DigitAll

Gaitasun
digitaletan
prestakuntza

4

Segurtasuna

DigitAll

Gaitasun
digitaletan
prestakuntza

Segurtasuna

C1 maila

AURKIBIDEA

DigitAll

Segurtasuna

4.1

GAILUEN BABESA

Segurtasuna

C1 maila 4.1 Gailuen babesa

Segurtasun-estandarrak enpresan

Segurtasun-estandarrak enpresan

Segurtasun-estandarrak

Segurtasun-estandar bat sistemen, datuen, azpiegituren edo prozesuen segurtasuna eta babesa bermatzeko ezarritako arauen eta jardunbide egokien multzo bat da. Informazioaren osotasuna, konfidentzialtasuna eta eskuragarritasuna auzitan jar ditzaketen arriskuak eta mehatxuak arintzeko helburuarekin garatzen dira estandar horiek.

Segurtasun-estandarrek hainbat arlo har ditzakete, hala nola segurtasun informatikoa, informazioaren segurtasuna, sareen segurtasuna, segurtasun fisikoa eta softwarearen garapenaren segurtasuna. Estandar horiek zehazten dute zer baldintza tekniko, kontrol, politika eta prozedura ezarri behar diren sistemak eta datuak modu eraginkorrean babestuta daudela ziurtatzeko.

Informazio gehiago

Segurtasun-estandar egokiak betetzeak erabiltzaileen, bezeroen eta merkataritza-bazkideen konfiantza bermatzen laguntzen du, eta segurtasun-gorabeherekin lotutako arriskuak murrizten ditu, hala nola baimenik gabe sartzea, datuak lapurtzea edo sistema etetea.

Munduan segurtasun-estandar ugari daude, eta, beraz, zein diren edo zenbat diren esatea oso zaila da, baina esan dezakegu hauek direla ezagunenak edo zabalduenak:

- **ISO/IEC, 27K familia** (*e.digitall.org.es/iso*): informazioaren segurtasunaren kudeaketarako nazioarteko estandarra. .
- **NIST SP 800** (*e.digitall.org.es/sp-800*): AEBko Estandar eta Teknologia Institutu Nazionalak (NIST) garatutako segurtasun-esparrua.
- **PCI DSS** (*e.digitall.org.es/pci*): ordainketa-txartelen industriarentzako datuen segurtasun-estandarra.
- **HIPAA** (*e.digitall.org.es/hipaa*): Aseguru Medikoaren Eramangarritasun eta Erantzukizunari buruzko Ameriketako Estatu Batuetako Legea, informazio medikoaren segurtasun- eta pribatutasun-betekizunak ezartzen dituena.
- **GDPR** (*e.digitall.org.es/gdpr*): Europar Batasuneko Datuak

Babesteko Erregelamendu Orokorra, EBko herritarren datuak babesteko eta haien pribatutasunerako arauak ezartzen dituena.

- **CIS Controls** (*e.digitall.org.es/cis*): informazio-sistemak babesten laguntzeko Interneteko Segurtasun Zentroak (CIS) garatutako segurtasun-kontrolen multzoa.

Segurtasun-estandarrak betetzen direla frogatzeko, estandar horren betekizuna ebaluatu eta egiaztatzen duen ziurtagiria lortu behar da. Garrantzitsua da azpimarratzea estandar guztiak ezin direla ziurtatu.

Segurtasuna ziurtatzeko prozesuak honako etapa hauek ditu:

1 | Hasierako ebaluazioa: segurtasun-antolaketaren, -sistemaren edo -prozesuaren ebaluazio sakona egiten da, ezarritako estandarrak eta betekizunak betetzen diren zehazteko. **2 | Kontrolak inplementatzea:** hasierako ebaluazioan gabeziak edo hobetu beharreko arloak identifikatzen badira, erakundeak kontrol eta segurtasun-neurri gehigarriak ezarri beharko ditu betekizunak betetzeko.

3 | Auditoretza: kanpoko auditore batek edo ziurtapen-erakunde independente batek segurtasun-sistemaren berrikuspen zehatza egiten du, ezarritako estandarrak eta irizpideak betetzen direla egiaztatzeko.

4 | Ziurtagiria ematea: antolaketak edo sistemak segurtasun-betekizunak behar bezala betetzen baditu, ezarritako segurtasun-estandarrak bete direla egiaztatzen duen ziurtagiri ofizial bat ematen da.

Jarraian, estandar horietako batzuk berrikusiko dira, hedatuenak dira eta.

ISO/IEC, ISO 27k familia

ISO 27k familia (ISO/IEC 27000 seriea ere esaten zaio) informazioaren segurtasun-kudeaketari heltzen dioten nazioarteko estandarren multzo bat da. Estandar horiek Estandarizaziorako Nazioarteko Erakundeak (ISO) eta Nazioarteko Batzorde Elektroteknikoak (IEC) garatzen dituzte, edozein tamaina eta sektoretako erakundeetan informazioaren segurtasun-jardunbide egokien esparru bat ezartzeko helburuarekin.

ISO/IEC 27000 serieak informazioaren segurtasun-kudeaketarako jarraibideak eta gomendioak ematen ditu, eta elkarri lotutako hainbat estandarrek osatzen dute. Hauek dira estandar ezagunenak:

- **ISO/IEC 27001:** Familiaren estandar nagusia da, eta erakunde baten barruan Informazioaren Segurtasuna Kudeatzeko Sistema (SGSI) bat ezartzeko, inplementatzeko, mantentzeko eta hobetzeko baldintzak zehazten ditu.
- **ISO/IEC 27002:** Informazioaren segurtasun-jardunbide egokien eta -kontrolen multzo bat ematen du, ISO/IEC 27001 estandarrean SGSIrako deskribatutako betekizunak inplementatzeko erabil daitekeena.
- **ISO/IEC 27005:** Informazioaren segurtasun-arriskuen kudeaketa lantzen du, eta arriskuak identifikatzeko eta ebaluatzeko jarraibideak ematen ditu, bai eta segurtasun-kontrol egokiak hautatu eta inplementatzekoak ere.

