DigitAll

Gaitasun
digitaletan
prestakuntza

4

Segurtasuna

DigitAll

Gaitasun
digitaletan
prestakuntza

Segurtasuna

A1 maila

AURKIBIDEA

DigitAll

Segurtasuna

4.1
GAILUEN BABESA

Segurtasuna

A1 maila 4.1 Gailuen babesa

Informazioaren segurtasun-printzipioak

Informazioaren segurtasun-printzipioak

Informazioaren segurtasunak funtsezko zeregina du gaur egungo gizartean. Guztiok erabiltzen ditugu egunero sistema informatikoak gure informazioa kudeatzeko, bai maila pertsonalean, bai enpresa batean edo administrazio publikoan. Gure datuak formatu digitalera migratzeak arrisku batzuk dakartza, eta arrisku horiek ezagutu eta kontrolatu behar ditugu, datu horiek arriskuan jar ditzakeen erasorik ez jasateko. Gai honetan, informazioaren segurtasunaren kontzeptua definituko dugu, harekin lotutako termino batzuk aurkeztuko ditugu eta gure datu digitalak babesteko jarraitu beharreko zenbait printzipio azalduko ditugu.

Informazioaren segurtasuna

Informatikaren munduan, sistemak edo horiek kudeatzen duten informazioaren babesarekin lotutako termino ugari daude. Informazioaren segurtasuna da horietan lehena. Kontzeptu hori ulertzeko, lehenik eta behin, informazioa zehatz-mehatz zer den definitu behar dugu. Informazioa da "edozein modutan komunikatu, aurkeztu edo gorde daitekeen ezagutza oro" (*CCN-STIC-431: 2006*). Ildo horretan, mezuen, mezu elektronikoen, datu-baseen eta abarren moduan aurki daiteke informazioa.

Informazioaren segurtasuna, beraz, informazioaren konfidentzialtasuna, osotasuna eta eskuragarritasuna babestea da (*UNE-ISO/IEC 27000:2014*). Hiru kontzeptu horiek informazioaren segurtasunaren hiru dimentsioak osatzen dituzte, eta **CIA Triada** (ingelesez, *Confidentiality, Integrity and Availability*) moduan izendatu dute era bateratuan. Ondoren, horietako bakoitza deskribatuko da labur:

1 | **Konfidentzialtasuna**: informazioa isilpekoa dela eta baimendutako pertsonek soilik eskuratu eta ikus dezaketela bermatzea.
2 | **Osotasuna:** informazioa baimenik gabe ez dela aldatzen ziurtatzea.
3 | **Eskuragarritasuna:** informazioa eskuragarria izateko eta, eskatzen denean, hura erabiltzeko prest egoteko ahalmena.

CIA TRIADA KONFIDENTZIALTASUNA, OSOTASUNA ETA ESKURAGARRITASUNA

CIA Triada kontzeptua sartu da: Konfidentzialtasuna, Osotasuna eta Eskuragarritasuna. Kontzeptu hori osatzen duten zati guztiak adibide erraz baina benetakoen bidez azalduko dira, eta kontzeptu horrek informazioaren segurtasunean duen garrantzia nabarmenduko da.

e.digitall.org.es/A4C41A1V02

ISO-7498-2 arauaren barruan, "segurtasun-zerbitzu" gisa definitzen dira CIA Triadaren segurtasunaren hiru dimentsioak. Konfidentzialtasunaz, osotasunaz eta eskuragarritasunaz gain, arau horretan jasotako beste segurtasun-zerbitzu batzuk ere badira:

1 | **Egiaztatzea:** bera dela dioena benetan bera dela bermatzea, bai komunikazio batean, bai informazio baten egile gisa.
2 | **Ez arbuiatzea:** igorleak edo hartzaileak mezu bat transmititzeari edo jasotzeari uko egitea saihestea, hurrenez hurren.
3 | **Sarbide-kontrola:** baliabide baterako baimenik gabeko sarbidea saihestea.

Informazioaren segurtasuna babesteko hainbat neurriri buruz pentsatzen dugunean, aurreko segurtasun-zerbitzu guztiak hartu behar ditugu kontuan. Puntu bakoitza ulertzeko, banka elektronikoan erabiltzen dugun aplikazioaren adibidea aztertuko dugu.

Gure bankuaren banka elektronikora web-nabigatzaile baten bidez sartzen garenean, lehenik eta behin, eskaintzen dituen zerbitzuen informazio publikoa ikusten dugu. Edozein akats dela eta, orrialdea ez badago eskuragarri, informazioa ez legoke **eskuragarri** kontsultak egiteko. Gure informazio pribatura sartu nahi badugu (gure banku-kontuetara eta -mugimenduetara, adibidez), geure burua identifikatu behar dugu. Horretarako, **egiaztatze-prozesua** egiten dugu, gure erabiltzaile-izena eta pasahitza adieraziz. Jakina, datu horiek zuzenak ez badira, ezin izango dugu gure informazioa eskuratu, **sarbide-kontrola** baitago. Egiaztatu ondoren, geure datuak ikusi ahal izango ditugu. Informazio hori zifratuta bidaltzen da bankuaren zerbitzarietatik gure ordenagailura; beraz, **konfidentziala**

da. Gainera, **osotasuna** kontrolatzeko mekanismoak ere aplikatzen dira, ikusten ari garen informazioa zuzena dela bermatzeko. Azkenik, egiaztatuta gaudenez, gure kontua erabiliz banku-mugimendu bat egiten badugu, bankuak agindua **ez arbuiatzea** bermatzen du.

Segurtasun informatikoa

Informazioaren segurtasunaz gain, antzeko beste kontzeptu batzuk ere erabiltzen dira, baina ñabardura batzuk dituzte. Horietako bat **segurtasun informatikoarena** da, informazioa prozesatzen, biltegiratzen, banatzen eta abar egiten duten bitarteko informatikoetan zuzenean eragiten duten segurtasun-alderdi teknologikoei erreferentzia egiten diena. Puntu honen adibide espezifiko bat da zifratua erabiltzea datuak babesteko, biltegiratuta edo bidean dauden bitartean.

Aitzitik, informazioaren segurtasuna termino zabalagoa da, segurtasun informatikoa barne hartzen duena eta segurtasunaren alderdi sistemikoak ere lantzen dituena, hala nola politikak edo prozedurak. Adibidez, informazioaren segurtasunaren barruan -baina ez segurtasun informatikoaren arloan- honako neurri hauek daude: arriskuak kudeatzeko politikak aplikatzea edo segurtasuna indarrean dagoen araudira egokitzea.

⚠ ADI

Termino oso antzekoak diren arren, **informazioaren segurtasuna** eta **segurtasun informatikoa** ez dira gauza bera. Informazioaren segurtasuna termino askoz ere zabalagoa da, segurtasun informatikoa barne hartzen duena.

Informazioaren segurtasun-printzipioak

Informazioaren segurtasun-maila ona bermatzeko, oinarrizko printzipio batzuk bete behar ditugu. Printzipio horiek oinarrizko ideiak ematen dizkigute, hainbat agertokitan aplika daitezkeenak. Behar bezala aplikatuz gero, ziurta dezakegu segurtasun-maila onargarria izango dugula gure sistemetan.

Pribilegio minimoen politika

Pribilegio minimoen politika jarraitzea baimenen banaketa bideratzeko modu egokia da, informazioa eskuratu eta prozesatzeko orduan. Ildo horretan, pribilegioak erabiltzaile batek informazio jakin baten gainean ekintza espezifiko bat egiteko dituen baimen jakin batzuei buruzkoak dira. Beraz, pribilegio minimoaren printzipioak planteatzen digu eguneroko jarduerak bermatzeko erabiltzaile bakoitzak behar dituen ekintzak soilik egiteko aukera emateko moduan konfiguratu behar ditugula informazioaren baimenak. Erabiltzaile batek edo erabiltzaile talde batek behar baino pribilegio gehiago izatea saihestu nahi da, horrek sistemaren segurtasuna arriskuan jar bailezake.

Ikus dezagun printzipio horren adibide bat. Demagun erakunde bereko erabiltzaile batzuek ordenagailu bera erabiltzen dutela informazio pertsonal jakin bat gordetzeko; adibidez, nominak. Egoera horretan, erabiltzaile bakar batek ere ez luke izan beharko beste erabiltzaile baten nomina kontsultatzeko aukera. Egoera horren konfigurazio posible bat erabiltzaile bakoitzarentzako karpeta bat sortu eta baimenak konfiguratzea izan daiteke, erabiltzaile bakoitzak bere karpeta pertsonalerako sarbidea soilik izan dezan. Kasu horretan, pribilegio minimoaren printzipioa aplikatzen ari gara, bere zereginak arazorik gabe egiteko behar dituen baimen bakarrak ematen ari baikatzaizkio erabiltzaile bakoitzari. Aitzitik, baimenak behar bezala konfiguratuko ez bagenitu, erabiltzaile guztiek karpeta guztien gaineko baimenak izango lituzkete. Ildo horretan, asmo txarreko edozein erabiltzaile, edo eraso bat jasan duen edonor, zeinaren kontua konprometitu den, sistemaren informazioari buruzko segurtasun-arazo potentzial bat izango litzateke.

Sarbide itxia lehenestearen kontrol-politika

Aurreko printzipioarekin hertsiki lotuta dago sarbide itxia lehenestearen kontrol-politika. Printzipio horren oinarria erabiltzaileek informazioaren gainean dituzten baimenak modu murriztailean konfiguratzea lehenestea da; besterik adierazi ezean, inork ez dezan sarbidea izan. Sarbide itxia lehenestearen kontrol-politikak informazio jakin bat nahi gabe eta oharkabean bidegabe eskuratzea saihestu nahi du.

Politika hori erraz uler daiteke suebakiei buruz hitz egiten badugu. Suebakiak sarearen konexioak kontrolatzen dituzten gailuak dira. Oro har, politika ona da suebaki bat konfiguratzea, sare-konexioak egitea lehenestea saihesteko, eta behar ditugunak berariaz gehitzeko. Hori gertatzen da, adibidez, Windows sistema eragilean berez konfiguratuta datorren suebakiarekin. Suebaki horrek ez dio uzten kanpoko inori gure ordenagailuarekin inolako konexiorik ezartzen, ekipoak berak aldez aurretik hasi ez badu behintzat.

Funtzioak bereiztea

Erakunde batean, garrantzitsua da eginkizunak erakundeko kideen artean banatuta egotea. Enpresetan, normalean, hainbat lan egiten dituzten sailak egoten dira, hala nola giza baliabideen saila, marketinarena edo Informazioaren Teknologiena (IT). Sistema informatikoak erabiltzean eta erakundearen informazioa kudeatzean, langile-talde bakoitzaren eginkizunen eta arduren halako bereizketak zehaztu eta ezarri beharko lirateke. Horrek interes-gatazkak izatea eta pertsona bakar batengan pribilegioak pilatzea saihesten du (segurtasun-arazoak eragin ditzake azken horrek).

Adibide argi bat enpresa bateko sail bakoitzeko langileek egin beharko lituzketen funtzio eta zereginetan ikus dezakegu. Ez luke zentzurik izango Finantza Saileko langileek enpresa baten sareko gailuetan konfigurazioak egin ahal izateak, edo marketin-saileko langile batek enpresako langile guztien nominetarako sarbidea izateak. Langileen artean funtzioak bereiziz gero, erabiltzaileen pribilegioak kontrolatuta eta haien eguneroko funtzioetara mugatuta daudela ziurta dezakegu.

