azken iruzurrez informazio eguneratua izateko.

2 | Softwarea eguneratuta izan ezazu. Funtsezko elementu bat azken bertsioaz eguneratutako tresnak erabiltzea da, bereziki web-nabigatzailea. Web-nabigatzaile modernoen teknologiak gai dira informazio pribatua lapurtzeko asmoz gaizkileek erabiltzen dituzten teknika asko detektatzeko eta prebenitzeko.

3 | Sinesgabea izan zaitez. Edozein mezu elektronikoren aurrean hobe da zuhurtzia handiegia izatea txikiegia izatea baino. Estekei dagokienez, egiazta ezazu testuak adierazten dituen webguneekin konektatzen zaituztela. Teknika bat da beti mezuak testu plano moduan irakurtzea. Hartara, loturen benetako helbideak ikusiko dituzu, edo "kamuflatutako" estekarik ote dagoen irudietan edo logoetan. Aplikaziorik badago, lehenik eta behin pentsa ezazu benetan deskargatu behar den. Gainera, arau orokor gisa, ez instalatu inoiz ofiziala ez den aplikaziorik erabiltzen duzun sistema eragilean: Google Play, Microsoft Store, Apple Store eta abar.

4 | Baieztatu ezazu jardun aurretik. Gaur egun, enpresa gehienek ez diete inoiz informazio pribaturik eskatzen bezeroei posta elektroniko edo telefono-dei bidez. Hala badagokio, ezaba ezazu mezua edo eskegi ezazu telefonoa, eta baiezta ezazu enpresarekin eskaera hori benetakoa dela. Adibidez, zeure bankuarekin konektatzeko mezu elektroniko baten estekan klik egin beharrean, has ezazu zeuk zuzenean konexioa, nabigatzailea erabiliz, eta sar ezazu web-helbidea. Deia bada, zeure bankura dei ezazu, eta galdetu benetakoa ote den deiaren xede izan den kanpaina.

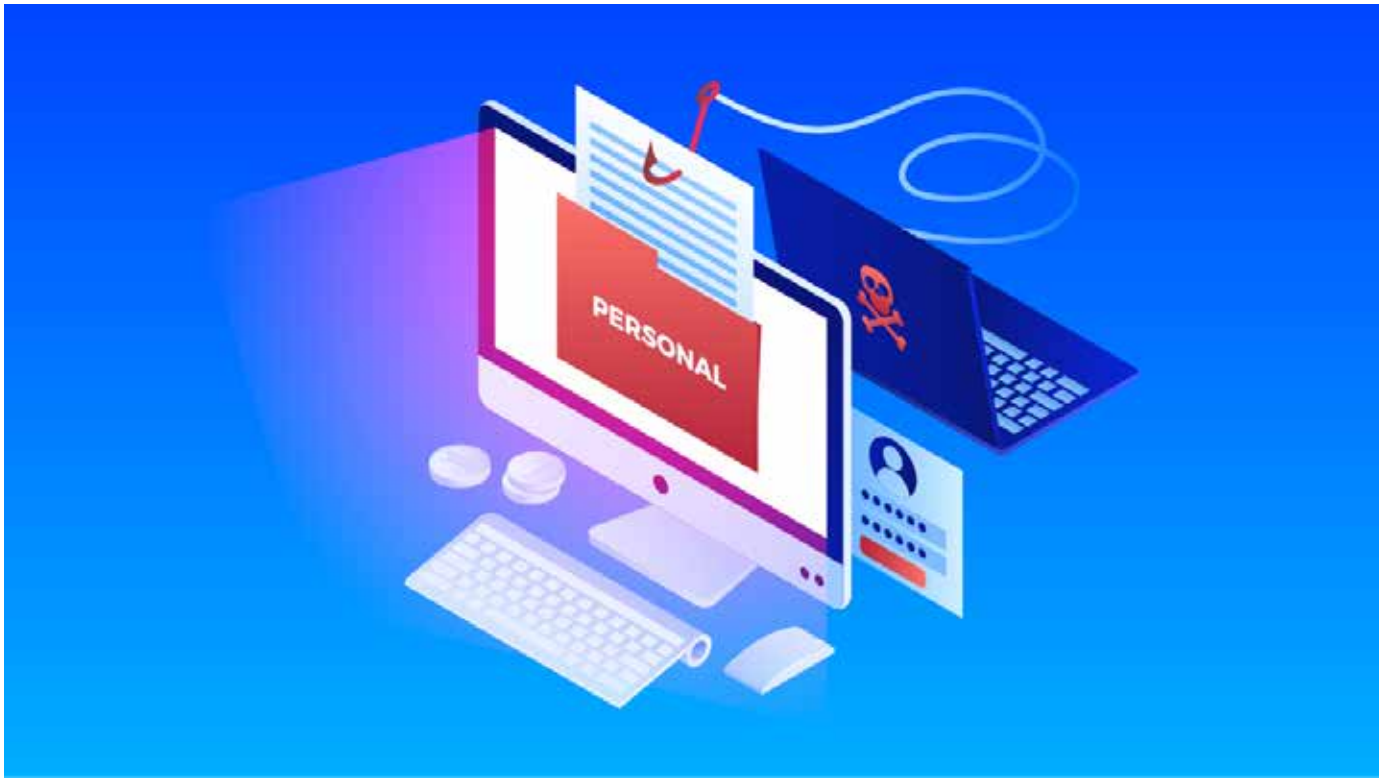
5 | Pasahitz-kudeatzaile bat erabil ezazu. Enpresa batek segurtasun-arrakala badu, baliteke bezeroak babesik gabe geratzea konprometituta geratu diren datu pertsonaletako batean oinarritutako pasahitz bera erabiltzen badute (adibidez, jaioteguna). Gomendagarria da pasahitz sendo desberdin bat erabiltzea erregistratuta gauden webgune bakoitzean. Pasahitz guztiak kudeatzeko pasahitz-kudeatzaile bat erabiliko dugu. Web nabigatzaile moderno gehienek pasahitz-kudeatzaile bat dute, baina horretarako software espezializatua ere badago.

Informazio gehiago

Internautaren Segurtasun Bulegoa. *incibe.es/ciudadanía*

Esperimentu soziala - gure datu pertsonalen arriskuak Interneten. *youtu.be/3S7qFGVfsqM*

Ingeniaritza soziala. *incibe.es/aprendeciberseguridad/ingenieria-social*



Segurtasuna

B1 maila 4.2 Datu pertsonalen eta pribatutasunaren babesa

Datu pertsonalak eremu jakin batzuetan behar bezala erabiltzeari buruzko FAQak

Datu pertsonalak eremu jakin batzuetan behar bezala erabiltzeari buruzko FAQak

Zilegi da datu pertsonalak tratatzeko isilbidezko onespena?