Horiez gain, badira, ISO 27k familiaren barruan, gai espezifikoak jorratzen dituzten beste estandar batzuk ere, hala nola segurtasun-gorabeheren kudeaketa, negozioaren jarraitutasuna eta informazioaren segurtasunaren auditoretza, besteak beste.

NIST SP 800

NIST SP 800 estandarra Ameriketako Estatu Batuetako Estandarren eta Teknologiaren Institutu Nazionalak (NIST) informazioaren segurtasunaz eta zibersegurtasunaz egindako argitalpenei dagokie. NIST SP 800 (Special Publication 800) estandarrak informazioaren segurtasunaren eta arriskuen kudeaketaren hainbat alderdiri buruzko jarraibideak,

gomendioak eta jardunbide egokiak eskaintzen ditu. NIST SP 800 hainbat argitalpenek osatzen dute, eta horietako bakoitzak segurtasunaren eta zibersegurtasunaren arlo espezifiko bati heltzen dio.

NIST oso ezaguna da segurtasun- eta zibersegurtasun-estandarren arloko agintaritza gisa, eta haren argitalpenak asko erabiltzen dituzte erakundeek eta industriek beren segurtasun-jarrera indartzeko eta informazioarekin eta sistemekin lotutako arriskuak kudeatzeko.

PCI DSS

PCI DSS (Payment Card Industry Data Security Standard) ordainketa-txartelen industriarentzako datuen segurtasun-estandar bat da. PCIko Segurtasun Arauen Kontseiluak (PCI SSC) garatu zuen. Kreditu- eta zordunketa-txartelen konpainia nagusiek (Visa, Mastercard, American Express, Discover eta JCB) osatzen dute erakunde hori.

PCI DSS estandarraren helburua da ordainketa-txartelen titularren informazio konfidentziala babestea, txartel-zenbakiak kasu, informazio hori maneiatzen, prozesatzen edo biltegiratzen duten erakundeetan segurtasun-praktikak sustatuta. PCI DSSk baldintza tekniko eta operatibo jakin batzuk ezartzen ditu, merkatariek, ordainketa-prozesadoreek, txartel-jaulkitzaileek eta ordainketa-txartelekin egindako transakzioetan parte hartzen duten beste zenbait eragilek bete beharrekoak.

Ordainketa-zerbitzuen hornitzaileek eta kreditu-txartelen sareek PCI DSS betetzea eskatzen dute, ordainketa-txartelen bidezko transakzioen segurtasuna bermatzeko. Ordainketa-txartelak erabiltzen dituzten erakundeek aldizkako auditoretzak egin behar dituzte estandarra betetzen dutela frogatzeko.

Segurtasuna

C1 maila 4.1 Gailuen babesa

Sareen aurkako erasoen kontrako babesa

Sareen aurkako erasoen kontrako babesa

Komunikazio-sareen babesa segurtasun informatikoaren funtsezko alderdia da. Horrek garrantzi berezia du enpresa-sareetan, non negozio baterako zerbitzu kritikoak gordetzen diren, eguneroko eragiketa ugari egiten diren eta informazio konfidentziala partekatzen den.

Maila honetako bideoetan ikusi ditugun erasoak etengabeko mehatxua dira, komunikazioa eta datu-fluxua eteteko edo arriskuan jartzeko.

ERASO OHIKOENAK SAREETAN

Etxeko sareetan zein enpresa-sareetan, eraso arruntak daude, baina eraginkorrak dira eta haien segurtasuna mehatxatzen dute. DHCP eta IP Spoofing, Man in the Middle edo zerbitzu-ukatzeak dira horietako batzuk.
e.digitall.org.es/A4C41C1V03

Jarraian, **eraso espezifikoak -**DHCP Spoofing, IP Spoofing, Man in the Middle (MitM) eta zerbitzu-ukatzea (DoS), adibidez- **arintzeko beharrezkoak diren babes-neurriak jorratuko dira**. Hau jardunbide egokien gida bat da, baina konfigurazioaren zehaztasun gehiago izateko, sareko gailu bakoitzaren eskuliburu espezifikoak kontsultatu beharko dira.

DHCP Spoofing

DHCP Spoofing erasoak, sare bateko DHCP-zerbitzari legitimo baten plantak egiteko eta **arriskuan jarritako sareko gailuen konfigurazioaren kontrola hartzeko erabiltzen dira**. Horrela, aldez aurretik zehaztutako lotura-atea aldatu eta arriskuan jarritako gailuen trafikoa birbideratu liteke erasotzailearen ordenagailuaren bidez; horrek komunikazioak atzemateko edo ikuskatzeko aukera emango luke.

Gailu bat sare batera konektatzen denean, erantzun dezakeen edozein DHCP-zerbitzariri eskatzen dio konfigurazioa. Horregatik, erasotzailearen DHCP-zerbitzari faltsuak legitimoak baino azkarrago erantzuten badu, gailuak konfigurazio okerra lortuko du. Halako erasoak prebenitzeko, funtsezko gomendio batzuk daude:

1 | Routerrak sarearekin behar bezala konektatzea

- Router bat okerreko ataka eta lehenetsitako konfigurazioa erabiliz konektatzen bada sarearekin, baliteke DHCP-eskaerei erantzutea eta sareko gailuak deskonfiguratzea.
- Oro har, ez da baimendu behar sarearen administratzaileak konfiguratu gabeko routerren erabilera, mehatxu izan baitaitezke harentzat.