Defentsa sakona

Printzipio hori informazioaren segurtasun-neurriei eta horien aplikazio-lekuari buruzkoa da. Gaur egun, mehatxu ugari eta askotarikoak jasaten dugunez, ez da nahikoa segurtasun-neurri bakar bat erakundearen puntu zehatz batean aplikatzea. Garrantzitsua da segurtasun-maila desberdinak ezartzea gure sistemetan eta horiek kudeatzen duten informazioan.

Segurtasun-maila bakoitzean aplika daitezkeen hainbat neurri edo kontrol daude. Ondoren, maila bakoitzerako adibide bat erakutsiko dugu:

- **Politikak, prozedurak eta kontzientziazioa:** enpresaren ekipoetan pasahitzak kudeatzeko politika bat izatea, erabiltzaileak aldian-aldian berritu behar izan dezan eta gutxieneko karaktere batzuk bete ditzan.
- **Segurtasun fisikoa:** giltzaz itxitako komunikazio-armairu bat izatea, non sareko gailuak egongo diren.
- **Perimetroa:** suebaki bat instalatzea eta konfiguratzea, enpresaren sarrerako eta irteerako konexioak kontrolatzeko.
- **Barne-sarea:** erakundearen barne-sareen bereizketa logikoa egitea, VLAN (Virtual Local Area Network) sareak erabiliz.
- **Host-a:** software gaiztoaren aurkako babesa, birusen kontrako sistemak instalatuz.
- **Aplikazioa:** maila korporatiboan identitate-sistema bat inplementatzea.
- **Datuak:** ekipoetan biltegiratutako informazioa zifratzea.

Maila batean neurri bat edo batzuk aplikatzeak ez digu bermatzen erabat seguru egongo garenik. Gerta liteke erakundean segurtasun fisiko handia izatea, segurtasun-guardia bat izanda, eraikinerako sarbideak kontrolatuta, sareko gailuak giltzaz itxitako komunikazio-armairu batean babestuta izanda... baina gainerako segurtasun-mailetan beste kontrolik ez aplikatzea. Edozein unetan izan dezakegu kanpoko sare-konexio baten bidezko eraso bat, eta gure ekipoetan gordetako datu guztiak bistaratu daitezke, ez badugu neurririk gainerako mailetan. Edozein sistema informatikotan, puntu ahulenaren segurtasun-mailaren arabera definitzen da multzo osoaren segurtasun-maila. Garrantzitsua da, beraz, geruza guztiak buruan izan eta horietako bakoitzean kontrolak ezartzea, defentsa sakonaren printzipioa aplikatuz.

Segurtasun-mailak (editoreak sortu zuen irudia)

Informazio gehiago

VLAN sare logiko bat da, sare fisiko bera partekatzen duten gailuen multzo bat biltzen duena eta multzo bakoitzaren trafikoa isolatzen duena.
eu.wikipedia.org/wiki/VLAN

ADI

Edozein sistema informatikotan, puntu ahulenaren segurtasun-mailaren arabera definitzen da multzo osoaren segurtasun-maila.

Segurtasun informatikoari buruzko prestakuntza

Aurreko puntuan aipatu den bezala, sistema baten segurtasun-maila haren puntu ahulenaren segurtasun-mailaren arabera definitzen da. Ildo horretan, edozein informazio-sistemaren ahulgune nagusia hura erabiltzen duten pertsonak dira, erabiltzaileak. Ez da nahikoa segurtasun-maila guztietan dauden neurri guztiak aplikatzea, baldin eta erabiltzaileek ez badakite zer mehatxuk eragin diezaieketen, edo ez badakite nola jokatu mehatxu baten aurrean daudenean.

Funtsezkoa da etxeko erabiltzaileek eta enpresetako langileek zibersegurtasunari buruzko ezagutza jakin batzuk izatea. Badakigu arrakasta duten eraso gehienak ez direla segurtasun-neurririk edo -kontrolik ez izatearen ondorio, baizik eta erabiltzaileek ez jakitearen ondorio. Zentzu horretan, arrakasta-tasa handiena duen adibide ohikoenetako bat phishinga da. Eraso horiek erabiltzaileari engainua egitean oinarritzen dira: mezu bat bidaltzen zaio, hirugarren pertsona edo entitate bat dela esanez, hark ekintza espezifiko bat egin dezan. Erabiltzailea fidatu egiten da mezuarekin eta urratsak jarraitzen ditu. Horren ondorioz, kasu askotan, datuak lapurtzen dira, kontuak eskuratzen dira eta abar.

Maila pertsonalean, interesgarria da segurtasunaren arloko informazio-iturriak ezagutzea, kontsultatu ahal izateko eta gai horri buruzko ezagutza eskuratzeko. Baliabide horiek informazio garrantzitsua dute, bai erabiltzaileentzat, bai enpresentzat, gaur egungo mehatxuez eta mehatxu horietatik babesteko moduez. Gainera, maila korporatiboan, interesgarria da langile guztientzako prestakuntza-programak ezartzea.

SEGURTASUNARI BURUZKO INFORMAZIO-ITURRIAK

Erreferentziazko dokumentua: ***A4C41A1D02***

Segurtasun informatikoari buruzko ikuskaritzak

Eremu pertsonalean zein lanean eragin diezaguketen mehatxuak ezagutzeaz eta babesteko neurriak aplikatzeaz gain, garrantzitsua da gure sistemen segurtasun-maila ezagutzea. Horretarako, segurtasun-ikuskaritzak egiten dira, informazio-sistemen multzo baten segurtasun-egoera ezagutzeko.

Segurtasun-ikuskaritzei esker, benetan, segurtasun-neurriak behar bezala aplikatzen ari direla eta beren funtzioa betetzen dutela egiazta daiteke. Ikuskaritza horiek, gainera, aurretik identifikatu ez diren eta erasoetarako bide izan daitezkeen ahuleziak daudela aurkitzeko balio dute. Ikuskaritzak funtsezko puntuak dira sistema edo erakunde baten segurtasun-egoera ezagutzeko.

Hainbat auditoria mota daude, baina, oro har, barne- edo kanpo-ikuskaritzetan sailka ditzakegu. Barne-ikuskaritzak erakundeko langileek egiten dituzte, beren sistemen gainean. Bestalde, kanpo-ikuskaritzak kanpoko enpresa bati kontratatzen zaizkio. Garrantzitsua da, ikuskaritzak egin aurretik. horien baldintzak eta irismena ezartzea, gaizki-ulertuak edo ezusteko arazoak saihesteko. Badira, halaber, egiaztatzeko aukera ematen duten ikuskaritzak, balizko bezero edo hornitzaileei nolabaiteko segurtasun-maila bermatzeko balio dutenak.

Informazioaren segurtasun-printzipioak ez aplikatzearen ondorioak

Gaur egungo gizartean, bai herritarrek bizitza pribatuan, bai enpresek eta erakunde publikoek informazio-sistemak erabiliz egiten dituzte eguneroko lanak. Gaur egun, negozio gehienak sistema informatikoen mende daude beren eragiketak egiteko. Izan ere, negoziorako balio handia dago enpresek erregistratzen, prozesatzen eta biltegiratzen dituzten datu guztietan.

Funtsezkoa da, beraz, ikusi ditugun informazioaren segurtasun-printzipioak betetzea, gure eguneroko zereginak eten ditzakeen erasorik jasango ez dugula bermatzeko. Bestela, ondorio negatibo ugari egon daitezke, bai maila pertsonalean, bai enpresentzat. Egunero, informazioaren segurtasunarekin lotutako eraso eta arriskuei buruzko albiste ugari ikus ditzakegu. Hauek dira, ingurune korporatiboan, ondorio horien adibide batzuk:

- **Sinesgarritasuna galtzea** eta, beraz, erakundearen irudiari eta ospeari kaltea eragitea.
- Bezeroen, langileen, hornitzaileen eta merkataritza-bazkideen **datu konfidentzialak lapurtzea.**
- Europar Batasunean datu pertsonalen babesaren arloan indarrean dauden **legeak ez betetzea.**
- **Galera ekonomikoa,** ezin bada berreskuratu gure sistemetatik ateratako edo ezabatutako informazioa. Gainera, erasotzaileek diru-kopuru bat ordaintzeko eska dezakete, *ransomware* izeneko software gaiztoa erabiliz. Horrelako programak dira gaur egungo mehatxu nagusietako bat.
- **Ekoizpen-prozesuak geldiaraztea**, salmentak galtzea eta zerbitzuaren kalitatean eragina izatea.

Segurtasuna

A1 maila 4.1 Gailuen babesa

Segurtasunari buruzko informazio-iturriak

Segurtasunari buruzko informazio-iturriak

Segurtasun-maila handiagoa izateko eta aurre egin beharreko arriskuez jabetzeko, beharrezkoa da informatuta egotea. Askotan, prentsan edo sare sozialetan izaten dugu zibersegurtasunari buruzko albisteen berri. Dokumentazio honetan zibersegurtasunari buruzko zenbait informazio-iturri fidagarri daude.

Zibersegurtasunaren arloko organismo garrantzitsuak

Azken hamarkadetan, zibersegurtasunean espezializatutako organismoak sortu dira. Esparru horretan diharduten enpresak egon arren, beharrezkoa da, halaber, **ziberespazioa zaintzen, herritarrari informazioa ematen, enpresei aholkua ematen edo azpiegitura kritikoak babesten aritzen diren** erakunde publikoak izatea.

Organismo horiek ezagutzeak informazioa edo aholkularitza behar dugunean haiengana jotzeko aukera ematen digu, baita, aldi berean, herritar gisa baliagarriak izan dakizkigukeen zibersegurtasun-kontzeptu berriei buruz ikasteko aukera ere.

Estatu-eremua: Espainiako organismoak

Espainian hainbat organismo daude, hainbat funtziotan dihardutenak. Organismo nagusietako bat **Zentro Kriptologiko Nazionala (CCN)** (*ccn-cert.cni.es*)da, Espainiako Inteligentzia Zentro Nazionalaren (CNI) mendekoa. CCNren aurpegi publikoa zibersegurtasuneko gorabeherei eta larrialdiei erantzuteko ekipoa da: CCN-CERT. Bere webgunean bere lanari buruzko informazio asko aurki dezakegu: ziberespazio seguruagoa eta fidagarriagoa lortzea, eta informazio klasifikatua eta kaltebera babestea.

CCN-CERT zentroarekin batera, beste organismo garrantzitsu batzuk daude, hala nola **Azpiegituren Babeserako eta Zibersegurtasunerako Zentro Nazionala (CNPIC)** edo Defentsa Ministerioaren **Ziberespazioaren Agintaritza Bateratua (MCCE)**. Bestalde, Guardia Zibilaren **Delitu Telematikoen Taldea (GDT)**

edo Polizia Nazionalaren **Ikerketa Teknologikorako Brigada Nagusia (BCIT)** Estatuko segurtasun-erakundeetako unitate bereziak dira informatikarekin lotutako delinkuentzia ikertzeko eta jazartzeko.
Badira beste organismo batzuk ere, hala nola OSI edo INCIBE, jarraian sakon aztertuko ditugunak.