Ez. Datuak Babesteko Erregelamendu Orokorrak agintzen duenez, onespenak berariazkoa izan behar du beti. Isiltasuna, markatutako laukitxoak edo jarduerarik eza ez dira onespena. Erregelamendu horrek onespena honela formulatzea eskatzen du: "Borondate libre baten adierazpena erakutsiko duen baiezko egintza argi baten bidez".

Adingabe batek baimena eman dezake bere datuak Facebook, Tik-tok, Twitter eta abarrek trata ditzaten?

Soilik adingabea 14 urtetik gorakoa bada oinarritu ahal izango da tratamendu hori haren onespenean.
Hamalau urtetik beherako adingabeen datuen tratamendua, onespenean oinarritua, guraso ahalaren edo tutoretzaren titularrak onespen hori eman badu soilik izango da legezkoa (guraso ahalaren edo tutoretzaren titularrek zehaztutako irismenarekin).

Emaitza akademikoak gurasoei edo tutoreei bidal dakizkieke adingabeen baimenik gabe?

Bai. Kasu horretan, hezkuntza-erakundeak egiten duen tratamendua beharrezkoa da hirugarren baten, gurasoen edo tutoreen interes legitimo bat asetzeko. Interes legitimo hori guraso-ahalaren ondorio da. Kontuan hartu behar da Kode Zibilaren 154. artikuluak gurasoei/tutoreei ezartzen diela seme-alaba emantzipatugabeak hezteko eta haiei heziketa integrala emateko betebeharra.

Lan-elkarrizketa batean galderei erantzutea tratamendu-baimen baten baliokidea da?

Ez. Lan-elkarrizketetan hautagaiak datu pertsonalak dituzten galdera ugariri erantzun ohi die (gai bati buruzko iritzia, zaletasunak, etorkizunerako perspektibak, familia-egoera eta abar). Galdera horiei erantzuteak ez du esan nahi datu pertsonal horiek tratatzeko baimena ematen denik.

Gainera, egingo den lanarekin zerikusirik ez duten galdera familiar eta pertsonalak egitea datuak minimizatzeko eta helburua mugatzeko betebeharren aurkako jokabidea da.

OHARRA

Arau-hauste administratibo oso astuna da "Hautaketa-prozesuetan datu pertsonalak eskatzea..., enplegurako sarbidea izateko diskriminazioak badira, sexua, jatorria – arraza edo etnia barne –, adina, egoera zibila, desgaitasuna, erlijioa edo sinesmenak, iritzi politikoa, orientazio eta identitate sexuala, genero-adierazpena, ezaugarri sexualak, afiliazio sindikala, egoera soziala eta hizkuntza direla-eta Estatuaren barruan» [*16.1.c) artikulua Ordena sozialeko arau-hauste eta zehapenei buruzko Legearen testu bategina*].

Enplegatzaileak eskura dezake prebentzio-zerbitzuek langileari buruz lortutako informazio medikoa?

Ez. Lan Arriskuen Prebentziorako Legeak enpresaria behartzen du langileei haien osasun-egoeraren aldizkako zaintza bermatzera, lanari datxezkion arriskuen arabera. Arau orokorra da zaintza hori langileak baimena ematen duenean bakarrik egin daitekeela. Izaera pertsonaleko eta bereziki babestutako informazio mediko hori osasunaren zaintzaz arduratzen diren medikuek eta osasun-agintariek baino ez dute izango. Ezin zaie enpresariari edo beste pertsona batzuei eman langilearen berariazko onespenik gabe.

Langileak lanpostua betetzeko duen gaitasunari buruz egindako azterketetatik eratorritako ondorioen berri baino ez zaio emango enpresariari.

Legezkoa da publizitate-deiak jasotzea?

Dei motaren arabera. Telekomunikazioei buruzko Lege Orokorraren arabera, bi kasu bereiz daitezke:

- **Dei automatikoek**, hau da, gizakiaren esku-hartzerik ez dutenek, abonatuaren aldez aurreko baimen informatua behar dute horiek egin ahal izateko.
- **Pertsona baten parte-hartzea duten deiak** legezkoak dira, betiere abonatuak horiek jasotzeko bere aurkakotasuna adierazi ez badu.

DATUEN BABESA ETA EREMU PARTIKULARRAK

Nahi ez duzun publizitatetik zeure burua nola babestu azaldu zen.
e.digitall.org.es/A4C42C1V08

Badago eskola-ekitaldietan irudiak hartzea edo bideoak grabatzea?

Datuak Babesteko Espainiako Agentziaren jarraibideen arabera, ikastetxeak antolatutako ekitaldiak badira, honako hauek bereizi behar dira:

a) Ekitaldia ikastetxearen hezkuntza-funtzioari badagokio (adibidez, literatura-irakasgaian programatutako antzerki-funtzio bat), datuen erabilera Hezkuntzaren Lege Organikoan babestuta dagoela ulertuko da. Horrenbestez, ez da beharrezkoa onespena.
b) Ikastetxeak betetzen duen hezkuntza-funtziotik kanpoko ekitaldia bada (adibidez, gabonetako jai bat edo mozorro-festa bat):

- Ikastetxeak grabatzen baditu irudiak, interesdunei, 14 urtetik gorako adingabeei eta, txikiagoak badira, gurasoei edo tutoreei jakinarazi beharko die zer helburu duen grabazioak eta zer zabalkunde egin nahi zaien irudi horiei (web-orrietan, sare sozialetan... argitaratuko diren), eta baimena eskatu beharko die.

- Irudiak ikasleen senideek hartzen badituzte eta erabilera pertsonala edo etxekoa besterik ez badute, Datuak Babesteko Erregelamendu Orokorraren aplikazio-eremutik kanpo egongo litzateke hori. Hala ere, pertsonen irudiak, haien onespenik gabe, esparru horretatik kanpo, hirugarren batzuei zabaltzea (adibidez, irudiak sare sozialetan "irekian" argitaratzea) ukituen onespena beharko lukeen datu-tratamendua da, kasu horretan datuak babesteko legeria aplikatu beharko litzaiokeelako.

Haur-hezkuntzako ikastetxe batek bideozaintza-sistemarik instalatu dezake ikasgeletan?