2 | DHCP-trafikoa gainbegiratzea DHCP Snooping-ekin

- DHCP Spoofing-en balizko erasoa saihesteko, sareko enpresa-gailuek, hala nola switch-ek, DHCP Snooping mekanismoa dute eskura.
- Mekanismo horrek baimendu gabeko DHCP-paketeen bidez eskaneatzeko aukera ematen du. Horrela, enpresaren zerbitzari legitimotik soilik baimenduko dira DHCP-erantzunak, sarearekin konektatutako erabiltzaileen erasoak arintzeko.

IP Spoofing

Era berean, **IP Spoofing** erasoek **sareko gailu legitimo baten identitatea ordeztea dute helburu**. Hau da, zerbitzari garrantzitsuen edo erabiltzaile baten sare-helbidea ordezten saiatzen da, baita routerrarena ere. Eraso horrek identitate-ordezpen horretan oinarritutako beste askori bide ematen die. Erasoa arintzeko, funtsezko neurri batzuk daude:

3 | Dynamic ARP Inspection (DAI) konfiguratzea

- Helbide fisiko faltsu batekin lotuz IP helbidea ordeztea saihesteko, ARP protokoloaren ikuskapena aktiba daiteke DAIrekin.
- Horrek ARP Spoofing erasoak arintzen ditu (eraso horiek haiei ez dagokien IP baten itxurak egiteko aukera ematen diete erasotzaileei).

4 | Suebaki baten bidez sartzeko arauak konfiguratzea

- Maila honetan ikusi den bezala, sarearen suebaki bidezko konfigurazioa eta haren segmentazioa mekanismo baliagarriak dira eraso asko saihesteko.

KONEXIOAK KONTROLATZEN: SUEBAKIETARAKO HURBILPENA

Sare bateko firewall edo suebakien bidez, sareko trafikoa iragazi eta blokeatu egin daiteke, sarbide-kontroleko zerrenden edo arauen bitartez. Suebaki motaren arabera, sare-paketeak blokeatu daitezke, komunikazioaren hainbat ezaugarri kontuan hartuta, hala nola IP helbidea edo ataka.

e.digitall.org.es/A4C41C1V05

- Sare batekoak ez diren IP-eskaerak suebaki bidez iragazi eta blokeatzeak arindu egiten ditu IPak ordezteko asmoz urrundik egindako erasoak.

Man in the Middle (MitM)

Bestalde, Man in the Middle (MitM) erasoak kontzeptu generiko bat dira, hainbat mehatxu biltzen dituena, non erasotzailea komunikazioaren erdian dagoen komunikazioa atzemateko, ikuskatzeko edo manipulatzeko asmoz. Halako erasorik ez izateko, garrantzitsua da IP, ARP eta DHCP ordezpen motak saihestea, lehen esan bezala. Gainera, badaude MitM erasoak arintzen laguntzen duten neurriak:

5 | Sare-topologia segurua eta segmentatua diseinatzea

- Sare bat segmentatuta mantentzeak aukera ematen du sare korporatibo baten zatiak bereizten dituzten arauak ezartzeko. Adibidez, eremu pribatu, publiko eta desmilitarizatuak (DMZ) ezarriz.
- Horrela, sare irisgarriago batekin konektatutako erasotzaile batek zerbitzari- edo administrazio-sarerako sarbidea izatea saihesten da.

6 | Komunikazioak zifratzea eta autentifikatzea

- Igarotzen ari den informazioa zifratzeak trafiko-ikuskapenak arintzen ditu eta informazioa konfidentzial mantentzen du.
- TLS bezalako zifratze-sistemak erabiltzeak zatiak autentifikatzeko eta bien artean informazio zifratua transmititzeko aukera ematen du, manipulazioak saihesteko.

SARE-TOPOLOGIA SEGURUA

Sare baten segmentazioak eta haren antolaketak sarbide-kontrol eraginkorragoak ezartzeko aukera ematen dute. Gainera, sare birtualak edo VLANak erabiliz gailu kritikoak, gailu publikoak eta erabiltzaileenak eremuetan bereiztea da sare-diseinu seguruagoa ezartzeko praktiketako bat.

e.digitall.org.es/A4C41C1V04

Zerbitzu-ukatzea (DoS)

Azkenik, zerbitzu-ukatzeak ez dira hain sofistikatuak, baina oso suntsitzaileak dira, eta **komunikazio-sarearen eta, beraz, informazioaren erabilgarritasunari eragiten diote**. Horrelako erasoen helburua komunikazioak neutralizatzea eta geldiaraztea da, informazio-sistemetarako sarbidea eragozteko; hain zuzen ere, horrek kaltea egin diezaion enpresa baten negozio-prozesuari.

Hainbat *Denial of Service (DoS)* eraso mota daude, eta, beraz, hainbat segurtasun-neurri mota hartu behar dira kontuan. Adibidez:

7 | Sareko eta erabiltzaileen gailuak eguneratuta mantentzea

- Sarean zehar bana daitekeen eta informazioaren eskuragarritasunari eragin diezaiokeen malwarea dago: ransomwarea edo beste hainbat zizare, esaterako.
- Softwarean dauden ahuleziez baliatzen da malwarea, eta, beraz, ekipoak eguneratuta izateak mota horretako mehatxuak arintzen ditu.