Erkidego-eremua: Europako organismoak

Azken urteotan, Europar Batasunak hainbat erregelamendu eta ekimen bultzatu ditu zibersegurtasunaren erkidego mailako egoera hobetzeko. Ildo horretan, Europako erakunde nagusia **European Union Agency for Cybersecurity (ENISA)** da. Erakunde horrek Batasuneko estatu kide guztiek zibersegurtasun-maila handia izatea zaintzen du.

ENISAz gain, ziberkrimen antolatuaren aurka borrokatzeko talde bat dago, **European Cybercrime Centre (EC3)** izenekoa. Organismo hori Europolek sortu zuen, eta Europar Batasuneko herritarrak, enpresak eta gobernuak online krimenetik babestea du helburu nagusi, horrelako mehatxuei eman beharreko erantzuna indartuz.

Nazioarteko eremua: beste herrialde batzuetako organismoak

Nazioartean, estatu bakoitzak zibersegurtasunaren arloko hainbat erakunde eta legeria ditu. Testuinguru horretan, bere garrantziagatik eta gaitasun operatiboengatik, ezagunenetako bat Ameriketako Estatu Batuetako **National Security Agency (NSA)** agentzia da. Inteligentzia-agentzia hori informazioa biltzen eta prozesatzen eta seinale-inteligentzian espezializatuta dago. Erlazionatutako beste agentzia bat **Cybersecurity & Infrastructure Security Agency (CISA)** da, zeinak baliabide ugari baititu ingelesez zibersegurtasunaz.

Informazio gehiago

CCN-CERTen webgunea: *ccn-cert.cni.es*
CNPICren webgunea: *cnpic.interior.gob.es/opencms* **MCCEren webgunea:** *e.digitall.org.es/emad* **GDTren webgunea:** *gdt.guardiacivil.es/webgdt*
BCITren webgunea: *e.digitall.org.es/bcit*
ENISAren webgunea: *enisa.europa.eu*
EC3ren webgunea: *e.digitall.org.es/EC3* **NSAren webgunea:** *nsa.gov* **CISAren webgunea:** *cisa.gov*

OSI: Internautaren Segurtasun Bulegoa

Internautaren Segurtasun Bulegoa (OSI) INCIBEren parte da, eta Interneten nabigatzean sor daitezkeen segurtasun-arazoak saihesteko eta konpontzeko behar diren informazioa eta euskarria ematen ditu. Helburu nagusia internautari eragin diezaioketen zibersegurtasun-arazoez kontzientziatzea eta horiek ikusaraztea da. Ematen digun informazioa oinarrizko ezagutza digitalak dituen herritarrari zuzenduta dago batez ere.

Bere webguneak mota guztietako informazio-baliabide ugari ditu: tresnak, gidak eta abar. Hona hemen herritarrentzako informazio erabilgarriaren adibide batzuk:

- **Eguneroko eguneraketak**: OSIk informazio eguneratua ematen du albisteei, zibersegurtasun-abisuei, blog-artikuluei eta abarri buruz. Atal horretako adibiderik argigarrienak "Benetako historiak" dira. Artikulu horietan, eraso edo mehatxu bat deskribatzen duten egoeren benetako adibideak aurki ditzakegu, baita guri gertatuz gero jarraitu beharreko jarraibideak ere. Adibidez, OSIk ***deepfake-mehatxuak*** azaltzen dizkigu, ***baita nola jokatu behar den ere gure kontuak bahitu badituzte*** (*incibe.es/ciudadanía*).
- **Kanpainak:** mota horretako argitalpenak hainbat gaitan banatzen dira: pasahitzak, gailu mugikorrak edo IoT-a, esaterako. Horietako bakoitzaren barruan, OSIk gai horri buruz dituen baliabideen zerrenda bat aurki dezakegu, hala nola infografiak, bideoak, benetako historiak eta abar. Horren adibide da "***Ingeniería social: que no te engañen*** " kanpaina (*incibe.es/ciudadanía/tematicas*).
- **Geure burua babesten ikasteko eskuliburuak:** OSIk hainbat eskuliburu argitaratzen ditu, babes-gomendioekin eta hainbat gairekin. Arazo zehatzei heltzeari, horiek ulertzeari eta horien aurrean babesteko hartu beharreko neurriei erreparatzen die. Hona hemen gai horietako batzuk: ***nola babestu zure Wi-Fi sarea*** edo ***nola zaindu zure pribatutasuna*** (*incibe.es/ciudadanía*).

Informazio gehiago

IoT Internet of Things-en siglak dira, eta euskaraz "Gauzen Internet" esan nahi du. Sentsoreak, softwarea eta beste teknologia batzuk dituzten objektu fisikoen sarea deskribatzen duen kontzeptua da (Internet bidez edo beste komunikazio-sare batzuen bidez beste gailu eta sistema batzuekin konektatzeko eta datuak trukatzeko).

e.digitall.org.es/iot

- **Baliabideak:** atal horretan hainbat baliabide daude, hala nola tailerrak, gidak, tresnak, zerbitzuak eta abar.
- **Jolas hezitzaileak:** bere webgunean, zibersegurtasunarekin lotutako kontzeptuak hobeto ulertzen laguntzen diguten jolasak ere topa ditzakegu, hala nola ***mahai-jokoak*** (*incibe.es/ciudadanía*), zuzenean deskarga daitezkeenak.

Aipatzekoa da OSIk eskaintzen dizkigun baliabideen artean ekimen partikular bat dagoela, txikienen kontzientziazioan eta babesean oinarritutakoa: **Internet Segura 4 Kids.** Ekimen horren helburua da adingabeei, irakasleei eta familiei zibersegurtasunaren arloko prestakuntza ematea.

Informazio gehiago

OSIren webgunea: *osi.es*
Internet Segura 4 Kids-en webgunea:*is4k.es*

INCIBE: Zibersegurtasunaren Institutu Nazionala

Zibersegurtasunaren Institutu Nazionala (INCIBE) zibersegurtasunean erabat diharduen gobernu-organismo bat da, eta herritarrak, enpresak, sare akademikoak edo ikerketa-sareak eta beste sektore estrategiko batzuk ditu ardatz.

Dagoeneko aipatu da OSI, herritar guztiei zuzendua. Enpresak ere material erabilgarriz hornitzeko, INCIBEk "Babestu zeure enpresa" ekimena dauka. Horren bidez, enpresak prestatu nahi dituzte, batez ere ETEak, eta baliabideak eskaini, hala nola ***enplegatuak entrenatzeko kontzientziazio-kit-a*** (*e.digitall.org.es/kit-incibe*). Gainera, institutuak zibersegurtasunaren sektorean ekintzailetza sustatzera bideratutako baliabideak ditu, hala nola “INCIBE Emprende” ekimena.

Informazio gehiago

INCIBEren webgunea: *incibe.es*
"Protege tu empresa" ekimena: *incibe.es/protege-tu-empresa*
"INCIBE Emprende" ekimena: *incibe.es/emprendimiento*

INCIBEk webgune interaktibo bat ere badu, ekintzaileak eta ETEak zibersegurtasunarekin lotutako kontzeptuetan sar daitezen. Horretarako, ikusleari haren prestakuntzan laguntzen dioten bi animazio-pertsonaia dituzte. Prestakuntza hori enpresa-sektore edo ibilbide desberdinetara egokituta dago.

ITINERARIOS DE CIBERSEGURIDAD INCIBE

itinarios.incibe.es

URRATS BAT HARATAGO: ZIBERSEGURTASUNAREN KUDEAKETA

Zibersegurtasuna enpresa txiki eta ertainetan nahiz enpresa handietan kudeatzen da. Bideo honetan, eragina eta arriskua bezalako kontzeptuak daude, enpresa baten mehatxuak kudeatzen laguntzen dutenak.

e.digitall.org.es/A4C41A2V02

CCN-CERT

Zentro Kriptologiko Nazionala (CCN-CERT) zibersegurtasunaz eta hari buruzko Espainiako legeriaz eguneratuta egoteko informazio-iturri nagusietakoa da. Organismo hori arduratzen da enpresa askok erabiltzen dituzten zibersegurtasun-tresnak garatzeaz. Zibersegurtasunari buruzko prestakuntza espezifiko eta teknikorako interesgarrienetako bat da ***Ángeles*** (*e.digitall.org.es/angeles*); enpresei bideratutako hainbat mailatako baliabide ugari duen tresna bat da, hala nola "ziberaholkuak" edo jardunbide egokiei buruzko txostenak.

CCNk aldizkako gida tekniko eta segurtasun-txosten ugari ditu, hala nola "Ciberamenazas y Tendencias" urteko txostena, urte bakoitzaren amaieran argitaratzen dena eta Espainiako zibersegurtasunaren egoera aztertzen duena.

Informazio gehiago

Zibersegurtasunaren Eskema Nazionalari (ENS) buruzko webgunea: *ens.ccn.cni.es/es*
CCN-CERTren txosten publikoen webgunea*e.digitall.org.es/informes-cert*
CCN-CERTren giden webgunea: *e.digitall.org.es/guias-cert*

ENISA

European Union Agency for Cybersecurity (ENISA) Europako organismo bat da, zibersegurtasunari buruzko ingelesezko baliabide ugari ematen dituena. CCN-CERTk bezala, Europako agentzia horrek aldizkako txostenak ditu, hala nola "Cyber Europe", urte amaieran argitaratzen dena eta Europako zibersegurtasun-joeren laburpena jasotzen duena.

Haren webgunea (***enisa.europa.eu***) oso erabilgarria da informazioa aurkitzeko, gaiaren arabera antolatutakoa.

DigitAll

Segurtasuna

4.2 DATU PERTSONALEN ETA PRIBATUTASUNAREN BABESA

Segurtasuna

A1 maila 4.2 Datu pertsonalen eta pribatutasunaren babesa

Datuen babesari buruzko herritarren eskubideak

Datu pertsonalen babesari buruzko herritarren eskubideak

Informazio-eskubidea

Espainiako Konstituzioak jasotzen dituen eskubideak hainbat kategoriatan sailkatzen dira, haien garrantziaren arabera. Garrantzitsuenak oinarrizko eskubideak dira. Datu pertsonalak babesteko eskubidea oinarrizko eskubidea da. Hortik aurrera, legegileak edukia ematen dio eskubide horri, hainbat bidetatik: betebeharrak ezartzen dizkie datu pertsonalak tratatzen edo manipulatzen dituzten subjektuei, eskubide zehatzagoak aitortzen dizkie herritarrei edo jarduteko aginduak ezartzen dizkie botere publikoei. Datu pertsonalak babesteko eskubidea hainbat eskubidetan banantzen da, eta dokumentu honek, hain zuzen, horiek garatzen ditu.

DATU PERTSONALEN BABESARI BURUZKO HERRITARREN ESKUBIDEAK (I)

e.digitall.org.es/A4C42A2V08

Lehena informazio-eskubidea da. Hori adierazteko moduak oso zabalak eta askotarikoak dira (adibidez, aurrerago landuko den informazioa eskuratzeko eskubidea informazio-eskubidearen zehaztapen gisa har daiteke).

Eskubide hori bermatzeko adierazpenetako bat tratamendu-arduradunari interesdunari informazio jakin bat emateko betebeharra ezartzea da. Araudiak informazio hori geruzen edo mailen arabera eman ahal izatea aurreikusi du:

- Lehen geruza, oinarrizko informazioa.
- Bigarren geruza, informazio zehatza.

