DigitAll

Gaitasun
digitaletan
prestakuntza

4

Segurtasuna

DigitAll

Gaitasun
digitaletan
prestakuntza

Segurtasuna

C2 maila

AURKIBIDEA

DigitAll

Segurtasuna

4.1
GAILUEN BABESA

Segurtasuna

C2 maila 4.1 Gailuen babesa

Gorabeherei erantzuteko plana

Gorabeherei erantzuteko plana

Gorabeherei erantzuteko plan bat prozedura eta neurrien multzo bat da, erakunde batean gerta daitezkeen informazioaren segurtasuneko edo zibersegurtasuneko gorabeherak modu efiziente eta eraginkorrean kudeatzeko diseinatu dena.

Gorabeherei erantzuteko plan baten helburuak hauek dira: inpaktua minimizatzea, normaltasuna berrezartzea, informazioko aktiboak babestea, erroko kausa identifikatzea, legeetako eta arauetako baldintzak betetzea, eta erakundearen erantzuteko gaitasunak etengabe hobetzea.

Gorabeherei erantzuteko plan baten etapak aldatu egin daitezke, plana ezartzeko jarraitzen den metodologiaren edo gidaren arabera, baina plan guztiek izan ohi dituzte etapa hauek edo horien aldaerak:

1 | **Prestaketa** etapa hau gorabehera gertatu aurreko prestaketan ardazten da. Barne hartzen ditu gorabeherei erantzuteko plana sortzea eta dokumentatzea, erantzun taldea izendatzea eta gaitzea, erakundearen aktibo kritikoak identifikatzea eta sailkatzea, eta politika eta prozedura argiak ezartzea.

2 | **Detekzioa eta jakinarazpena:** etapa honetan, sistemak monitorizatzen dira eta detekzio tresnak erabiltzen dira, erantzun taldeari jakinarazi beharko zaizkion gorabeherak identifikatzeko.

3 | **Ebaluazioa eta sailkapena:** etapa honetan, gorabeheraren hasierako ebaluazioa egiten da, haren izaera, irismena eta larritasuna zehazteko.

4 | **Eustea eta arintzea:** etapa honetan, neurriak hartzen dira gorabeheraren inpaktuari eusteko eta inpaktua mugatzeko. Helburua da gorabehera ez zabaltzea, eta kalte gehiago ez eragitea.

5 | **Ikerketa eta analisia:** gorabeherari eutsi ondoren, ikerketa sakona egiten da erroko kausa eta eraso metodoa ulertzeko. Analisiaren bidez, gorabehera zer-nola gertatu zen eta zer neurri hartu behar diren jakin daiteke, etorkizunean antzeko gorabeherak ekiditeko.

GORABEHEREN KUDEAKETA

Gorabeherak kudeatzea eta mota horretako politikak diseinatzea erakundeetan. Segurtasuneko gorabehera motak eta urrats ohikoenak. Kontingentzia eta negozio jarraitutasuneko plana.

e.digitall.org.es/A4C44C1V02

6 | **Berreskuratzea eta berrezartzea:** gorabehera geldiarazi eta ikerketa egin ondoren, kaltetutako sistemak berreskuratu eta berrezartzen dira.

7 | **Ikasitakoa:** gorabeherari erantzun ondoren, gauzatutako ekintzen berrikuspen eta azterketa sakona egiten da, gorabeherei erantzuteko plana hobetzeko eta erakundearen segurtasun neurriak indartzeko.

Plan mota horiek ezartzen laguntzeko, bi tresna ditugu nagusiki: ***ISO 27035*** araua (*e.digitall.org.es/iso-27035*) eta ***NIST SP 800-61*** gida (*e.digitall.org.es/nist-sp800-61*).

ISO 27035

ISO 27035 araua ISOren nazioarteko estandar bat da, eta informazioaren segurtasuneko gorabeherak, gertaerak eta kalteberatasunak kudeatzeko jarraibideak eta jardunbide egokiak ematen ditu.

Xehe jorratzen du informazioaren segurtasuneko gorabeheren kudeaketa, eta gorabehera baten bizi ziklo osoa hartzen du, prestaketatik eta detekziotik hasi eta erantzun, berreskuratu eta ikasteraino.

Arauaren xedea da erakundeei laguntzea gorabeherei erantzuteko gaitasunak ezartzen eta hobetzen eta segurtasuneko gorabeheren inpaktu negatiboak arintzen. Arau hori har daiteke ISO 27002 arauan jasotako segurtasuneko gorabeherak kudeatzeko atalaren hedapen gisa.

NIST SP 800-61

NIST SP 800-61 Ameriketako Estatu Batuetako National Institute of Standards and Technology (NIST) erakundeak argitaratutako gida bat da, erakundeei lagundu nahi diena behar duten zibersegurtasuna ezartzen, gorabeheren aurrean erantzuteko eta horiek modu efizientean tratatzeko gaitasuna izan dezaten. Argitalpen honek gorabeherak kudeatzeko jarraibideak ematen ditu, gehienbat datuak aztertzeko eta gorabehera mota bakoitzari dagokion erantzuna zehazteko.
Jarraibide horiek modu independentean bete daitezke, hardware plataformaren, sistema eragilearen, protokoloen edo erabilitako aplikazioen arabera.

ISO 27035 arauak bezala, gorabeheren kudeaketaren bizi zikloaren alderdi guztiak jorratzen ditu, eta informazioaren segurtasuneko gorabeherak kudeatzeko erreferentziazko gida da askorentzat.

Segurtasuna

C2 maila 4.1 Gailuen babesa

Kalteberatasun hedatuenak: OWASP Top 10

Kalteberatasun hedatuenak: OWASP Top 10

Web teknologiak gure bizitza digitalaren funtsezko zati bat dira. Egunero erabiltzen ditugun zerbitzu gehienak, esaterako, banka elektronikoa edo osasun digitalaren kudeaketa, web teknologietan oinarrituta daude: batez ere HTML, CSS eta JavaScript erabiltzen dituzten web orriak, aplikazioak eta zerbitzariak.

Atal honetan web aplikazioen segurtasunaren garrantziaren eta teknologia horien kalteberatasun bereizgarrien aurkezpena egiten da. Horretarako, web kalteberatasunak kategorizatzeko erreferentzia zabaldu eta onartuenetako batean sakontzen da, hots, OWASP Top 10.

OWASP Top Ten (*Open Web Application Security Project Top Ten*) web aplikazioen hamar segurtasuneko kalteberatasun kritikoenen zerrenda da. OWASP proiektuak sortu zuen. Web aplikazioen segurtasuneko aditu komunitate bat da, softwarearen segurtasuna hobetzea duena xede.

OWASP Top 10en webgune ofiziala

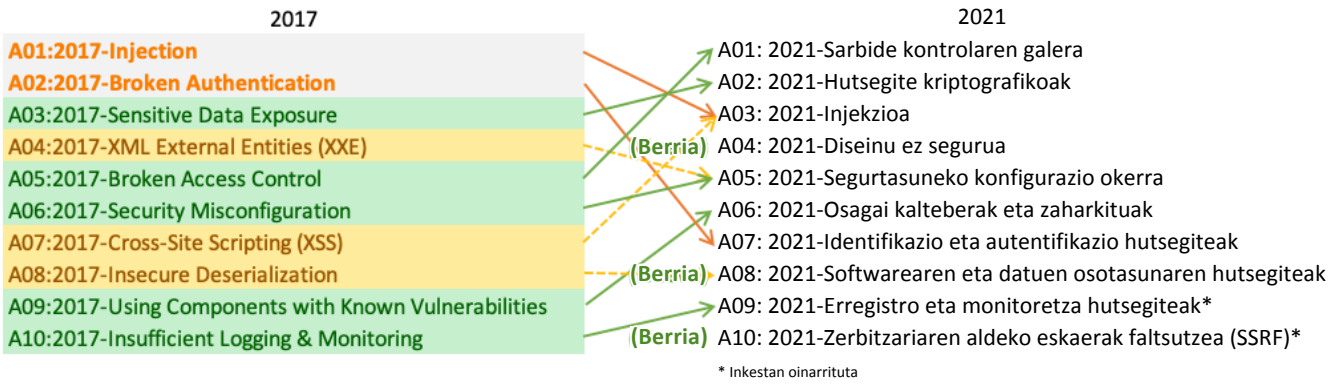
owasp.org/www-project-top-ten

OWASP Top Tenen helburu nagusia gida bat eskaintzea da, garatzaileek, segurtasuneko profesionalek eta erakundeek **web aplikazioek aurre egin beharreko mehatxu nagusiak** uler ditzaten eta arrisku horiek arintzeko neurriak har ditzaten.

Zerrenda aldizka eguneratzen da, web aplikazioen segurtasun arloko mehatxu eta joera berriak islatzeko. Argitaratutako azken bertsioa, dokumentu hau egin den datan, **OWASP Top 10 2021** da. Hala ere, ariketa interesgarria da aurreko bertsioa, OWASP Top 10 2017, gaur egungo bertsioarekin alderatzea, web mehatxuen arloko azken urteetako joerak zein diren jakiteko. Hurrengo azpiataletan kategoria bakoitzaren kalteberatasunak zertan dautzan azaltzen da. Kode honen bidez identifikatzen dira: A<ranking>:2021.

OHARRA

Web kalteberatasunen katalogazio hori egiteko erabilitako informazioa hainbat iturritakoa da, hala nola txostenak, gorabeheren azterketak, inkestak, etab. Datu horiek segurtasuneko adituek eta sektorean espezializatutako enpresek ematen dituzte; izan ere, horien eguneroko lana da horrelako aplikazioen segurtasuna garatzea eta bermatzea.



Sarbide kontrolaren galera

OWASP Top 10 2021en lehenengo kategoria “A01:2021-Broken Access Control” da, hots, sarbide kontrolaren galera. Kalteberatasun mota horretan, sistema batek zenbait funtzionalitatetan edo datutan baimenik gabe sartzea oker ahalbidetzen du.

Adibidez, pribilegiorik ez duen erabiltzaile batek informazio konfidentziala eskuratzea edo mugatuta egon beharko luketen ekintzak gauzatu ahal izatea; adibidez, beste erabiltzaile batzuen erregistroak aldatzea edo administrazio ataletan baimen egokirik gabe sartzea.

Azpimarratzekoa da azken urteotan kalteberatasun mota horrek izan duen joera, 2017ko sailkapenean bosgarren egotetik lehenengo postura igo baita.

Hutsegite kriptografikoak

OWASP Top 10 2021ean, bigarren kategoria “A02:2021-Cryptographic Failures” da, euskaraz, hutsegite kriptografikoak. Kategoria honek barne hartzen ditu algoritmo kriptografikoak, gakoen kudeaketa eta datuen biltegiratze segurua modu desegokian erabiltzearekin loturiko kalteberatasunak. Utilitate horiek erabiltzaileen zein aplikazioen datuen konfidentzialtasuna eta osotasuna bermatzeko erabiltzen dira.

Hutsegite kriptografikoen adibide tipiko bat da zifratze algoritmo ahulak edo kalteberak erabiltzea, hala nola zifratze zaharkitua erabiltzea edo gakoak modu ez seguruan biltegiratzea. Hala, erasotzaile batek datu konfidentzialak deszifratzeko aukera izan lezake.

Gida honen aurreko bertsioan, kategoria horri “Sensitive Data Exposure” esaten zitzaion (datu sentikorrak agerian geratzea), eta hirugarren postuan zegoen. Oraingo bertsioan, postu bat igo da, eta kalteberatasun kritikoenetako bigarrena da.

Injekzioa

Kalteberatasunetako hirugarrenak dira “A03:2021-Injection” kategoriakoak, hots, injekzioko kalteberatasunak. Kategoria honek barne hartzen du web aplikazioetan nahi ez den kode gaiztoa txertatzea, normalean, iragazi gabeko edo gaizki baliozkotutako sarrera eremuen bidez.

XSS ETA SQL INJECTION

Cross-Site Scripting (XSS) eta SQL Injection (SQLi) kontzeptuak, garrantzi handikoak web aplikazioen segurtasunaren testuinguruan. Eraso mota horren ondorioak eta horien aurrean nola babestu azaltzen da.
e.digitall.org.es/A4C41C2V05

OWASP Top Ten 2017an, kalteberatasun hori lehen postuan zegoen, eta azken urteetan beste kategoria batzuek sailkapenean gainditu duten arren, web segurtasunaren kalteberatasun kritikoenetako bat izaten jarraitzen du.

Diseinu ez segurua

“A04:2021-Insecure Design” edo diseinu ez segurua kategoriak aplikazio baten segurtasuna arriskuan jar dezaketen diseinuko hutsegiteak biltzen ditu. Alegia, ez dira kontuan hartu segurtasuneko printzipioak garapen prozesuaren hasieratik.

Adibidez, sistema batean ez da autentifikazio egokirik egiten, eta ez da neurri sendorik hartzen erabiltzaileak egiaztatzeko eta baimentzeko. Hori dela eta, baimenik gabe sar daiteke baliabide edo datu konfidentzialetan.

