DigitAll

Gaitasun
digitaletan
prestakuntza

4

Segurtasuna

DigitAll

Gaitasun
digitaletan
prestakuntza

Segurtasuna

A2 maila

AURKIBIDEA

DigitAll

Segurtasuna

4.1 GAILUEN BABESA

Segurtasuna

A2 maila 4.1 Gailuen babesa

OSINT: Iturri irekietako informazioa

OSINT: iturri irekietako informazioa

Geure bizitza digitalean datu ugari sortzen ditugu, horietako asko pertsonalak, eta mota guztietakoak: argazkiak, bideoak, testua, audioak, kokapenak eta abar. Informazio horren zati handi bat edonoren eskura dago, Interneteko konexio batekin. Gure pribatutasuna babesteko, garrantzitsua da une oro ohartzea sareetan argitaratzen dugun informazioaz, bai eta beste iturri batzuetatik guri buruz eskuragarri dagoen informazioaz ere.

Atal honetan azalduko da nola erabil daitekeen pertsonen informazio publikoa ikerketak egiteko. Datu publikoak berreskuratzeko eta haiek informazio garrantzitsu bihurtzeko teknika eta prozedurei OSINT esaten zaie.

Zer da OSINT?

Kode irekiko adimena edo Open Source Intelligence (OSINT) informazioa biltzeko metodo bat da. Metodo horretan, publikoki eskuragarri dagoen informazioa erabiltzen da, informatutako erabakiak hartzeko erabil daitezkeen datu baliagarri eta garrantzitsuak ateratzeko.

OSINTerako **informazio-iturriak** askotarikoak izan daitezke, hala nola komunikabideak, sare sozialak, foroak, blogak, gobernuaren webguneak, datu-base publikoak, eta abar. OSINT bidez bildutako informazioa hainbat eremutan erabiltzen da: adibidez, segurtasun nazionalean, ikerketa kriminalean, arrisku-kudeaketan, enpresa-adimenean eta beste hainbat arlotan.

OSINTen ospea nabarmen handitu da azken urteotan, **eskuragarritasunagatik eta publikoki informazio ugari dagoelako eskuragarri**. Gainera, datuak biltzeko, aztertzeko eta bistaratzeko teknologia eta tresna espezifikoak garatu izanak teknika hori hainbat arlotan erabiltzea erraztu du.
OSINTen helburu nagusia da jendeari eskuragarri dagoen informazioaren ikuspegi argia eta objektiboa ematea, informatutako erabakiak hartzen laguntzeko. Publikoki eskuragarri dagoen informazioa erabilita, OSINTek gai jakin

baten ikuspegi bakarra eta osatuagoa eman dezake, bestela lortzen zaila izango litzatekeena.

Laburbilduz, OSINT teknika eraginkorra da, eta asko erabiltzen da, informatutako erabakiak hartzeko, publikoki eskuragarri dagoen informazio garrantzitsua eta erabilgarria biltzeko. Teknika hori gero eta garrantzitsuagoa eta ezagunagoa da, informazioaren eskuragarritasunagatik eta teknologia eta tresna espezifikoen garapenagatik.

OSINT prozesua

Informazio publikoko iturriak erabiliz ikerketa eraginkor bat egiteko jarraitu beharreko urratsen multzoa da OSINT prozesua. Prozesua aldatu egin daiteke ikerketa motaren eta erabiltzen diren tresnen arabera, baina, oro har, urrats hauek osatzen dute:

1 | Plangintza
Hori da prozesuaren lehen urratsa, eta ikerketaren helburuak ezartzera, haren irismena definitzera eta erabiliko diren informazio-iturriak zehaztera bideratzen da. Garrantzitsua da ikerketa-plan bat ezartzea, etengabe azken helburua buruan izateko eta garrantzirik gabeko informazioaz denbora edo baliabideak alferrik ez galtzeko.

2 | Bilduma
Urrats horretan, plangintza-fasean identifikatutako iturrietako informazioa biltzen da. Garrantzitsua da kontuan hartzea eskuragarri dagoen informazio guztia ez dela garrantzitsua edo zehatza; beraz, bildutako informazioaren ebaluazio kritikoa egin behar da.

3 | Analisia
Informazioa bildu ondoren, aztertu eta ebaluatu egin behar da, ikerketaren testuinguruan zer garrantzi eta erabilgarritasun duen zehazteko. Garrantzitsua da analisi-tresnak eta -teknikak erabiltzea informazio-kopuru handiak efizientziaz eta eraginkortasunez prozesatzeko.

4 | Interpretazioa
Urrats horretan, azterketaren emaitzak interpretatzen dira, informazioa ondo ulertzeko eta ikerketaren helburuekin nola erlazionatzen den jakiteko. Interpretazioak informazioa baliozkotzea eta patroi eta erlazio garrantzitsuak identifikatzea eska dezake.

5 | Aurkezpena
Aurkezpena prozesuaren azken urratsa da, eta ikerketaren emaitzak interesdunei jakinaraztea da. Garrantzitsua da informazioa argi eta labur aurkeztea, datuak bistaratuta eta ulermena errazteko beste bitarteko batzuk erabilita.

Nabarmendu behar da ez dagoela OSINT prozesuaren faseak zertan linealki egin. Izan ere, ikerketa gehienetan aurreko faseetara itzuli ohi da, gertakarien norabidea aldatzen duen informazio interesgarriren bat aurkitu ondoren.

Laburbilduz, OSINT prozesuak informazio publikoa planifikatzea, biltzea, aztertzea, interpretatzea eta aurkeztea eskatzen du, jakintzak lortzeko eta informatutako erabakiak hartzeko. Prozesuaren urrats bakoitza garrantzitsua da, eta kontu handiz egin behar da, bildutako eta aztertutako informazioa ikerketaren testuinguruan garrantzitsua eta zehatza dela bermatzeko.

Informazio-iturriak

OSINTen informazio-iturriak asko alda daitezke: sare sozialak eta datu-base publikoak, gobernuaren webguneak eta komunikabideak. Gainera, funtsezkoa da lortutako informazioa legezkoa eta etikoa dela ziurtatzea. Hona hemen OSINTen erabilitako informazio-iturri ohikoenetako batzuk:

1 | Sare sozialak
Sare sozialak dira OSINTen iturri erabilienetako eta eskuragarrienetako bat. Facebook, Twitter, Instagram eta LinkedIn plataformek informazio pertsonala, iritziak eta bisitatutako lekuak partekatzeko aukera ematen diete erabiltzaileei. Gainera, plataforma horiek informazio baliotsua ematen dute pertsona baten kontaktu-sareari buruz, hala nola lagunez, senideez, lankideez eta kontaktu profesionalez. Hona hemen sare sozialetan aurki daitezkeen informazio-adibide batzuk: argazkiak, kokapenak, norberaren gustuak eta lehentasunak eta iritziei buruzko argitalpenak, besteak beste.

2 | Datu-base publikoak
Datu-base publikoak informazio-iturri garrantzitsuak dira OSINTentzat. Gehien erabiltzen diren datu-baseetako batzuk jabetza-erregistroak, enpresa-erregistroak, erregistro judizialak eta ibilgailu-erregistroak dira.

Adibidez, etxe bat erosi nahi duen pertsonak jabetza-erregistroen datu-base bat erabil dezake jabetzaren historialari, gaur egungo balioari eta kokapenari buruzko informazioa lortzeko.

3 | Gobernuaren webguneak
Gobernuaren webguneak politika publikoei, gobernu-txostenei eta estatistikei buruzko informazio-iturri fidagarriak dira. Adibidez, ikasle bat bere herrialdeko biztanleriari eta ekonomiari buruzko informazioa bilatzen ari bada, gobernuaren webgune bat bisita dezake datu eguneratuak eta fidagarriak lortzeko.

4 | Hedabideak
Hedabideek, tradizionalek zein online-koek, gertaera eta albiste garrantzitsuei buruzko informazio eguneratua eman dezakete. Egunkariak, aldizkariak, telebista-kanalak eta albiste-webguneak dira gaur egungo gertaerei buruzko informazioa lortzeko gehien erabiltzen diren iturrietako zenbait. Adibidez, eguraldiari eta trafiko-baldintzei buruzko informazioa bilatzen duen pertsonak tokiko albisteen webgunea kontsulta dezake.