Informazioaren edukia aldatu egiten da datu pertsonalak interesdunak zuzenean emandakoak badira (adibidez, datuak sartzen badira Facebooken edo YouTuben kontu bat irekitzeko) edo hirugarren batek emandakoak (adibidez, hotel-kate batek datu pertsonal jakin batzuk lagatzen badizkio bidaia-agentzia bati publizitate-kanpaina bat egiteko).

Datu pertsonalak interesdunak ematen dituenean eman beharreko informazioa

Lehen geruzan (oinarrizko informazioa), Datuak Babesteko Espainiako Agentziak honako informazio hau ematea gomendatzen du:

- Tratamendu-arduradunaren identitatea.
- Tratamenduaren helburuen deskribapen erraza, profilak egitea barne, halakorik balego.
- Tratamenduaren oinarri juridikoa.
- Datuak hirugarrenei laga ahal izatea aurreikusi ote den. Hirugarren herrialdeetarako transferentziak aurreikusi diren ala ez.
- Dokumentu honetan azaltzen diren eskubideak baliatzeko aukera.
- Helbide elektroniko bat edo beste bitarteko bat (adibidez, pdf dokumentu bat deskargatzea), gainerako informazioa erraz eta berehala eskuratu ahal izateko.

Bigarren geruzan (informazio zehatza), honako informazio hau txertatzea gomendatzen da:

- Arduradunarekin harremanetan jartzeko datuak. Ordezkariaren identitatea eta datuak (halakorik balego). Datuen babeseko ordezkariarekin harremanetan jartzeko datuak (halakorik balego).
- Tratamenduaren xedearen deskribapen luzeagoa. Datuak gordetzeko epeak edo irizpideak. Erabaki automatizatuak, profilak eta aplikatutako logika.
- Tratamenduaren oinarri juridikoaren xehetasuna, legezko betebeharraren, interes publikoaren edo interes legitimoaren kasuetan. Datuak emateko obligaziorik dagoen edo ez, eta ez egitearen ondorioak.
- Hartzaileak edo hartzaile-kategoriak. Egokitasunari buruzko erabakiak, bermeak, arau korporatibo lotesleak edo egoera espezifiko aplikagarriak.
- Nola baliatu datuetara sartzeko eta horiek zuzendu, ezabatu edo eramateko, eta tratamendua mugatzeko edo horri uko egiteko eskubideak. Emandako baimena ezeztatzeko eskubidea. Kontrol-agintaritzaren aurrean erreklamazioa aurkezteko eskubidea.

⚠ ADI

Datu pertsonalak interesdunek emandakoak badira, bilketa hori egin aurretik eman behar da informazioa.

Datu pertsonalak interesdunak ematen ez dituenean eman beharreko informazioa

Datu pertsonalak interesdunarengandik jaso ez direnean, **aurreko atalean adierazitako informazioaz gain**, honako hau eman behar da:

Lehen geruzan (oinarrizkoa):

- Datuen iturria; hau da, jatorria.

Bigarren geruzan (zehatza):

- Datuen jatorriari buruzko informazioa, sarbide publikoko iturrietatik atera badira ere. Sarbide publikoko iturriak dira, adibidez, egunkari eta aldizkari ofizialak, gizarte-komunikabideak, webguneak eta abar.
- Tratatzen diren datuen kategoria (adibidez, identifikazio-datu orokorrak, hala nola izena edo telefonoa; edo datu kalteberak, hala nola arraza-jatorria edo erlijio-iritziak).

ADI

Datu pertsonalak interesdunarengandik jasotzen ez direnean, tratamendu-arduradunak hilabeteko epean eman behar dio bilketa horren berri, eta, gehienez ere, interesdunari egindako lehen jakinarazpenean.

Informazio gehiago

29. artikuluko datuen babesari buruzko lantaldea. Gardentasunari buruzko gidalerroak (EB) 2016/679 Erregelamenduaren arabera (WP 260). *e.digitall.org.es/articulo29*

Sarbiderako eskubidea

Interesdunak eskubidea du tratamendu-arduradunak egiazta diezaion berari buruzko datu pertsonalak tratatzen ari diren ala ez.

Kasu horretan, arduradunak bi gauza eman behar ditu:

- Datu horien kopia bat edo datuetara urrunetik, zuzenean eta segurtasunez sartzeko sistema bat.
- Aurreko atalean azaldutakoarekin bat datorren informazioa (tratamenduaren xedeak, datu pertsonalen kategoriak, hartzaileak, kontserbazio-epea eta abar).

ADI

Datuetara sartzeko eskubidea baliatzeak aukera ematen dio interesdunari jakiteko enpresek zer dakiten berari buruz -hau da, zer datu pertsonal tratatzen dituzten- eta haien zilegitasuna eta zehaztasuna kontrolatzeko.

Eskubide horrek muga material eta formal batzuk ditu. Materialei dagokienez, bi dira:

- Ez du eragin negatiborik izan behar hirugarrenen eskubide eta askatasunetan (merkataritza-sekretuak edo jabetza intelektuala barne).
- Interes publiko jakin batzuk (Estatuaren segurtasuna, defentsa, segurtasun publikoa...).

Muga formalari dagokionez, arduradunak ukituari buruzko datu asko tratatzen dituenean eta ukituak datuetara sartzeko duen eskubidea baliatzen duenean, baina ez duenean zehazten datu guztiez edo horietako batzuez ari den, arduradunak eskatu ahal izango dio zehaztu dezala zer tratamendu-datu edo -jarduerari buruz ari den.

Informazio gehiago

Datuak Babesteko Europako Batzordea. 1/2022 Jarraibideak, sarbide-eskubideari buruzkoak.*e.digitall.org.es / directrices*

Zuzentzeko eskubidea

ADI

Datuak zuzentzeko eskubidea datu okerrak edo osatugabeak tratatzen ari direnean erabil daiteke.

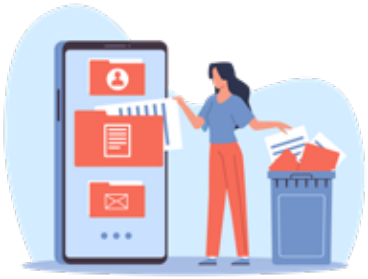
Datuak zuzentzeko eskubideak bi adierazpen ditu:

- Eskubide horren bidez, interesdunak eskubidea du tratamendu-arduradunak zuzen diezazkion, justifikaziorik gabeko luzamendurik gabe, berari buruzko datu okerrak. Interesdunak argi adierazi behar du eskaeran zer daturi buruz ari den eta zer zuzenketa egin behar den.
- Bestalde, tratamenduaren xedeak kontuan hartuta, osatu gabeko datu pertsonalak osatzeko eskubidea. Horrek esan nahi du interesdunak ematen duen informazioa tratamenduaren xedeetara egokitzen bada eta arduradunak tratatzen dituen datuak osatzen baditu, arduradunak onartu eta bere tratamenduan sartu beharko duela (adibidez, kreditu-kaudimenari buruzko datuak).

Beharrezkoa izanez gero, interesdunak, eskabidearekin batera, tratatu beharreko datuak zehatzak ez direla edo osatu gabe daudela egiaztatzen duten agiriak aurkeztu beharko ditu.

Nolanahi ere, arduradunak datuak zehatzak direla bermatu behar du; hau da, ofizioz ere egin behar du, inolako eskaerarik egin gabe.

Datuak ezabatzeko eta ahaztuak izateko eskubidea



Datuak ezabatzeko eskubideak esan nahi du interesdunak eskubidea duela tratamendu-arduradunak, justifikaziorik gabeko luzamendurik gabe, berari buruzko datu pertsonalak ezaba diezazkion. Tratatzen diren datu guztiekin edo horietakoren batekin bakarrik erabil daiteke.

Ezabaketa derrigorrezkoa da kasu hauetakoren batzuk gertatzen badira:

1 | Datu pertsonalak jada beharrezkoak ez badira bilketaren edo tratamenduaren xedeetarako.
2 | Interesdunak tratamenduaren oinarri den baimena erretiratzen badu, eta tratamenduak beste oinarri juridikorik ez badu.
3 | Interesdunak tratamenduaren aurka egiten badu eta tratamendu horretarako beste arrazoi legitimorik ez badago.
4 | Datu pertsonalak legez kontra tratatu badira.
5 | Datu pertsonalak legezko betebehar bat betetzeko ezabatu behar badira.
6 | Datu pertsonalak informazio-gizartearen haurrei buruzko zerbitzu-eskaintzaren inguruan lortu badira.

⚠ ADI

Arduradunak datu pertsonalak publiko egin baditu eta horiek ezabatzera behartuta badago, arrazoizko neurriak hartuko ditu datu pertsonal horiek tratatzen ari diren beste arduradun batzuei jakinarazteko, haiek ere ezaba ditzaten datu horiek. Hori da **ahaztua izateko eskubidea**.

Ezabatzeko eskubidea publiko egin diren datuen gainean baliatzen bada, ahaztua izateko eskubideaz hitz egiten da. Beraz, ahaztua izateko eskubidea datu pertsonalak argitaratu dituen arduradunaren aurrean baino ez da eskatu behar, eta ez da datuen komunikazio hutsaren kasuetara iristen, hau da, datu horiek pertsona edo entitate bereziei eman zaizkienean.

OHARRA

Auzitegi Gorenak adierazi du ezin dela ezabatze-eskubidea egikaritu bataio-liburuko datuen gainean.

OHARRA

2014tik 2020ra, Googlek 4 milioi esteka baino gehiago kentzeko eskaerak jaso zituen. Espainian, onartutako eskaeren ehunekoa % 40 ingurukoa da.

Nolanahi ere, ezabatzeko eskubidea ez da absolutua, eta araudiak jasotzen duenez, baldintza jakin batzuekin bada ere, kasu batzuetan ez da egokia. Nagusiak:

1 | Adierazpen- eta informazio-askatasunerako eskubidea baliatzeko (adibidez, prentsa digitalean argitaratutako albisteak).
2 | Datuen tratamendua eskatzen duen eta tratamendu-arduradunari aplikatzen zaion legezko betebehar bat betetzeko, edo interes publikoaren izenean edo arduradunari emandako botere publikoen izenean egin beharreko eginkizun bat betetzeko (adibidez, ikerketa polizial edo penalei buruzko zenbait datu).
3 | Osasun publikoaren arloko interes publikoko arrazoiengatik.
4 | Interes publikoaren izenean artxibatzeko, ikerketa zientifiko edo historikorako, edo estatistika-xedeetarako.
5 | Erreklamazioak formulatzeko, egikaritzeko edo aldezteko.

Informazio gehiago

Datuak Babesteko Europako Batzordea. 5/2019 Jarraibideak, ahazteko eskubidearen irizpideei buruzkoak, DBEOren araberako bilaketa-motorren kasuan. *e.digitall.org.es /directrices*

Tratamendua mugatzeko eskubidea

DATU PERTSONAREN BABESARI BURUZKO HERRITARREN ESKUBIDEAK (II)

e.digitall.org.es/A4C42B1V08

Horrek esan nahi du interesdunak eskubidea duela gordetako datu pertsonalak arduradunak marka diezazkion, behin-behineko tratamendua mugatzeko asmoz, kasu hauetakoren bat gertatzen bada:

- Interesdunak datuen zehaztasuna aurkaratzen badu, arduradunak egiaztatzen duen bitartean.