Kategoria berria da, ez baitzen ageri OWASP Top 10 sailkapenaren 2017ko bertsioan.

Segurtasuneko konfigurazio okerra

Bosgarren postuan daude “A05:2021-Security Misconfiguration” motako kalteberatasunak, alegia, segurtasuneko konfigurazio okerra motakoak. Horietan, aplikazioaren osagaien eta zerbitzarien konfigurazioa okerra da, eta baimenik gabe sartzea edo informazio sentikorra agerian geratzea ahalbidetu dezake.

Adibidez, direktorioak edo fitxategi konfidentzialak eskuragarri leudeke, fitxategien baimenen konfigurazio okerren edo web zerbitzari baten segurtasuneko konfigurazioen bidez.

Osagai kalteberak eta eguneratu gabeak

Kategoria honek, “A06:2021-Vulnerable and Outdated Components” edo osagai kalteberak eta eguneratu gabeak, kalteberatasun ezagunak edo eguneratu gabeak dituzten software-osagaien erabilerari lotutako arriskuak nabarmentzen ditu.

Adibidez, kalteberatasun ezagunak dituen liburutegi edo plugin zaharkitu bat erabiltzea web aplikazio batean, erasotzaile batek baliatu litzakeenak aplikazioaren segurtasuna arriskuan jartzeko.

Identifikazio eta autentifikazio hutsegiteak

Sailkapeneko zazpigarren kategoria “A07:2021-Identification and Authentication Failures” da, euskaraz, identifikazio eta autentifikazio hutsegiteak. Web aplikazio bateko erabiltzaileak identifikatzeko eta autentifikatzeko mekanismoen ahuleziak dira. Besteak beste, pasahitz ahulak, indar handiko erasoen aurkako babesik eza edo pasahitzak berreskuratzeko prozesuko kalteberatasunak.

Adibidez, kontuak ez blokeatzea saioa hasteko huts egindako saiakeren kopuru jakin baten ondoren; horrek indar handiko erasoak errazten ditu.

Softwarearen eta datuen osotasunaren hutsegiteak

OWASP Top 10 2021ean zortzigarren dagoen kategoria berria da 2017ko bertsioarekin alderatuta: "A08:2021-Software and Data Integrity Failures" (euskaraz, softwarearen eta datuen osotasunaren hutsegiteak). Kategoria honek softwarearen osotasunarekin eta portaera zuzenarekin lotutako arriskuak ditu ardatz, baita datu kritikoen baimenik gabeko manipulazioa ere.

Adibidez, sarrerako datuen baliozkotze egokia egiten ez duen aplikazio bat. Horrek aukera eman lezake datu maltzurrak sartzeko, aplikazioan hutsegiteak eragin ditzaketenak edo haren osotasuna arriskuan jar dezaketenak.

Erregistro eta monitoretza hutsegiteak

Bederatzigarren postuan dago "A09:2021-Security Logging and Monitoring Failures" (euskaraz, erregistro eta monitoretza hutsegiteak). Kalteberatasun horretan, web aplikazio bateko gorabeheren eta jardueren erregistroa eta monitoretza ez dira egokiak. Horrek zaildu egin dezake segurtasuneko gorabeherak detektatzea eta horiei erantzutea.

Adibidez, segurtasuneko gorabeheren erregistro sistemarik ez egotea. Horrek zaildu egiten du jarduera susmagarriak edo abian diren erasoak identifikatzea.

Zerbitzariaren aldeko eskaerak faltsutzea

Azkenik, oso kategoria espezifiko bat dugu, "A10:2021-Server-Side Request Forgery" (zerbitzariaren aldeko eskaerak faltsutzea). Kategoria honetan, erasotzaile batek zerbitzaria engaina dezake, nahi ez diren ekintzak egin ditzan erabiltzaile legitimoaren izenean.

CSRF erasoa da (*Cross-Site Request Forgery*) adibide tipikoa; alegia, erasotzaile batek erabiltzailea engainatzen du, honen baimenik gabe ekintzak gauzatu ahal izateko, hala nola pasahitza aldatzea edo baimendu gabeko transakzioak egitea.

Segurtasuna

C2 maila 4.1 Gailuen babesa

TOR sarea

TOR sarea

TOR sarea da Interneteko sare anonimo ezagunena. Web iluneko zerbitzu ezkutuetan nabigatzeko aukera ematen du, baina baita Interneteko edozein zerbitzutara sartzeko ere. Hori guztia, modu anonimoan. Jarraian, anonimotasuna, sare anonimoak eta TOR zer diren definitzen da.

Anonimotasuna eta pribatutasuna

Pribatutasuna eta anonimotasuna bi termino erlazionatu dira, baina esanahi desberdina dute.

Pribatutasuna da pertsona batek bere buruari buruz ematen duen informazioa kontrolatzeko eta informazio hori nork eskura dezakeen erabakitzeko duen eskubidea. Eremu digitalean, pribatutasunak berekin dakar datu pertsonalen babesa eta baimendutako pertsonek soilik eskuratuko dituztelako bermea. Alegia, kontrolpean izatea zer informazio biltzen den, nola erabiltzen den, nork erabiltzen duen eta nola partekatzen den.

Anonimotasuna, bestalde, pertsona baten identitatea ezkutatzeko edo ezezaguna izateko gaitasuna da. Aukera ematen du online jarduketak egiteko informazio pertsonal identifikagarrik eman gabe, hala nola izena, helbidea edo ekintza baten egilea identifikatzea ahalbidetzen duen beste edozein datu.

Pertsona bat sarean anonimoa izateko hainbat arrazoi daude. Adibidez, hauek:

- **Adierazpen askatasuna:** iritziak askatasunez ematea, gehienbat gobernuen edo erakunde errepresiboen errepresalien beldurrik gabe.
- **Pertsonen arteko konexioa:** antzeko interesak partekatzen dituzten komunitateetan eta taldeetan konektatzea, errepresioaren beldurrik gabe.
- **Ikerketa askatasuna:** informazioa bilatzea, epaien edo diskriminazioaren beldurrik gabe.
- **Kazetaritza eta aktibismoa:** informazioa filtratzea edo gobernuei buruzko albisteak argitaratzea.

Pribatutasuna eta anonimotasuna eskubide digital garrantzitsuak dira, ingurune digitalean informazio pertsonala edo identitatea babesteko. Hala ere, garrantzitsua da kontuan hartzea erabateko anonimotasunak legea eta online erantzukizuna aplikatzeko erronkak ekar ditzakeela, legez kanpoko jarduerak egin litezke-eta arrastorik utzi gabe.

Interneteko sare anonimoak: Web sakona eta web iluna

Interneten anonimotasuna lortzeko hainbat bide daude. Dagoeneko ikusi ditugu zenbait modu, hala nola sare birtualen (VPN) edo proxyen erabilera. Horiek aukera ematen dute jatorrizko IP helbidea edo kokapen geografikoa ezkutatzeko. Hala ere, horretarako, fidatzekoa izan behar da VPN edo proxy hornitzailea.

VPNAK, PROXYAK ETA ANONIMOTASUNA SAREAN

Sare pribatu birtualek edo VPNek, proxyekin batera, sare edo webgune desberdinetara konektatzeko aukera ematen dute, IP helbide propioa erabili gabe. Horrela, Interneteko zerbitzu eta baliabide batzuetara nolabaiteko anonimotasun mailarekin sartzeko aukera ematen dute.
e.digitall.org.es/A4C41C2V09

Hori dela eta, hainbat ekimenek sare anonimoak sortu dituzte. Sare anonimoek Internet erabiltzen dute erabiltzaileen anonimotasuna bermatuko duten komunikazio protokoloak sortzeko. Adibidez, Freenet eta Invisible Internet Project (I2P) sareek edukiak partekatzeko eta modu anonimoan komunikatzeko aukera ematen diete konektatutako erabiltzaileei. TOR, jarraian ikusiko duguna, sare anonimo bat da, eta, sarearen barruko edukietan sartzeko aukera emateaz gain, Interneten ikusgai dauden zerbitzuetara konektatzeko aukera ematen du. Hau da, sare anonimotik kanpokoetara.

Internetek webaren bidez informazioa partekatzeko aukera ematen du, baina baita edukiak modu anonimoan partekatzen dituzten sare anonimoak sortzekoa ere. Ohiko webaren eta sare anonimoen arteko aldea irudi honen bidez adierazi ohi da:

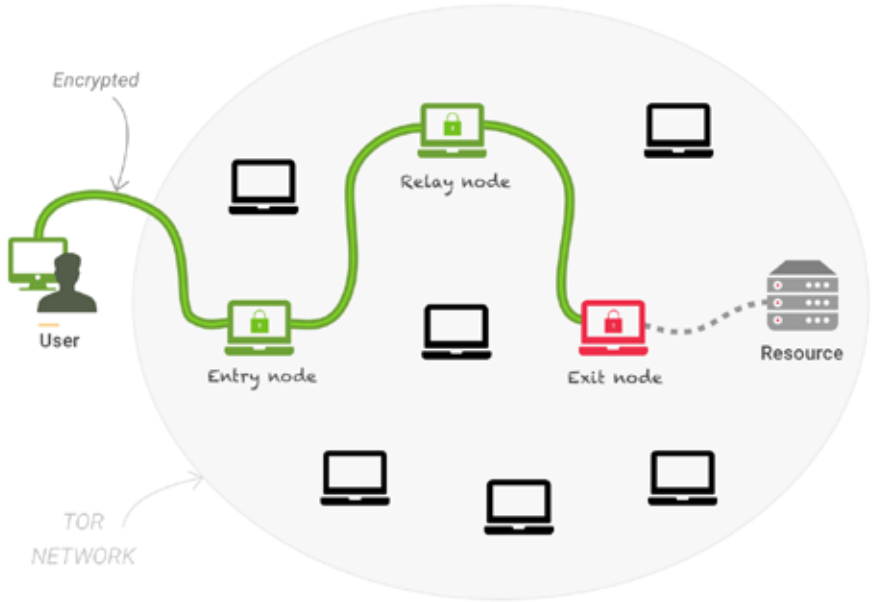
Azaleko weba osatzen dute (***Surface web***) Internet bidez modu konbentzionalean sar gaitezkeen web orri guztiek. Gainera, eduki horiek indexatu egiten dituzte bilatzaileek, hala nola Googlek edo Bingek. Beraz, erraz aurki eta eskura daitezke. Benetan, eduki mota hori Internet bidez eskura daitekeen eduki guztiaren zati txiki bat da.
Horrela, foro pribatuek, sare pribatuek edo sarbide kontrol nahitaezkoa duen edozein edukik **web sakona** osatzen dute. Informazio hori ez dago zuzenean eskuragarri, eta ezin da Google eta antzeko bilatzaileak erabiliz aurkitu.

Azkenik, sare anonimoak **web ilunaren** parte dira. Eduki horiek sare horien bidez baino ezin dira eskuratu, teknologia hori erabilita.

The Onion Router (TOR)

The Onion Router (TOR) proiektuak software bat eskaintzen du, erabiltzaileari TOR sarera konektatzeko eta edukietara modu anonimoan sartzeko aukera ematen diona. Software horrek *onion routing* komunikazio protokoloa erabiltzen du (geruzakako bideraketa).
Erabiltzailearen anonimotasuna ziurtatzeko, geruzakako bideraketak gutxienez bi nodo-errepikagailu edo *relay* erabiltzen ditu. Webgune batera konektatzeko, erabiltzailea

nodo-errepikagailu batera konektatuko da, eta nodo hori beste errepikagailu batera konektatuko da. Amaierako nodo-errepikagailua da, azkenean, webgunera konektatuko dena.



Horrela, lehenengo nodo-errepikagailua da erabiltzailea ezagutzen duen bakarra, baina ez daki nora konektatuko den. Era berean, amaierako errepikagailuak bakarrik jakingo du nora konektatzen ari den, baina ez daki zein den konexioa hasi duen erabiltzailearen nortasuna.
TOR sarera sartzeko, ***TOR nabigatzailea*** (*torproject.org*) deskargatu besterik ez da egin behar. Firefoxen oinarritutako nabigatzaile honek aukera ematen du TOR sarera konektatzeko eta bertan nabigatzeko. Sarea zerbitzu ezkutuz osatuta dago, eta ".ONION" domeinuagatik ezagutzen dira.

⚠ ADI

Hidden Wiki TOR sarean eskuragarri dagoen zerbitzu ezkutua da. Bertan sartzeko, beharrezkoa da TOR nabigatzailea erabiltzea eta webgune honen ".ONION" domeinua erabiltzea:

http://paavlaytlfsqyvkg3yqj7hflfg5jw2jdg2fgkza5ruf6lplwseeqtvyd.onion/

Azkenik, garrantzitsua da gomendio batzuk kontuan hartzea. TOR sarean nabigatzeko, komeni da VPN batera konektatuta nabigatzea. Gainera, oso garrantzitsua da kontuan hartzea TOR sarean anonimotasuna dela nagusi, eta, beraz, kontu handiz ibili behar da ziberdelinkuentziarekin eta kontuz nabigatu behar da.