8 | Intrusioak detektatzeko eta prebenitzeko sistemak instalatzea

- IDS eta IPS sistemek sarea monitorizatzeko aukera ematen dute, baita zerbitzu-ukatze gisa ezagutzen diren erasoak detektatzeko eta blokeatzeko ere.
- Mekanismo horiek instalatu eta eguneratuta izateak komunikazioa blokeatzen duen eta sistemak saturatzen dituen DoS prebenitzen laguntzen du.

9 | Sistema erredundanteak diseinatzea eta segurtasun-kopiak izatea

- Zerbitzu-ukatzeek sistemetarako sarbidea eragozten dute, horiek asez edo jasotako informazioa eskuraezin bihurtuz.
- Zerbitzu- edo informazio-galera saihesteko, informazioaren segurtasun-kopiak eta sistema erredundanteak izan behar dira. Akatsa edo saturazioa gertatuz gero, erabiltzaileak sistema erredundantera bideratuko dira, edo informazioaren segurtasun-kopia berrezarriko da.

Ikusi dugun bezala, sareetako eraso ohikoenak arintzeko aplika daitezkeen neurri ugari daude. Segurtasuna prozesu bat da, eta, beraz, kontraneurri horiek pixkanaka aplikatu behar dira, soluzioak eguneratuta mantenduz eta aldian behin horien funtzionamendu zuzena berrikusiz.

INTRUSIOAK DETEKTATZEKO ETA PREBENITZEKO SISTEMAK (IDS/IPS)

Intrusioak detektatzeko eta prebenitzeko sistemek sareko trafikoa monitorizatzeko aukera ematen dute, eraso ezagunak edo ezezagunak ere detektatzeko. IPSek, gainera, komunikazioa blokeatzeko aukera ematen dute, eraso motaren bat detektatzen bada, hala nola zerbitzu-ukatzea.

e.digitall.org.es/A4C41C2V08

Segurtasuna

C1 *maila* 4.1 Gailuen babesa

Ziurtagiri digitalak

Ziurtagiri digitalak

Aro digitalean, non informazioaren segurtasuna ezinbestekoa den, ziurtagiri digitalek funtsezko zeregina betetzen dute autentifikazioan eta datuen osotasunaren babesean. Ziurtagiri digitalak dokumentu elektronikoak dira, informazio kriptografikoa dutenak, eta entitate baten identitatea ingurune digitaletan egiaztatzea ahalbidetzen dute. Artikulu honetan, ziurtagiri digitalen formatu ohikoenak aztertuko ditugu, baita zer informazio biltegiratzen duten eta zertarako erabiltzen diren ere.

Ziurtagiri digitalen kontzeptua eta funtzionamendua

Zer da ziurtagiri digitala eta nola funtzionatzen du?

Ikusi dugunez, ziurtagiri digitala artxibo elektroniko bat da, identitate digital bat entitate edo pertsona fisiko batekin lotzeko erabiltzen dena. Ziurtapen-agintaritza (CA, ingelesezko siglen arabera) fidagarri batek ematen du, eta ingurune digitaletan identitatea eta fidagarritasuna ezartzeko erabiltzen da.

Ziurtagiri digitalek gako publikoko kriptografia erabiltzen dute, haiekin lotutako erakundeen benetakotasuna bermatzeko. Ziurtagiriak entitatearen gako publikoa du, eta ziurtapen-agintaritza jaulkitzaileak digitalki sinatuta dago. Erabiltzaile edo sistema batek entitate baten identitatea egiaztatu behar badu, ziurtagiriaren sinadura digitala egiaztatzen du, ziurtapen-agintaritzaren gako publikoa erabiliz.

Ziurtagiri digital motak eta haien aplikazioak

- **Agintariek emandako ziurtagiriak – X.509 formatua:** X.509 formatua da ziurtagiri digitaletarako gehien erabilitakoetako bat. Oso ezaguna da, eta bateragarria da segurtasun-aplikazio eta -protokolo ugarirekin. X.509 formatuko ziurtagiriek informazioa jasotzen dute, hala nola titularraren izena, balio-epea, gako publikoa, ziurtapen-agintaritza jaulkitzailearen izena eta haren sinadura digitala.

  - Ziurtagiri mota horren adibide dira Espainiako Moneta eta Tinbre Fabrika Nazionalak (FNMT) emandako pertsona fisikoen ziurtagiriak. Horiek eskatzeko, web-nabigatzaile bateragarri bat erabili behar da, eta haren webguneko prozedurari jarraitu behar zaio.
  - Ziurtagiri hori lortutakoan, erabili dugun nabigatzailean instalatuko da. Ziurtagiri horren kopia bat egin dezakegu nabigatzailearen konfiguraziotik, pasahitz bidez babestutako fitxategi batera esportatuta, beste nabigatzaile edo gailu batzuetara inportatu ahal izateko.

- **Posta zifratzeko norberak sortutako ziurtagiri pertsonalak - PGP/GPG protokoloa:** Pretty Good Privacy (PGP) eta GNU Privacy Guard (GPG) kriptografia-protokoloak dira, eta berezko ziurtagiri-formatuak erabiltzen dituzte. Ziurtagiri horiek ezagunak dira posta elektronikoaren segurtasun-arloan, eta mezuak autentifikatzeko eta zifratzeko aukera ematen dute.
  - Sortu eta erabili ahal izateko, beharrezkoa da Kleopatra eta OpenPGP bezalako software bat instalatuta izatea. Posta elektronikoko zenbait bezerok, hala nola Thunderbirdek, PGP/GPG erabiliz posta elektronikoa zifratzeko eta sinatzeko aukera ematen dute.