Ez. Datuak Babesteko Espainiako Agentziaren 475/2014 txostenaren arabera, neurriz kanpokoa da lan-kontratudun langileak kontrolatzeko bideozaintza-sistemak instalatzea, mekanismo ez hain oldarkorren edota intrusiboen bidez lor baitaiteke hori. Finean, datuak minimizatzeko printzipioa urratuko litzateke. Ondorio horietarako, berdin du gurasoen baimena (seme-alaben irudiengatik) edo lan-kontratudunena ere izateak.

Sistema hori ezar daiteke, ordea, laneko ez-betetze oso larrien egoera jakin bat edo haren erabilera proportzionala egiten duen beste helburu bat dela eta.

Administrazio-organo batek argitaratu dezake administrazio-egintza bat non NAN osoa ageri den (adibidez, oposizio-lehiaketan onartutakoen zerrenda)?

Ez. Datu Pertsonalak Babesteko Lege Organikoak ezartzen duenez, interesdunaren datu pertsonalak jasotzen dituen administrazio-egintza bat argitaratu behar denean, haren izen-abizenak erabiliko dira identifikatzeko, eta, horrez gain, nortasun-agiri nazionalaren, atzerritarraren identifikazio-zenbakiaren, pasaportearen edo dokumentu baliokidearen lau zenbaki aleatorio gehituko dira.

Nola ezabatzen dira Internetetik gure irudia duten argazkiak eta bideoak?

Irudia datu pertsonala da, bai argazki batean bai bideo batean. Ohikoa da Interneten argazkiak eta bideoak agertzea, tratamendu hori legitimatzeko arrazoirik egon gabe. Kasu horietan, ezabatze hori lortzeko, ezabaketa-eskubidea baliatu behar da tratamenduaren arduradunaren aurrean.

Interneteko zerbitzu-emaile ezagunenek mekanismo propioak dituzte eskubide hori baliatzeko:

Facebook:

- Laguntza-zerbitzuaren bitartez: *e.digitall.org.es/ayuda-facebook*
- Salaketa-estekaren bidez ere bai, argitaratutako eduki gehienetan agertzen baita.

Google:

- Edukia kentzeko eskaera-inprimakia: *e.digitall.org.es/contenido-google*

Youtube:

- Bideoaren azpian agertzen den salaketa-estekaren bidez.
- Badira beste salaketa-aukera batzuk, arazoa era zehatzagoan adierazteko: *e.digitall.org.es/denuncia-youtube*

Twitter:

- Orri honetan informazioa eta loturak jaso dira: *e.digitall.org.es/denuncia-x*
- Zuzenean ere sala daiteke txio, zerrenda edo profil batetik.

Instagram:

- Esteka honetan informazio hori dago: *e.digitall.org.es/ayuda-instagram*

TikTok:

- Orri honetan arazoaren araberako informazioa eta estekak ematen dira: *e.digitall.org.es/ayuda-tiktok*

Enpresa horiek guztiek eta beste edozeinek gehienez ere hilabeteko epean ebatzi behar dute ezabaketa-eskaera, hura jasotzen denetik zenbatzen hasita. Epe hori igarota, ez badiote berariaz erantzun eskaerari, edo interesdunak uste badu erantzun hori ez dela egokia, dagokion erreklamazioa jar daiteke Datuak Babesteko Espainiako Agentzian, haren egoitza elektronikoaren bidez:
e.digitall.org.es/sede-electronica

Erreklamazio horrekin batera, dagokion entitatean ezabatzea eskatu izana egiaztatzen duen dokumentazioa aurkeztu behar da.

Nola ezabatzen dira eduki kalteberak Internetetik?

Datuak Babesteko Espainiako Agentziak lehentasunezko kanal bat du egoera bereziki delikatuei erantzuteko, edukiek (argazkiak edo bideoak) izaera sexuala dutenean edo eraso-ekintzak erakusten dituztenean eta kaltetuen eskubideak eta askatasunak arrisku handian jartzen ari direnean. Kanal horretara Agentziaren egoitza elektronikoaren bidez sartzen da:
e.digitall.org.es/sede-electronica

Emandako informazioa lehentasunez aztertuko da, eta, hala badagokio, Datuak Babesteko Espainiako Agentziak edukia erretiratzeko aginduko dio informazioa zabaltzen ari den zerbitzu edo plataformari. Gainera, delitu-zantzurik badago, Fiskaltzari jakinaraziko dio.

DigitAll

Segurtasuna

4.3

OSASUNAREN ETA ONGIZATEAREN BABESA

Segurtasuna

B1 maila 4.3 Osasunaren eta ongizatearen babesa

Gailuen denbora-kontrola erabiltzeko gida bisuala

Gailuen denbora-kontrola erabiltzeko gida bisuala

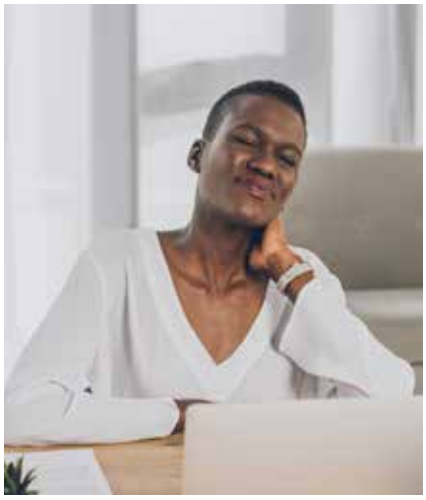
Dokumentu honetan, gailuen denbora-kontrola erabiltzeko gida bisual bat erakutsiko da. Lehenik, gailuen gehiegizko erabilerari buruzko sarrera bat egingo da, eta, ondoren, denbora eta osasunean hark duen eragina kontrolatzeko beharra azalduko da; denbora kontrolatzeko hainbat metodo erakutsiko dira.

Gailuen gehiegizko erabilera

Gailu elektronikoek, hala nola mugikorrek, tabletek eta ordenagailuek, gero eta leku garrantzitsuagoa hartu dute jendearen eguneroko bizitzan. Gaur egun, ia jende guztiak ditu halakoak, eta maiz erabiltzen ditu, bai lan-eremuan, bai esparru ludikoan, baita familian ere, besteak beste.

Teknologia berri horiek aurrerapen handia ekarri dute hainbat eremutan, eta bizitza erraztu digute modu positiboan.
Dena dela, kontuan izan behar da gure osasun fisikoan eta mentalean ere inpaktu negatiboa izan dezaketela. Neurrigabeko erabilerak mendekotasun maila handiak eragin diezazkieke erabiltzaileei.