Interneten publiko dagoen informazio oro pribatutasun-arazo garrantzitsua izan daiteke pertsonentzat. Sareko zerbitzuak erabiltze hutsagatik, hala nola web-nabigazioa edo sare sozialak, ezkutatu edo aldatzeko oso zaila den aztarna digitala uzten ari gara. Ildo horretan, datu pertsonalek garrantzi handia dute, eta haien erabilera eta trukea modu seguruan babesten dituen legeria dago, hala nola Datuak Babesteko Erregelamendu Orokorra (DBEO). Gai horri buruz gehiago jakin nahi baduzu, bideo hau ikus dezakezu:

PRIBATUTASUNA, AZTARNA DIGITALA ETA ONLINE-OSPEA

Bideo honetan, erabiltzaile bati buruz Interneten dagoen informazioaren garrantzia azpimarratzen da, haren aztarna digitalaren bidez, eta sare sozialen erabilera eta online-ospea nabarmentzen dira.

e.digitall.org.es/A4C41A2D02

OHARRA

Interneterako sarbidea duen edonork eskura dezake sarearen zati irekian argitaratuta dagoen informazioa. Garrantzitsua da, beraz, **sareetara igotzen dugun informazio guztiaz jabetzea**, hala nola argazkiez, bideoez, mezuez..., datu garrantzitsuak izan baititzake informazio horren zati handi batek. Erasotzaile batek informazio hori erabil dezake engainu sinesgarriagoak sortzeko edo identitatea ordezteko.

Tresnak

OSINT tresna ugari daude eskuragarri, eta funtzionaltasunaren arabera, hainbat eremutan sailka daitezke. Hona hemen tresna ezagunenetako batzuk:

- **Bilatzaileak.** Bilatzaileak dira OSINTen gehien erabilitako tresnetako bat. Google bilatzaile ezagunenetako bat da, eta informazioa online bilatzeko erabiltzen da. Beste bilatzaile ezagun batzuk Bing, Yahoo! eta DuckDuckGo dira. Gainera, sare sozialetan informazioaren bilaketan espezializatutako bilatzaileak daude, hala nola Social Catfish eta PeekYou.
- **Sare sozialak monitorizatzeko tresnak** Sare sozialetako hainbat plataformatako informazioa monitorizatzeko eta biltzeko erabiltzen dira tresna horiek. Tresna ezagun batzuk Hootsuite, TweetDeck eta Meltwater dira.
- **Irudiak aztertzeko tresnak** Irudien informazioa aztertzeko eta ateratzeko erabiltzen dira tresna horiek. Tresna ezagun batzuk Google Images, TinEye eta Yandex Images dira.
- **Metadatuak aztertzeko tresnak** Metadatuak fitxategi digitaletan ezkutuan dagoen informazioa dira, hala nola irudiak eta dokumentuak. Informazio hori ateratzeko erabiltzen dira metadatuak aztertzeko tresnak. Tresna ezagun batzuk ExifTool eta Metagoofil dira.
- **Webeko datuak aztertzeko tresnak** Tresna horiek

webeko datuak ateratzeko eta aztertzeko erabiltzen dira, webguneak eta sare sozialak barne. Tresna ezagun batzuk Import.io, Scrapy eta BeautifulSoup dira.

- **Posta elektronikoa aztertzeko tresnak** Tresna horiek mezu elektronikoak aztertzeko erabiltzen dira, goiburuko informazioa eta edukia barne. Tresna ezagun batzuk MxToolbox eta Header Analyzer dira.
- **Domeinu-izenak aztertzeko tresnak** Tresna horiek domeinu-izenak aztertzeko erabiltzen dira, erregistro-informazioa, IP helbidea eta kokapen geografikoa barne. Tresna ezagun batzuk DomainTools eta Whois dira.

Garrantzitsua da kontuan hartzea tresna horiek behar bezala erabilita baino ez direla erabilgarriak. Emaitzarik onenak lortzeko, garrantzitsua da aztertzen ari den informazio-iturriaren eta OSINTen tekniken eta metodologien ulermen sendoa izatea.

Erabilera-kasua: Google Dorks

Google Dorks bilaketa-komando aurreratuak dira, erabiltzaileei Googlen bilaketa zehatzagoak egiteko aukera ematen dietenak. Gako-hitzak bilatu beharrean, erabiltzaileek Google Dorks erabil ditzakete bilaketa-emaitzak iragazteko, parametro espezifikoak erabiliz.
Zergatik dira erabilgarriak Google Dorks? Google Dorks erabilgarriak dira, informazio espezifikoa eta zehatza online aurkitzeko aukera ematen dietelako erabiltzaileei. Google Dorks OSINTen erabili ohi dira pertsona, erakunde edo gai jakin bati buruzko informazioa online bilatzeko.
Hona hemen erabiltzaile ez-aurreratuentzat erabilgarriak diren Google Dorks komandoen adibide batzuk:

- **site:** komando horren bidez, erabiltzaileek webgune espezifiko batean bila dezakete. Adibidez, "site: nytimes.com coronavirus" jarriz gero, The New York Timesen webgunean "koronabirus" hitza duten emaitzak bilatuko ditugu.
- **filetype:** komando horren bidez, erabiltzaileek fitxategi espezifiko bat bila dezakete, hala nola PDF edo DOCX bat. Adibidez, "filetype: pdf hackeo informatikoa" jarriz gero, "hackeo informatikoa" esaldia duten emaitzak bilatuko ditugu PDF fitxategietan.

- **intext:** komando horren bidez, erabiltzaileek hitz edo esaldi espezifikoak bila ditzakete webgune baten edukiaren barruan. Adibidez, "intext: password security" jarriz gero, "security" eta "password" hitzak dituzten emaitzak bilatuko ditugu.
- **inurl:** komando horren bidez, erabiltzaileek URL espezifiko bat edo URLaren zati bat bila dezakete. Adibidez, "inurl: segurtasun informatikoa" jarriz gero, URLan "segurtasun informatikoa" esaldia duten emaitzak bilatuko ditugu.
- **intitle:** komando horren bidez, erabiltzaileek izenburuaren arabera bila dezakete webgune bat. Adibidez, "intitle: segurtasun informatikoa" jarriz gero, webgunearen izenburuan "segurtasun informatikoa" esaldia duten emaitzak bilatuko ditugu.

Informazio zehatza aurkitzeko komando mota horien benetako adibideak nahi baditugu, Google Hacking Database izeneko Exploit Database datu-basea erabil dezakegu. Gune horretan Google Dorks zehatz asko aurki ditzakegu, segurtasun informatikoaren eremuan praktikan zer aplikazio duten ikusteko, bai eta lehen aldiz oharkabean pasa zitekeen informazio jakin bat berreskuratzeko ere. Horrelako baliabideei esker, iturri irekiekin ikerketa bat egiteko OSINT teknikek zer garrantzi eta potentzial duten ulertzeko aukera dugu.

OHARRA

Garrantzitsua da kontuan hartzea, Google Dorks erabilgarriak izan daitezkeen arren, segurtasun- eta pribatutasun-arriskuak ere izan ditzaketela gaizki erabiliz gero. Beraz, kontu handiz erabili behar dira, eta aurkitutako informazioa legezkoa eta etikoa dela kontuan hartu behar da beti.

OSINT komunitatea

Trace Labs OSINT komunitate bat da, ikerketa eta teknologia aurreratuko teknikak erabiliz desagertutako pertsonak bilatzen dituena. Pertsonen bilaketan arrakasta izan dute kasu askotan, baina aipagarrienetako bat "Mary" kasua da.
Maryren kasuan, emakume bat desagertu zen, arrastorik utzi gabe, New Yorkeko estatuan (AEB) 2019an. Tokiko polizia hilabete luzez saiatu zen hura aurkitzen, arrakastarik gabe, eta, beraz, Maryren familiak Trace Labs-era jo zuen laguntza eske. Trace Labs komunitatea kasuan lanean hasi zen, eta zenbait OSINT teknika erabili zituen Maryri buruzko informazioa online bilatzeko. Sare sozialetan informazioa bilatzea, erregistro publikoak ikertzea eta segurtasun-kamerak berrikustea izan ziren erabilitako metodoetako batzuk.

Azkenik, Trace Labs-eko taldeak informazio garrantzitsua aurkitu zuen, Maryren kokapenera eraman zuena. Informazioaren barruan, segurtasun-kameren erregistro bat zegoen, Mary aintzira batetik gertu erakusten zuena eta, beraz, polizia eremu horretan bilatzera eraman zuena. Mary bizirik aurkitu zuten eta familiari itzuli zioten.

Kasu horrek OSINTen boterea erakusten du, baita elkarrekin lan egiteko Trace Labs komunitatearen gaitasuna ere (familiei desagertutako pertsona maiteak aurkitzen laguntzeko, hain zuzen ere). Trace Labs-ek antzeko kasu arrakastatsu asko egin ditu, eta lanean jarraitzen du mundu osoan desagertutako pertsonak aurkitzen laguntzeko.