- Tratamendua legez kontrakoa bada eta interesduna bere datuak ezabatzearen aurka badago eta, horren ordez, erabilera mugatzeko eskatzen badu. Kasu horretan, arduradunak egindako arau-haustea egiaztatzeko frogak suntsitzea saihestu nahi da funtsean.
- Arduradunak datuak behar ez baditu tratamenduaren xedeetarako, baina interesdunak behar baditu erreklamazioak egikaritu edo aldezteko.
- Interesdunak tratamenduaren aurka egin badu, tratamendua jarraitzeko arduradunak emandako arrazoi legitimoak interesdunaren arrazoien gainetik dauden egiaztatzen den bitartean.

Muga horrek irauten duen bitartean, tasatutako arrazoi batzuengatik bakarrik tratatu ahal izango dira datuak, datuen kontserbazioa salbu: interesdunaren onespena, erreklamazioak egitea, beste pertsona baten eskubideak babestea eta interes publikoko arrazoiak.

Azaldu berri dugun bezala, muga hori interesdunaren eskubide gisa arautzen da, eta ez tratamenduaren arduradunaren betebehar gisa. Hau da, tratamendu-arduradunak ez du tratamendua ofizioz mugatzeko betebeharrik, azaldutako kasuetakoren batzuk gertatzen badira; aitzitik, hori gertatzeko, interesdunak berariaz baliatu beharko du eskubide hori.

ADI

Tratamendua behin-behinean mugatuko da, kasu jakin batzuk gertatzen edo egiaztatzen diren bitartean.

Datuen eramangarritasun-eskubidea

Interesdunak eskubidea du berari buruzko datu pertsonalak, tratamendu-arduradun bati emandakoak, erabilera komuneko eta irakurketa mekanikoko formatu egituratu batean jasotzeko, bai eta beste tratamendu-arduradun bati transmititzeko ere, hasierako arduradunak, zeinari eman zizkion datuak, hori eragotzi gabe.

Interesdunak emandako datuen gainean baliatu ahal izango da eskubide hori. Horiek ez dira soilik interesdunak kontzienteki eta aktiboki eman zituenak (adibidez, formulario baten bidez); erabiltzaileak zerbitzu edo gailu jakin baten erabileran egindako jardueratik lortutakoak ere sartzen dira kontzeptu horretan, nahiz eta horiek ez diren benetan aktiboki entregatzen (adibidez, entrenamenduko app batean erregistratutako erabiltzaile baten jarduera fisikoaren historiala). Kanpoan geratzen dira tratamendu-arduradunak sortutako datuak (adibidez, app horrek datu horietatik abiatuta sortzen dituen puntuazioak edo estatistikak).
Eskubide horrek bi baldintza bete behar ditu:

1 | Tratamendua onespenean edo kontratu batean oinarrituta egotea. Tratamenduaren zilegitasun-arrazoiak beste batzuk badira (adibidez, legezko betebehar bat), datuak ezin izango dira eskubide horren xede izan.
2 | Tratamendua bitarteko automatizatuen bidez egitea.

Eskubide hori baliatuta, interesdunak eskubidea izango du datu pertsonalak zuzenean arduradunez arduradun transmititzeko, teknikoki posible denean. Adibidez, pertsona batek banku-entitate batean helbideratutako ordainagirien datuak beste banku-entitate batera eramatea.

Begi-bistakoak dira eskubide hori baliatzeak ekar ditzakeen inplikazio eta zailtasun praktiko eta teknikoak. Pentsa dezagun mota guztietako eta formatu desberdinetako zenbat datu pertsonal mugitzen diren sare sozial, blog, *cloud computing* zerbitzu, posta elektronikoko zerbitzu eta abarretan. Zerbitzu horien guztien esku uzten da datu pertsonalak biltegiratzea eta tratamendu masiboa ematea. Helburua da mekanismo juridikoak ezartzea -zailtasun teknikoak argudiatuta- interesdunak betiko gera ez daitezen, digitalki, hornitzaile jakin baten gatibu. Gainera, horrek eragin onuragarria du lehiaren sustapenean.

Hori dela eta, arau eta formatu komun elkarreragingarrien multzo bat egin behar da, datuen eramangarritasun-eskubidearen eskakizunei erantzuteko. Hala ere, bide izugarri luzea dago egiteke.

Eskubide horren eta sarbide-eskubidearen arteko aldeari dagokionez, eramangarritasunak interesdunari bermatzen dio beste subjektu batek erraz prozesa lezakeen informazioaren kopia bat lortzea; sarbidea, aldiz, informazioa bera bermatzera mugatzen da. Alde horrek ondorioak ditu, halaber, eskubidea baliatzeko eskaera betetzeko moduan. Sarbide-eskubideari dagokionez, datuak irakurtzeko formatu irisgarrian eman behar zaizkio interesdunari, informazioa ezagutu eta ulertu ahal izateko. Eramangarritasun-eskubideari dagokionez, datuak emateko formatua ulertezina izan daiteke gizakiarentzat, baina ez, ordea, informatizatutako tratamendurako. Halaber, bi eskubideen artean desberdintasunen bat ezar daiteke irismenari dagokionez. Adibidez, subjektu batek bere historia klinikoa ospitale pribatu batean ikusteko eskubidea du. Horrek proba medikoak eta diagnostikoa barne hartzen ditu. Baina interesdunak beste ospitale pribatu batera eramatea eskatzen badu, proben emaitza gordinetara muga daiteke eramangarritasuna (datuak, alegia), diagnostiko medikoak sartu gabe, arduradunak sortutako informazioa baitira horiek.

ADI

Eramangarritasun-eskubideak esan nahi du erabiltzaile baten datu pertsonalak zuzenean entitate edo enpresa batetik beste batera transmititu ahal izatea, erabiltzaileari berari eman beharrik gabe, betiere teknikoki posible bada.

Informazio gehiago

Datuak babesteko Europako Agintaritzen Taldea. Datuak transferitzeko eskubideari buruzko gidalerroak (WP 242). *e.digitall.org.es/wp-242*

OHARRA

Banku-araudiak kontuen eramangarritasuna ahalbidetzen du, zerbitzu eta datu pertsonal guztiak banku batetik bestera migratuz, hala nola aldizkako transferentziak edo helbideratzeak.

Aurka egiteko eskubidea

Aurka egiteko eskubideak bere datu pertsonalen tratamendua eragozteko ahalmena ematen dio interesdunari. Bi kasu daude:

- Tratamenduaren xedea zuzeneko marketina (publizitatea) edo marketinarekin lotutako profilak egitea bada, interesdunak aurka egin ahal izango du inolako justifikaziorik gabe, eta arduradunak nahitaez onartu beharko du.
- Tratamenduaren oinarria interes publikoa, botere publikoen erabilera edo arduradunaren edo hirugarren baten interes legitimoa bada, aurkakotasun hori arrazoitu beharko du, bere egoera partikularraren arabera.

Adibidez, unibertsitate publiko batek, interes publikoaren izenean egindako bere misioa oinarri hartuta, ikasleak *online* irakaskuntzan kamerak piztera behartzea. Hala ere, ikasle batek, bere inguruabar pertsonal eta familiar bereziak direla-eta (familiako beste kide batzuk dauden lekuetan bakarrik konekta daiteke), tratamendu horri aurka egiteko eskubidea balia dezake.

Bigarren kasu horretan, arduradunak datuak tratatzen jarrai dezake, baldin eta egiaztatzen badu arrazoi legitimoak daudela interesdunarenen gainetik. Adibidez, Unibertsitateak aurreko neurria ezar lezake azterketa bat egiterakoan ikaslearen nortasuna egiaztatzeko.

Nolanahi ere, arduradunak interesdunari erantzun behar dio, aurka egiteko eskaera ukatzeko arrazoiak adieraziz.

ADI

Aurka egiteko eskubidea ezin da baliatu administrazio publikoek (Ogasuna, polizia, Gizarte Segurantza eta abar) egiten dituzten datu-tratamendu askoren gainean.

Informazio gehiago

Datuak Babesteko Espainiako Agentzia. Ezagutu zure eskubideak.
e.digitall.org.es/conoce-tus-derechos

DigitAll

Segurtasuna

4.3 OSASUNAREN ETA ONGIZATEAREN BABESA

Segurtasuna

A1 maila 4.3 Osasunaren eta ongizatearen babesa

Osasun digitalaren printzipioak

Osasun digitalaren printzipioak

Dokumentu honetan osasun digitalaren kontzeptua, e-osasuna eta horien arteko desberdintasunak eta antzekotasunak jorratuko dira. Teknologiak osasunari eta ongizateari ekar diezazkiekeen onurak ezagunak badira ere, osasun digitalarekin lotutako arrisku eta mehatxuen arteko desberdintasun nagusiak identifikatuko dira -oinarrizko mailan-, maila psikologikoan, fisikoan eta/edo sozialean.

Osasun digitalaren kontzepturako sarrera

Osasunarekin eta mundu digitalarekin lotutako gaietan, ebidentzia gutxi dago soluzio digitalek pertsonen osasunean eta ongizatean dituzten onurei eta kalteei buruz. Hala ere, dokumentu honetan teknologiak gure osasunean izan ditzakeen ondorioak identifikatzen saiatuko gara.

Osasun digitala informazioaren eta komunikazioaren teknologiek (IKT) pertsonen osasunean eta ongizatean duten eragin positiboa edo negatiboa (ordenagailu eramangarrietatik edo adimen artifizialetik gailu jargarrietara) atzemateko sortutako kontzeptua da. Osasunaren Mundu Erakundearen (OME) arabera, 2012. urtean "osasun digitala" terminoa kontzeptualizatu egin da, osasuna eta horrekin lotutako beste arlo batzuk hobetzeko teknologia-erabilera barne hartzen duena. OMEren arabera, osasun digitalak kontsumitzaile digitaletatik robotikaraino barne hartzen du, adimendun gailuak eta konektatutakoak kontuan hartzen ditu, eta osasunerako teknologia-erabilera desberdinak barne hartzen ditu, hala nola Gauzen Internet, ikaskuntza automatikoa, adimen artifiziala, informatika aurreratua eta datu-bolumen handien analisia.

Osasun digitalak, osasunean hainbat tresna teknologiko aplikatzeaz gain, aldaketa dakar osasun- eta arreta-praktikan. Horregatik, teknologia erabiliz, osasun-laguntza hobea sustatzea eta bultzatzea du helburu. Hala, esan dezakegu kontzeptu horrek osasun-sistemen eraldaketa digitala ekarri duela, eta lege-, administrazio- eta finantza-mailako erreformak eragin dituela.

OHARRA

Osasun digitala: IKTen erabilerak osasunean eta ongizatean duen eragina barne hartzen duen kontzeptua.

Osasunaren digitalizazioari esker, gaixotasunak prebenitu ahal izango ditugu, baita fase goiztiarretan detektatu ere, arreta eraginkorragoa eta kalitate handiagokoa izan ahal izango dugu, osasun-arretaren kostuak murriztu ahal izango ditugu eta pertsonen osasunaren jarraipen pertsonalizatua egin ahal izango dugu, bai familia-medikuaren bidez, bai osasunaren autokudeaketaren bidez.