Mendekotasuna ez ezik, teknologien gehiegizko erabilera horrek ondorio fisikoak, emozionalak edo sozialak ere eragin diezazkioke haiek erabiltzen dituen pertsonari. Ondorio ohikoenak insomnioa, antsietatea, estresa, depresioa, suminkortasuna edota artikulazioetako edo muskuluetako mina izaten dira, besteak beste.

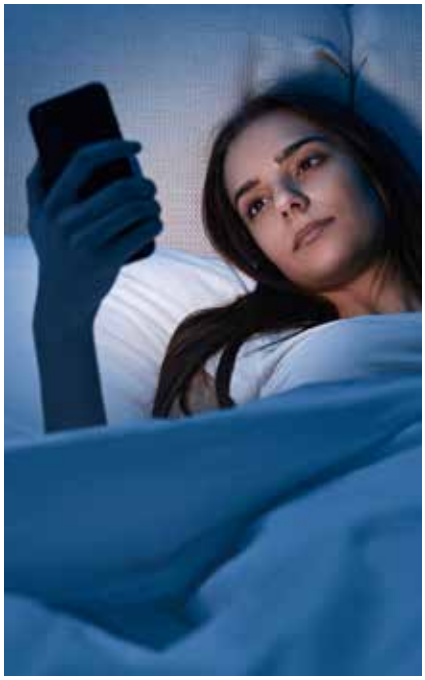


OHARRA

Kaperskyren webgunean artikulu oso interesgarri bat argitaratu dute, gailu elektronikoen erabilerak erabiltzaileen osasunean nola eragiten duen azaltzen duena. Hainbat arazori heltzen die, hala nola arazo muskulu-eskeletiko edo psikologikoei, ikusmen-nekeari, lo egiteko eragin negatiboari...

Teknologiaren eragina osasunean (*e.digitall.org.es/kapersky*)

Denbora kontrolatzeko beharra



Lehen aipatu dugun mendekotasuna saihesteko, ikasi behar da deskonektatzen eta gailuak erabiliz igarotzen den denbora modu kontzientean kontrolatzen.

Horregatik, oso gomendagarria da gailu elektronikoen erabilera ahalik eta denbora laburrenera mugatzea, eta betiere behar-beharrezkoa bada. Kontrol hori egiteko, hainbat aplikazio eta funtzionalitate daude, teknologia erabiltzen egunean zehar pasatzen den denbora kronometratzeko aukera ematen dutenak.

Horrez gain, gomendio xumeagoak ere badaude, neurriz kanpoko erabilera hobeto kontrolatzeko eta mugatzeko lagungarriak izan daitezkeenak:

Ez begiratzea telefono mugikorrari edo beste gailu batzuei lotara joan baino lehen, ezta jaiki baino lehen ere; izan ere, ekintza horiek maiz errepikatzeak errutina bihurtzen ditu, eta horrek gailuekin ordu gehiago pasatzea ekartzen du. Gainera, eragin negatiboa izan dezake erabiltzailearen atsedenaldian eta aldartean.

Informazio gehiago

Lotara joan aurretik gailu elektronikoak denbora luzez erabiltzeak guruin pinealari eragingo dio. Guruin hori garunaren zati bat da, eta melatonina sortzen du, gure loaren zikloa erregulatzen duen hormona. Atseden hartu aurretik mugikorra etengabe berrikusteak lo egiteko orduak galtzea eragingo digu. Horretarako, onena izango da mugikorra ordu erdi lehenago uztea, eta ohetik urruntzea, berriz hartzea gehiago kosta dakigun.

Gailuak erabiltzailearenean ez beste gela batean uztea; horrek zuzeneko sarbidea mugatuko du eta aurrean dituen beste zeregin batzuetan zentratzea erraztuko du. Aurreko adibidean bezala, erabiltzaileak ezin izango ditu jakinarazpenak ikusi, eta, beraz, ez da horrenbeste entzumen- eta ikus-estimuluren mende egongo.

Denbora kontrolatzeko metodoak

Teknologiaren erabilera-denbora kontrolatzeko aplikazio eta funtzionalitateei dagokienez (aurreko atalean aipatutakoak), honako hauek nabarmendu behar dira:

Alarmak eta kronometroa

Mugikorren, tableten edo wearableen alarmak eta kronometroa erabiltzeak teknologiaz jarduten pasatzen den denboraz jabetzeko balioko du. Horiek gailuaren erabilera-denboraz edo erabilerarik gabekoaz ohartarazten dute, eta, gainera, kronometroak denbora zehaztasun handiagoz kalkulatzeko aukera ematen du.

Oro har, gailu mugikor gehienek erloju-app propioa dute. Bertara sartzeko eta alarma aktibatzeko, hau egin behar da:

1 | Telefonoaren erlojuaren app-a ireki.
2 | Behealdean, sakatu "Alarma".
3 | Alarma bat aukeratu.
- Alarma bat gehitzeko, sakatu "Gehitu".

4 | Alarma-ordua ezarri.
- **Erloju analogikoan:** orratza nahi den orduraino irristatu eta gero gauza bera egin nahi diren minutuak aurkitzeko.
- **Erloju digitalean:** nahi dituzun ordua eta minutuak sartu.
- **12 orduko formatuan:** sakatu A.M. edo P.M.

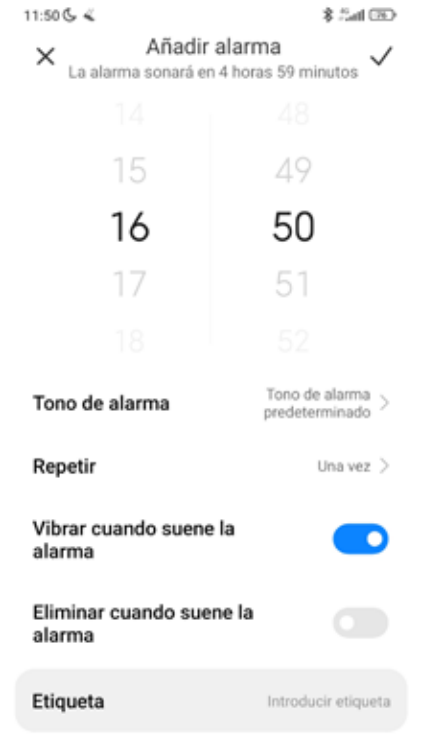
5 | Sakatu "Onartu".