Ikerketari dagokionez, badira hainbat gertaera, non segurtasun-sektoreko hainbat profesionalek, kasu honetan OSINTen espezializatutakoek, beren ikerketak eta tresnak azaltzen dituzten. Esate baterako, **Osintomático Conference** edo **IntelCon**.

Segurtasuna

A2 maila 4.1 Gailuen babesa

Pribatutasuna, aztarna digitala eta online-ospea

Pribatutasuna, aztarna digitala eta online-ospea

Internet erabiltzeak eta guri buruzko informazioa argitaratzeak identitate digital bat sortzen dute. Identitate horrek mundu errealarekin lotzen dugun identitatea isla dezake, baina, mundu errealean ez bezala, edonork erraz eskura dezakeen informazioak osatzen du identitate digital hori.

Atal honetan, Google, Bing eta antzeko bilatzaileek nola funtzionatzen duten ikasiko dugu, bai eta gure aztarna digitala zer informaziok osatzen duen ere. Garrantzitsua da hori ezagutzea eta guretzat zer ondorio izan ditzakeen kontzienteki aztertzea.

Identitate eta aztarna digitala

Identitate digitala Interneteko erabiltzaile baten aztarna digitaletik sortutakoa da. Hau da, publikoki eskuragarri dagoen eta identitate batekin lotu daitekeen informazioak osatzen du identitate digitala.

Sare sozialak

Sare sozialak egunero erabiltzen ditugu, baina jende asko ez da ohartzen sare horietan partekatzen ari denaz. Sare sozialetako geure profilak erabiltzen ditugunean, kontu handiz ibili behar dugu gure informazioa partekatzerakoan, eta zer arrisku eragin diezagukeen ere pentsatu behar dugu.

Askotan, xehetasun gehiegi partekatzen ditugu egunero sare sozialetan, eta areago, nahitaez eman beharreko informazio jakin bat ere bada, horiek erabili nahi baditugu; normalean, informazio pertsonala izaten da. Horrek ez gintuzke kezkatu beharko, baldin eta datuak hirugarren pertsonek eskuratzen ez badituzte.

⚠ ADI

Informazio pertsonala, datu pertsonalak edo pertsonalki identifika daitekeen informazioa pertsona bat identifikatzeko aukera ematen dutenak dira. Adibidez, NANa, bizilekua, egoera zibila edo nazionalitatea.

Bada sarean publiko egin beharko ez genukeen informazio jakin bat. Hau da, komeni da hura argitaratu aurretik bi aldiz pentsatzea:

- **Datu pertsonalak:** izen-abizenak, telefonoa, NANa, e-maila... Haien bidez identifikatu egin gaitzakete!
- **Planak eta oporrak:** etxean noiz ez gauden jakin dezakete, lapurreta-saioren bat egiteko.
- **Egungo kokapena:** gure eguneroko ohiturak, etxea eta lana ezagutzeko aukera ematen dute.
- **Banku-informazioa:** lapurretak edo iruzur-zordunketak egin ditzakete gure kontuetan.
- **Adingabeei buruzko informazioa:** etorkizunean haien sentsibilitatea mindu edo esku txarretan amaitu lezakete.

OHARRA

Zeure sare sozialetako segurtasun- eta pribatutasun-aukerak berrikusi behar dituzu. Konfigurazio-aukera ohikoenak "pribatutasuna eta segurtasuna" izeneko ezarpen-atal baten azpian egoten dira. Hor, informazioa ezkuta dezakezu publikoki ez erakusteko, eta partekatzen duzuna eta sarean duzun esposizioa kudeatu.

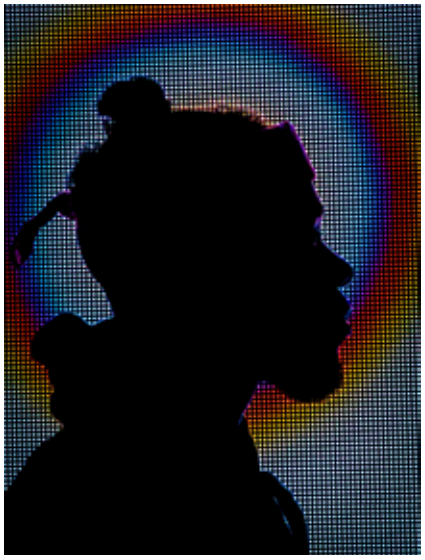
Online-ospea

Aurreko informazioaz gain, birritan pentsatu behar dugu jokabide desegokiak edo iritzi pertsonalen bat argitaratu baino lehen. Hori guztia gure online-ospearen parte da. Zehazki, osatzen dugun aztarna digitalak gure identitate digitala sortuko du, eta hori bat etor daiteke, neurri handiagoan edo txikiagoan, gure benetako identitatearekin.

Argitalpen mota batzuek modu negatiboan eragin diezagukete. Zerbait argitaratzen dugunean, haren gaineko kontrola izateari uzten diogu.

Argitalpen askok eragin diezaiokete **online-ospeari**. Adibidez:

- **Argitalpen iraingarriak edo iruzkin negatiboak:** sareen bidez iraintzea edo mehatxatzea delitua izan daiteke, eta argitalpen iraingarriak egitea gure aurkako bihur daiteke.
- **Ziberjazarpena:** pertsona baten kontrako isekak, irainak edo umiliazioak. Biktima edo lekukoa bazara, salatu egin behar duzu.
- **Laneko kexak:** enpresa askok beren langileen sare sozialak berrikusten dituzte eduki desegokiak parteka ditzaten saihesteko, baita hautaketa-prozesuetan ere.
- **Argazki eta bideo desegokiak:** argazki bat sare sozial batera igotzen baduzu, haren gaineko kontrola galduko duzu. Gainera, arriskuan jar gaitzaketen argazkiak



hirugarren pertsonen eskuetara irits daitezke xantaia egiteko edo gu kaltetzeko.
- **Albiste faltsuak edo "fake news"-ak zabaltzea:** ez dugu sinetsi behar sare sozialetan edo Interneten ikusten dugun guztia.

Albiste bat argitaratu aurretik, komeni da haren iturriak egiaztatzea. Gezur edo iruzur bat partekatzeak oso eragin negatiboa izan dezake zure online-ospean.

Bilatzaileak

Google, Bing, DuckDuckGo eta Ecosia Interneteko bilatzaileak dira. Publikoki eskuragarri dagoen informazioa bilatzeko aukera ematen digute, gako-hitzen edo kontsulten bidez bilatuta. Konplexua dirudien arren, geure egunerokotasunean erabiltzen oso ohituta gaude; webeko edukiari buruzko esteka edo erreferentzia ugariren bidez gure zalantzei erantzuten diete.

Hala ere, **bilatzaileek edukiak ere izan ditzakete, hala nola sare sozialetako profilak, irudiak, albisteak edo guri buruzko informazio orokorra.** Horregatik, garrantzitsua da ulertzea nola funtzionatzen duten eta nola kudeatzen den sarean guri buruzko informazioa, bilatzaile horien bidez eskuragarria.

Nola funtzionatzen dute?

Bilatzaileen helburu nagusia **erabiltzaileei Interneten informazio garrantzitsua eta erabilgarria aurkitzen laguntzea da**. Hori lortzeko, bilatzaileek modu eraginkor eta efizientean biltzen, antolatzen eta aurkezten dute webean eskuragarri dagoen informazioa, erabiltzaileei kontsultatzeko emaitzarik garrantzitsuenak emateko.

Erabiltzailearen esperientzia hobetzea ere bada zenbait bilatzaileren helburua, bilaketa-emaitza zehatzak eta eguneratuak emanez formatu erabilerrazean eta eskuragarrian.

> **OHARRA**
>
> Testuinguru horretan, elkarrizketan oinarritutako adimen artifizialak sortu dira, hala nola OpenAIren ChatGPT. Sistema horiek webeko informazio ugarirekin entrenatu dira eta galdera konplexuei erantzuteko gai dira, bilatzaileak ez bezala, horiek informazioari buruzko erreferentziak baino ez baitizkigute ematen.

Bilatzaileek, kontsulta baten ondoren, erabiltzaileari informazio garrantzitsua eman ahal izateko, weba arakatu behar dute aldez aurretik. Weba arakatzeko prozesuan (***web crawling***), bilatzaileek zerrenda batean ordenatzen dute informazioa. Horri **"edukien indexazioa"** esaten zaio. Hau da, bilatzaileek weba arakatu eta haren edukia prozesatzen dute, webgune ezagunen zerrendan sartzeko.

Zerrenda edo aurkibide horixe kontsultatzen du bilatzaileak, erabiltzaileak bilaketa- edo kontsulta-barran idazten duenean. Hortaz, azken minutuetan Interneten argitaratu berri den edukiren bat badago, ziurrenik bilatzaileak ez du erakutsiko, oraindik ez baita "indexatuta" egongo.