- **Posta elektronikoko ziurtagiriak - S/MIME protokoloa:** S/MIME estandarrak (Secure/Multipurpose Internet Mail Extensions) ziurtagiri digitalak erabiltzen ditu posta elektronikoan segurtasuna eta autentifikazioa emateko. S/MIME ziurtagiriak X.509 formatuan oinarritzen dira, eta posta elektronikoko mezuak sinatzeko eta zifratzeko erabiltzen dira.
  - X.509 ziurtagiri batzuek mezu elektronikoak zifratzeko erabiltzeko aukera ematen dute. Outlook edo Thunderbird bezalako posta-bezeroak erabiliz gero, ziurtagiri bateragarriak dituzten mezu elektronikoak zifratu eta sina daitezke.

Ziurtagiri digitaletan gordetako informazioa

- **Titularraren identitatea** Ziurtagiri digital baten funtsezko osagaietako bat titularraren identitate-informazioa da. Horren barruan sar daitezke izena, helbide elektronikoa, lotutako erakundea edo enpresa eta entitatearen identitatea egiaztatzeko beste datu garrantzitsu batzuk.
- **Gako publikoa** Ziurtagiri digitalek beraiekin lotutako entitateen gako publikoa ere gordetzen dute. Benetakotasuna egiaztatzeko eta dagokion entitatearekin komunikazio segurua ezartzeko erabiltzen da gako publikoa.
- **Ziurtapen-agintaritzaren sinadura digitala** Ziurtagiriaren osotasuna bermatzeko, agintaritza jaulkitzaileak digitalki sinatzen du bere gako pribatua erabiliz. Sinadura horri esker, erabiltzaileek eta sistemek egiaztatu ahal izango dute ziurtagiria ez dela aldatu eta iturri fidagarri batetik datorrela.

Ziurtagiri digitalen aplikazioak

Webguneetan autentifikatzea

Ziurtagiri digitalek funtsezko zeregina betetzen dute webguneak HTTPS protokoloaren bidez autentifikatzeko. SSL/TLS ziurtagiriek (Secure Sockets Layer/Transport Layer Security) aukera ematen dute konexio seguruak ezartzeko eta webgune baten identitatea autentifikatzeko; horrek konfiantza ematen die erabiltzaileei eta helarazitako informazioa babesten du. Erabiltzaile bat webgune seguru batera sartzen saiatzen denean, nabigatzaileak baliozko ziurtagiri bat aurkezteko eskatuko dio zerbitzariari. Nabigatzaileak egiaztatuko du, batetik, ziurtagiriaren benetakotasuna, eta, bestetik, sartu nahi den domeinuarekin bat ote datorren. Ziurtagiria baliozkoa eta fidagarria bada, konexio segurua ezarri eta adierazle bisual bat erakutsiko da, hala nola giltzarrapo bat, erabiltzaileari konexioa segurua dela adierazteko.

Sinadura digitalak

Ziurtagiri digitalak dokumentu elektronikoetako sinadura digitalerako ere erabiltzen dira. Dokumentu bat baliozko ziurtagiri batekin digitalki sinatzen bada, dokumentuaren osotasuna eta sinatzailearen identitatea egiazta daitezke, eta hori funtsezkoa da lege- eta enpresa-inguruneetan. Sinadura digitalak gako publikoko kriptografia erabiltzen du dokumentuaren aztarna digital bakarra sortzeko. Aztarna digital hori dokumentuari eransten zaio, eta lotutako ziurtagiriaren gako publikoa erabiliz egiazta daiteke. Dokumentua nolabait aldatu bada, sinadura digitalaren egiaztapenak huts egingo du, eta horrek edukiaren osotasuna bermatuko du. Gainera, sinadura digitala sinatzailearen identitateari lotuta dago, eta horrek konfiantza eta benetakotasun handiagoa ematen du.

Posta elektronikoa zifratzea

S/MIME ziurtagirien bidez, posta elektronikoko mezuak zifratu eta sina daitezke, haien konfidentzialtasuna eta benetakotasuna bermatzeko. Horrek komunikazioen pribatutasuna babesten du, eta mezuak atzematea edo aldatzea saihesten du. Erabiltzaile batek S/MIME bidez zifratutako mezu elektroniko bat bidaltzen duenean, mezua hartzailearen gako publikoa erabiliz enkriptatzen da, eta horrek bermatzen du hartzaileak bakarrik deszifratu eta irakurri ahal izango duela edukia. Gainera, mezua bidaltzailearen ziurtagiriarekin digitalki sinatzen denez, bidaltzailearen benetakotasuna egiaztatzen da eta mezuaren edukia bidean aldatu ez dela ziurtatzen da.

Ondorioa

Laburbilduz, ziurtagiri digitalak funtsezko pieza dira ingurune digitalen segurtasunerako eta autentifikaziorako. Gako publikoko kriptografia eta X.509, PGP/GPG eta S/MIME bezalako formatuak erabiltzen direnez, ziurtagiri digitalek aukera ematen dute entitateen identitatea egiaztatzeko, informazioaren osotasuna babesteko eta komunikazio seguruak ezartzeko. Webguneetako autentifikaziotik hasi eta sinadura digitaleraino eta posta elektronikoa zifratzeraino, ziurtagiri digitalak tresna moldakorrak dira eta funtsezkoak dira aro digitalean konfiantza eta segurtasuna bermatzeko.

Segurtasuna

C1 maila 4.1 Gailuen babesa

Gako publikoaren azpiegitura (PKI)

Gako publikoaren azpiegitura (PKI)

Gako Publikoaren Azpiegitura (PKI, ingelesezko siglen arabera) informazioaren segurtasunerako ezinbesteko sistema da.

PKIren bidez, konfiantzazko azpiegitura bat ezartzen da, komunikazio digitalen autentifikazioa, osotasuna eta konfidentzialtasuna ahalbidetzen dituena.