Alarma hori baliogabetu nahi izanez gero:

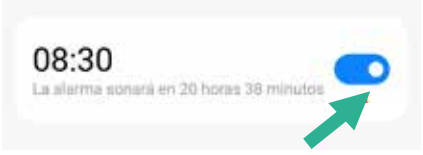
1 | Telefonoaren erlojuaren app-a ireki.
2 | Behealdean, sakatu "Alarma".
3 | Dagokion alarman, sakatu gezia beherantz.
- **Ezeztatu:** hurrengo bi orduetan jotzeko programatutako alarma bat ezeztatu nahi bada, sakatu "Baztertu".
- **Ezabatu:** alarma etengabe kentzeko, sakatu "Ezabatu".

Beste kasu batzuetan, alboko botoi batekin agertzen da alarma, eta horrek aukera ematen du zuzenean aktibatzeko eta desaktibatzeko, 3. urratsa osorik jarraitu beharrik gabe.

Iturria: sormen propioa.



Iturria: sormen propioa.



Iturria: sormen propioa.

Hegazkin-modua

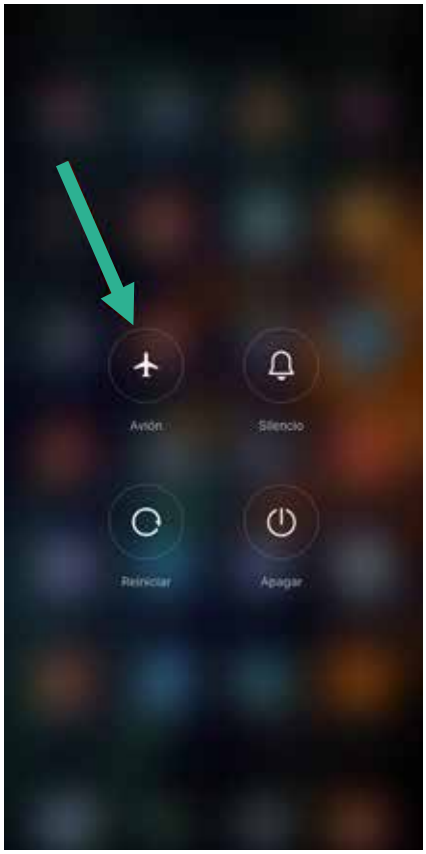
Telefonoaren edo tabletaren hegazkin-modua erabiltzea, erabilera-denbora mugatzen saiatzeko, edo aldi batez itzaltzea. Hegazkin-moduak eragotzi egiten du gailuak jakinarazpenak edo deiak jasotzea; beraz, erabiltzailea ez da hain adi egongo estimulu horiez, eta deskonektatzen lagunduko dio.

Gailu mugikor baten hegazkin-modura sartzeko hiru modu daude:

1 | Gailua itzaltzeko botoia sakatuta mantenduz gero, hegazkin-moduaren aukera agertuko da. Hor aktiba eta desaktiba daiteke.

2 | Gailuaren ezarpenen atalera sartuta. Oro har, zerrendako lehen aukeren artean egon ohi da; itzaltzeko eta pizteko botoi bat du ondoan.

3 | Gailuaren jakinarazpen-barraren bidez. Nahikoa da barra hori gailuaren goialdetik jaistea. Lehenengo aukeren artean agertzen da hori ere, eta aktibatu eta desaktibatu egin daiteke.



Iturria: sormen propioa.

Iturria: sormen propioa.

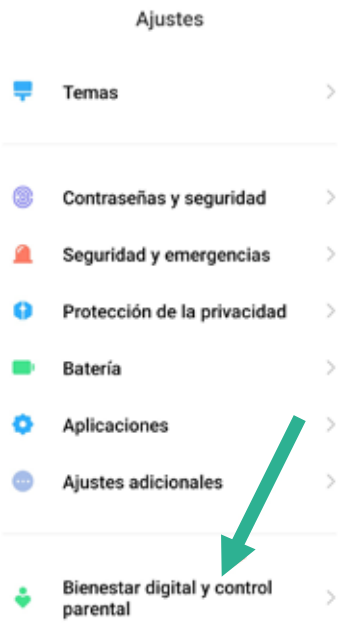
Ongizate Digitala (Android)

Android 9n ezarritako aplikazio natiboa da. Aplikazio horrek aukera ematen du app bakoitza zenbat denboraz erabiltzen ari den monitorizatzeko, eta web edo app jakin batean igarotzen den denbora mugatzeko aukera ere ematen du.

Beste fabrikatzaile batzuek, hala nola Huawei-k, beren Ongizate Digitaleko aplikazioak dituzte ezarriak beren gailuetan. Kasu horietan, izen bera edo beste batzuk erabil ditzakete, hala nola Huaweiren Equilibrio Digital. Aukera horietako bakoitzak bere interfazea eta kontrolak ditu.

Android-gailuen kasuan, Ongizate Digitalaren atalean sartzeko, hau egin behar da:

1 | Gailu mugikorraren ezarpenen aukerara sartu.
2 | Hautatu Ongizate Digitala eta Gurasoen Kontrola aukera. Beste kasu batzuetan, lehen aipatu bezala, beste izen bat ager liteke, hala nola "Equilibrio Digital".
3 | Behin barruan, grafiko bat ikusi ahal izango da, gailua oro har zenbat denboraz erabili den adierazten duena (erabilera-denbora); tarte horretan gehien erabilitako aplikazioa ere erakutsiko da. Behean, kontagailu bat ikusi ahal izango da, gailuaren desblokeo-kopurua eta egun osoan zehar jasotako jakinarazpen-kopurua jasotzen dituena.



Iturria: sormen propioa.

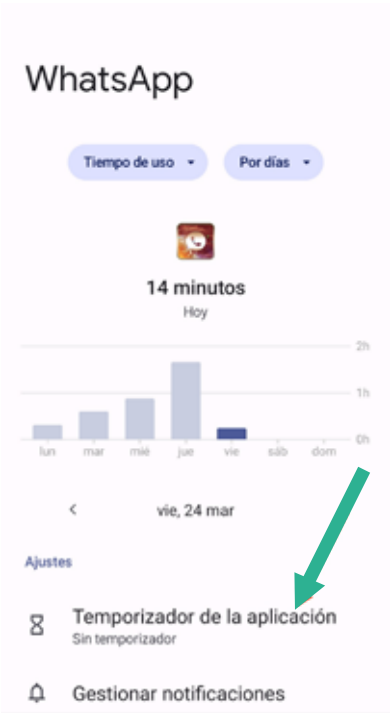
Iturria: sormen propioa.

4 | Mugikorrari begira zenbat minutu pasatu ditugun sakatuz gero, gailuaren erabilera-denboraren eta erabilitako aplikazioen zerrenda agertuko da pantailan: irekitako aplikazio guztiak ikusi ahal izango dira eta zenbat denboraz erabili diren. Aste osoko datuak dituen konparazio-grafiko bat ere ikus daiteke; aurreko egun batzuetakoak kontsultatzeko aukera dago.