Segurtasuna

C2 maila 4.1 Gailuen babesa

Anonimotasun soluzioak sarean

Anonimotasun soluzioak sarean

Sareko anonimotasuna zer den ikusi ondoren, atal honetan, zure identitatea babestuta mantentzeko ezagutu behar dituzun hainbat utilitate aipatuko dira.

TOR SAREA

Erreferentziazko dokumentua: ***A4C41C2D03***

VPN zerbitzuak

Sare pribatu birtualek aukera ematen dute sare batera urrunetik konektatzeko. Etxeko erabileran, VPN zerbitzuak webguneetan modu anonimoan sartzeko edo herrialde jakin batzuetarako soilik eskuragarri dagoen edukia kontsultatzeko erabiltzen dira.

Garrantzitsua da ordainpeko VPN fidagarriak erabiltzearen ziurtasuna izatea. VPN zerbitzuek pribatutasun politika zorrotza izan behar dute, Interneterako konexioaren hornitzaileek bezala.

NordVPN

NordVPN da VPN zerbitzu ezagunenetako bat, 5.700 zerbitzari baino gehiago ditu 60 bat herrialdetan. Gainera, gailu askorekin bateragarria da, Linux, MacOS eta Windows barne, baina baita gailu mugikorrekin eta Android TVrekin ere.

NordVPN
nordvpn.com/es

ProtonVPN

ProtonVPN enpresa suitzar batek eskaintzen duen zerbitzua da, erabiltzaileen pribatutasunaren alde egiten duena. Aukera ematen du 10 gailura arte erabiltzeko, eta abiadura handiak eskaintzen ditu. Gainera, aukera ematen du iragarkiak blokeatzeko eta pribatutasun aurreratuko zerbitzuak konfiguratzeko. NordVPNk bezala, gailu mota askorekin bateragarria da.

ProtonVPN
protonvpn.com/es

Mullvad VPN

Mullvad VPN zerbitzuak pribatutasun eta anonimotasun maila handia eskaintzen die erabiltzaileei, modu anonimoan erregistratzeko eta ordaintzeko aukera ematen baitu. Aplikazio erabilerrazak eta sinpleak ditu.

ProtonVPN
mullvad.net/es

Proxy zerbitzuak

Bestalde, zerbitzu batzuek aukera ematen dute gure izenean web kontsultak egiteko. Hau da, webguneetan nabigatzeko bitartekari bat erabiltzeko aukera ematen dute IP helbidea agerian jarri gabe. Aipatzekoa da zerbitzu horietako gehienak dagoeneko VPN zerbitzuetara aldatu direla.

ProxySite

ProxySite

proxysite.com

ProxySite zerbitzuaren webgunearen bidez, edozein webgune kontsultatu daiteke. Blokeatutako edo soilik beste herrialde batzuetan eskuragarri dauden edukiak URL helbide batekin bakarrik bistaratu daitezke.

IP Vanish

VPN batez gain, IP Vanish-ek SOCKS5 teknologia duen proxy zerbitzu bat eskaintzen du. Teknologia hori proxy gisa konfigura daiteke hainbat aplikaziotan, hala nola berehalako mezularitzan edo web nabigatzailean.

IP VANISH

ipvanish.com/socks5-proxy

Identitate anonimoari eustea

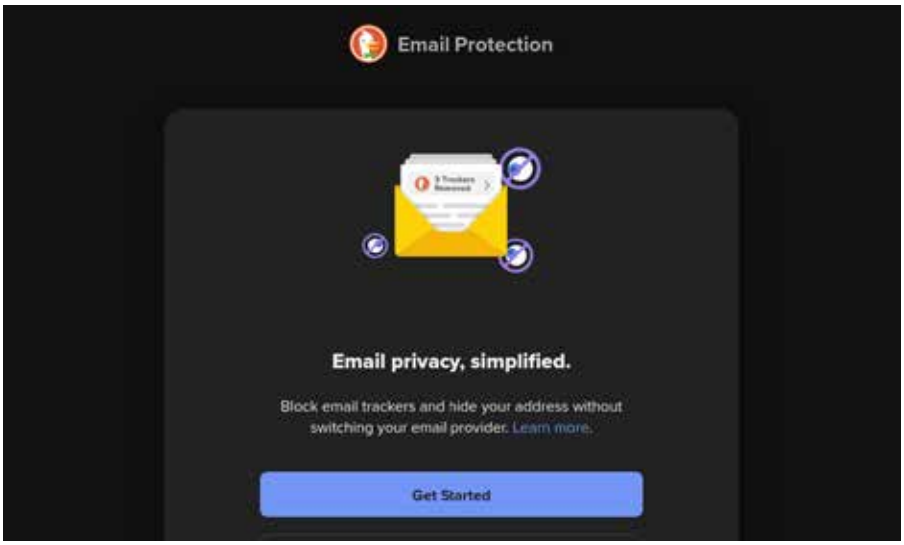
Sareko anonimotasunak ahalegin handia eskatzen du. TOR erabili arren, anonimotasunari eusteko oso garrantzitsua da datu pertsonal identifikagarri oro ezkutatuta edukitzea.

Aldi baterako postarako ontzia

TEMPMAIL
temp-mail.org/es

Lehenik eta behin, online zerbitzu batzuek helbide elektroniko bat eskatzen dute erregistratzeko. Norberaren helbidea ez erabiltzeko, aldi baterako posta zerbitzuak erabil daitezke. Ezagunenetako bat Temp Mail da, baina badira beste batzuk ere. Garrantzitsua da kontuan izatea zerbitzu hori aldi baterako dela; beraz, helbide horretara sartzeko aukera galduko dugu erabilera epea igarotakoan.

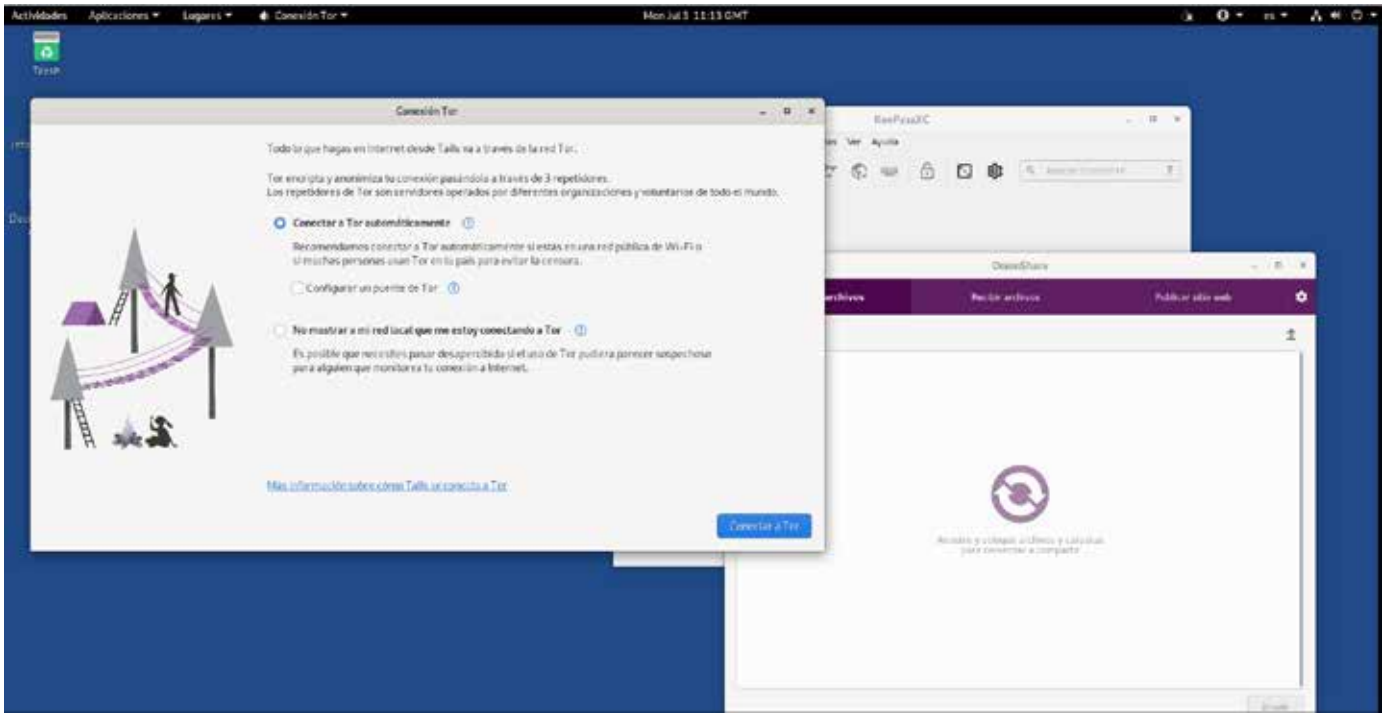
DuckDuckGo Email Protection



DuckDuckGO
duckduckgo.com/e-maila

Aldi baterako postarako sarbideari eutsi nahi badiogu, edo gure kontua erabili nahi badugu benetako helbidea jakinarazi gabe, posta elektronikoko proxy bat erabil dezakegu. Horri esker, helbide elektroniko erreala ezkutatu dezakegu ausazko helbide batekin. Zerbitzu ezagunenetako bat da DuckDuckGo Email Protection, bilatzaile ospetsuarena. Kontu bat sortu ondoren, benetako helbidearen "ezizenak" edo pseudonimoak sortzeko aukera ematen du.

TailsOS: sistema eragile anonimoa



TailsOS hainbat teknologia bateratzen dituen sistema eragilea da, eguneroko erabilerarako pribatutasun eta anonimotasun maila altua eskaintzen duena. Besterik adierazi ezean, TOR erabiltzen du Interneteko konexiorako.

Sistema eragile hori edozein ordenagailutan exekutatzen da USB batetik, fidagarria ez den edozein sistema eragile saihesten saiatuz eta "amnesia" eraginez. Hau da, jarduera ororen erregistroa minimizatuz.

TailsOS
tails.net

DigitAll

Segurtasuna

4.2 DATU PERTSONALEN ETA PRIBATUTASUNAREN BABESA

Segurtasuna

C2 maila 4.2 Datu pertsonalen eta pribatutasunaren babesa

Pribatutasuna posta elektronikoan

Pribatutasuna posta elektronikoan

Posta elektronikoaren erabilera oso zabalduta dago gaur egun. Zenbatespenen arabera, 2022an 330.000 milioi mezu elektroniko baino gehiago bidali ziren 4.000 milioi erabiltzaile ingururen artean. Bolumena izugarria izanik, posta elektronikoa hain negozio zabala da, enpresa asko baitaude tartean. Baita posta elektronikoko zerbitzua doan eskaintzen duten batzuk ere. Mezu elektronikoen kopurua eta erabilitako posta elektronikoko plataforma edo aplikazioa edozein izanda ere, erabiltzaileen pribatutasuna arriskuan ez dagoela bermatu behar da.

Web posta

Posta elektronikoa aplikazioen zein web plataformen bidez erabil daiteke. Azken mekanismo hori hodeiko zerbitzu bat da, web posta izenekoa. Sistema hori erabiliz, erabiltzaileek mezu elektronikoak bidali eta jaso ditzakete, aplikaziorik instalatu beharrik gabe.

Enpresa askok web posta eskaintzen dute, batzuek ordainpekoa eta beste batzuek doakoa. Horiek helbide elektronikoa eskaintzen dute webgunetik mezu elektronikoak jaso eta bidaltzeko, baina hornitzaile batzuek zerbitzu gehigarri batzuk ematen dituzte: posta elektronikoko bezeroekin konektatzea, mezu elektronikoak enkriptatzea, etab.

Enpresa askok eskaintzen duten web posta ez zaigu dirurik kostatzen, kostua gure pribatutasunaren kontura kobratzen baitute.

Enpresa horiek gure datuak eta posta elektronikoaren erabilera profilak nahi dituzte, hirugarrenei saldu ahal izateko. Gure pribatutasuna arriskuan jar dezaketen praktika batzuk aztertuko ditugu.

Pribatutasuneko arriskuak web postaren erabileran

Web postako zerbitzuak erabiltzean, neurri batzuk hartzen ez baditugu, informazio asko babesik gabe utz dezakegu. Arrazoi nagusia da mezuak enkriptatu gabe bidaltzen direla, aukera hori kontratatu eta aktibatu ezean.

ADI

Edukia eskura izango du bitarteko edozein sistemak.

Bigarren arrazoia da web postako zerbitzariek mezuak desenkriptatuta gordetzen dituztela; beraz, zerbitzaria bera sar daiteke edukian, eta pribatutasuna galtzea eragin. Zerbitzarien arabera, sarbide hori beharrezkoa da jasotako mezuak sailkatu eta hodeiko zerbitzu desberdinetan integratu ahal izateko, hala nola egutegi pertsonalean, oharretan eta abarretan.

⚠ ADI

Zerbitzariak gure mezuen eta datuen edukian sar daitezke.