PKI ziurtapen-agintaritza batek emandako ziurtagiri digitalen erabileran oinarritzen da. Ziurtagiri horiek parte-hartzaileen identitatea egiaztatzeko eta informazioa zifratzeko erabilitako gako publikoak dituzte. Lehen ikusi dugun bezala, ziurtagiri digitalek funtsezko zeregina dute hainbat aplikaziotan, hala nola posta elektronikoa zifratzean, sinadura digitalean eta online-konexio seguruen babesean.

ZIURTAGIRI DIGITALAK

Erreferentziazko dokumentua: ***A4C41C1D03***

Ondo ulertu behar da PKIk nola funtzionatzen duen eta haren printzipioak nola gauzatzen diren, abantailak aprobetxatzeko eta ziurtagiri digitalen erabilera praktikan jartzeko.

Ziurtapen-agintaritzak

Ziurtapen-agintaritzak (CA, ingelesezko siglen arabera) PKIren barruko funtsezko osagaiak dira. Ziurtagiri digitalak emateaz eta kudeatzeaz arduratzen diren konfiantzazko entitateak dira.

Maila teknikoan, ziurtapen-agintaritzek beren gako pribatuak erabiltzen dituzte ematen dituzten ziurtagiri digitalak sinatzeko. Hartara, ziurtagiri digitalen sinadurak baliozkotzen direnean, ziurtapen agintaritzaren gako publikoarekin egiten da.
Har dezagun adibidetzat Espainiako Moneta eta Tinbre Fabrika Nazionalak (FNMT) ziurtapen-agintaritza gisa emandako ziurtagiri digital batekin PDF dokumentu bat sinatu duen erabiltzaile bat. Sinadura gako publikoak erabiliz baliozkotzen denean, FNMTren VALIDe zerbitzua erabil daiteke. Zerbitzu horrek egiaztatu egingo du eta, horretarako, ziurtagiri hori egiteko erabilitako ziurtapen-agintaritzaren gakoak erabiliko ditu autentifikaziorako. Horrela, sinadura hori pertsona fisiko jakin bati dagokiola identifika daiteke: dokumentua sinatu duen erabiltzaileari.

Informazio gehiago

VALIDe zerbitzuak (*valide.redsara.es/valide*) aukera ematen du Industria, Turismo eta Merkataritza Ministerioko Telekomunikazioen eta Informazio Gizarterako Estatu Idazkaritzaren erregistroan inskribatutako zerbitzu-emaile guztiek ematen dituzten ziurtagiriekin sinatutako dokumentuen sinadura baliozkotzeko.

PKI baten egitura

SINADURA DIGITALAREN OINARRI TEKNIKOAK

e.digitall.org.es/A4C41C1V08

Ziurtagiri digitalak normalean azken mailako ziurtapen-agintaritza batek sinatzen ditu. PKI bat egitura hierarkiko bat da, hainbat maila dituena.

Egitura horren gailurrean, jatorrizko ziurtapen-agintaritzak daude, zeinetan jartzen baita konfiantza handiena. Jatorrizko ziurtapen-agintaritza horiek arduratzen dira konfiantza-hierarkia horretan azpian dauden beste agintaritza batzuen ziurtagiriak sinatzeaz. Beraz, azken ziurtapen-agintaritza horiek sinatzen dituzte erabiltzaileen ziurtagiriak.

Horrela, gako asimetrikoak eta horiekiko konfiantza hobeto kudeatzeko aukera dago. Ziurtapen-agintaritzen gako pribatuek oso ondo babestuta egon behar dute, horiek sinatzen baitituzte ziurtagiriak. PKIren katean zenbat eta gorago egon, orduan eta konfiantza handiagoa jartzen dugu ziurtapen-agintaritzan eta, beraz, gakoen haren kudeaketan. Tarteko agintaritza bat arriskuan badago, hark sinatutako ziurtagiriak soilik ezeztatu beharko dira, hau da, baliogabetu.

PKI egiturek aukera ematen digute konfiantza-kate bat sortzeko, ziurtagiriak eraginkortasun handiagoz kudeatzeko eta haien baliozkotasuna eta fidagarritasuna bermatzeko. Horrela, legezko balioarekin erabil daitezke, eta gobernuek eta estatuek babestuta egon daitezke.

DigitAll

Segurtasuna

4.2

DATU PERTSONALEN ETA PRIBATUTASUNAREN BABESA

Segurtasuna

C1 maila 4.2 Datu pertsonalen eta pribatutasunaren babesa

Online-erosketetan eta -ordainketetan pribatutasuna hobetzea

Online-erosketetan eta -ordainketetan pribatutasuna hobetzea

Erosketa-weba

Interneti eta haren erabilera orokorrari esker, pertsonen eta zerbitzuen arteko elkarreragin handia duen ingurune digital baterantz eboluzionatzen joan da gaur egungo gizartea. Digitalizatu den eta harrera handia izan duen zerbitzuetako bat produktuen eta zerbitzuen salerosketa-merkatua da. Dagoeneko ez da beharrezkoa erosketak inguruko establezimenduetara mugatzea, ia munduko edozein tokitan eros baitezakezu nahi duzun produktua edo zerbitzua.

Milaka enpresa hasi dira beren weben bidez produktuak eta zerbitzuak eskaintzen. Erosteko modua erraza da, eta jarraian deskribatutako urratsak ditu.

Produktu bat online erosteko ohiko prozedura:

1 | Erabiltzailea enpresaren webera sartzen da.
2 | Erabiltzaileak nahi duen produktua bilatzen du.
3 | Erabiltzaileak bere erosketa-organ sartzen du produktua.
4 | Erabiltzaileak entrega-datuak ematen ditu.
5 | Erabiltzaileak fakturazio-datuak ematen ditu.
6 | Erabiltzaileak ordaindu egiten du.
7 | Enpresak ordainketa jasotzen du.
8 | Enpresak produktua paketatzen du.
9 | Enpresak produktua duen paketea entregatzen dio logistika-operadore bati.