Europako Batzordeak espero du osasun digitalak pertsonek beren osasunaren kudeaketan parte hartzea sustatzea, bizi-estiloa eta prebentzioa azpimarratuz, eta osasun-sistemako eta gizarte-laguntzako eragileak eta sektoreak konektatuz, larrialdi-egoerak, epidemiak eta prozedurak hobetzeko eta, batez ere, gaur egungo osasun-arretaren gabeziak murrizteko.

Ildo horretan, gutxi gorabehera 1999tik, bada osasun digitalarekin lotutako termino bat, nahasmendua sortu duena eta sinonimo gisa oker erabili dena; “e-osasuna” edo “e-health” kontzeptuaz ari gara.

e-osasuna osasun digitalaren barruko adar gisa definitu da. IKTak barne hartzen ditu, osasun-ingurunean prebentzioaren, diagnostikoaren, tratamenduaren eta jarraipenaren arloetan erabilitako tresna gisa (baita osasunaren kudeaketan ere): osasun-sistemari kostuak aurrezten dizkiote eta sistema horren eraginkortasuna hobetzen dute. Bien arteko alde nagusia da e-osasunaren ekimenak ez direla pazientearengandik sortzen, osasun digitalean gertatzen den bezala. Gainera, e-osasunaren barruko kategoriak erlazionatuago daude osasun-datuen tratamendu informatikoarekin, eta honako tresna hauek sartzen dira termino horretan:

- Erregistro mediko elektronikoa edo klinika elektronikoaren historiala.
- Teleosasuna (telemedikuntza barne).
- Urrutiko ikaskuntza edo prestakuntza digitala, “e-Learning” ere esaten zaiona.
- Informazioaren eta komunikazioaren teknologien arloko etengabeko hezkuntza.

⚠ ADI

e-osasuna eta osasun digitala ez dira sinonimoak; lehenengoa bigarrenaren barruko adar bat da.

Dena dela, teknologiak ekar diezazkigukeen onura guztiak gorabehera, eragin negatiboa ere izan dezake osasunean eta ongizatean, zuzenean edo zeharka, eguneroko erabileran. Teknologiaren erabilerak eragin ditzakeen arrisku eta mehatxuen artean, mendekotasun digitalaren eta ziberjazarpenaren kontzeptuak ditugu. Hala ere, e-osasunarekin eta datuen tratamenduarekin lotutako beste mehatxu digital batzuk ere landuko dira.

e-osasunarekin lotutako mehatxu digitalak

IKTen bilakaera azkarrak aldaketa batzuk eragin ditu, eta horietara egokitu behar da osasun-sistema. Horietako bat erabiltzaileen pribatutasuna da, informazio horren tratamendua oso alderdi kaltebera baita. Horregatik, gobernuek eta osasunarekin eta segurtasunarekin lotutako entitate publikoek gero eta gehiago egiten dute biztanleen datuak modu seguruagoan biltzeko. Ildo horretan, teknologia berriak erabili eta datuak hodeian biltegiratzea osasun digitalaren hobekuntza bat da; izan ere, osasun parte-hartzailea ahalbidetzen eta sustatzen du herritarren artean, haien osasunari buruzko datuak bistaratuz eta partekatuz, eta arreta eta kudeaketa sanitarioa erraztuz.

Informazio gehiago

Aintzat hartutako mehatxu nagusiak mendekotasun digitalari eta ziberjazarpenari buruzkoak dira.

ADI

Erabiltzaileen osasun-datuei buruzko pribatutasuna oso gai kaltebera da, eta tratatu egin behar da.

Ingurune fisikoarekin elkarreragiten duten eta urrunetik monitorizatu eta kontrola daitezkeen teknologiak txertatzeak (intsulina-adabaki "adimendunak", haririk gabeko sareen bidez programagarriak diren taupada-markagailuak, desgaitasun fisikoak konpentsatzeko protesiak eta abar) osasunaren posizioa ekarri du, pertsonen bizitzari eragiteko aukera askoz ere arrisku kezkagarriagotzat jo du eta. Izan ere, berriki gertatutako adibide batzuek hori erakutsi dute, hala nola taupada-markagailuen eta intsulina-ponpen hackeoak.

OHARRA

Aurrerapen horiek ere erronka dira segurtasunerako; izan ere, sistema horiek hackeoen edo ihesen borrokari aurre egin behar diote, pertsona baten osasun-egoerari buruzko informazio pertsonala publikoa izatea eragin baitezakete. Horregatik, Estatuan eta Europan, informazio pertsonala babesteko legeak lantzen ari dira. Hala, osasun digitalak Datuak Babesteko Europako Erregelamenduaren eta Datuak Babesteko eta Eskubide Digitalak Bermatzeko Legearen mende egon behar du, zeintzuek eragiten baitiete informazio hori guztia erabiltzen duten osasun-profesionalei, ospitaleei, klinikei eta zentro medikoei. Araudi hori lotuta dago datu medikoen konfidentzialtasunarekin, datuen kalitatea hobetzearekin, pazientearen baimena une oro erabiltzearekin eta pazienteari bere diagnostikoaren eta tratamenduaren berri ematearekin.

Testuinguru teknologiko berriaren konplexutasunaren ondorioz, prozesu digital berrien bizi-zikloan parte hartzen duten aktoreen kopurua hain da handia, ezen haietako batzuk ez baitira jabetu ere egiten prozesu horietan duten eraginaz eta elkarreraginaz, eta, beraz, ez dira segurtasun-kontrol nahikoak sartzen ari beren funtzioetan, ez eta ematen dituzten teknologietan ere.

Gauzen Interneteko teknologietan dauden gabeziei gehitu behar zaie telelaguntzako edo pertsonen urruneko monitorizazioko zerbitzu berri batzuek kontsumitzaileen/bezeroen telefono mugikor partikularrak informazio-iturri gisa erabiltzea aurreikusten dutela (biometriak, geoposizionamendua, alertak sortzea eta abar), zehaztasun-gailu espezializatu eta fidagarriak ote diren behar bezala kontuan hartu gabe.

Informazio gehiago

Gauzen Internetek barne hartzen dituen teknologien artean telelaguntza edo pertsonen osasunaren urruneko monitorizazioa daude.

Gainera, aurreko konplexutasun eta gabeziei zerbitzu horiek ematen dituzten eraikinen gabeziak ere gehitu behar zaizkie, izan teknologia medikoa eraikitzen duten fabrikak, sendagaiak ekoizten dituzten farmazeutikoak, osasun-arretako zentroak edo, oro har, medikuntza- eta osasun-zerbitzuekin lotutako beste edozein instalazio mota. Instalazio horietako askok Internetera konektatutako teknologia adimendunak txertatu dituzte beren baliabideak optimizatzeko (berokuntza, argiztapena, sarbideen kontrola, igogailuak, bideozaintza, prebentzioko mantentze-lanak eta abar), eta teknologia horiek, era berean, urrutitik ustia daitezkeen ahuleziak izan ditzakete. Kalteberatasun horiek, eraikinaren funtzionamenduari eragiteaz gain, sarbidea erraztu diezaiekete baimendu gabeko pertsonei, eta horrek bertan gauzatzen diren prozesuak alda ditzake eta eragina izan dezake azken kontsumitzaileen osasunean.

Teknologiaren arriskuak eta mehatxuak osasun digitalean

Arriskuak eta mehatxuak maila fisikoan

Teknologia modu desegokian erabiltzeak eragin handia izan dezake gure osasun fisikoan. Eragin hori, batez ere, gehiegizko erabileragatik edo jarrera desegokiagatik gertatzen da. Egoera hori lan-inguruneetan, gure etxean edo aisialdi-guneetan gerta daiteke. Hona hemen izan ditzakegun arazoetako zenbait:

- **Kaltea ikusmenean:** oso denbora luzez pantailak erabiltzeak arazoak sor ditzake begietan, hala nola, erremina, malko-jarioa edo gorritasuna. Hori, neurri handi batean, pantaila osatzen duten LEDen argi urdinaren ondorio izaten da, haren esposizioak erretinari eragiten baitio. Nabarmendu beharreko beste arazo nagusietako bat begietako nekea da, begiak kliskatzeko maiztasuna murriztearen ondorioz. Era berean, ikusmenarekin lotutako arazo horiek buruko mina eragin dezakete.
- **Bizkarra eta zerbikalak:** gailu teknologikoak luzaroan erabiltzeak sorbaldak aurrerantz okertuta izatea eragiten du, baita zerbikalak denbora luzez tentsioan mantentzea ere, eta horrek kontrakturak eragin ditzake.

OHARRA

Gainera, eraikinak bezalako azpiegiturak ez dira prest egoten aurrerapen teknologikoetarako, dela konektibitateagatik, dela Wi-Fi, Bluetooth edo beste alternatiba batzuengatik.

ADI

Gailu teknologikoak modu desegokian erabiltzeak hainbat arrisku eta mehatxu eragin ditzake, maila fisikoan, sozialean eta psikologikoan.

- **Karpo-tunelaren sindromea:** teklatua eta sagua luzaroan erabiltzeak sindrome hori eragin dezake. Besaurretik eskualdera doan nerbioa karpo-tuneletik igarotzen denean konprimitzen denean gertatzen da. Esku-ahurraren azpian dagoen lokailu-eremua da karpo-tunela. Afekzio horrek, besteak beste, kaltetutako eskumuturra inurritzea, sorgortzea edo indarra eta mugikortasuna galtzea eragiten du.

Aurreko arazoek zuzenean eragiten diete gure gorputzaren hainbat atalei, baina kontuan izan behar dugu teknologia gehiegi erabiltzeak **bizimodu sedentarioa** ere eragin dezakeela. Horrek arriskua ekar diezaioke gure osasunari, oro har, eta hainbat gaixotasun eragin ditzake, hala nola **obesitatea**, **bihotzeko arazoak** edo **kolesterol handia**.

Arriskuak eta mehatxuak maila sozialean

Gizartean teknologia berriak erabiltzea positiboa izan daiteke, betiere eguneroko bizimoduko jarduerak alde batera uzten ez badira, hala nola ikastea, kirola egitea, lagunekin ateratzea eta familian egotea, besteak beste. Neurrigabe eta kontrolik gabe erabiltzen bada, zenbait arrisku sor daitezke:

- **Isolamendu soziala:** sare sozialekiko, bideojokoekiko edo hainbat aplikazioekiko mendekotasunak erabiltzailea mundutik isolatzea eragin dezake; horrek eragina izango du lagun, senide, ikaskide eta abarrekiko harremanetan. Nerabeen kasuan, eragin negatiboa izan dezake haien gizarte-trebetasunen garapenean. Adibidez, kontaktu fisikoa galtzea edo emozioak eta keinuak hautemateko zailtasuna.
- **Mundu errealarekiko erlaziorik eza:** IKTak neurriz kanpo erabiltzeak gizabanakoa bizi den mundutik erabat baztertzera eraman dezake, ingurunearekiko erabateko deskonexioa sortuz. Kasu askotan, hautematen duten errealitatearen zatirik handiena bat dator errealitate digitalarekin.

ADI

Teknologia berriak neurriz kanpo erabiltzeak hainbat gizarte-arrisku eragin ditzake, hala nola gizarte-isolamendua edo mundu errealarekiko erlaziorik eza.