Bilatzaile jakin batek guri buruz zer informazio "indexatu" duen hautemateko, komeni da "ego surfing"-a egitea. Horretarako, gure izena edo informazio pertsonala bilatu behar dugu Google, Bing edo Yahoo bilatzaileetan. Hau da, webean norberari buruzko informazioa bilatu, eta, horrela, gure online-ospea edo aztarna digitala aztertu.

SEO posizionamendua

Search Engine Optimisation (SEO) eduki-sortzaileek, erakundeek eta enpresek erabiltzen duten teknika-multzo bat da, **erabiltzaileak kontsulta jakin batzuk egiten dituenean edukiren bat bilatzaileen lehen emaitzen artean agertzea helburu duena**. Adibidez, Bartzelonako autoen kontzesionario batek lehen postuan eduki nahi izango du bere webgunea erabiltzaileak "Bartzelonan autoen salmenta" bilatzen duenean.

Hala ere, SEO teknikak **SEO pozoidura** bezalako erasoak egiteko ere erabil daitezke asmo maltzurren batekin informazio faltsua sartzeko. Adibidez, iruzurrak egitea edo pertsona edo erakunde baten ospea kaltetzea.

Garrantzitsua da bilatzaileen eta SEO posizionamenduaren funtzionamendua ezagutzea, hark gure alde joka dezan. Gure online-ospeak eta aztarna digitalak osatzen dute gure identitatea Interneten.

Horregatik, garrantzitsua da sustatu nahi dugun informazioa ondo kokatzen laguntzea, eta kalte egin diezagukeen informazio pertsonal egiazko edo faltsurik agertzen ote den zaintzea. Ildo horretan, gogoan izan OSINT teknikek erasotzaileei aukera ematen dietela bilatzaileez baliatzeko eta guri buruzko informazioa lortzeko. Hori saihesteko, edukia ezaba dezakegu edota zerrendan edo aurkibidean ez sartzeko eska diezaiekegu bilatzaileei.

OSINT: ITURRI IREKIETAKO INFORMAZIOA

Erreferentziazko dokumentua: ***A4C41A2D01***

DigitAll

Segurtasuna

4.2

DATU PERTSONALEN ETA PRIBATUTASUNAREN BABESA

Segurtasuna

A2 maila 4.2 Datu pertsonalen eta pribatutasunaren babesa

Segurtasun-politikak. Informazio pribatua

Segurtasun-politikak. Informazio pribatua

Sarrera

Informatikaren arloko segurtasun-politikek informazioaren konfidentzialtasuna, osotasuna eta eskuragarritasuna bermatzea ahalbidetzen duten prozedurak eta arauak jasotzen dituzte. Prozedura eta araudi horiek eragina dute sistema eta gailuetara sartzeko mekanismo edo modu guztietan, bai informazioa gordetzen den lekuetan, bai informazioa eskuratzeko lekuetan. Segurtasun-politikek segurtasun fisikoari eragiten diote, sistema mekanikoen bitartez, bai eta segurtasun logikoari ere, zuzeneko edo komunikazio-sareen bidezko sarbidea duten sistema elektronikoen bitartez. Segurtasuneko oinarrizko prozedurak ISO 27000 nazioarteko arauan ezartzen dira (Estandarren Nazioarteko Erakundeak ezarritakoa), baita arau horretatik eratorritakoetan ere; informazioaren segurtasunarekin lotutako alderdi guztiak jorratzen ditu aipatutako arauak. Dokumentu honetan laburbilduko dira oinarrizko prozedura horiek. Arau hori Nazioarteko Batzorde Elektroteknikoarekiko (IEC - International Electrotechnical Commission) lankidetzan garatu da eta, beraz, ISO/IEC 27000 ere esaten zaio.

Segurtasun-politikak, besteak beste, sistemen sarbidean eta erabileran erabiltzaileen informazio pribatua babesteko ezarri dira (edozein motatakoa eta edozein mailatan). Beraz, informazio pribatua norbanakoaren pribatutasunari dagokion informazioa da, eta babestu egin behar da, bai datu pribatuei dagokiena (izen-abizenak, helbidea, NANa, telefonoa, emaila, egindako jarduerak, lagunak, iruzkinak eta abar), bai lan egiten duen edo bisitatzen dituen sistema konputatzaileetan norbanakoak duen nortasunari dagokiona.

Segurtasun-politikak

Informazio-sistemetako segurtasun-politikek kontuan hartu behar dituzte, batetik, segurtasun fisikoa (sistemetara sartzeko murrizketei, sarbide mugatuko segurtasun-ateei, suteen aurkako babesari, hozteari, azpiegituren diseinu eta egitura efizienteei eta abarri dagokienez ezarri beharreko prozedurak identifikatuz) eta, bestetik, segurtasun logikoa (informazio-sistemen segurtasunerako baldintza guztiak, edozein mekanismo edo gailu elektroniko edo informatikoren bidezko sarbideari, prozesamenduari eta erasoei dagokienez). Gainera, araudiak ezarritako jarraibideen artean, administrazio-alderdiei buruzko arauak daude: besteak beste, ardurak esleitzeaz edo hirugarrenekiko kontratuen segurtasunaz eta hirugarrenek informazioa eskuratzeaz.

Arauak eta estandarrak erakundeetan erabilitako xedapenak dira, erakunde horiek eskaintzen dituzten produktuek edota zerbitzuek bezeroaren kalitate-eskakizunak eta aurreikusitako helburuak betetzen dituztela bermatzea helburu dutenak. Ildo horretan, eta eskuartean dugun alderdi partikularrari buruz, ISO 27000 arauak eta haren eratorriek, arau nagusitik sortutako arauek, informazio-sistemen segurtasuna jorratzen dute alderdi guztietan.

SEGURTASUN-POLITIKAK. SISTEMA ETA GAILUETARAKO SARBIDEA

Informazio-sistemen segurtasun-politiken inguruko orokortasunak (segurtasun mekanikoa, zuzeneko sarbidea, sareen bidezko sarbidea).

e.digitall.org.es/A4C42A2V06

ISO 27000 araua. Informazioaren segurtasuna

ISO 27000 serieak metatzen ditu informazioaren segurtasunaren arloko araudi guztiak. Arriskuen prebentzioan zentratutako Informazioaren Segurtasuna Kudeatzeko Sistema (ISKS) baten bidez informazioaren segurtasuna eraginkortasunez ezartzeko, familia horretako arau garrantzitsuenak ISO 27001 eta ISO 27002 arauak dira. Araudi horren bidez, informazioa edozein mehatxutatik babesteko neurriak adierazten dira, formatua

edozein dela ere (elektronikoki biltegiratua, postaz edo bitarteko elektronikoen bidez transmititua, paperean inprimatua, bideoan erakutsia edo elkarrizketan hitz egina), informazioaren konfidentzialtasuna, osotasuna eta eskuragarritasuna une oro bermatzeko.

Araudi horrek nazioarteko aintzatespena du, eta informazioaren segurtasuna kudeatzeko esparru bat ematen du, edozein erakunde publikok edo pribatuk, handik edo txikik, erabil dezan. ISO/IEC 27001 arauak enpresa, erakundea edo negozioa eta haren ospea babesten laguntzen du, eta aparteko balioa gehitzen dio edozein transakziori; erregistro pertsonalak eta informazio kaltebera babesten ditu; agente gaiztoek hackeatzeko edo erasotzeko arriskuak murrizten ditu, eta konfiantza ematen dio hura ezartzen duen erakundeari.

ISO/IEC 27002:2022 araua, jardunbide egokien kode gisa tratatua, 27001 arauaren ezarpena egiaztatzea ahalbidetzen duen segurtasun-kontrol multzo baten moduan berritu da.

27001 eta 27002 arauen jarraibideak

Oro har, araudi horrek sistemen segurtasunerako eta fidagarritasunerako ezarri beharreko protokoloak ezartzen ditu. Zehazki, arauak sistemen segurtasun fisikoari dagokienez ezarri beharreko protokoloak edo prozedurak identifikatzen ditu, baita segurtasun logikoari, mekanismo elektroniko edo informatikoen bidezko sarbideari, informazioaren prozesamenduari edo informazio-sistemen aurkako erasoei dagokienez ezarri beharrekoak ere. Kode gaiztoaren aurkako babeserako, segurtasun-kopietarako, sareetako segurtasunerako edo informazioa trukatzeko eta hirugarrenekin zerbitzuak kudeatzeko jarraitu beharreko prozedurak barne hartzen ditu horrek. Gertaeren eta segurtasun-ahulguneen jakinarazpenari buruzko gomendioak, eta gorabeherak kudeatzeko eta informazioaren segurtasuna hobetzeko prozedurak eta erantzukizunak. Giza baliabideei eta administrazio- edo antolakuntza-alderdiei buruzko protokoloak ere jasotzen dira: besteak beste, informazioaren sarbiderako ardurak esleitzeaz edo hirugarrenekiko kontratuen segurtasunaz eta hirugarrenek informazioa eskuratzeaz.