10 | Logistika-operadorea hura helarazteaz arduratzen da..

Mekanismo horrek nolabaiteko konfiantza eskatzen du erabiltzailearen, enpresaren eta logistika-operadorearen artean: erabiltzaileak arriskua hartzen du dirua produktua bidali behar dion enpresari emanda, enpresak erabiltzailearen diru-transferentzia benetan ez egiteko arriskua hartzen du eta logistika-enpresak azken erabiltzaileak produktua ez jasotzeko eta, beraz, enpresa saltzaileari itzultzeko gastuak berak ordaindu behar izateko arriskua hartzen du.

Logistika-enpresa eragile garrantzitsua da transakzio horretan, baina arrisku txikiagoa du; izan ere, gastu horiek estaltzen dituzten aseguruak kontratatu ohi dituzte, eta hornitzaile berek entrega asko egiten dituztenez, berriz ere enpresara joan behar izan arte itxaron dezakete itzulketa egiteko eta, beraz, joan-etorrien kostuak murrizteko.

Beraz, erabiltzaileek eta enpresa saltzaileek ziurtatu behar dute ez dituztela engainatuko. Erabiltzaileengan jarriko dugu arreta, eta online-erosketetan segurtasuna eta pribatutasuna areagotzeko jarraitu beharreko oinarrizko ideia batzuk ikusiko ditugu.

Erosketa-webarekiko konfiantza

Pribatutasun handia izateko, erabiltzaile batek egiaztatu behar duen lehenengo gauza da erosketa egin nahi duen weba konfiantzazkoa dela: ez dizkiogu geure datu pertsonalak emango konfiantza ematen ez digun inori. Bizitza errealean, pertsonek nahiago izaten dute produktuak enpresa ezagunen dendetan erosi, kalean ezezagun bati erosi baino. Hori berdin aplikatzen da erosketak Internet bidez egiten ditugunean. Ezagutu behar dugu erosketa-weba, eta ziur egon behar dugu kudeatzen duen enpresak ospe ona duela.

Milaka eta milioika web daude Interneten. Gehienak benetako salmentak egin nahi dituzten eta truke horretan etekina duten enpresak dira. Hala ere, gure dirua eta gure datu pertsonalak lortzeko bakarrik engainatu nahi gaituzten iruzurrezko web gutxi horiek detektatu eta baztertu behar ditugu.

Ospe oneko enpresa ezagunen webetan erosten badugu (Amazon, El Corte Inglés, Carrefour, MediaMarkt eta abar), esperientzia luzea eta ospe handia duten konpainia handien babesa dugu. Adierazle horiek guztiek erakusten dute konfiantza handia izan dezakegula web horietan, eta fidagarria dela gure datu pertsonalak ematea, datu horiek bidezko eran erabiliko baitituzte.

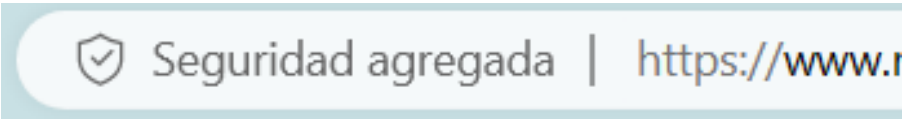
Erosketa-weba enpresa ezagun batena ez bada, beste erabiltzaile batzuen ezaupideak bila ditzakegu. Hobe da iritzi horiek webekoak ez izatea; izan ere, agian, enpresaren aldekoak baino ez dituzte jarri edo asmatutakoak ere izan litezke.

Aholku batzuk jarrai daitezke web bat iruzurrezkoa den jakiteko:

- Gaizki itzulita dago.
- Gehiegizko publizitatea du edo, egin nahi den erosketa kontuan hartuta "arraroak" edo garrantzi gutxikoak diren produktuen leiho sortu berri gehiegi ditu.
- Itxura orokorra ez da oso profesionala.
- Atalen izenburuak ez datoz bat erakutsitako edukiarekin.
- Prezioak merkeegiak dira, hori argi eta garbi justifikatzen duen arrazoirik eman gabe (adibidez, merkeak dira bigarren eskuko produktuak direlako, itzulketak direlako, katalogotik kanpo daudelako eta abarrengatik).