Azkenik, zerbitzaria dagoen herrialdearen arabera, herrialde horretako segurtasun zerbitzuak zure mezu elektronikoen edukian sar daitezke. Horretarako, hornitzaileari eskatzea besterik ez dute egin behar. Adibidez, zerbitzaria AEBn badago, CIAk edo NSAk zure mezu elektronikoak lor ditzakete hornitzaileari eskatu besterik ez eginda.

⚠ ADI

Atzerriko erakundeek gure datuak eta mezuak eskura ditzakete, gure baimenik gabe.

Gmail

Googleren posta elektronikoko zerbitzuak Gmail du izena, eta, ziurrenik, munduan gehien erabiltzen den web postako zerbitzua da, hain zuzen ere, Googleren zerbitzuen eta aplikazioen ekosistema osoarekin integratzen delako.

2017tik, Google ez da zure mezu elektronikoetan sartzen; sartu nahi badu, zure baimena behar du. Kasu horietan, Gmailek zure mezuen edukia aztertzeko zerbitzu bat erabiltzen du zure interesetara hobeto egokitutako iragarkiak eskaintzeko, hitzorduak detektatzeko eta zure egutegian sartzeko, egindako bilaketak eta web postan sartzeko baliatzen ari zaren nabigatzailearen erabilera profilak uztartzeko, etab.

Kokapena aktibatuta duten gailuak erabiliz gero, Gmailek jakin dezake web postan zer kokapenetik sartu garen, eta horrek pribatutasuna galtzea dakar.

HODEIKO PRIBATUTASUNA

Nola ezarri neurriak, hodeian zerbitzuak erabiltzean pribatutasuna galtzea saihesteko? Besteak beste, nola saihestu zer kokapenetik sartu garen jakitea?
e.digitall.org.es/A4C42C2V04

Gmailek ez du mezuak enkriptatzeko sistemarik eskaintzen, ezta sinadura digitalik ere. Beraz, ezin da mezu zifraturik edo digitalki sinaturik bidali luzapenik erabili gabe.

Hotmail, Outlook.com

Microsoftek hainbat web postako plataforma jarri zituen martxan, nahiz eta pixkanaka-pixkanaka guztiak zerbitzu berera migratu diren. Beraz, nabigatzailean Hotmail (***hotmail.com***) bilatzen baduzu, ***Outlook***era (***outlook.com***) birbideratzen zaitu.

Outlookek segurtasuneko sistema indartua du, mezu elektronikoak enkriptatzen ditu eta.

Gmailek bezala, Outlookeko mezu elektronikoen edukia Microsoft Officek hodeian dituen aplikazioen ekosistemarekin lotu daiteke, baina ez da automatikoa, erabiltzaileak kasuan-kasuan aktibatu behar baitu edukia aplikazio bakoitzera transferitzea.

Outlook ez da Gmail bezain web postako sistema intrusiboa, baina bere ezaugarrietako batzuek erabiltzaileen pribatutasunari eragiten diote hein batean.

Pribatutasun handiagoko beste web postako sistema batzuk

Beste hornitzaile batzuek kontuan hartu dituzte aurreko puntuetan deskribatutako web postako plataformek baino pribatutasun maila handiagoa eskatzen zuten erabiltzaile batzuen eskakizunak, eta pribatutasun handiagoko beste web plataforma batzuk abiarazi zituzten.

Esaterako, ***ProtonMail*** (***proton.me***), egoitza Suitzan duena, edo ***tutanota*** (***tutanota.com/es***), egoitza Alemanian duena. Biek ala biek hainbat pribatutasun neurri dituzte. AEBko lurraldetik kanpo egoteak pribatutasuna indartzen du, ezinezkoa baita mezu elektronikoen edukian sartzea, ez bada epailearen aginduz.

ProtonMailek pasahitz bikoitza erabiltzen du: lehenengoa, zerbitzura sartzeko, eta bigarrena, postontzia desenkriptatzeko. Horrela, bezeroaren nabigatzailean bertan zifratzea egiten da bigarren pasahitz hori erabiliz, ProtonMailek inola ere ezagutzen ez duena. Beraz, mezu guztiak zifratuta bidaltzen ditu bezeroak, eta ProtonMailek ezin du inola ere mezuen edukian sartu.

Tutanota muturretik muturrera zifratutako web postako zerbitzua da, segurtasun oso handikoa, eta software librearen erabileran oinarritzen da. Tutanotan ez dagoen erabiltzaile bati mezuak bidaliz gero, aldi baterako Tutanota kontu baterako hiperesteka bat sortuko da. Kontu horretan gako bat sartuko da, aldez aurretik erabiltzaile hartzaileari jakinarazi zaiona, eta desenkriptatutako mezua irakurri ahal izango da.

Posta elektronikoko aplikazioak

Beste aukera bat da zure ordenagailuan, tabletan edo smartphonean mezu elektronikoak zuzenean bidaltzeaz arduratzen diren aplikazioak erabiltzea, web postako plataformetan sartu gabe.

Aurrekoa egia bada ere, oro har, neurri batzuk hartu behar dira pribatutasuna bermatzeko. Neurri horiek are beharrezkoagoak dira gailu mugikorren kasuan.

ADI

Posta elektronikoko aplikazioak web postako bertsioak baino seguruagoak eta pribatuagoak dira.

PRIBATUTASUNA GAILU MUGIKORRETAN

Hainbat gogoeta gailu mugikorren erabileran gure pribatutasuna bermatzeko.
e.digitall.org.es/A4C42C2V03

Pribatutasuneko arriskuak web postaren erabileran

Esan bezala, posta elektronikoko aplikazioak erabiltzea web posta erabiltzea baino askoz seguruagoa da, eta pribatutasun berme handiagoa du. Hala ere, interkonektatutako zerbitzua izanik, zenbait pribatutasun arrisku izan ditzake.

Urruneko zerbitzarietan ostatatutako irudiak, bideoak eta bestelako HTML elementuak sartzeak arriskua ekar dezake. Elementu horiek deskargatzean, ostatatuta dauden zerbitzaria gai da posta elektronikoko aplikaziotik informazioa lortzeko: noiz erabili den, zein den IP helbidea, zer sistema erabili den, etab.

ADI

Egokiena da igorle ezezagunen deskargen blokeo automatikoa lehenetsita edukitzea.

Arriskua ekar dezake, orobat, mezua jaso dela baieztatzeko erantzun automatikoak. Horrela, mezu elektronikoaren igorleak badaki mezu elektronikoa jaso eta ireki duzula. Erantzun automatikoa aztertuta, jatorrizko igorleak hartzailearen informazioa lor dezake: helbide elektroniko aktiboa dela, erantzun automatikoa bidaltzeko erabili den IP helbidea, etab.

⚠ ADI

Komeni da lehenetsita ez edukitzea mezuak jaso direla baieztatzeko erantzuna.

Microsoft Outlook 365

Munduan gehien erabiltzen den posta elektronikoko aplikazioetako bat Outlook web postaren gailuko bertsioa da. Azken bertsioak **Microsoft Outlook 365** izena du. Microsoftek garatutako aplikazio horrek aukera ematen du posta elektronikoaren kudeatzaile hori enpresa horren Office suitearen beste aplikazio batzuekin integratzeko.

Microsoft Outlook 365
outlook.com

Aplikazio horrek aplikazio bakar batean barne hartzen ditu posta elektronikoaren kudeatzailea, egutegia, ataza zerrenden sistema eta kontaktuen agenda.

Outlook aplikazioak aukera ematen du mezu guztiak ziurtagiri digitala erabiliz enkriptatzeko, gako publiko eta pribatuko zifratze asimetrikoa egite aldera. Horrek oso pribatutasun maila handia ematen du muturretik muturrera, hau da, hartzaileak bakarrik irakurri ahal izango du mezu zifratuaren edukia, eta ez da desenkriptatuta gordeko bitarteko ezein zerbitzaritan.

Ordenagailurako, Windowserako eta Macerako bertsioak daude, bai eta smartphonerako bertsioak ere, Androiderako zein iOSerako.

Thunderbird

Thunderbird, Mozillak garatua, alegia, Firefox nabigatzaile ospetsuaren atzean dagoen enpresak, posta elektronikoko aplikazio oso interesgarria da ordenagailu pertsonaletan, Linux, Windows zein macOS erabili, bai eta gailu mugikorretan ere, Android zein iOS erabili. Software librea erabiliz sortua da, eta guztiz librea eta doakoa da.

Thunderbird
thunderbird.net/es-ES

Pribatutasuneko ezaugarri asko ditu, hala nola mezu elektronikoak arakatzearen aurka babestea, urruneko edukia blokeatzea, ziurtagiri digitalaren bidezko enkriptatzea, etab.

The Bat!

Posta elektronikoko aplikazio hori ez da aurrekoak bezain ezaguna, baina pribatutasun eta segurtasun maximoa bermatzeko diseinatuta dago. Enkriptatzea erabiltzen du maila guztietan: komunikazio guztiak enkriptatutako kanal seguruen bidez egiten ditu, informazio guztia tokiko ordenagailuan zifratzen du, muturretik muturrerako enkriptazioa du mezu elektronikoak bidaltzeko, etab.

Hodeiko hornitzaile globalen babesik gabe funtzionatzeko gai da, mezurik ez uzteko zure ordenagailutik kanpo.

The Bat! ordainpekoa da eta Windowserako bertsioak baino ez ditu.

The Bat!
e.digitall.org.es/thebat

Canary Mail

Canay Mail aplikazioak pribatutasuna eta produktibitatea biltzen ditu. Zifratze asimetrikoa eta muturretik muturrerako enkriptazioa konbinatuz bermatzen da pribatutasuna. Produktibitatea sustatzeko, adimen artifiziala erabiltzen da, eta, hala, ekintza asko modu adimendunean automatizatzen dira; besteak beste, identitatea ordeztearen iruzurra hautematea, iragarkiak kentzea eta mezu elektronikoen SPAM izaeraz ohartaraztea.

Aplikazio honek ordenagailurako bertsioak ditu, Windowserako zein macOSerako, baita smartphoneetarako ere, Androiderako zein iOSerako.

Canary Mail
canarymail.io/es

Informazio gehiago

e.digitall.org.es/privacidad-email
Hona zure pribatutasuna errespetatzen duten posta elektronikoko 5 zerbitzu. e.digitall.org.es/privacidad-email-2

ProtonMail. proton.me

tutanota. tutanota.com/es

Microsoft Outlook. outlook.com

Thunderbirden ezaugarriak. e.digitall.org.es/thunderbird

The Bat! e.digitall.org.es/thebat

Canary Mail. canarymail.io/es

Segurtasuna

C2 maila 4.2 Datu pertsonalen eta pribatutasunaren babesa

Pribatutasuna eta adimen artifiziala

Pribatutasuna eta adimen artifiziala

Sarrera

Gaur egun, aurrerapen teknologikoei esker, sistema informatikoek informazio asko erabili ahal izan dute, eta konputazio, biltegiratze zein komunikazio gaitasuna handitu egin dira. Informazio hori iturri askotatik jasotzen da, besteak beste, gure ordenagailuetan zuzenean sartzen dugun informazioa, gailu sentsore ugarik (bideokamerak, giroko sentsoreak, igarotze kontagailuak, pisu sentsoreak, etab.) eskuratzen edo biltzen duten informazioa, eta sare sozialetan eta, oro har, Interneten nabigatzean geuk sortzen dugun informazioa (bisitatzen ditugun orriak, bistaratutako bideoak, iruzkinak, erabilera lehentasunak, etab.).

Informazio hori guztia datuen zerbitzarietan biltzen da. Zerbitzari horiek informazio hori modu gutxi gorabehera egituratuan biltegiratzen dute, baina algoritmoak edo prozesuak ezarri ahal izateko moduan, eta horietatik informazio erabilgarria atera daiteke kasu gehienetan. Datu meatzaritzako prozesu horrek erakunde eta enpresei laguntzen die ezarri beharreko estrategia edo garapenei edo erabiltzaile jakin batzuei eskaini beharreko sustapen eta eskaintzei buruzko erabakiak hartzen.

Aurrerapen teknologiko horiei esker, gainera, sistema automatikoak ezarri ahal izan dira makinek informazioa aurkezteko edo erabakiak hartzeko modu autonomoan; alegia, adimen artifiziala.

Teknologia horiek, gailu mugikor pertsonalekin batera, geure egunerokoan erabiltzen ditugu, eta gure bizitzatik bereizi ezin diren elementuak dira. Haien Gailuok elkarreraginean dihardute eta lanean erabiltzen ditugun edo gure gailu pertsonaletara zuzenean iristen diren informazio zein edukiei zuzenean eragiten diete. Sare sozialak eta gailu mugikorren eguneroko eta ohiko erabilera datu iturri garrantzitsua dira datu meatzaritzarako zein adimen artifizialerako, elkarren osagarri dira eta, eta eduki digitala kontsumitzen dugun modua eraldatzen baitute. Ildo horretatik, kontuan hartu behar dugu, halaber, zer-nola dauden babestuta gure informazio partikularra eta datu pertsonalak, hots, gure pribatutasuna, eta teknologia horiek zenbatean eta nola erabiltzen duten.