Zehazki, arau horietako batzuk honako hauei buruzkoak dira:

- **Sistemetara sartzeko murrizketa mekanikoak.** Informazioa gordetzen duten zerbitzariak babestu egin behar dira, baimenik gabe instalazioetara fisikoki sartzea saihesteko. Informazioa prozesatzen eta biltegiratzen duten ekipoek eremu seguru eta babestuetan egon behar dute, definitutako perimetro baten barruan, kontrolekin, jakiteko nor sartzen den haietara.
- **Suteen eta bestelako hondamendien aurkako babesa.** Eraikin, industria-instalazio eta ingurune naturaletako suteen aurkako babesari buruzko araudiaz gain, suteen aurkako babeserako araudi espezifiko oso zorrotz bat dago, informazioak kalterik jasan ez dezan edo gal ez dadin, bereziki datuak prozesatzeko zentroetan non gure informazioa gordetzen den. Zentro horietako hardwareak bero gisa isurtzen du erabiltzen duen energiaren ia % 100, eta tenperatura gehiegi igotzeak sistemei kalte egin diezaieke; beraz, hoztea funtsezkoa da (detektagailu-sare trinko bat eta suteak goiz detektatzeko sistema bat ezartzen dira). Kasu askotan, nahitaezkoa da informazio-sistemaren erreplika sinkronizatuak edukitzea, elkarrengandik urrun, halako moldez non, sistema batek huts egiten badu edo erortzen bada, suteagatik edo hondamendi naturalagatik, zerbitzuak aurrera jarraituko duen azken erabiltzailearentzat.
- **Azpiegituren eta hozte-sistemen diseinu eta egitura efizienteak.** Normalean, erakunde, instituzio edo enpresetan, informazio-sistemak datuak prozesatzeko zentroetan kokatzen dira, eta zentro horiek informazio-zerbitzu eta -sistemak aktibo mantentzen dituzte. Datuak prozesatzeko zentro horiek azpiegiturak behar dituzte, barneko zein kanpoko erabiltzaileei, modu antolatuan eta egituratuan, zerbitzua ematea ahalbidetuko dietenak. Araudiak ezartzen du zer baldintza bete behar diren komunikazio- eta konexio-bideetarako euskarri eta kanalen diseinuan. Kable-sistema egituratu bat izan beharko da, akatsei aurre egiteko eta transmisio-premia handietara erraz zabaldu ahal izateko modukoa. Baita elikadura elektriko seguruko sistemak eta etenik gabeko elikatze-sistema (SAI) bat ere; hornidura elektriko nagusiak huts eginez gero, SAI sistemako bateriek txanda hartuko dute aldi baterako. Zerbitzarien rack-en hedapena ere bai,

Sistema informatikoetara sartzeko identifikazio-sistema.

Datuak prozesatzeko zentro baten diseinua, konexioa eta rack-ak.

datuak prozesatzeko zentroaren barrualdean, informazio-sistemako elementuak konfiguratu, lotu eta, hala badagokio, aldatzen errazteko.

- **Giza baliabideak.** Arauak eta bere eguneraketek langileen kontratazioari, diziplina-prozesuei, lan-harremana eteteari edo lanpostu-aldaketari buruzko alderdiak jorratzen dituzte, baita sarbiderako kredentzialen etenari buruzkoak ere. Zehatz-mehatz adierazten ditu sarbide-kontroleko politikari, erabiltzaileen sarbideen kudeaketari edo sarerako, sistema eragilerako eta aplikazioetarako sarbideei buruzko jarduketak, ordenagailu eramangarrien eta telelanaren erabilera barne.
- **Segurtasuna eta kontrol kriptografikoak.** Informazioaren segurtasunaren aurkako erasoek informazioaren segurtasunari buruzko araudia gero eta eguneratuagoa izatea eragiten dute, eta sistemen segurtasunari buruzko kontrolei behar adineko garrantzia ematea ahalbidetzen dute. Ildo horretan, informazioa eta hura tratatzeko instalazioak kode gaiztoaren aurka babestuta daudela bermatu behar da. Horretarako, lehenik eta behin, kode gaiztoa detektatzeko sistemak eduki behar dira zerbitzarietan eta lanpostuetan. Gainera, kontrol kriptografikoen helburua informazioa babestea da, baldin eta arrotz batek informaziorako sarbide fisikoa izan badezake; horretarako, zifratze-sistema bat ezartzen da, informazioaren konfidentzialtasun eta osotasunari eusteko.

ISO 27002 araua. Informazioaren segurtasuna egiaztatzeko kontrolak.

ISO 27002 arauan aurkeztutako araudia informazioaren segurtasun-kontrolei buruzko jardunbide egokien inbentario gisa planteatu da. Arauak kontrol batzuk eskaintzen ditu, aurreko arauetan informazioaren segurtasunaren inguruan ezarritako helburuak lortzeko inplementazio-gida gisa erabiltzen direnak.

Arau horrek jasotako kontrol-parametroek, beraz, honako hauei eragiten diete, besteak beste: informazioaren segurtasun-politikei, segurtasun horren antolamenduari eta erabilitako baliabideei, sarbide-kontrolei eta ingurunearen segurtasun fisikoari, komunikazio eta eragiketen kriptografiari eta segurtasunari, eta aktiboen kudeaketari.

ISO 27017 eta ISO 27018 arauak. Informazio-sistemak hodeian (cloud). Datu pertsonalen babesa.

ISO 27017 arauak informazioaren segurtasun-kontrolak ezartzen ditu hodeiko zerbitzuetarako, halakotzat hartuta Internet bidez egiten direnak, hau da, ordenagailuan bertan instalatuta ez dauden aplikazioak eskaintzen dituztenak. Horretarako, aplikazio edo programa horien zerbitzariak eskuragarri egon behar du Internetera konektatutako edozein gailutatik, eta edozein erabiltzailerentzako segurtasun-berme eta biltegiratze-gaitasun nahikoak izan behar ditu. Arau horrek ISO 27002 arauan ezarritakoez bestelako kontrol gehigarrien gida bat du, hodeirako berariazkoak.

ISO 270018 arauak, berriz, hodeian identifikazio pertsonaleko informazioa babesteko jarraibideak adierazten ditu. Aplikazio horiekin lan egiteko, beharrezkoa da identifikatzea, eta oso zorrotzak dira identifikazio pertsonal hori egiteko beharrezkoak diren segurtasun-baldintzak. Arau horrek ezartzen ditu identifikazio pertsonaleko informazioaren babesa inplementatzen duten kontrol-helburuak, jarraibideak eta kontrolak, hodeiko konputazio-sistemetarako pribatutasun-printzipioei buruz indarrean dagoen araudiaren arabera.

ISO 27799 araua. Informazioaren segurtasunaren kudeaketa osasungintzan.

Osasunari buruzko datu pertsonalak babesteko modurik onena adierazten duen nazioarteko araua da. Besteak beste, datuetara sartzeko kontrolak ezartzen ditu, sarbide pribilegiatua adierazita; datu konfidentzialen kudeaketa kriptografikoa egiten du, zifratze-gakoak babestuta, eta erabiltzaileen datuen erabilera erregistratzen du, datu horiek baimenduta ez dauden aldaketetatik eta sarbideetatik babestuz.

Informazio pribatua

Informazio-sistemetan, batez ere Internet bidezko nabigazioan eta hodeiko sarbideetan, erabiltzaileen informazio pribatuaren babesari eutsi behar zaio sarbidean eta erabileran. Informazio pribatua norbanakoaren pribatutasunari dagokiona da; bai datu pribatuak, bai pertsonaren identitate digitalari buruzkoa.