Arriskuak eta mehatxuak maila psikologikoan

Teknologiak maila psikologikoan ere eragin handia du herritarrengan. Teknologiatik eratorritako arrisku eta nahasmendu psikologikoak ohikoagoak dira nerabeen artean. Arriskuen eta mehatxuen artean, honako hauek nabarmentzen dira:

- **Nomofobia:** gizartean gero eta ohikoagoa den arazoa da. Gailu mugikorrik gabe egoteko beldur irrazionala da, pertsona askok beren gailuarekiko erabateko mendekotasuna baitute. Egoera horrek buruko edo urdaileko mina, antsietatea eta estresa eragin ditzake, eta, kasu larriagoetan, nahasmendu mentalak ere bai, hala nola nahasmendu obsesiboak.
- **Alegiazko deiaren sindromea:** telefonoa bibratzen eta jotzen ari deneko sentsazioari egiten dio erreferentzia arazo horrek, nahiz eta hala ez izan, eta gailua begiratu beharra eragiten du. Arazo horren arrazoia da garunak jasotzen duen edozein bulkada mugikorrarekin erlazionatzen duela.
- **Internetekiko mendekotasuna:** sare informatiko horri ematen zaion etengabeko erabilerak eragiten du mendekotasun hori, eskaintzen digun edukiarengatik eta eduki horrek gure smartphonea, sare sozialak, txatak, kontaktu-orriak eta abar erabiltzera eramaten gaituelako. Mendekotasun horrek antsietate-, estres-, jokabide- edo isolamendu-arazoak eragin ditzake.
- **Segurtasunik ezeko arazoak:** sare sozialak erabiltzeko gailu mugikorrak maiz erabiltzeak pertsonak beste pertsona batzuekin konparatzen hastea eragin dezake, edo plataforma horien bidez bizitza ideal bat irudikatu nahi izatea; horrek kritikak eragin ditzake, bai eta sare sozialetatik feedback bat lortu beharra ere, hala nola "atsegin dut" motakoak. Faktore horiek guztiek kalte psikologikoak eragin diezazkiekete pertsonei, hala nola ezinegona, antsietatea, depresioa edo elikadura-nahasmenduak.

- **Teknoestresa:** teknologia erabiltzeak herritarrengan eragin dezakeen beste arrisku bat teknoestresa da. Arazo hori teknologiarekin modu osasungarrian jarduteko trebetasunik eza da. Horrek antsietate- eta frustrazio-maila handiak eragin diezazkioke pertsonari, baita teknologiarekiko jarrera negatiboak garatzea ere. Pertsona batzuek gailu horiekiko nolabaiteko beldurra izan dezakete, teknologiaz hitz egiteko eta horretan pentsatzeko erresistentzia ere izan dezakete, eta IKTen munduaren kontrako pentsamendu oldarkorrak izan ditzakete.

⚠ ADI

Mendekotasuna, nomofobia edo deiaren sindromea dira teknologiaren gehiegizko erabilerak eragindako arrisku psikologikoetako batzuk.

Osasunaren arloko profesionalek teknologiaren beste arrisku batzuk ere aipatu dituzte, pertsona baten eguneroko bizitzan eragina izan dezaketenak: lo-arazoak, norberaren buruarekin gustura sentitzeko IKTen beharra, kontzentraziorik eza, komunikazio-arazoak edo erabilera-denbora kontrolik gabe handitzea, esaterako.

Informazio gehiago

Activa Printzipioa. Zer dira osasun digitala eta e-osasuna? *principioactiva.com*
Osasun Digitala. Carlos Slim Fundazioa. *saluddigital.com*

DigitAll

Segurtasuna

4.4 INGURUMENAREN BABESA

Segurtasuna

A1 maila 4.4 Ingurumenaren babesa

Teknologiaren kontsumo jasangarria

Teknologiaren kontsumo jasangarria

Sarrera: teknologia digitalaren energia-kontsumoa

Gailu teknologikoen fabrikazioari eta erabilerari lotutako materialen eta energiaren kontsumoa etengabe hazten ari da mundu osoan, baita COVID-19aren pandemiaren ondoren ere.

Serieko 2. bideoan ("***Behar ditugu ekoizten ditugun baliabide teknologikoak?***"), ikusi genuen bezala, datu batzuk sendoak dira fenomenoa ilustratzeko orduan. Telefonia mugikorraren sektorearen interesak ordezkatzen dituen *GSMA Intelligence* plataformaren txostenen arabera, 2017az geroztik, erabiltzen diren gailu mugikorren kopurua altuagoa da, planetan, pertsonena baino. Une hartan, GSMAren arabera, ia 8.092 milioi konexio mugikor zeuden; mundu osoko biztanleria, berriz, 7.373 milioikoa zen, guztira (GSMA, 2017). Azken txostenean, gainera, gutxienez gailu mugikor bat duten pertsonen datuak gehitu dituzte, eta datu horiek erakusten dute 2021. urtearen amaieran 5.300 milioi pertsona egongo zirela abonatuta zerbitzu mugikorretan; hau da, munduko biztanleriaren % 67 (GSMA, 2022).

BEHAR DITUGU EKOIZTEN DITUGUN BALIABIDE TEKNOLOGIKOAK?

e.digitall.org.es/A4C44A1V02

ADI

Telefonia mugikorraren sektorearen interesak ordezkatzen dituen *GSMA Intelligence* plataformaren txostenen arabera, 2017az geroztik, erabiltzen diren gailu mugikorren kopurua altuagoa da, planetan, pertsonena baino.

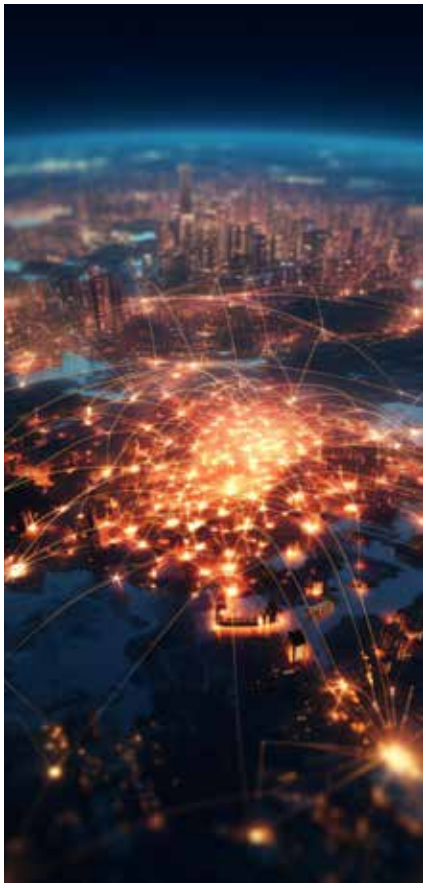
Txosten berean zehazten denez, munduko biztanleriaren % 95 banda zabal mugikorreko sare batez estalita egonik, erronka nagusia erabilera-arrakalari heltzea da; hau da, oraindik ere Internet erabiltzen ez duen banda zabal mugikorreko sare batek estalitako munduko biztanleriaren % 40. Beraz, oso litekeena da konexio eta gailu mugikorren erabilerari buruzko datu horiek epe laburrean handitzea.

Hain zuzen ere, Interneten erabileraren hazkunde hori datu benetan deigarrien bidez ere adieraz daiteke. Greenpeace-ren *Clicking Clean* txostenaren arabera (2017), informazioaren teknologien sektorearen aztarna energetikoa munduko

elektrizitatearen % 7 inguru kontsumitzearen parekoa dela kalkulatzen da, eta hazten jarraitzen du. Datu horretatik harago, txostenak berak zehazten du Internetek energia-eskariaren lau arlo nagusi sortzen dituela: datu-zentroak, komunikazio-sareak, erabiltzaileen gailuak eta aurreko hiruretarako beharrezkoak diren ekipoak fabrikatzeko energia.

Teknologia digitala gero eta gehiago kontsumitzen denez, horretarako beharrezkoa den azpiegituraren sorrera bultzatzen ari da; zehazki, energia asko kontsumitzen duten datu-zentro berri ugari sortzea, ekonomia digital berriaren ezinbesteko elementu gisa erabiltzeko. Gure mezuak, argazkiak eta gailu mugikorren eta ordenagailuen artean trukatzen diren gainerako fitxategiak gordetzeko balio duten zerbitzariak daude datu-zentro horietan. Zentro horiek gero eta handiagoak dira tamainari eta behar dituzten baliabideei dagokienez, baina gaur egun ere instalazio handienek tamaina ertaineko hiri batek adina energia kontsumitu behar izaten dute, batez ere hozteko (Greenpeace, 2017:2).

Azpiegitura digital globala eraikitzeko eta energiaz elikatzeko moduak zehaztuko du nola aurre egin ahal izango zaien gaur egungo gizarteek dituzten gizarte- eta ingurumen-erronka nagusietako batzuei, baita klima-krisiari ere. Izan ere, datu-zentroak eta azpiegitura digitalak energia berriztagarriekin elikatzen badira, teknologia digitalarekiko mendekotasun eta haren behar gero eta handiagoak gidatu eta bizkortu egin dezake eredu ekonomiko jasangarriago eta karbono-aztarna txikiagoko bateranzko trantsizioa.
Azpiegitura digitalen jasangarritasunaren ebaluazioari buruzko hainbat txostenek azpimarratzen dute beharrezkoa dela teknologia digitalaren sektoreko korporazio handiek beren garapenetarako behar duten energia iturri berriztagarrietatik sortzearen aldeko apustu irmoa egitea eta karbono dioxidoaren emisioak ez isurtzea edo murriztea. Izan ere, Interneteko enpresa handienetako batzuen artean, gorakada nabarmena ikusten ari gara energia berriztagarrien erabilera lehenesteari dagokionez. Ez bakarrik klima-krisiari aurre egiteko emisioak murriztearekin lotutako beharrengatik, baita etorkizunean erregai fosilak agortuko direlako ere.



Ildo beretik, deskarbonizazioa ezarri da klima-aldaketaren aurkako borrokaren funtsezko helburu gisa, eta, horregatik, Europako Batzordeak gasa eta energia nuklearra sartu ditu taxonomia berdean, hau da, ingurumenaren aldetik jasangarriak diren jarduera ekonomikoen zerrendan.

Sektorean lider diren korporazioek, hala nola Apple, Facebook eta Googlek, duela 10 urte, jatorri berriztagarriko % 100eko sorkuntzara igarotzeko konpromisoa hartu zuten, eta azken hamarkadan sektoreko 20 konpainia baino gehiago batu zaizkio konpromiso horri. Pisu handiko hainbat arrazoik bultzatu dituzte enpresa horiek horretara; izan ere, beren bezeroak teknologia digitalaren jasangarritasunaz kezkatzen hasiak dira. Baina, gainera, energia berriztagarriak zenbait erregai fosil baino errentagarriagoak izaten hasi dira eskala handiko produkzioetarako, bereziki epe luzeko kontratuetan, eta, gainera, alderdi geopolitikoekin lotutako hornidura-segurtasun handiagoa ematen dute.

Baina egia den arren gero eta enpresa gehiago ari direla bat egiten jatorri berriztagarriko % 100eko energia-kontsumoaren aldeko apustuarekin, eredu eraldatzaile baten aldeko apustuak irmoak direla zaindu behar da, eta ez korporazioentzako itxurakeria hutsa edo *greenwashing* metodo bat. Beraz, kontsumitzaileen eta elkarteen jarrera kritikoa ezinbestekoa da apustu horiek betetzen direla zaintzeko.