5 | Aurreko zerrendako aplikazioetako bat sakatuz gero, pantaila bat agertuko da, ia berdina, baina aplikazio zehatz horren datuekin bakarrik. Horrela jakin daiteke zenbat erabiltzen den egunero app bakoitza. Behealdean jakinarazpenen konfiguraziora joateko aukerak eta aplikazioaren tenporizadorea daude.

6 | Aplikazioaren Tenporizadorea aukeran klik eginez gero, app jakin bat erabili ahal izateko Androidek emango duen gehieneko denbora ezarri ahal izango da. Horrela, app-en erabilera mugatu nahi bada, ezarritako denbora-mugara iritsitakoan, Androidek app hori blokeatu egingo du.

Iturria: sormen propioa.



Iturria: sormen propioa.

Iturria: sormen propioa.

OHARRA

Ezarritako mugetakoren bat gainditu ondoren, dagokion aplikazioa ilunduta agertuko da pantaila nagusian. Eta horra sartzea erabakitzen baduzu, kartel bat agertuko zaizu, ezarritako blokeoa gogoraraziko dizuna, nahiz eta beti izango duzun ezikusiarena egiteko aukera.

Informazio gehiago

GAILU TEKNOLOGIKOEN MENDEKOTASUNA, ERABILERA ETA ABUSUA - Gloria Martínez Ayala psikologoa *https://psicologaglciumartinezayala.es/dependencia-uso-y-abuso-de-los-dispositivos-tecnologicos /*

Zer da hegazkin-modua eta nola aktibatu/desaktibatu Androiden? *https://androidspain.es/modo-avion /*

Nola ezarri, ezeztatu edo atzeratu alarmak - Androiden laguntza. *https://support.google.com/android/answer/2840926? hl = es-419 #zippy = %2Cc%C3%B3mo-establecer -hora-de-la-alarma*

Erabilera-denbora Androiden: nola jakin zenbat denbora pasatzen duzun mugikorrean eta zein app erabiltzen dituzun gehien. *https://www.xataka.com/basics/tiempo-uso-android-como-saber-cuanto-tiempo-pasas-movil-que-apps-usas*

Teknologiaren eragina osasunean. *https://www.kaspersky.es/resource-center/preemptive-safety/impacts-of-technology-on-health*

Ongizate digitala mugikorretan: nola funtzionatzen du erabilera-denborak iPhone eta iPad-en? | Blog Educación y Bienestar digital. *https://gaptain.com/blog/bienestar-digital-en-moviles-como-funciona-el-tiempo-de-uso-en-iphone-y-ipad/*

Zergatik ez zenukeen mugikorrarekin egon beharko lo egin aurretik *https://www.movilzona.es/noticias/problemas/utilizar -movil-antes-lomir /*

DigitAll

Segurtasuna

4.4 INGURUMENAREN BABESA

Segurtasuna

B1 maila 4.4 Ingurumenaren babesa

Teknologiaren kontsumo "e-erantzunkide" -ko ohiturak

Teknologiaren kontsumo "e-erantzunkide"-ko ohiturak

Sarrera. "e-erantzunkide" kontzeptua

Dokumentu honetan "e-erantzunkide" terminoaren inguruko esparru kontzeptual bat aurkeztuko da; terminoak teknologia digitalaren kontsumoak gizartean eta ingurumenean izan ditzakeen ekintzen inguruko ardurak nork bere gain hartzeko beharrari egiten dio erreferentzia. Ikuspegi horretatik, kontzeptuak hiru alderdi ditu.

Lehenik eta behin, ingurumenarena ("eko-erantzule"), gailu teknologikoak eta haien euskarri diren azpiegiturak ekoiztearekin, merkaturatzearekin eta mantentzearekin eta haien hondakinekin lotutako prozesuek ingurune naturalean duten inpaktuez. Inpaktu horiek aurreko bideo eta dokumentuetan deskribatu dira: adibidez, A1 mailako bideoetan ("**Baliabide teknologikoen ekoizpen-prozesuak**" eta "**Teknologia garatzeko lehengaiak**"); A2 mailako bideoan ("**Gailu teknologikoen energia-kontsumoa (zure emailaren aztarna)**"); edo A2 mailako dokumentuan ("**Teknologiaren ingurumen-inpaktuak**").

Beraz, testu honetan diseinurako, ekoizpenerako, merkaturatzerako eta kontsumorako proposamen-ekintzak aztertuko ditugu, ingurunean inpaktu txikiagoa izango duten jardun-bideetarantz jo dezaketenak.

Bestalde, alderdi soziala ere kontzeptuaren ardatz nagusitzat hartu behar da. "Erantzunkide" izateak esan nahi du gizarte batean elkarri lotutako elementu gisa dugun zeregina ulertzea, non banakakoen ekintzek ondorioak izan ditzaketen, bai ingurunearentzat, bai beste pertsona batzuentzat. Beraz, ikuspegi hori kontuan hartu behar da gure portaera indibidualei buruz hausnartzeko, baina baita eragin politikoko esku-hartze kolektiboak planteatzeko ere.

Kontzeptuaren hirugarren ardatzak sektore teknologikoak gure gizarte garaikideetan maila ekonomikoan eta sozialean duen garrantziari egiten dio erreferentzia; horregatik da hain garrantzitsua elektronikaren "e" letra kontuan hartzea "e-erantzunkide" kontzeptuan.

BALIABIDE TEKNOLOGIKOEN EKOIZPEN-PROZESUAK

e.digitall.org.es/A4C44A1V03

TEKNOLOGIA GARATZEKO LEHENGAIAK

e.digitall.org.esA4C44A1V05

GAILU TEKNOLOGIKOEN ENERGIA-KONTSUMOA (ZURE EMAILAREN AZTARNA)

e.digitall.org.es/A4C44A2V03

TEKNOLOGIAREN INGURUMEN-INPAKTUAK

Erreferentzia-dokumentua: ***A4C44A2D01***

ADI

Laburbilduz, arduratsuak eta erantzunkideak izan behar dugu, ingurumen- zein gizarte-aldetik, teknologiaren kontsumitzaile eta erabiltzaile gisa dugun zeregina betetzean, bai banaka, bai kolektiboki.