Europa lanean ari dira teknologia horien erabilera arduratsua bermatzeko eta haiei eragin diezaieketen alderdi etikoak ezartzeko, eta adimen artifiziala erabiltzen duten produktuak eta zerbitzuak DBEOra (Datuak Babesteko Erregelamendu Orokorra) egokitzeko gida bat garatzen eta zabaltzen ari da.

Informazioaren pribatutasunaren eta datuen babesaren kontzeptuak bideo hauetan garatu dira, besteak beste:

PRIBATUTASUN-POLITIKA INTERNETEN ETA APLIKAZIOETAN

Pribatutasun politikaren kontzeptua azalduko da. Non aurkitu pribatutasun politiken dokumentua, bai Interneten, bai edozein aplikaziotan. Pribatutasun politikaren garrantzia. Pribatutasun politikako dokumentu baten edukia.
e.digitall.org.es/A4C42A1V07

PRIBATUTASUN POLITIKA INFORMAZIO PRIBATUA

Bideoak berehalako mezularitzako aplikazioen erabileraren alderdi orokorrak azaltzen ditu, eta arreta berezia jartzen du datuen pribatutasun eta partekatze politiketan.
e.digitall.org.es/A4C42A2V05

ZER SARTZEN DUGU GEURE ORDENAGAILUAN NABIGATZEN DUGUNEAN?

Cookiearen kontzeptu teknikoa, nola biltegiratzen den gure nabigatzailean webgune batetik bidaltzen diguten informazioa. Cookien hasierako funtzioa eta erabilera maltzurrak (malwarea eta harrak). Kontuz ibili fidagarriak ez diren sistemen cookieak onartzearekin.
e.digitall.org.es/A4C42B2V06

Gainera, jarraian adierazten den bideoan azaltzen da nola jokatu behar dugun adimen artifizialaren, datu meatzaritzaren eta gizabanakoen pribatutasuna babesteko.

ADIMEN ARTIFIZIALA, DATU MEATZARITZA ETA PRIBATUTASUNA

Adimen artifizialak, datu meatzaritzak eta, oro har, algoritmoek gero eta gehiago erabiltzen dituzte gure datu pertsonalak. Horrek erronka berriak dakartza, eta horiei adi egon behar dugu gure pribatutasuna babesteko.
e.digitall.org.es/A4C42C2V06

Dokumentu honetan, laburbilduta, adimen artifizialaren, datu meatzaritzaren eta teknologia horiek gure datu pertsonalen pribatutasunarekin eta babesarekin izan dezaketen harremanaren kontzeptuak garatzen dira.

Adimen artifiziala. Kontzeptua eta aplikazioak

Hainbat egileren arabera, adimen artifiziala honela defini daiteke: makina edo sistema automatiko batek, gizakiak bezala, modu autonomoan arrazoitzeko, ikasteko, planifikatzeko eta sortzeko gaitasuna izatea. Adimen artifizialari esker, sistema automatiko horiek beren ingurunea sentsoreen bidez hauteman dezakete, harekin harremanetan jarri daitezke, arazoak konpondu ditzakete eta helburu jakin batekin jardun daitezke.

Adimen artifizialeko sistemak gai dira beren inguruneko informazioa edo ingurunetik kanpoko beste informazio bat prozesatzeko, erantzun bat espero den portaerara egokitzeko eta beren erabakiak izango dituen ondorioak aztertzeko, aldez aurretik egindako ekintzak kontuan hartuta.

Adimen artifizialaren erabilera goraldian da zenbait aplikazioren garapena dela eta, tartean, hainbat arlotan gaur egun funtsezkoak diren aplikazioak nabarmendu litezke, esaterako, hauek: marketinean, merkataritza elektronikorako berariazko IA aplikazioak, mezu elektronikoak bidaltzea edo online publizitatea; laguntzaile birtualak, galderei erantzuten dietenak, zeregin eta gomendio jakin batzuk egiten dituztenak, adibidez, Siri edo Alexa; etxearen automatizazioa; multimedia edukia ikusteko gomendio sistemak, hala nola telebista kanalak edo web hobespenak; itzulpen automatikoko sistemak; gidatze autonomoko sistemak; aholkularitza eta iragarpenak, iragarpen meteorologikoetatik finantza aholkularitzara; aurpegi ezagutza; eta diagnostiko medikoak.

Laburtzeko, esan liteke adimen artifiziala bi motatakoa dela, Europar Batasuneko batzordearen arabera: Softwareko adimen artifiziala, barne hartuta irudien analisiak, laguntzaile birtualak, bilaketa motorrak eta ahotsa eta aurpegia ezagutzeko sistemak; eta adimen artifizial integratua, barne hartuta robotak, droneak, ibilgailu autonomoak edo gauzen Internet.

Datu meatzaritza. Definizioa, metodoak eta teknikak

Datu meatzaritza honela defini daiteke: formatu digitaleko informazioaren (testuak, soinuak, irudiak eta datuak) analisi konputazional automatizatua, Europako Batzordearen arabera. Datu meatzaritzak informazio bolumen handiak tratatzea ahalbidetzen du, ezagutza berriak eskuratzeko eta joera, jarraibide edo korrelazio berriak aurkitzeko. Benetan, datu multzo handietan portaera ereduak eta bestelako informazio baliotsua aurkitzean datza.

Informazioaren biltegiratzearen eta konputazio gaitasunen bilakaera teknologikoari esker, datu kopuru handien prozesamendua (big data) jakintzagai bilakatu da, eta datu bolumen handiak prozesatzeko teknologia zientzia oso bihurtu da. Datuetan emaitzak bilatzeko teknikak eta ereduak aplikatu aurretik, beharrezkoa da horiek aztertzea eta datuak aurrez prozesatzea, benetan esanguratsuak zein diren eta azken analisitik zein baztertu edo ezabatu behar diren zehazteko.

Gaur egun, enpresek eta erakundeek datu meatzaritzako teknikak eta teknologia erabiltzen dituzte maiz erabakiak hartzeko, datuak aztertzen dituzten tresna askoren bidez (besteak beste, Excel, Qlik, Knime, R, Tableau edota Oracle Data Mining).

Gaur egun, *datuen espazioa* kontzeptua eta biki digitalak garatzen ari dira, hainbat lan eremu edo inguruneri buruzko aurreikuspen zehatzak ezagutzeko metodo gisa. Horrela, nekazaritza, abeltzaintza, industria arloetan zein arlo soziokulturalean topa dezakegu datu espazioaren kontzeptua. Datu espazio bat datu kantitate handien iturri desberdinen multzoa da, aurreko antzeko egoerak kontuan hartuta, etorkizunean zer gertatuko den jakiten laguntzen dutenak, hartara, hori gertatzeko edo ez gertatzeko erabakirik egokiena

hartzeko. Adibidez, posible da aldez aurretik jakitea zein izango den oliba olioaren ekoizpena, aurreko kanpainetan gertatu zenari buruzko datu posible guztiak ditugunean. Meteorologiari, ingurumen baldintzei, lurraren ezaugarriei, hezetasunari, ongarriei, izurriteei eta abarri buruzko datu kopuru handiak izanez gero, egungo informazioan oinarrituta, bilduko den oliba kantitatea eta kalitatea aurreikus ditzakegu. Adibide sinple bat dirudien arren, alegia, adibidez, Excel tresnan eskuragarri dagoen analisiarekin alderdi horiek jakin ahal izatea (datuen analisiaren atalean oinarrizko hainbat analisi tresna dauzkagu, hala nola korrelazioa, batezbestekoak, histogramak, erregresioa, estatistika deskriptiboak, kobariantza, etab.), nahiko ohikoa da tresna konplexuagoak eta neurrira garatutakoak erabiltzea, sistema motaren arabera.

Adimen artifizialaren eta datu meatzaritzaren arteko erlazioa

Datu meatzaritzaren prozesuko etapak gauzatuta (hala nola meatzaritza prozesuaren helburua zehaztea eta datuak araztea, aztertzea edo aurreprozesatzea), eta datu meatzaritzako lana egingo den datu multzoa zehaztuta, datu meatzaritzako lan horretan behar edo erabiliko da adimen artifiziala. Horri ikaskuntza automatikoa esaten zaio, eta gainbegiratua izan daiteke edo gainbegiratu gabea.

Ikaskuntza gainbegiratuan gehien erabiltzen den teknika sare neuronalak dira. Bertan, datuak bi multzotan banatzen dira eta sareari bere datuak sailkatzen "ikasten" uzten zaio; sarea entrenatzen da datuak sailkatzeko. **Bestalde**, **gainbegiratu gabeko ikaskuntzan** teknikarik ohikoena algoritmo genetikoa da, zeinean ez baita gainbegiratzen ez duelako ezer irakasten; algoritmoa datu multzoan exekutatzen da eta datuen arteko erlazio ezkutuak aurkitu arte itxaroten da.

Datu bolumen handiak eta biga data adimen artifizialaren parte dira, prozesatu daitekeen informazioa edukitzea dakarren heinean. Adimen artifizialak datuak aztertzen ditu gizakiak gauza ez diren moduan; guretzat, pertsona gehiegi konparatu beharko lirateke, eta informazio puntu gehiegiri begiratu beharko litzaieke. Hala ere, adimen artifizialaren soluzioek patroiak aurkitzen dituzte, are gizakiei begiratzea otuko ez litzaiekeen lekuan ere. Joera berriak aurki ditzakete sare sozialetako datuetan, finantza datuetan eta are datu

geografikoetan ere. Adibidez, adimen artifizialak jakin dezake norbaitek produktu bat erostea probablea den, bere joera politikoen arabera; horretarako, sare sozialen profilei begiratu eta horiek big dataren bidez duen informazio guztiarekin alderatu besterik ez du egin behar; datuak dira adimen artifiziala funtzionamenduan mantentzen duen erregaia. Gainera, adimen artifizialak informazioa biltzen du patroiak bilatzen dituen bitartean, eta informazio hori informazioz betetako datu baseetara gehitzen da: big dataren azpiegitura. Horrela, big datak eta adimen artifizialak elkarri laguntzen diote analisi makina ahaltsu bat sortzeko. Adibidez, gustatu zaizun Netflixeko telesail bat gomendatu badizute noizbait, plataformaren adimen artifizialak zure kontsumo datuak erabili dituelako da.

Datuen pribatutasuna, adimen artifizialaren erabilerari lotuta; datu meatzaritza

Gure identitate digitala eta Interneten nabigatzeko ohiturak cookieen bidez erregistratzen dira, guk horretarako baimena emanda, eta hirugarrenei informazio hori eskuratzeko aukera ematen diegu. Hirugarren horiek, normalean, datu meatzaritzako eta adimen artifizialeko teknikak lantzen eta garatzen dituzten enpresak dira, gure interesekoak izan daitezkeen eskaintzak, produktuak, sustapenak edo zerbitzuak eskaintzeko. Gainera, sare sozialetan edo gure datuen baimenean partekatzen dugun informazioaren arabera, eskaintza, produktu edo informazio gehiago edo gutxiago aurkituko dugu Interneten. Ildo horretatik, gure interesekoak izan daitezkeen produktuak eskainiko dizkigute, hori nola edo zergatik gertatzen den jakin ez dakigula. Baina denok dakigu nola erabiltzen diren gure sare sozialetako lehentasunak.

Esandakoaren kontrara, Datuak Babesteko Erregelamendu Orokorra dago, gure informazio partikularra besteek erabiltzetik babesten duena edo babestu beharko lukeena. Ildo horretatik, datu meatzaritzan nahiz adimen artifizialean izandako aldaketa teknologikoen eta aurrerapenen aurrean, teknologia horien aurrean izan dezakegun babesgabetasunerako irtenbideak edo erantzunak proposatzen ari dira.

Zehazki, Datuak Babesteko Espainiako Agentziak argitara eman du ***adimen artifiziala erabiltzen duten produktuak eta zerbitzuak Datuak Babesteko Erregelamendu Orokorrera egokitzeko gida*** (*e.digitall.org.es/adaptacion-rgdp*). Dokumentu horren aztergaia da arazo jakin eta mugatu baterako konponbideak garatzen dituzten adimen artifizialeko zatiak dituzten datuen tratamenduak datuen babeserako erregelamendura egokitzea, eta ez dio heltzen, oro har, adimen artifizialaren garapenari, teknologia gisa, ezta horretan inplikatutako ikerketa prozesuei ere.

Programetan edo datu tratamenduetan adimen artifizialeko elementuak sartzen dituzten edo horiei euskarria ematen dieten sistemetako arduradunei eta garatzaileei zuzenduta dago gida; izan ere, baliteke elementu horiek sistemaren bizi zikloaren fase edo etapa desberdinetan datu pertsonalak tratatzea, eta, beraz, DBEOren betebeharrak bete behar dituzte. Gainera, datu pertsonalen tratamenduaren arduradunaren eta datu horiekin adimen artifiziala garatzeko interesa izan dezaketen hirugarrenen artean ezar litezkeen harremanak aztertzen dira.