PRIBATUTASUN-POLITIKA INTERNETEN ETA APLIKAZIOETAN

Pribatutasun politikaren garrantzia. Pribatutasun politikari buruzko dokumentu baten edukia.

e.digitall.org.es/A4C42A1V07

Informazioaren pribatutasunaren eta norbanakoaren identitatearen garrantzia kontuan hartuta, bisitatzen ditugun edo lan egiten dugun sistema guztiek bete beharreko pribatutasun-politika batzuk ezarri dira. Erabiltzaileari eskatu behar zaio politika horietan ezarritako baldintzak berariaz onartzea, bereziki gure datuak eskatzen diren lekuetan. Pribatutasun-politikari buruzko dokumentua lehen informazio-mailan erakutsi behar da, erabiltzaileen datuak bildu aurretik. Gainera, inprimaki bakoitzean honako hauek jaso behar dira: datuen arduraduna nor den, datu horiek biltzeko helburua, legitimazioa, non biltegiratuko diren eta erabiltzaileek zein eskubide dituzten. Pribatutasun-politikan honako hauek jaso behar dira:

- Aplikatu beharreko araudia eta legeria.
- Erabiltzaileek datuak nola sartzen dituzten.
- Zertarako erabiliko diren datuak.
- Zergatik sartu behar dituzten datuak eta zer gertatuko den hori egiten ez badute.
- Zer datu behar diren webgunearekin edo aplikazioarekin komunikatzeko.
- Konfidentzialtasun-konpromisoa.
- Datuak hirugarrenekin ez partekatzeko konpromisoa.
- Baimenik gabe publizitaterik ez bidaltzeko konpromisoa.
- Datuak ezeztatzeko, zuzentzeko edo eramateko edo datuen tratamendua mugatzeko eskubideari buruzko informazioa.

Pribatutasun-politikak hirugarrenek gure datu pertsonalak erabiltzea saihesten du, berariaz hori adierazten badugu.

ISO 29100 araua. Datu pertsonalen babesa eta pribatutasuna hodeian.

Nazioarteko estandar horrek maila handiko erreferentzia-esparru bat ematen du identifikazio pertsonaleko informazioa (PII) babesteko, erakundeei datuen pribatutasunarekin lotutako babes-mekanismoak definitzen laguntzeko asmoz. Zehazki, arauak terminologia komun bat zehazten du pribatutasunaz; identifikazio pertsonaleko informazioa prozesatzeari dagokionez, eragileak eta haien rolak definitzen ditu; pribatutasuna babesteko kontuan hartu beharreko gomendioak eta gogoetak adierazten ditu, eta Informazioaren eta Komunikazioen Teknologiei buruzko pribatutasun-printzipioak ezartzen ditu.

DigitAll

Segurtasuna

4.3

OSASUNAREN ETA ONGIZATEAREN BABESA

Segurtasuna

A1 maila 4.3 Osasunaren eta ongizatearen babesa

Osasun digitalarekin lotutako seinaleak eta sintomak. Kasu tipikoak

Osasun digitalarekin lotutako seinaleak eta sintomak. Kasu tipikoak

Dokumentu honek osasun digitalaren eta kasu tipikoen kontzeptura hurbilduko zaitu, baita osasun digitalarekin lotutako seinale eta sintoma tipiko nagusietara ere, ikuspegi biopsikosozialetik; hau da, inplikazio fisiko, psikologiko eta soziala, Osasunaren Mundu Erakundeak definitutako osasun-kontzeptuarekin bat etorriz.

Osasun digitaleko kasu tipikoak

Osasun digitalaren kontzeptuak Informazioaren eta Komunikazioaren Teknologien (IKT) erabilerak pertsonen osasunean eta ongizatean duen eragina barne hartzen du. Jarraian, osasun digital ona duzula pentsaraz lezaketen hainbat egoera tipiko azalduko dira:

- Teknologiari eskainitako denbora errespetatzen duzu, teknologiaren erabileran oreka bilatuz edo, ahal den neurrian, beharrezkoa denean baino ez erabiltzeko ahalegina eginez. Denbora luzez erabiliz gero, etenaldiak sartzen dituzu tarteka eta errespetatu egiten dituzu.
- Ohartzen zara teknologia erabiltzeari eskaintzen diozun denboraz, eta batzuetan, zehatz-mehatz zenbat denbora pasatzen duzun kronometratzen duzu. Aldian behin, zure telefono mugikorraren estatistikak berrikusten dituzu, ikusteko zer aplikaziotan pasatzen duzun denbora gehien.
- Jakitun zara gailu elektronikoak neurriz kanpo eta kontrolik gabe erabiltzeak mendekotasun digitalera eraman zaitzakeela. Badakizu mendekotasun mota horri buruzko informazioa edukitzeak teknologiaren erabilera hobeto kontrolatzen eta haren ondorioak aurreikusten lagunduko dizula.
- Gorputz-jarrera egokia izaten duzu telefono mugikorra, ordenagailua, tableta edo beste edozein gailu erabiltzen duzunean. Gainera, ez duzu eskuekin mugimendu errepikakor eta gehiegizkorik egiten gailuak erabiltzen dituzunean.
- Bizitza sozial aktiboa duzu, teknologia erabiltzeaz gain, mundu errealetik isolatuta egon gabe.

Osasun digitalarekin lotutako seinaleak eta sintomak maila fisikoan

Aparatu edo gailu teknologikoak neurriz kanpo erabiltzeak, pantaila baten aurrean denbora luzez egoteak bezala, eragina izan dezake gure osasun fisikoan. Kontu handiz ibili beharko zenuke, teknologiaren erabilera desegokiarekin lotutako kasu hauetakoren bat identifikatzen baduzu (eta agian ez zara konturatu ere egin horretaz):

- Lauso ikusten baduzu edo ikusmena nekatuta sentitzen baduzu, gailu teknologiko baten pantailari begira ordu luzez egon ondoren. Batzuetan, gauzak bikoiztuta edo lerroak okertuta ere ikus ditzakezu. Familiako medikuarekin kontsultatu beharreko seinale edo sintomak izan daitezke.
- Bizkarra, sorbaldak, lepoa edo gorputz-adarrak gogortuta sentitzen badituzu (mina sentitzeraino), teknologia berriak erabiliz luzaroan eserita egon ondoren. Baliteke pantailaren edo erabiltzen duzun gailuaren altuerak jarrera desegokia izatera behartzea. Seinale horiek guztiek, denboran luzatuz gero, lesio kronikoak eragin ditzakete.
- Lepoa eta eskuak gogortzen badira edo ondoez txiki bat badute, gailu mugikorrak (telefonoa, adibidez) etengabe erabili ondoren, edo ordenagailuaren teklak behin eta berriz erabiltzearen poderioz; denboran luzatuz gero, horrek egoera larriagoak ekar ditzake.
- Buruko mina ohi baino gehiagotan baduzu, baliteke etengabe pantaila bati begira denbora luzez egon izanarekin lotuta egotea.
- Buruko mina ohi baino gehiagotan baduzu, baliteke etengabe pantaila bati begira denbora luzez egon izanarekin lotuta egotea.

Osasun digitalarekin lotutako seinaleak eta sintomak maila psikologikoan

Teknologiak eta, bereziki, Instagram edo Facebook bezalako hainbat sare sozialek arazo psikologikoak eragin ditzakete, hainbat faktoreren ondorioz. Horregatik, puntu honetan, teknologiak maila psikologikoan eragiten dizkigun zenbait arazo identifikatzen lagun diezaguketen alderdiak landuko ditugu.

- Gailu elektronikoa non dagoen ez jakiteak edo galtzeak eragindako antsietate-garapena.
- Mendekotasun digitala dela-eta teknologia erabiltzea eskatzen ez duten eguneroko jarduerak egiteari uztea.
- Zure emozioak teknologiaren erabileraren arabera aldatzen direla sentitzea. Alde batetik, gailu teknologikoetarako sarbiderik ez izateak tristura eta suminkortasun sentimendua eragiten dizu. Bestetik, zoriontasuna sentitzen duzu gailu teknologiko berri bat erosi edo erabiltzeagatik.
- Bakardade-sentsazioa duzu gailua gertu ez duzunean. Pertsonekin teknologiaren bidez elkarreragiteko beharra sentitzen duzu, eta, ildo horretan, gailu horiekiko mendekotasuna areagotzen duzu.
- Ez zara gai, denbora-tarte batean, zure gailua, sare sozialak edo aplikazioak modu kontrolatuan erabiltzeko. Horrek zure ohiturak aldatzen ditu, eta lo egiteko orduak murriztea eragiten du.
- Zure gorputz-irudia banantzen duzu, Instagram edo Snapchat bezalako sare sozialetako iragazkiak gehiegi erabiltzen dituzulako zure irudia manipulatzeko, edo, bestela, ez zara identifikatzen zure gorputz errealaren zatiren batekin, eta horrek autopertzepzio estetikoko alterazioak eragiten ditu.

Osasun digitalarekin lotutako seinaleak eta sintomak maila sozialean

Gailu teknologikoak gehiegi edo kontrolik gabe erabiltzeak eragina izan dezake beste pertsona batzuekin harremanak izateko moduan. Hala, gure egunerokoan oso ohikoak diren gailuak (mugikorra, ordenagailua edo kontsola) modu desegokian erabiltzeak gure familiarekin, lagunekin, lankideekin eta, oro har, gizarteko gainerakoekin harremanetan jartzeko modua eta maiztasuna alda ditzake.