Eko-erantzukizuna enpresa-sektorean

Teknologia digitalaren kontsumoan eta erabileran gizarte- eta ingurumen-aldetik arduratsuak diren ohiturak hartzeko erabakiak ez dituzte soilik ondasun eta zerbitzu teknologikoen erabiltzaileek edo kontsumitzaileek hartu behar. Aitzitik, erantzukizun horren zati handi bat legeria espezifikoaz arduratzen diren erakundeetara eta teknologia digitalaren sektoreko enpresetara bideratu behar da.

Aurreko dokumentuetan ikusi genuen bezala, abian dira, dagoeneko, zenbait ekimen instituzional, produktu eta gailu teknologikoak haien bizi-ziklo osoak ingurumenean eta gizartean izan ditzakeen inpaktuak kontuan hartuta diseinatzeko premian arreta jartzen dutenak; adibidez, konpontzeko eskubidea sustatzen duen Europako Parlamentuaren proposamena (Europako Parlamentua, 2022).

Xedapen horien ondorioz, hainbat esparru eta sektoretako gero eta enpresa gehiagok bilatzen dute, beren jardueretan, eko-erantzukizuneko proposamenetan inplikatzea. Espainiak Belgikan eta Luxenburgon duen Merkataritza Ganbera Ofizialak egindako txosten baten arabera (2022), Europako gero eta enpresa gehiago ari dira inplikatzen ekoizpen- eta merkataritza-prozesuen eraldaketan, eko-erantzukizunaren alde. Apustu horrek lau arrazoi nagusi ditu:

1 | **Irudia.** Gaur egun, kontsumitzaileek gero eta gehiago erreparatzen diete erosten dutenaren jatorriari eta ekoizpen-prozesuei buruzko xehetasunei, eta ohikoagoa da haiek produktuak edo zerbitzuak erostea baldin eta badakite beren enpresa kezkatuta dagoela ingurumenean eta gizartean duten inpaktuagatik.

2 | **Aurreztea.** Ekintza zehatzak aplikatzeak honako hau bilatzen du: prozesuen ingurumen-jasangarritasunak (energia-kontsumoa murriztea, birziklatzea, berrerabiltzea edo kudeatzea, adibidez) dirua aurrezteko aukera ematea epe ertainera, baita laburrera ere.

OHARRA

Nabarmendu beharreko beste ekimen bat da Europako Batzordearen helburuetan (2021) gailu digitalek trantsizio ekologikoari laguntzeko xedeak txertatu izana.

3 | Ebaluazio-irizpideak. Energia-erabilera optimizatzea eta ingurumen-inpaktua murriztea eta, oro har, jasangarritasuna bilatzen dituzten ikuspegiak irizpide garrantzitsuak dira orain enpresen ebaluazioan eta kalifikazioan. Inbertitzaile askok, HSBC bankuak adibidez, gizarte- eta ingurumen-inpaktuaren ebaluazioan egiaztatutako zorroztasuna duten proiektuak baino ez dituzte finantzatzen.

4 | Talentua erakartzea. Gizarte- eta prestakuntza-sektore jakin batzuetan gero eta ingurumen-kontzientziazio handiagoa dagoenez, etorkizuneko langile askok joera handiagoa dute gizarte- eta ingurumen-aldetik ospe handia duten enpresetan lan egiteko. Bestela esanda: talentu berrien iman bat izateko, berdea izan behar da.

Baina, nola bihur dezake enpresa batek bere funtzionamendua eko-erantzule? Ziurtatze-prozesuetan egiazta daitezkeen ingurumen-estandar jakin batzuk bermatzen dituzten ISO 14000 arauetan oinarritutako ingurumen-jasangarritasuneko edo -kudeaketako plan zehatzetatik harago, badira urrats erraz batzuk, eta edozein konpainiak modu autonomoan abian jar ditzake horiek ekoizpen- eta merkaturatze-prozesu eko-erantzuleak sustatzeko.

Materialen erabilera murrizteko, hondakinak bereizi eta birziklatzeko, baliabideak berrerabiltzeko eta ur- eta energia-gastua kudeatzeko ohiko prozesuez gain, beste aholku interesgarri batzuk ere badaude, enpresen ekoizpen-prozesuen eko-erantzukizuna sustatzeko.

Lehenik eta behin, iturri berriztagarrietatik (eguzki-panelak, haizea, biogasa edo energia geotermikoa) sortutako energia-kontsumoa sustatu behar da. Gaur egun, 2030 Agendaren sustapenaren esparruan, Europako testuinguruan, trantsizio energetikoa sustatzeko dirulaguntza eta laguntza instituzional ugari daude, eta enpresa-sektoreak funtsezkoa izan behar du trantsizio horretan.

Bestalde, **mugikortasuna** landu beharreko funtsezko beste ardatz bat da. Hain zuzen ere, teknologia digitalak aukera ematen du telelaneko lanaldiak sartzeko, joan-etorrietako denbora aurrezteaz gain ingurumen-inpaktua murriztuko dutenak.

Maila zehatzagoan eta ia anekdotikoan, ekimen "mikro" batzuek lagundu dezakete instalazioetan jasangarritasuna sustatzen, lan-segurtasuna eta -osasuna sustatzeaz gain: lantokietako airea garbitzeko landare berdeak erabiltzea, esaterako.. Izan ere, landare batzuek osasunerako kaltegarriak diren substantzia jakin batzuk xurga ditzakete (adibidez, bentzenoa eta trikloroetilenoa).

Azkenik, **pizgarri fiskalak** nabarmendu behar dira, enpresen eko-erantzukizuna sustatzeko funtsezko tresna gisa. Adibidez, Belgikan abian jarri duten eko-txekearen ekimena nabarmendu dezakegu hemen. Enpresa batek, ingurumena errespetatzen duten produktuak eta zerbitzuak erosteko, langileei ematen dizkien txeke gisa definitzen da eko-txekea.

Abantaila ekonomiko eta fiskal jakin batez gain, kontsumo-eredua modu jasangarriagoetara egokitzeko aukera ere bada. Eko-txekeak aukera ematen du konturatzeko kontsumitzeko moduak eragina izan dezakeela mugikortasun-aukeretan, aisialdi-jarduera jasangarrietan, berrerabilpenean, birziklapenean, hondakinen prebentzioan edo tokiko produktuen erosketan eta merkaturatze-zirkuitu laburretan.

Beraz, kontsumo eko-erantzunkidearen aukerak ez dira ekimen indibidualetatik soilik abiatu behar; apustu instituzional eta korporatiboek lagundu eta sustatu ahal eta behar dituzte, aurreko adibideekin ikusi dugun bezala.