Teknologia horiek tratamendua DBEOra egokitzen dela bermatzeko eta frogatzeko bete behar dituzten baldintzak jasotzen dira gidan. Baldintza horien artean daude, besteak beste, datuen tratamendurako legitimazioa, prozesatutako eta sortutako informazioa, eskubideen erabilera eta erabaki automatizatuak hartzea. Dokumentuak, halaber, alderdi hauek lantzen ditu: informazioaren zehaztasuna, ahalik eta datu gutxien erabiltzea, adimen artifiziala aplikatzearen emaitzen inpaktuen ebaluazioa eta datuen tratamenduaren proportzionaltasunaren azterketa. Gainera, adimen artifizialean oinarritutako teknologien erabilerak datuen nazioarteko transferentziak eragiteko aukera aztertzen du.

Azken batean, Agentziak agerian utzi du adimen artifiziala erabiltzen duten datuen tratamenduak egiten dituzten teknologiak merkatuan jartzeak kalitateko eta pribatutasuneko bermeak aplikatzea eskatzen duela, eta adimen artifizialaren ereduek heldutasun maila jakin bat izan behar dutela, tratamenduak objektiboki egokiak diren eta sor daitezkeen arriskuak kudeatzeko neurriak hartu diren zehaztu ahal izateko.

Informazio gehiago

Zer da adimen artifiziala eta nola erabiltzen da? Europako Parlamentua. *e.digitall.org.es/inteligencia-artificial-uso*

Datu pertsonalak babestea. Espainiako Administrazio Publikoaren Institutua. *e.digitall.org.es/proteccion-datos-sede*

Big data, pribatutasuna eta datuen babesa. Datuak Babesteko Espainiako Agentzia. *e-digitall.org.es/big-data*

Adimen artifizialeko produktuak eta zerbitzuak DBEOra egokitzeko gida. Datuak Babesteko Espainiako Agentzia. *e.digitall.org.es/adecuacion-rgdp*

Segurtasuna

C2 maila 4.2 Datu pertsonalen eta pribatutasunaren babesa

Delitu informatikoetan sakontzea

Delitu informatikoetan sakontzea

Sistema informatikoen aurkako delituak edo IKTak

"Delitu informatikoak" edo "ziberdelituak" esamoldeak ez dira agertzen Espainiako Zigor Kodean. Hala ere, horietan, bi delitu kategoria hauek sartu ohi dira:

1 | Delitu jardueraren xedea dira sistema informatikoak edo IKTak.
2 | Delitu jardueran informatika edo IKTak modu erabakigarrian baliatu dira.

DELITU INFORMATIKOAK

Bideo honetan, bi kategorietan sar daitezkeen delitu garrantzitsuenak aztertu dira, modu generikoan eta sintetikoan, eta horren guztiaren adibideak eman dira.
e.digitall.org.es/A4C42C2V07

Osagarri gisa, dokumentu honetan xehetasun handiagoz jasoko dira delitu horietako bakoitzean sar daitezkeen jokabideak, delitu horiek definitzen edo tipifikatzen dituzten Zigor Kodeko manuak adierazita. Definizio edo mota horiek funtsezkoak dira; izan ere, jokabide bat zigortu ahal izateko, horietara zehatz-mehatz doitu behar da. Betekizunen bat falta bada, ezingo da zehatu.

OHARRA

Birus bat programatu eta besterik gabe nire ordenagailuan gordetzen badut, ez dago deliturik, Zigor Kodearen definizioaren arabera, delituren batean baliatzeko asmoz egina izan behar baitu.

ADI

Jokabide bat zehatu ahal izateko, Zigor Kodean jasotako definiziora edo motara zehatz-mehatz doitu behar da.

Aipatutako lehen kategorian, azpiepigrafe hauetan zerrendatzen diren delituak sar daitezke:

Kalte delituak, sabotaje informatikoa eta zerbitzu ukatzearen bidezko erasoak

"Edozein bide erabilita, baimenik gabe eta modu larrian beste batzuen datu informatikoak, programa informatikoak edo agiri elektronikoak ezabatu, kaltetu, degradatu, aldatu, kendu edo sartuezin bihurtzen dituenari, eragindako emaitza larria denean" (*Zigor Kodearen 264. artikulua*).

Datu, programa edo sistema informatikoetan baimenik gabe sartzearen delituak

"...baimenik gabe, hirugarren baten kalterako, izaera pertsonaleko edo familiako inoren datu erreserbatuak harrapatu, erabili nahiz aldatzen dituenari, betiere erregistraturik daudenean fitxategi edo euskarri informatiko, elektroniko zein telematikoetan, edo beste edozein motatako artxibo nahiz erregistro publiko edo pribatuetan" (*Zigor Kodearen 197.2 artikulua*).

Euskarri informatiko edo elektronikoetan artxibatutako enpresa sekretuak ezagutaraztearen delituak

"Norbaitek, enpresaren sekretu bat ezagutarazteko, edozein bide erabiliz, sekretu horri buruzko datuak, agiri idatzi zein elektronikoak, euskarri informatikoak edo bestelako objektuak harrapatzen baditu, edo pertsona horrek 197. artikuluaren 1. paragrafoan adierazitako bide edo tresnetatik bat erabiltzen badu..." (*Zigor Kodearen 278. artikulua*).

Irrati difusioko zerbitzuen edo zerbitzu interaktiboen aurkako delituak

"...zerbitzu-emailearen baimenik gabe eta helburu komertzialekin, soinuzko edo irudizko irrati difusioko zerbitzu baterako edo bide elektronikoz emandako urruneko zerbitzu interaktiboetarako sarbide ulergarria ematen duenari, edo horietarako baldintzapeko sarbidea ematen duenari, zerbitzu independentetzat hartuta, honako hauen bidez:

1. Europar Batasuneko beste estatu kide batean baimendu gabeko ekipamendu edo programa informatikoak fabrikatzea, inportatzea, banatzea, bide elektronikoz eskuragarri jartzea, saltzea, alokatzea edo edukitzea, sarbide hori ahalbidetzeko diseinatuta edo egokituta egonik.

2. 1. apartatuan aipatutako ekipamendu edo programa informatikoak instalatzea, mantentzea edo ordeztea" (*Zigor Kodearen 286. artikulua*).

Delitu jardueran informatika edo IKTak modu erabakigarrian baliatu dira

Iruzur delituak

"1. [...] a) Irabazi-asmoarekin, informazio sistema baten funtzionamendua bidegabe oztopatuz edo eragotziz, edo datu informatikoak sartu, aldatu, ezabatu, transmititu edo behar ez bezala kenduz, edo bestelako manipulazio informatikoak edo antzeko azpikeriak baliatuz, edozein ondarezko aktiboren baimenik gabeko transferentzia lortzen dutenak, beste baten kalterako.

b) Kreditu edo zordunketa txartelak, bidaia txekeak edo eskudirua ez den beste edozein ordainketa tresna material edo immmaterial edo horietako edozeinetan dauden datuak iruzurrez erabiliz, titularraren edo hirugarren baten kalterako edozein motatako eragiketak egiten dituztenak".

«2. [...] a) Artikulu honetan adierazitako iruzurrak egiteko, hirugarrenei gailu, tresna edo datu edo programa informatikoak, edo berariaz diseinatutako edo egokitutako beste edozein bitarteko fabrikatzen, inportatzen, lortzen, edukitzen, garraiatzen, merkaturatzen edo beste modu batera ematen dizkietenak". (*Zigor Kodearen 249. artikulua*).

Adingabeen/desgaitasunen bat duten pertsonen jazarpen eta galbideratze delituak; edo haurren/desgaitasunen bat duten pertsonen pornografiari buruzkoak

"Interneten, telefonoaren edo informazioaren eta komunikazioaren beste edozein teknologiaren bidez hamasei urteko adingabe batekin harremanetan jartzen dena eta harekin topaketa bat hitzartzea proposatzen duena, 181. artikuluan (sexu izaerako egintzak gauzatzea) eta 189. artikuluan (pornografia) deskribatutako edozein delitu egiteko..." (*Zigor Kodearen 183. artikulua*).

Jazarpen delituak

«1. ...pertsona bati behin eta berriro jazartzen zaionari, legez baimenduta egon gabe, honako jokaera hauetako bat izaten badu, eta jokaera horrek haren eguneroko bizitza era larrian nahasten badu: [...]

2.a Edozein komunikazio-bideren bidez [...], pertsona harekin harremanetan jartzea edo jartzen saiatzea.

3.a Pertsona horren datu pertsonalak bidegabe erabiliz, produktu edo salgaiak eskuratzea, zerbitzuak kontratatzea, edo hirugarren pertsona batzuk harekin harremanetan jarraraztea. [...]

5. Titularraren baimenik gabe, pertsona baten irudia erabiltzen duena sare sozialetan, harremanetarako orrietan edo edozein komunikazio-bidetan iragarkiak egiteko edo profil faltsuak irekitzeko, hura jazarpen edo umiliazio egoeran jarriz..."(*Zigor Kodearen 172 ter artikulua*).

Jabetza intelektualaren aurkako delituak

"...zuzeneko edo zeharkako onura ekonomikoa lortzeko asmoz, eta hirugarren baten kaltean, jabetza intelektualaren eskubideen titularren edo lagapen-hartzaileen baimenik gabe, informazio-gizartean zerbitzuak ematean, era aktibo eta ez-neutralean, eta tratamendu tekniko hutsera mugatu gabe, jabetza intelektualeko lanak edo prestazioak Internet bidez eskuratzen edo lokalizatzen laguntzen duenari; eta, bereziki, lehen aipatutako lan edo edukietan sartzeko estekak biltzen dituzten sailkapen-zerrenda ordenatuak ematen dituenari, nahiz eta esteka horiek hasiera batean zerbitzu horien hartzaileek eman" (*Zigor Kodearen 270. artikulua*).

Informazio gehiago

10/1995 Lege Organikoa, azaroaren 23koa, Zigor Kodeari buruzkoa.
e.digitall.org.es/boe-25444

Barne Ministerioa. Espainiako ziberkriminalitateari buruzko txostena 2021.
e.digitall.org.es/estadisticas

DigitAll

Segurtasuna

4.3 OSASUNAREN ETA ONGIZATEAREN BABESA

Segurtasuna

C2 maila 4.3 Osasunaren eta ongizatearen babesa

Interneteko iturri fidagarrien bilduma, osasun arloari dagokionez

Interneteko iturri fidagarrien bilduma, osasun arloari dagokionez

Interneteko iturri fidagarrien bilduma

Dokumentu honetan bildu ditugu osasunarekin lotutako gaiak kontsultatzeko Interneteko iturri fidagarri batzuk. Horregatik, baliagarriak izan daitezkeen baliabide batzuk hautatu ditugu, eta, batez ere, beste iturri batzuk hautatzeko erreferentziatzat har ditzazun.

Medline

MedlinePlus pazienteentzako, familientzako eta lagunentzako online informazio zerbitzua da. Osasunari eta ongizateari buruzko kalitatezko informazioa ematea du helburu, datu fidagarriak eta ulerterrazak eskainiz.

Osasun arloko iturri horren informazioa AEBko Medikuntza Liburutegi Nazionalean jasota dago (NLM), munduko mediku-liburutegirik handiena, AEBetako Osasun Institutu Nazionaletako kide dena (NIH).

Webgunerako sarbidea doakoa da, eta edozein gailu erabili daiteke. Ingelesez eta gaztelaniaz dago.

Salupedia

Salupedia online entziklopedia mediko bat da, eta sektoreko profesionalen bermea duen Interneteko informazio sanitarioa berreskuratu, sailkatu eta antolatzen du.

Sektoreko profesionalek egiten dituzten argitalpenetan oinarritzen da, eta pazienteei, senideei eta herritarrei sarean dauden osasun edukiak gomendatzen dizkie.

Horrela, herritarrentzat, profesionalek gomendatutako informazio fidagarria eskuratzeko gunea da; profesionalentzat, berriz, konfiantzazko leku bat da, pazienteei informazioa preskribatzeko erabili dezaketena.

Sendagaien eta Osasun Produktuen Espainiako Agentzia

Sendagaien eta Osasun Produktuen Espainiako Agentzia (AEMPS) Osasun Ministerioari atxikitako estatu agentzia bat da.

Sendagaien eta produktu sanitarioen kalitatea, segurtasuna, eraginkortasuna eta informazio zuzena bermatzea du helburu, hasi ikertzen direnetik eta erabiltzen diren arte.

Bere webgunean medikamentuei, produktu sanitarioei, kosmetikoei, norberaren zaintzarako produktuei eta biozidei buruzko informazioa eskaintzen du, ezagutza zientifiko-teknikoa sustatuz.

Familia Medikuntzako eta Medikuntza Komunitarioko Espainiako Elkartea

Elkarte zientifiko-medikoa da, irabazi-asmorik gabea, eta Espainian familia medikuntza eta medikuntza komunitarioa egoki garatzea zaintzen du. Gaur egun, Espainiako zientzia elkarterik handiena da.

Familia Medikuntzako eta Medikuntza Komunitarioko Espainiako Elkartea Espainiako familia medikuntzako eta medikuntza komunitarioko 17 elkarteek osatzen dute, eta familia medikuntzan 20.000 bazkide espezialista baino gehiago biltzen ditu.