Seinale eta sintoma batzuek adieraz diezagukete gailu jakin baten erabilerak eragina duela guregan maila sozialean. Horiek identifikatzea lagungarria izan daiteke portaera hasieran aldatzeko, eta beraz, gure bizitzan ondorio larriagoak saihesteko. Jarraian, seinale eta sintoma ohikoenetako batzuk aipatuko ditugu:

- Familiarekin edo lagunekin elkartzeko ohiko maiztasuna murriztea eta denbora hori gailu teknologikoak erabiltzen inbertitu nahiago izatea.
- Eguneroko bizitzan egin ohi zenituen kirol- edo aisialdi-jarduerak uztea edo murriztea.
- Online-komunikazioak lehenestea presentzialtasunaren gainetik; hau da, nahiago duzu, besteak beste, deiaren, bideodeiaren eta WhatsApparen bidez hitz egin, zure inguruko pertsonekin aurrez aurre geratu baino. Erosotasunagatik aukera ezin hobea izan daiteke, baina denboran luzatuz gero, mundu errealetik isolatu gaitzake.

ADI

Harremanak izateko modua ez da berehala aldatzen; aitzitik, prozesu progresibo bat da, pertsonak berak eta gailu teknologikoen erabilera kudeatzeko moduak baldintzatua.

OHARRA

Pandemiaren ondoren, batzuetan, IKTen abantailak erabiltzeko joera dugu, bilera birtualak eta bideodeiak, besteak beste, egiten baititugu; aldiz, gomendagarriena, ahal den neurrian, presentzialtasuna eta besteekiko kontaktu fisikoa mantentzea da. Bakardade-indizeek gora egin dute biztanlerian, eta gazteak eta adinekoak izan dira kaltetuenak; era berean, suizidioak ere igo dira, eta, ondorioz, ageriago daude osasun mentaleko arazoak.

Informazio gehiago

Osasunaren Mundu Erakundea. Osasun-sistemak indartzeko esku-hartze digitalei buruzko gomendioak.
e.digitall.org.es/directriz-oms

DigitAll

Segurtasuna

4.4 INGURUMENAREN BABESA

Segurtasuna

A2 maila 4.4 Ingurumenaren babesa

Teknologiaren ingurumen-inpaktuak

Teknologiaren ingurumen-inpaktuak

Sarrera

Maila honetako bideoetan ikusi dugun bezala -bereziki, 3. bideoan, "***Gailu teknologikoen energia-kontsumoa (zure emailaren aztarna)***" izenekoan, eta 5. bideoan, "***Teknologia modu efiziente eta jasangarrian erabiltzen dugu?***" izenekoan-, gero eta argiago dago teknologia digitalaren erabilera etengabe handitzeak kalte egiten diola planetaren osasunari. Bideoetan adierazten denez eta Greenpeacek 2017an egindako txosten batean zehazten denez, teknologia digitalen sektorearen aztarna energetikoa munduko elektrizitatearen guztizko kontsumoaren % 7 ingurukoa zen (Greenpeace, 2017). Gai hori gero eta kezkagarriagoa da, pandemiaren osteko testuingurua eta trantsizio energetiko globalaren gaur egungo egoera kontuan hartuta.

GAILU TEKNOLOGIKOEN ENERGIA-KONTSUMOA (ZURE EMAILAREN AZTARNA)

e.digitall.org.esA4C44A2V03

TEKNOLOGIA MODU EFIZIENTE ETA JASANGARRIAN ERABILTZEN DUGU?

e.digitall.org.es/A4C44A2V05

Txosten horrek produktu digitalen gero eta kontsumo handiagoan jartzen du arreta: bai hardwarean, bai softwarean, eta horiek ekoizteko eta erabiltzeko behar diren materialetan eta energian.

Beste gai kezkagarrienetako bat hondakin teknologikoena da, etengabe hazten ari baitira eta zaharkitzearen fenomenoarekin lotuta baitaude, programatutakoa, hautemandakoa edo espekulaziokoa izan.

⚠ ADI

Adibidez, telefono mugikorrei erreparatzen badiegu, adituek ohartarazi dute haien bizi-zikloa laburregia dela; izan ere, kalkulu batzuek erakusten dute erabiltzaileen % 40k bi urtean behin aldatzen duela telefonoa, eta ia % 60k zortzi aldiz baino gehiagotan aldatzen duela telefonoa bizitzan zehar (ONTSI, 2021).

Beraz, teknologia digitalekin lotutako ingurumen-inpaktuak askotarikoak diren arren, hiru bloke handitan bana ditzakegu: materialen erauzketarekin eta gailuen ekoizpen-prozesuarekin lotutako inpaktuak, teknologia digitalen sektorearen energia-kontsumoa eta hondakin elektronikoen sorrera. Teknologia digitalaren energia-kontsumoa aurreko mailan aztertu zenez, aipatutako beste bi blokeei helduko diegu dokumentu honetan.

Teknologia digitalerako materialak erauztearen inpaktuak

Aurreko mailan ikusi genuen bezala, bereziki 3. bideoan ("***Baliabide teknologikoen ekoizpen prozesuak***"), gailu digitalak fabrikatzeko behar diren elementu gehienak (telefono mugikorrak, adibidez, baina baita ordenagailu pertsonalak edo tabletak ere) meatzaritza-jardueren bidez erauzi behar izaten dira.

BALIABIDE TEKNOLOGIKOEN EKOIZPEN-PROZESUAK

e.digitall.org.es/A4C44A1V03

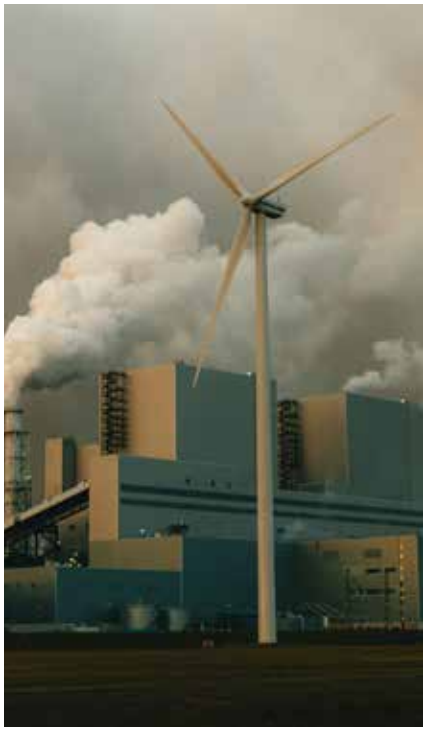
Meatzaritza-jarduerak hainbat motatakoak izan daitezke, hainbat irizpideren arabera. Erauzketa-bolumenari erreparatzen badiogu, esan dezakegu meatzaritza handia, ertaina eta txikia dela, eta artisautza-meatzaritza ere badago. Erauzketa motaren arabera ere sailka dezakegu: barruko edo lurpeko meatzaritza eta aire zabalekoa.

Tradizioz, galerian edo zanga txikietan egindako meatzaritza erabili da gehien ikatza eta beste material batzuk erauzteko, eta oraindik ere artisautza-meatzaritza erabiltzen da urrea eta beste mineral batzuk kantitate txikietan ateratzeko. Baina, gaur egun, aire zabaleko meatzaritza mota guztietako materialak erauzteko formula gogokoena bihurtzen ari da; bereziki, teknologia digitala garatzeko beharrezkoak direnak.

Aire zabaleko eskala handiko meatzaritzako erauzketa-proiektuak oso ohikoak dira kobrezko edo litiozko hobiak ustiatzeko. Funtsezkoak dira industria digitalerako, baina baita meatoki polimetalikoetarako ere, hainbat mineral baitituzte kontzentrazio desberdinetan.

OHARRA

Konparatuta, aire zabaleko meatzaritza merkeagoa da, bai azpiegiturari dagokionez, bai eskulanari dagokionez, azalera handia ustia baitaiteke proiektu berean. Baina, hain zuzen ere horregatik, ingurumen- eta gizarte-inpaktu askoz handiagoa du ustiatutako ingurunean eta bertan bizi diren komunitateetan.