Eko-diseinua, kontsumo eko-erantzunkidearen elementu nagusi gisa

Eko-diseinua funtsezko kontzeptuetako bat da gure ekoizpen- eta kontsumo-eredua ingurumen- eta gizarte-mailan inpaktu txikiagoa duten beste eredu batzuetara aldatzeko, ekonomia zirkularraren antzeko proposamenen ildotik. Oinarrizko mailan, eko-diseinua honetan datza: produktu eta sistemen diseinu-fasean ingurumen-jasangarritasuna funtsezko irizpidetzat hartzea, hala nola funtzionaltasuna, segurtasuna edo ergonomia. Eko-diseinuaren azken helburua produktuaren edo zerbitzuaren ingurumen-inpaktua murriztea da.

OHARRA

Kontzeptuak ospe handia hartu zuen 1970eko hamarkadaren amaieran; batez ere, Victor Papanek-en "Mundu errealerako diseinatzea" argitaratu ondoren (Papanek, 1977). Gaur egun, kontzeptuak garrantzia hartu du, eko-diseinuari buruzko Europako zuzentaraua sortzeraino (2005/32/EE).

Zuzentarau hori 2009an eguneratu zen (2009/125/EE), eta haren helburu nagusia esparru bat definitzea da energia erabiltzen duten eta ingurumen-inpaktua sor dezaketen produktuetarako diseinu ekologikoaren funtsezko betekizunak ezartzeko. Zuzentarau hori aurreko hamarkadan aholkularitza-elementu eta ia bigarren mailako gisa hartu zen arren, eko-diseinuaren kontzeptua elementu nagusi bihurtu da 2030 Agendaren eta EBk Europako Itun Berdearen barruan aurkeztutako **2020ko Ekonomia Zirkularrerako Ekintza Planaren** esparruan.

Aurreko araudia eta hainbat ikerketa-talderen lana erreferentziatzat hartuta, hala nola Bartzelonako Unibertsitate Autonomoko *Institut de Ciència i Tecnologia Ambientals* (ICTA) institutuarena, eko-diseinuan oinarritutako produktuak garatzeko hainbat ekimen nabarmendu daitezke hainbat sektoretan: altzarietan edo ontzietan, esaterako (González-García et al., 2011; Sanyé-Mengual et al., 2014).

Ildo horretan, tresna kualitatibo eta kuantitatibo ugari daude produktuaren ingurumen-profila aztertzeko eta ingurumen-kontsiderazioak ezartzeko. Tresna horietako bakoitza egokia izango da aplikazio eta egoera jakin batzuetarako, konplexutasunari eta kostuari dagokienez desberdinak baitira. Produktuen/zerbitzuen eko-diseinurako aplika daitezkeen metodologien artean, honako hauek aipa daitezke: Bizi Zikloaren Analisia (BZA), Aztarna Ekologikoa, Karbono Aztarna, Intentsitate Materiala Zerbitzu Unitateko, Diseinu Aldaketaren Ebaluazioa, Energia Eskari Metatua, Egiaztapen Zerrendak, Ingurumen Alderdien Analisi Matrizeak edo Produktuaren Ingurumen Estrategiaren Balorizazioa (Merkataritza Ganbera, 2023).

Aurreko bideo eta dokumentuetan ikusi dugun bezala, ingurumen- eta gizarte-arloan jasangarriagoak diren ekoizpen- eta kontsumo-moduetarantz eraldatu behar da teknologia digitalaren sektorea, eta konpongarritasuna, birziklapena, berrerabilpena edo bizitza baliagarriaren luzapena sustatzeko proposamenak eta estrategiak, guztiak eko-diseinuari lotuak, funtsezkoak izan daitezke eraldaketa horretan.

ADI

Aurreko guztia kontuan hartuta, argi dago eko-diseinua estrategia nagusia izan daitekeela eta izan behar duela ekonomia zirkularreko ereduetaranzko eraldaketa-prozesuan, gure ekoizpen- eta kontsumo-ohituren gizarte- eta ingurumen-inpaktuak minimizatzeko. Eta, jakina, teknologia digitalaren sektorea prozesu horren bultzatzaile bihurtu behar da.

Ondorio gisa, dokumentu honetan adierazi nahi dugu garrantzitsua dela teknologia-kontsumoko ohituren eredu "e-erantzunkide" bateranzko eraldaketa ez uztea soilik kontsumitzaileen bizkar eta, beraz, sektorean inplikatutako erakundeek, enpresek eta konpainiek ere egin beharreko aldaketak sustatzea eko-diseinuaren moduko estrategien bidez.

Informazio gehiago

Merkataritza Ganbera (2023) Eko-diseinua: Produktu/Zerbitzu Jasangarrien Diseinua. *https://www.camara.es/innovacion-y-competitividad/como-innovar/diseno-sostenible*

Europako Parlamentuaren eta Kontseiluaren 2009ko urriaren 21eko 2009/125/EE Zuzentaraua, energiarekin lotutako produktuek bete beharreko diseinu ekologikoari buruzko baldintzak zehazteko esparrua ezartzen duena. *https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32009L0125&from=LV*

Europako Batzordea (2021). Europako Hamarkada Digitala: 2030erako jomuga digitalak. *https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_es*

González-García, Sara, Carles M. Gasol, Raúl García Lozano, M Teresa Moreira, Xavier Gabarrell, Joan Rieradevall i Pons, Gumersindo Feijoo (2014) Assessing the global warming potential of wooden products from the furniture sector to improve their ecodesign, Science of The Total Environment, Volumes 410–411. *https://www.sciencedirect.com/science/article/abs/pii/S004896971101093X*

Papanek, Victor (1977) Mundu errealerako diseinatzea. *https://www.academia.edu/28853738/Dise%C3%B1ar_para_el_mundo_real_Victor_Papanek_pdf*

Europako Parlamentua (2022). Konpontzeko eskubidea: Europako Parlamentuak produktu iraunkorragoak eta konpontzen errazagoak nahi ditu. *https://www.europarl.europa.eu/news/es/press-room/20220401IPR26537/derecho-a-reparar-el-pe-quiere-productos-mas-duraderos-y-faciles-de-reparar*

Sanyé-Mengual, E., Lozano, R.G., Oliver-Solà, J.,Gasol, C.M., Rieradevall, J. (2014) Eco-design and product carbon footprint use in the packagingsector, In: Subramanian, S.M.: Assessment of carbon footprint in different industrial sectors, 1. bolumena, EcoProduction 2014, Springer, Singapore, 221-245 orrialdeak. *https://www.researchgate.net/publication/276266546_Eco-Design_and_Product_Carbon_Footprint_Use_in_the_Packaging_Sector*

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