Bere web orriaren bidez, hainbat gaitasun klinikoren arabera iragazitako bilaketak egin daitezke (ekografia, kardiobaskularra, dermatologia, infekzioak...), zientzia eta osasun arloetako argitalpenak topatu, eta sektoreko ekitaldien eta medikuntzari buruzko gaurkotasuneko beste gai batzuen berri jakin daiteke.

Lehen Mailako Arretako Medikuen Espainiako Elkartea

Lehen Mailako Arretako Medikuen Espainiako Elkarteak (SEMERGEN) webgune bat sortu du pazienteari medikuntzaren eta osasunaren arloko hainbat gairi buruzko informazioa eta prestakuntza emateko, irizpide mediko egoki, adostu eta dokumentatuen arabera.

Pacientes Semergen izenda du webguneak, eta edozein internautaren eskura dagoen gehiegizko informazio medikoari aurre egiteko sortu da, informazio hori herritarren osasunerako arriskutsua izan daiteke eta.

Bertan, galdera eta erantzunen atal bat dago, profesionalek zuzenean erantzuten dutena, baita gaixotasun arrunten atal bat ere, osasunarekin lotutako berrien atalaz gain.

PiCuida

PiCuida Andaluziako Zainketen Sarea da, Andaluziako Zainketen Estrategiak sortua (Andaluziako Osasun Zerbitzua). Bere webgune ofizialean osasun arloko hainbat gairi buruzko informazio zientifikoa eta medikoa dago.

Plataformak liburutegi bat du, eta horretan bilaketak egin daitezke nahi den gako hitzaren arabera, edo aurrez ezarritako sektoreko kategoria baten arabera (haurren arreta, zainketak eta osasun mentala, etika eta zainketak, galdera klinikoak...).

Informazio gehiago

Osasunaren Mundu Erakundearen (OME) webgune ofizialak bilatzaile alfabetiko bat du, eta, bertan, hainbat gaixotasun edo patologia bila daitezke, hasierako letraren arabera. Gainera, osasun arloko argitalpen, komunikazio edo artikuluen atal bat ere badu.

who.int/es

Orrialde bat fidagarria ote den jakiteko gomendioak

Internetek informazio iturri askotarako sarbidea ematen digu askotariko gaietan, hala nola osasunean. Hala ere, maila honetako 03 bideoan azaldutakoari jarraikiz, eskura dauzkagun osasunari buruzko webgune guztiak ez dira fidagarriak. Interneten osasunari buruzko informazio fidagarria hautatzea eta biltzea garrantzitsua da gure osasun mentalean zenbait arazo saihesteko. Baina zer jarraibide bete behar dugu orri bat fidagarria ote den jakiteko? Jarraian, orri horiek bereizteko bete beharreko oinarrizko printzipio batzuk azalduko ditugu.

OHARRA

Interneteko informazioaren fidagarritasuna web orri horretan eskainitako informazioa baliozkoa eta kalitatezkoa izateko probabilitatea da, batez ere iturri zientifikoetan oinarrituta. Informazio gehiago nahi izanez gero, bideoa berriro ikusi dezakezu: ***Interneteko osasun informazioaren fidagarritasuna***.

INTERNETEKO OSASUN INFORMAZIOAREN FIDAGARRITASUNA

e.digitall.org.es/A4C43C2V03

Webgunearen babeslea

Eskura dugun informazioa idazten duen egileari buruzko informazio garrantzitsua ezagutzeaz gain. Web orri hau nork babesten duen ere jakin behar da. Beraz, orrialde horren URLak informazio baliagarria eskain diezaguke alde horretatik. Adibidez: .gov (gobernuaren agentziak adierazten ditu), .edu (hezkuntza erakundeak identifikatzen ditu), .org (irabazi-asmorik gabeko erakundeak definitzen ditu) eta .com (web orriak merkataritza helburuak dituela adierazten du).

Pribatutasun politika

Webgune guztiek pribatutasun politika bat izan beharko lukete ikusgai. Ildo horretatik, bisitatu ditzakegun webgune askok cookieak erabiltzen dituzte, eta horiek bisitarien pribatutasuna uki dezakete orri horietan. Hori saihesteko, cookieen erabilera desaktiba daiteke Interneteko nabigatzailearen bidez.

Interneteko osasun informazioaren fidagarritasuna

Garrantzitsua da informazio hori nola bilduko den jakitea. Webgune seguru gehienek “http” bat izaten dute, amaieran “s” bat duena. Izan ere, orri askok erabiltzailea eta pasahitza eskatzen dute.

Gogoratu gai honekin lotutako jarraibide hauek: erabili pasahitz seguru bat, erabili autentifikazio faktoreak, ez partekatu zure osasunari buruzko informazio pribatua erabilera publikoko wifi sare batean.

Informazio gehiago

Web orri bat fidagarria ote den jakiten lagun diezaguketen hainbat egiaztapen zerrenda daude. Jarraian, osasunari buruzko web orriak erabiltzeko garaian norberak bere buruari egin beharko lizkiokeen galdera batzuk azalduko ditugu:

- Web orria erakunde, erakunde edo gobernuren batena al da? Nor da osasunari buruzko informazio honen egilea?

- Web orri honen helburua da? Zertarako sortu zen? web orri hau?

- Zergatik sortu zen webgunea? Argi al dago xedea edo helburua webguneko babeslearen?

- Web orriak aipatzen al du harremanetarako pertsonarik edo erreferentziazko talderik?

- Noiz eguneratu zen azken aldiz webgunea?
- Zure pribatutasunari buruzko informazioa babestuta dago?
- Mirarizko sendatzeei buruzko informazioa ematen du orrialde honek?

Fidagarriak ez diren osasun arloko orrien adibideak

Osasunari buruzko web orri baten fidagarritasuna ezagutzeko hainbat puntu garrantzitsu aipatu ondoren, hona fidagarriak ez diren osasun arloko zenbait web orri.

- Nutrizio gaiei buruzko blogak eta orriak, obesitatearen aurka borrokatzeko dietak eta botikak eskaintzen dituztenak, azkenean mirarizkoak ez direnak eta osasun egoeran eragin negatiboa izan dezaketenak. Gainera, horrelako guneek ez dute edukiaren egilea zehazten.
- Emakumearen osasunarekin lotutako web orriak. Gune horietan, emakumearen bizitzako une jakin batzuetan kontuan hartu beharreko konponbideak eta oharrak jasotzen dira. Gainera, produktuak ere saltzen dituzte. Oro har, prestakuntza medikorik ez duten pertsonek kudeatzen dituzte orri horiek.

Informazio gehiago

- medlineplus.gov/spanish
- who.int/es
- salupedia.org
- aemps.gob.es
- semfyc.es/medikoak
- pacientessemergen.es
- picuida.es
- e.digitall.org.es/informacion-salud
- e.digitall.org.es/bulos-salud

DigitAll

Segurtasuna

4.4 INGURUMENAREN BABESA

Segurtasuna

C2 maila 4.4 Ingurumenaren babesa

GJHak eta teknologia digitalak

GJHak eta teknologia digitalak

Sarrera

Dokumentu honetan, C1 eta C2 mailetako GJHak eta Teknologia digitalak (I. eta II.) bideoetan sartu diren kontzeptuak zehatzago aztertuko dira.

GJHAK ETA TEKNOLOGIA DIGITALAK (I)

Teknologia digitalarekin lotutako arazoen eta erronken egungo egoera, GJHak betetzeari dagokionez.
e.digitall.org.es/A4C44C1V05

GJHAK ETA TEKNOLOGIA DIGITALAK (II)

Teknologia digitalen balizko aplikazioak, GJHak betetzeari dagokionez.
e.digitall.org.es/A4C44C2V05

Helburua da 2015ean Nazio Batuetako estatu kideek onartutako Garapen Jasangarrirako Helburuei (GJH) buruzko informazio gehiago ematea.

Dokumentu honetan, batez ere, GJHen garrantzia ezagutaraziko da, zein den haien helburua eta aurre egin beharreko erronka horiek zer eragin duten eta zer eragin izango duten planetan, gizakiengan, oparotasunean, bakean eta nazioarteko aliantzetan.

Ikusiko dugu *Garapen Jasangarrirako 2030 Agenda*, NBEren Batzar Nagusiak onartua (2015), 17 GJHen xedeak ezartzeko programak gidatzen dituen ekintza plana dela: elkarrekin lotutako 169 xede dira, ekonomiaren, gizartearen eta ingurumenaren esparruak optimizatzera bideratuak (jasangarritasuna), eta 2030. urtea da helburuak lortzeko data.

Herrialdeek GJHekin hartutako konpromisoak mugarri bat ezartzen du nazioarteko apustuan eta baliabideen mobilizazioan, munduak egun dituen erronkarik handienak lortzeko: gosea, pobrezia edo desberdintasun soziala desagerraraztetik hasi eta osasunerako, hezkuntzarako eta lan duinerako sarbide unibertsala izateraino eta datozen belaunaldiek natura baliabideak eskuratu ahal izateraino.

Gainera, emango den informazioaren bidez, ulertuko dugu aurrerabidea ekonomia zirkularrean oinarritu beste aukerarik ez dagoela, erronka horiek lortuko badira; hau da, aurrerabidea eta ingurumen eta gizarte babesa, natura baliabideen kontsumo jasangarria eta sortutako hondakinen kudeaketa eta birziklatze egokia batera joan behar dira.

Azken batean, ulertuko dugu GJHek hauxe jartzen dutela agerian: *Ekonomia* eta *Gizartea* ezinbestean gure planetako *Biosfera*ren jasangarritasunaren mende dauden alderdi gisa ikusi behar ditugu.

Halaber, ulertuko dugu garrantzitsua dela jasangarritasun printzipioak aplikatzea teknologia digitalaren fabrikazioan, digitalizazio jasangarriaren prozesuan funtsezko tresna izan daitezen.

Azkenik, digitalizazio jasangarriak GJHen ezarpenean duen ekarpena erakutsiko dugu: kontuan izan behar dugu teknologia digitala XXI. mendeko gizarteko enpresa, industria, enpresa eta giza jarduera guztietan ageri dela.

GJHen *Eztei Tarta*

Bideo sortarekin jakin dugu teknologia digitalak bizimolde berri bateranzko bidea ireki digula, eta bizimolde hori etengabeko bilakaeran dagoen eraldaketa digitalean oinarrituta dagoela. Zalantzarik gabe, gizartearen zerbitzura dagoen berrikuntza digitalak gure bizi sistema errazten du. Baina, egia da, halaber, haiek eraldaketa digitalean erabiltzeak gailu digitalen eskari eskerga dakarrela, eta gailu horiek fabrikatu, erabili eta kontsumitzea munduko natura erreserbak arriskuak jartzen ari da.

Bi alderdiak hartu behar ditugu gogoan:

- Batetik, eraldaketa digitalaren onura, gure aurrerabidearen jasangarritasunean laguntzeko.
- Bestetik, eraldaketa digitalaren ondoriozko ingurumen inpaktua.

Eta, hain zuzen ere, giza aurrerabidearen jasangarritasunaren eta jasangarritasunik ezaren eta egungo baliabideen arteko ustezko bateraezintasun hori dela eta, besteak beste, eraldaketa digitala, *Garapen Jasangarrirako 2030 Agendak* (2015) hainbat helburu ezartzen ditu gure eta etorkizuneko belaunaldien bizi sistema hobetzeko.

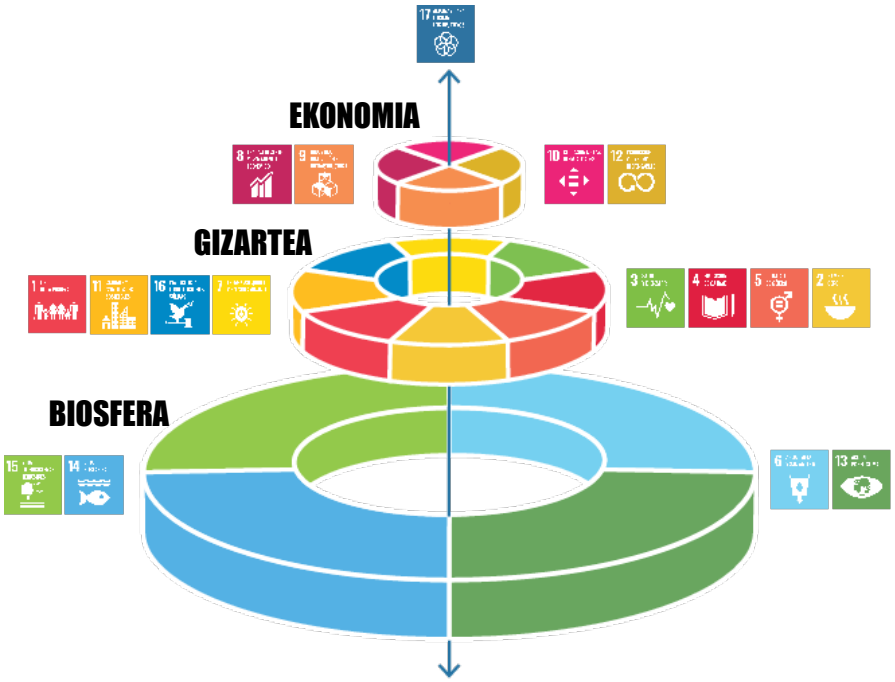
Garapen Jasangarrirako Helburuak (GJH) gizadiaren aurrerabidea gidatzeko ezarri dira, kontuan hartuta aurrerabideak integratzailea, inklusiboa eta unibertsalki bidezkoa eta ekitatiboa izan behar duela. Horretarako, NBEko herrialdeek konpromiso hau hartu zuten: 2030a baino lehen gure gizarteak ongizatean eta bizi kalitatean aurrera egingo du, baina ingurumenaren eta ekonomiaren aldetik jasangarria izateko betebeharra alde batera utzi gabe.