Aire zabaleko meatzaritzaren ingurumen-inpaktuen artean, honako hauek nabarmen ditzakegu:

1. **Kutsadura atmosferikoa.** Material-erauzketen eta lurra ebakitzeko egin beharreko leherketen ondorioz inpaktuak sortzen dira atmosferan; zarata handia sortzen da eta hauts-kantitate handiak airera isurtzen dira.
2. **Lurzoruaren gaineko inpaktuak**. Batez ere, deforestazioa, higadura eta tokiko erliebearen eta morfologiaren aldaketak, lur-mugimenduen ondorioz, baita hondakin-materialen metaketak ere.
3. **Lurzorua kutsatzea.** Lurzoruetan zenbait propietate fisiko eta kimiko aldatzen dira, eta, are gehiago, propietate horiek beste erabilera batzuetarako erabat erabilezin bihur daitezke, hala nola nekazaritzarako.
4. **Lurrazaleko urak kutsatzea eta kalteak akuiferoetan.** Ibaien ibilguetan eta akuiferoetan eragina izan daiteke, bai eta metal astunen ondoriozko kutsadura eta lurpeko uren pH-aldaketak ere.
5. **Floraren eta faunaren gaineko inpaktuak.** Eremuan bertan zuzenean egindako aldaketek lurrazaleko flora ezabatu eta fauna lekualdarazten dute. Horrez gain, habitatean ere gertatzen dira aldaketak eta ur-iturriak kutsatzen dira; horrek populazioei eragin diezaieke.
6. **Kutsadura bisuala.** Lurraren morfologiaren aldaketak eta meatzaritza-ustiapenean sortutako hutsune edo krater erraldoiek inpaktu bisuala eragiten dute.
7. **Komunitateen eta meatzaritza-enpresen arteko gatazkak**, lurren erabilera desegokiaren eta bizirauteko modu tradizionalen aurkako mehatxuaren ondorioz.

Beste eskala batean, teknologia digitala garatzeko beharrezkoak diren baliabide naturalak kontrolatzearen inguruko liskarrek garrantzi eta intentsitate handiagoko gatazkak sortzen dituzte, faktore geopolitiko eta estrategikoek definitutakoak, eta horiek hurrengo mailetan aztertuko dira.

Hondakin elektronikoak eta teknologikoak

Teknologia digitala garatzeko behar diren aparatu elektriko eta elektronikoak oso produktu konplexuak izaten dira, eta, normalean, askotariko piezak eta osagaiak izaten dituzte, hala nola plastikoa, zura edo metala, zirkuitu inprimatuetako txartelen osagaiak edo kristal likidozko pantailak, ahaztu gabe kableak, pilak, bateriak edo inprimaketa-kartutxoak (Miteco, 2022).

ADI

Munduko Ekonomia Foroaren eta Lanaren Nazioarteko Erakundearen (LANE) kalkuluen arabera, 2018tik, gailu elektroniko eta elektrikoen 50 milioi tona hondakin baino gehiago sortzen dira urtero, eta zifra hori gora egiten ari da (World Economic Forum, 2019).

Kopuru horretatik, % 20 baino gutxiago birziklatzen da formalki, eta gainerakoa hondakindegietan uzten da, non hondakin horiek baztertu egiten diren eta ingurunean hainbat inpaktu mota sortzen dituzten; hondakindegi horietan milioika pertsonak modu informalean lan egiten dute hondakin elektronikoak biltzeko, birziklatzeko eta baztertzeko, eta lan horren zati handi bat baldintza kaltegarrietan egiten da, bai osasunerako, bai ingurumenerako (LANE, 2019).

Kontrolatu gabeko hondakindegietan amaitzen duten hondakin horietako asko iparraldeko herrialdeetatik datoz, eta herrialde horietan birziklatze-prozesu formalen mende egon beharko lirateke. Aldiz, ingurumen-erregulazio hain zorrotza ez duten herrialdeetan amaitzen dute, nazioarteko akordio bat dagoen arren, Nazio Batuen Erakundearen Basileako Konbentzioa, herrialdeen arteko hondakin arriskutsuen zirkulazioa arautzen duena eta "dumping ekologikoa" deritzona debekatzen duena.

Baina konbentzio hori ez da eraginkorra, eta Ghanak, Nigeriak, Indiak eta beste zenbait herrialdek gainezka egiten dute hondakin teknologikoekin. BANek (Basel Action Network) idatzitako “Zuloak ekonomia zirkularrean: ihesak Europako hondakin elektronikoetan” txostenak salatu duenez, Europako 10 herrialdek, Espainiak barne, gailu elektroniko eta elektrikoen 350.000 tona hondakin (GEEH) baino gehiago esportatu zituzten, legez kanpo, 2017an.

OHARRA

Txosten berean zehazten da, gainera, Europan pertsona bakoitzak 17,7 kg GEEH sortzen dituela urtean; estatubatuar bakoitzak, 20 kg, eta Afrikan, aldiz, batez bestekoa 1,7 kg da pertsonako.

Hurrengo mailetan ikusiko dugunez, hondakin horiek behar bezala birziklatzeak eta kontsumoa murriztea eta erabiltzen ari diren gailuak berrerabiltzea sustatzeak gaur egungo arazoa arintzera eraman gaitzakete. Haien material balioztagarriak baliabide bat dira eta beraz, ez dira galdu behar, eta ezin dira galdu. Adibidez, urtero botatzen diren telefono mugikorrak behar bezala eta arduraz birziklatzeak kobre-, urre- edo litio-kantitate handiak berreskuratzeko aukera emango luke, ingurumenean eragin handia duten eta era askotako gatazkak eragin ditzaketen erauzketa-prozesuak behar dituzten materialen adibidea jartzeagatik.

Hala ere, aparatu edo ekipo horiek substantzia arriskutsuak ere badituzte, eta, haien funtzionaltasuna bermatzeko beharrezkoak diren arren, ingurumen-kutsadura eta giza osasunerako kalteak eragin ditzakete, behin hondakin bihurtuta, aparatuak behar bezala kudeatzen eta tratatzen ez badira.

Adibidez, aparatu edo gailu askok kadmioa, merkurioa, beruna, artsenikoa eta fosforoa izan ditzakete, kutsatzeko ahalmen handia dutenak. Horregatik, GEEHak kudeatzeko etapa guztiak, bilketa, biltegiratzea, garraioa eta tratamendua barne, baldintza seguruetan egin behar dira, horrelako substantzia arriskutsuak ingurunera aska ditzaketen manipulazioak edo hausturak saihesteko, baita, tratamenduan dauden bitartean, hondakin horiekin kontaktuan dauden langileak arriskuan jartzea ekiditeko ere (Miteco, 2019).

Arazo nagusia da gaur egun produktu elektronikoak ez daudela diseinatuta eguneratzeko edo bizitza luzea izateko aukera izan dezaten, eta, beraz, hondakin-sorreraren arazoa larriagotu egiten da. Egoera horren aurrean, aurreko mailan ikusi genuen bezala, Europako Batzordearen "Europako Hamarkada Digitala: 2030erako jomuga digitalak" txostenak proposatu du erabiltzaileek beren gailuen ingurumen-inpaktuari eta horiek minimizatzeko aukerei buruzko ezagutza izatea.

Egoera horren aurrean, argi dago GEEHen kudeaketa arduratsua funtsezkoa dela Garapen Jasangarrirako Helburuak lortzeko. Behar bezalako tratamendu batek pertsonen eta ingurunearen osasuna eta ongizatea hobetzen lagunduko luke, bai eta ekoizpen- eta kontsumo-eredua alternatiba jasangarriagoetarantz aldatzen ere.

Baina, jakina, gai hori ez da soilik teknologia digitala kontsumitzen duten pertsonen erantzukizuna. Arreta prozesu kolektiboetan jarri behar da, eta lankidetza sustatu behar da multinazionalen, enpresa txiki eta ertainen (ETE), ekintzaileen, unibertsitateen, sindikatuen, gizarte zibilaren eta enpresa-elkarteen artean, elektronikaren ekonomia zirkularra pixkanaka lortzeko behar diren bideak sortzeko, baliabide eta materialen xahuketa mugatzeko, ingurumen-inpaktua murrizteko eta milioika pertsonarentzako enplegu duinak sortzeko (LANE, 2019).

Informazio gehiago

Europako Batzordea (2021). *Europako Hamarkada Digitala: 2030erako jomuga digitalak.* e.digitall.org.es/metas-2030

Greenpeace (2017). *Clicking Clean.* e.digitall.org.es/clicking-ckean

Lillo (2010). *Meatzaritzaren inpaktuak ingurune naturalean.* e.digitall.org.es/impactos-minería

Miteco (2019). *Gailu elektrikoak eta elektronikoak.* e.digitall.org.es/miteco

National Geographic (2022). *Lur arraroak.* e.digitall.org.es/tierras-raras

Teknologiaren eta Gizartearen Behatoki Nazionala (ONTSI, 2021). *Gailu teknologikoak erabiltzeko joerak.* e.digitall.org.es/tendencias-uso-dispositivos

Lanaren Nazioarteko Erakundea (2019). *50 milioi tona hondakin elektroniko botatzen dira urtero.* e.digitall.org.es/residuos-tecnologicos

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

World Economic Forum (2019). A New Circular Vision for Electronics. e.digitall.org.es/vision-electronics

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