Informazio gehiago

"Greenwashing" terminoa enpresa baten produktuen edo zerbitzuen jasangarritasun- edo ekologia-mailaz irudi edo informazio engainagarria transmititzeko prozesuari dagokio. Marketin-modu bat da, kontsumitzaileek ingurumena gehiago errespetatzen duten aukerak gero eta gehiago eskatzen dituztela aprobetxatu nahi duena.

eu.wikipedia.org/wiki/Zuriketa_berde

Teknologia digitalerako materialen eskaria

Aurreko puntuan ikusi dugun energia-eskariaz gain, gailuak ekoizteko eta azpiegiturak eraikitzeko materialen eskari handia ere egiten du teknologia digitalaren industriak. Adibidez, kalkulatzen da smartphone bakoitzak 60 osagai baino gehiago behar dituela fabrikazio-prozesurako, eta horien artean daude aspalditik naturatik kantitate handitan erauzten diren materialak, hala nola aluminioa, urrea, kobrea edo kobaltoa, baina baita beste batzuk ere, hala nola litioa edo silizioa, zeinen erauzketa biderkatzen ari baita teknologia digitalaren beharrak asetzeko, "***Baliabide teknologikoen ekoizpen-prozesuak***" mailako 3. bideoan ikusi genuen bezala.

BALIABIDE TEKNOLOGIKOEN EKOIZPEN-PROZESUAK

e.digitall.org.es/A4C44A1V03

Hain zuzen ere, litioa gero eta gehiago eskatzen da, bateria gehienen funtsezko osagaia baita. Funtsean, bateria bat bi gelaxka elektrokimikok edo gehiagok eta energia kimikoa energia elektriko bihurtzeko bi elektrodok osatzen dute. Ion-litiozko bateria batean, bateriaren elektrodo positiboak litio-konposatu batekin funtzionatzen du nagusiki; bateriaren elektrodo negatiboak, berriz, karbonoa erabiltzen du grafito moduan. Gainera, aluminiozko karkasa batek estalita egon behar du, eta kobaltoa ere egon daiteke bertan.

Bestalde, osagai mikroelektronikoak eta telefonoaren kableatua, funtsean, kobrea, zilarra eta urrea bezalako metalekin fabrikatzen dira, elektrizitatearen eroale oso onak baitira, baina platinoa, eztainua, beruna eta paladioa ere izan ditzakete. Gailuen elektronika silizio puruzko txipetan oinarritzen da. Txip horiek elementu erdieroaleekin bonbardatzen dira, hala nola fosforoarekin, antimonioarekin, artsenikoarekin, boroarekin, galioarekin edo indioarekin, haien propietate elektrikoak hobetzeko.

Gailuen kondentsadoreetarako zein kameren lenteetarako tantaloa behar da. Elementu hori koltanean ageri da (Afrikako zenbait lekutan "Columbita - Tantalita" izendatzeko erabiltzen den merkataritza-laburdura da). Jakina denez, koltana da Kongoko Errepublika Demokratikoak jasaten dituen gatazka belikoen zeharkako erantzulea. Bertan daude munduko erreserba nagusiak, baina Txinan, Errusian edo Afrikako beste herrialde batzuetan ere badago: Etiopian, Mozambiken, Nigerian eta Ruandan, esaterako. Herrialde horietako ekoizpen-maila

aldatu egiten da gordailuen arabera, horietako asko artisautza-ustiapenekoak baitira. Tantalo-kontzentratu batek % 10 eta % 40 arteko Ta2O5 kontzentrazioa izan dezake; haren merkataritza-balioa tantalo-oxidoaren kontzentratuaren gainean kalkulatzen da.

Gailu digital baten mikrofonoa eta bozgorailua imanez osatuta daude. Imanek neodimio-, burdin- eta boro-aleazioak dituzte, bai eta disprosioa eta praseodimioa ere. Azken bi elementu horiek "lur arraroak" izenekoak dira (taula periodikoko 17 elementu, eta horietatik, 15 lantanidoei dagozkie). Beren propietate nabarmenenak kimikoak, optikoak eta magnetikoak dira, eta kritikoak dira trantsizio energetikorako eta teknologia digitalerako. Disprosioa eta praseodimioa ez ezik, itrioa, lantanoa, terbioa, europioa eta gadolinioa ere erabiltzen dira gailu digitalen pantailetarako, eta neodimioa, gailu horien elektronikarako.

Eta, azkenik, gure gailuetako karkasa metalikoak magnesio-aleazioz osatuta daude. Gainera, nikela aurki daiteke, interferentzia elektromagnetikoak saihesteko. Baita bromoaren konposatuak ere, suaren kontrako bere propietateak direla-eta, gailua beroarekiko erresistenteagoa izatea lortzen dutelako.

Errepaso horren ondoren, gailu mugikorrak fabrikatzeko beharrezkoak diren 30 elementuren zerrenda ez-zehatza egin dezakegu (eskuinean).

Elementu kimiko horiek erauzteko behar den kostu ekonomiko eta energetikoari meatze-jardueren ingurumen-inpaktua gehitu behar zaio. Gainera, natura-baliabide horiek guztiak mugatuak dira, hau da, agortzen ari dira, eta eskura dauden aztarnategiak gero eta zailagoak dira ustiatzen. Kalkulatzen da 2050. urtea baino lehen agortu litezkeela teknologia digitala fabrikatzeko ezinbestekoak diren material nagusiak, eta horren arrazoia mundu mailako kontsumoaren hazkunde esponentziala izango da.

Era berean, urtero 46 milioi tona hondakin elektroniko baino gehiago sortzen dira smartphone eta ordenagailuetatik, besteak beste. Tresna horiek bota egiten dira, eta horiekin mineral eta material preziatu ugari galtzen dira.

1 | Kobrea
2 | Zilarra
3 | Urrea
4 | Platinoa
5 | Paladioa
6 | Silizioa
7 | Fosforoa
8 | Antimonioa
9 | Artsenikoa
10 | Eztainua
11 | Beruna
12 | Aluminioa
13 | Kobaltoa
14 | Boroa
15 | Galioa
16 | Indioa
17 | Tantaloa
18 | Neodimioa
19 | Burdina
20 | Boroa
21 | Disprosioa
22 | Praseodimioa
23 | Itrioa
24 | Lantanoa
25 | Terbioa
26 | Europioa
27 | Gadolinioa
28 | Magnesioa
29 | Níkela
30 | Bromoa

Gailu mugikorrak fabrikatzeko 30 elementu behar dira.

Teknologiaren kontsumo jasangarrirako ohiturak

Egoera horren aurrean, ezinbestekoa da ikuspegi berriak planteatzea, teknologia digitalaren ekoizpenaren eta kontsumoaren jasangarritasuna optimizatzeko. "***Teknologiaren kontsumo jasangarria***" izeneko serieko 4. bideoan ikusi dugun bezala, lehenik eta behin, jasangarritasunaren hiru kontzeptu klasikoetan oinarritu behar dugu; hau da, gure kontsumoa murriztea, bai gailuena, bai energiarena; gailuak eta osagaiak ahal den neurrian berrerabiltzea, eta, azkenik, fabrikazioan erabiltzen diren materialak birziklatzea.

TEKNOLOGIAREN KONTSUMO JASANGARRIA
e.digitall.org.es/A4C44A1V04

Berrerabiltzeari eta birziklatzeari dagokienez, kontuan izan behar da orain arte erabili eta baztertutako gailu guztiak ("zabor elektronikoa" edo "tresna elektriko eta elektronikoen hondakinak" bezala ezagunak), gero eta material urriagoen ezinbesteko iturri izan daitezkeela, berrerabiltzea edo birziklatzea lortzen den neurrian. Zabor elektronikoa birziklatzeak eta berrerabiltzeak, baliabide natural berari "bizitza" luzeagoa emateaz gain, energiaren ikuspegitik ere asko aurreztea dakarte, askoz ere errentagarriagoa baita material bat berregokitzea, bere iturri naturaletik erauzi eta eraldatzea baino.

Gure gailuen kontsumoa murrizteari dagokionez, ez da norberaren borondatearen kontua soilik. Gailu berri bat eskuratu aurretik erabilgarri dauden gailuak berrerabili edo berregokitzeko aukerak kontuan hartzeaz gain, beharrezkoa da eragin politikoa izatea eta administrazio eskudunei erregulazio handiagoa eskatzea horrelako gailuetan haien diseinuetatik eta merkaturatze-prozesuetatik jarduten duten zaharkitzeak mugatzeko; bai zaharkitze programatua, bai hautemandako zaharkitzeak edo espekulaziokoak.

Horrela, gailu digitalak eta elektronikoak "konpontzeko eskubidea" bultzatu beharko litzateke, zenbait urtez horiek konpontzea eta ordezko piezak eskuratzea ahalbidetuko duten diseinuetatik abiatuta. Ildo horretan, dagoeneko badira adibide batzuk, hala nola *Fairphone* edo "bidezko telefonoa". Ekimen horrek lehentasuna ematen dio gailuen bizitza baliagarria luzatzeari, konponketa errazak errazten dituen diseinu modular batetik abiatuta; gainera, hondakin elektronikoak murrizten laguntzen du berrerabilpenaren eta konponketaren bidez,

baita fabrikazioan material birziklatuen erabilera handituz ere. Azkenik, ekimen horrek bermatzen du erabilitako materialak ez datozela gatazka-eremuetatik eta fabrikazioan lan egiten duten pertsonek bidezko baldintzetan egiten dutela.

Teknologia digitalari lotutako energia-kontsumoari dagokionez, errazena eguneroko ohitura eta keinuekin hastea da, gure aztarna digitala murrizteko. Frantziako *Agence de la transition écologique* agentziaren txosten baten arabera, pertsonen % 43k ez du inoiz itzaltzen bere telebistako kutxa edo routerra. Ohitura horiek diferentzia ekar dezakete maila globalean: adibidez, etengailuak itzaltzea; telebista, inprimagailua edo kontsola *stand by* eran ez uztea; ordenagailua esekita ez uztea, eta itzaltze-etengailua duten erregeletak jartzea (izan ere, ekipoa sarearekin zuzenean konektatuta badago, kontsumitzen jarraituko du).

Europako Batzordeak, "Europako Hamarkada Digitala: 2030erako jomuga digitalak" programan, hitzez hitz azaltzen duenez, "gailu digitalek jasangarritasunaren eta trantsizio ekologikoaren alde egin behar dute, eta ezinbestekoa da erabiltzaileek, beren gailuen ingurumen-inpaktua eta energia-kontsumoa ezagutzeaz gain, prozesu demokratikoan maila guztietan parte hartzeko eta beren datuen gaineko kontrola izateko aukera izatea".

Informazio gehiago

Agence de la transition écologique, (2022). Evaluation environnementale des équipements et infrastructures numériques en France. (Frantziako ekipamendu eta azpiegitura digitalen ingurumen-ebaluazioa). *e.digitall.org.es/evaluacion-ambiental*

Greenpeace (2017) «Clicking Clean». *e.digitall.org.es/clicking-clean*

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

Teknologia eta Gizartearen Behatoki Nazionala (ONTSI), (2021) "Tendencias en el uso de dispositivos tecnológicos" *e.dgitall.org.es/ontsi*

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

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

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