GJHek mundu mailako erronken alde egiten dute, eta horiek testuinguru jakin bat dute. GJHak lortuko badira, erakunde publikoen, esparru politikoaren, industria eta enpresa ehun produktiboaren eta gutako bakoitzaren inplikazioa beharrezkoa da.

Ezinbestean ezagutarazi behar ziren GJHak, ulertu ahal izateko zeinen funtsezkoak diren eta horietan inplikatzeak gizarte, ekonomia eta ingurumen alderdietan zenbateko garrantzia duen. GJHei "begiratzeko" modu bat izan behar genuen, argi izateko zer dagokion horretan guztian gure gizarteari, alegia, guri, gizabanako eta kontsumitzaile garenoi, eta gure bizimodua zer-nola datorren bat horrekin guztiarekin.

Horretarako, Stockholmeko Unibertsitateko Erresilientzia Zentroak GJHei begiratzeko modu berri bat aurkeztu zuen

2016an, eta "GJHen Eztei Tarta" izena eman zion (2016). 2016ko *Stockholm EAT Food Forum* ekitaldian aurkeztu zen, mundu mailan osasunaren eta jasangarritasunaren arloetako erronka garrantzitsuenetako bat elikadurarena dela ikusarazteko.



Ilustrazio honek agerian jartzen du **Ekonomia** eta **Gizartea** ezinbestean gure planetako **Biosfera**ren jasangarritasunaren mende dauden alderdi gisa ikusi behar direla. Ikuspegi berritzailea da, egungo ikuspegi sektorialetik aldentzen dena; alegia, garapen soziala, ekonomikoa eta ekologikoa zati bereizitzat hartzen dituen ikuspegitik.

Tarta horren oinarrian, ingurumeneko GJHak daude, hau da, gainerako GJHei eusten dietenak tartak behea ez jotzeko. Ez geneukake ezer, ez bageneuzka Ur garbia eta Saneamendua (6. GJH), Itsaspeko bizitza (14. GJH), Klimaren aldeko ekintza (13. GJH) eta Lehorreko ekosistemetako bizitza (15. GJH).

Tartaren lehen mailan daude gure bizitzari zentzua ematen dioten GJHak: pertsonak eta gizartea. Gizateria bidezkoa izango da hauek lortzen dituguneanean: Pobrezia desagerraraztea (1. GJH), Goserik ez (2. GJH) egotea, Osasuna eta Ongizatea (3. GJH) denon eskura izatea, Kalitateko Hezkuntza (4. GJH) denon eskura izatea, Energia irisgarria eta ez-kutsagarria (7. GJH) denon eskura izatea eta Hiri eta Komunitate jasangarriak (11. GJH) bizileku izatea, hori guztia Genero Berdintasuna (5. GJH) guztiz lortu den inguruanean.

Eta non geratzen da ekonomia? Tartaren hirugarren maila egokitu zaio; izan ere, ekonomiarekin lotuta Daude Lan duina eta Hazkunde ekonomikoa (8. GJH), Industria, Berrikuntza eta Azpiegitura (9. GJH), Ekoizpen eta kontsumo arduratsuak (12. GJH) eta Desberdintasunak murriztea (10. GJH).

GJH horiek guztiak lortuko badira, nazioarteko inplikazio eta ekintza eraginkorra ezinbestekoak dira. Beraz, GJHak lortzeko aliantzak (17. GJH) erronka horiei guztiei eusten dien eta horiek bermatzen dituen helburu koordinatzaile gisa ezartzen dira.

Ekintza Digitalerako GJHen 5Pak

Ikusi dugunez, GJHek gure bizi balioentzat oso garrantzitsuak diren erronken alde apustu egiten dute, gure *planeta*, *pertsonak* eta haien *oparotasuna* babestean oinarritzen baitira, eta, aldi berean, *unibertsalizazioa* zaintzen dute, guztiontzako *bakea*ren babesean, nazioarteko *aliantzak* horretarako tresna izanik.

Euskaraz termino horiek *p* letraz hasten ez diren arren, erronka horiek 2030 Agendaren 5P gisa ezagutarazi dira ingelesezko terminoengatik: *Planet* (planeta), *People* (pertsonak), *Prosperity* (oparotasuna), *Peace* (bakea) eta *Partnership* (aliantzak).

Ikus dezagun zergatik eta zer harreman duten ekintza digitalarekin. Hasteko, P horietako bakoitzean biltzen diren GJHak bereiziko ditugu:

- **Pertsonak** (***People***): erraz identifikatzen ditugu pertsonak ardatz dituzten GJHak. 1. GJH Pobrezia desagerraraztea, 2. GJH Goserik ez, 3. GJH Osasuna eta Ongizatea, 4. GJH Kalitatezko hezkuntza eta 5. GJH Genero berdintasuna.
- **Planeta** (***Planet***): ingurumenaren babesa gure existentziaren beraren oinarria da, eta ez da ezer posible izango horrekin lotutako GJHak lortu ezean: 6. GJH Ur garbia eta Saneamendua, 12. GJH Ekoizpen eta kontsumo arduratsuak, 13. GJH Klimaren aldeko ekintza, 14. GJH Itsaspeko bizitza eta 15. GJH Lehorreko ekosistemetako bizitza.
- **Oparotasuna** (***Prosperity***): naturak eskaintzen digunarekin harmoniaz bizitzea izan behar dugu helburu, GJH hauekin koherenteak izateko: 7. GJH Energia irisgarria eta ez-kutsagarria, 8. GJH Lan duina eta Hazkunde ekonomikoa, 9. GJH Industria, Berrikuntza eta Azpiegitura, 10. GJH Desberdintasunak murriztea eta 11. GJH Hiri eta komunitate jasangarriak.

- **Bakea** (***Peace***): zalantzarik gabe, gatazkak, gerrak, segurtasunik eza, erakunde ahulak eta desberdintasunak eta injustizia soziala dira garapen jasangarrirantz aurrera egiteko mehatxu larrienetako bat, eta egoera hori hobetzea du xede 16. GJHak (Bakea, Justizia eta Instituzio sendoak).
- **Aliantzak** (***Partnership***): 17. GJHak (GHJak lortzeko aliantzak) munduko liderren arteko lankidetza harremanak sustatzen ditu, finantzaketa eta ekintza koordinatua emateko nazioartean.

Gogora dezagun zeri esaten diogun digitalizazio jasangarri: gizarteak ingurumena, ekonomia zirkularra eta pertsonen ongizatea babestuz digitalizatzeko prozesua. Definizio hori irakurrita, erraz ikus dezakegu 5Pekiko erlazioren bat, baina ikus ditzagun adibide batzuk.

Has gaitezen teknologia digitalaren ingurumen inpaktuarekin. Bideoetan ikusi dugunez, ingurune digitalean egiten dugun edozein jarduerak inpaktuak sortzen ditu, bai berotegi efektuko gasen emisioak, bai gailu digitalak fabrikatzeko eta horiek funtzionatzeko azpiegituretarako ezinbestekoak diren natura baliabideen erabilera. Horri gehitu behar zaio prozesu osoak behar duen energia kontsumoa, bai eta sortzen dugun hondakin kopuru izugarria ere. Hondakin horiek behar bezala kudeatu behar dira, gizakien eta planetaren segurtasunerako ondorio kaltegarriak murrizteko eta eragozteko.

Kutsadura digitalak eragin zuzenekoa du GJHetan, bai horiek lortzea zailduz, bai erraztuz. Aztertzen ari garen gaiari dagokionez, GJHek edozein eragin negatiboz —tartean, kutsadura digitala— ohartarazten duten xedeak ezartzen dituzte, eta horiei galga jartzea eta etengabe arreta ematea eskatzen dute, prebenitzeko, minimizatzeko eta, ahal dela, saihesteko. 2010ean, Jonathan Koomey ikertzaileak adierazi zuen aurre egin beharko litzaiokeela gailu digitalen energia gastuaren goranzko joerari, gero eta efizienteagoak izan zitezen (Koomeyren legea, 2010), eta, horretarako, prozesuak hobetu behar zirela ekoizpena eta azpiegitura digitalak jasangarriak izateko, softwarea, hardwarea, sarbide sareak eta datu zentroak optimizatzea barne.

GJHekiko koherentzian oinarritutako trantsizio ekologikoan, teknologia digitala ez da behar operatiboa soilik, baizik eta, gainera, gaur egun eraldaketa digital jasangarria gauzatzeko aukera ematen duen tresna nagusia. EBren Estrategia Digitalak (2021), "*Iparrorratz Digitala 2030: Europaren ikuspegia Hamarkada Digitalerako*" dokumentuan, horretarako ikuspegi eta helburu zehatzak markatzen ditu: Gaitasun digitalak dituzten herritarrak (Gaitasun Digitalen Plan Nazionala. DigitAll), Zerbitzu publikoen digitalizazioa, Azpiegitura digital seguru eta jasangarriak eta Enpresen eraldaketa digitala.

Iparrorratz Digitala 2030 dokumentuan nabarmentzen da gailu digitalek jasangarritasuna eta trantsizio ekologikoa bultzatu behar dituztela, eta eskubide eta printzipio digitalak nabarmentzen ditu GJHei laguntzeko bide gisa, gizartearen, erakundeen eta enpresen inplikazioa eta babesa izanda. Honela adierazten du asmo hori: "*Politika digitalak aplikatu behar dira, eta horien bidez pertsonak eta enpresak gaitu, gizakian ardaztuta egon dadin etorkizuna digita, eta jasangarriagoa eta oparoagoa izan dadin*" (EB, 2021).

Bestalde, NBEren Munduko Itunak (2019) azaltzen du teknologia digitalak potentzial handia eskaintzen duela GJHen betetzea bizkortzeko eta horien inplementazio prozesuak murrizteko. Adibidez, kalitatezko informaziorako sarbidea eta datuen eskala handiko analisia eta bilketa (big data) sustatzeak eragin positiboa du GJH guztietan, besteak beste, hezkuntzako, osasuneko, elikadurako, enpleguko, aukera berdintasuneko eta abarreko gizarte zerbitzuak eskurago izateko, bai eta ingurumen edo ekonomia gaietan erabakiak hartzen laguntzeko ere.

Enpresa eta industria digitalizazioari esker, prozesuak modu jasangarrian optimizatu ahal izango dira, bai eta negozio modu berriak sortu ere. Horiek digitalizazioaren potentziala aprobetxatuko dute beren ingurumen aztarna murrizteko. Orobat, digitalizazioak mesede egingo die merkataritza elektronikoari, nekazaritza lanen optimizazioari zein osasun sistemei, besteak beste.

Beraz, gailu elektronikoak gero eta efizienteagoak eta jasangarriagoak izateak Ekintza Digitalari bultzada ematen dio, 2030 Agendako GJHak eta eraldaketa digitala lortzeko; alegia, "*gizarte osasuntsuagoa eta ekologikoagoa lortzeko*" (EB, 2021).

Informazio gehiago

Europako Parlamentua (2021). Brusela, 2021.3.9 COM(2021) 118 EBren Estrategia Digitala (2021), *Iparrorratz Digitala 2030: Europaren ikuspegia Hamarkada Digitalerako*. e.digitall.org.es/brujula-digital

Munduko Ituna, Espainiako Sarea (2019) Teknologiak GJHei laguntzeko zazpi modu. e.digitall.org.es/pacto-mundial

The SDGs wedding cake. Stockholm Resilience Centre. Stockholm University (2016). e.digitall.org.es/tarta-boda

NBEren Batzar Nagusia (2015). *Gure mundua eraldatzea: Garapen Jasangarrirako 2030 Agenda*. e.digitall.org.es/onu-agenda2030

NBEren GJHen komunikazio materialak (2015). e.digitall.org.es/materiales-ods

Koomey, J. et all. (2010) *Implications of Historical Trends in the Electrical Efficiency of Computing*. DOI:10.1109/MAHC.2010.28. Corpus ID: 8305701. e.digitall.org.es/koomey

Bestelako baliabideak:

- Stockholm EAT Food Forum (2016). e.digitall.org.es/2016-eat
- e.digitall.org.es/tarta-bbva
- e.digitall.org.es/5p

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

El material del proyecto DigitAll se distribuye bajo licencia CC BY-NC-SA 4.0. Puede obtener los detalles de la licencia completa en: https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es