Erosketa-weba zifratzea

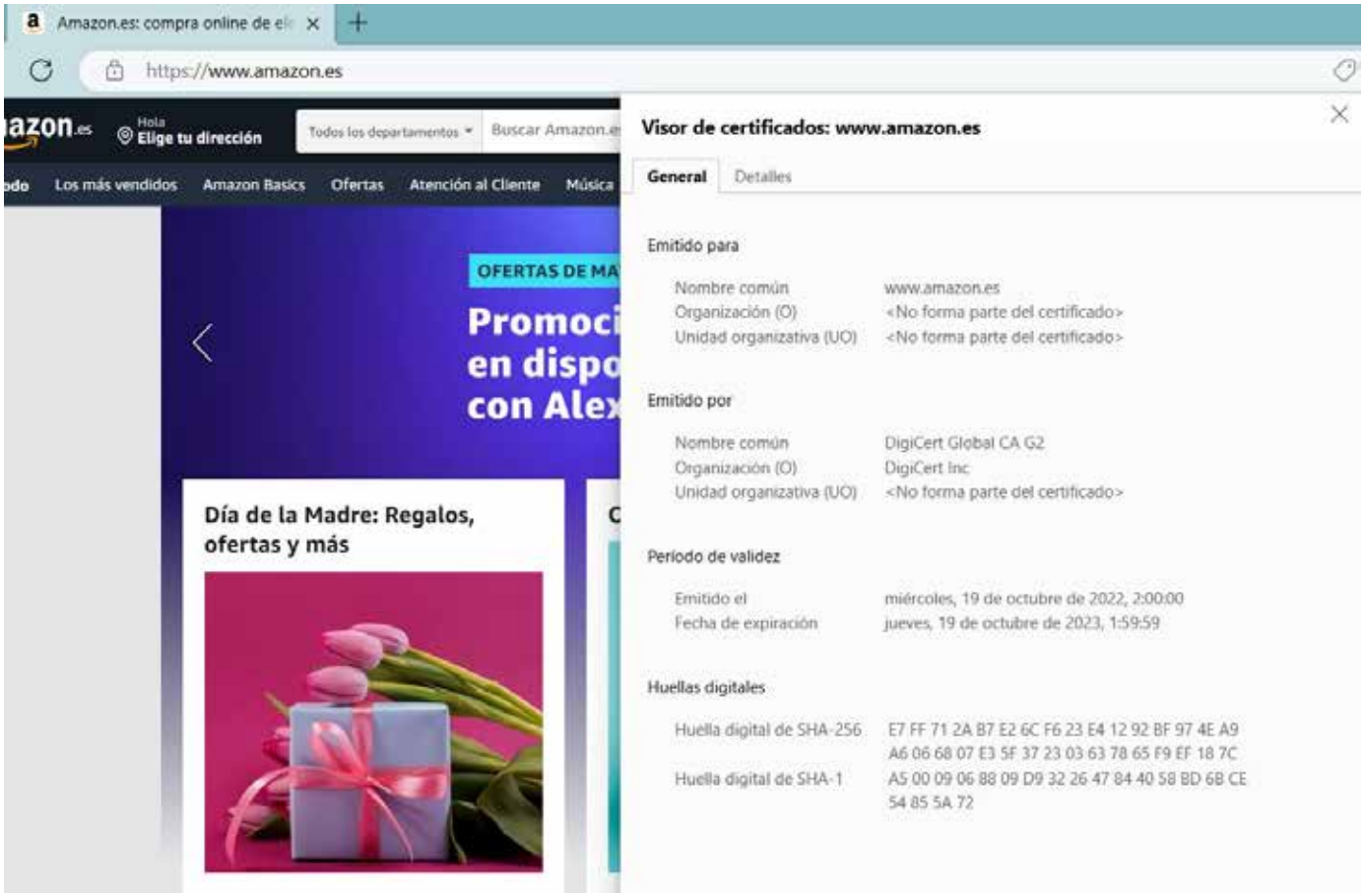
Erosketa-web bati datu pertsonalik eman aurretik, konexioa segurua den begiratu behar duzu. Horretarako, nabigatzailearekin egiten duzun konexioa zifratuta dagoela egiaztatu behar duzu. Konexio seguruak **https** protokolo segurua erabiliz egiten dira.



https protokoloa duen konexioa duen nabigatzailearen xehetasuna eta segurtasun-ikurra.

https protokolo segururik ez duten web-orriak legitimoak izan daitezke, baina haien segurtasunik ezak gure datuak edozein erasotzailek atzematea eragin dezake.

Gainera, **https** protokoloak identitate-ziurtagiria nork sortu duen jakiteko aukera ematen du. **SSL ziurtagiri** hori gure nabigatzailearen eta enpresaren erosketa-webaren artean konexio segurua ezartzeko erabiltzen da. Horrela, ziurtagiria berrikusita, ziurtatu dezakegu weba bat datorrela ziurtatutako izenarekin eta erakunde ziurtatzailea fidagarria dela.



www.amazon.es-en ziurtagiri digitalaren xehetasuna.

Beste segurtasun-estandar batzuk

Nahiz eta **https** protokoloaren erabilera izan segurtasun-estandar nagusia, badira beste estandar batzuk, eta horiei ere erreparatu behar diegu erosketa-webean konfiantza handiagoa izateko.

Zure datu pribatuak betekizun oso zorrotzei jarraituz modu seguruan kudeatzen dituzten enpresek ISO 27001 ziurtagiria lortzen dute. Beraz, ziurtagiri hori duten enpresek frogatu dute gure datu pertsonalen pribatutasuna bermatzen duen prozedura oso segurua dutela.

ISO/IEC 27001 ziurtagiria eta beste ziurtagiri batzuk dituen enpresaren webaren adibidea.

Interneten enpresa batzuek enpresen web-orrien pribatutasuna aztertzen dute eta fidagarritasun-zigiluak ematen dizkiete. Pribatutasun-zigilu ezagunenetako bat TRUSTe ® da. Hori edukitzeak erabiltzaileen segurtasuna areagotzen du web horrek datuen pribatutasuna maneiatzen duen moduari dagokionez, eta horrek askoz ere fidagarriagoa egiten du.

Enpresen eta weben segurtasun- eta pribatutasun-arloko TRUSTe ® berme-zigiluaren logoa.

Pribatutasun-politikak, entrega eta erosketa-metodoak

Erabiltzaileak webean konfiantza-maila bat behin ezarri duenean, bigarren mailara pasa daiteke. Maila horretan, erabiltzaileak ebaluatu behar du enpresak bere datu pertsonalak berak nahi duen moduan erabiliko dituen eta interesatzen zaion erosketa-metodorik ote dagoen, nahi duen pribatutasun-maila bermatzen dionik.

Pribatutasun-politikak

Gure datu pertsonalak web batean eman aurretik, informatu behar dugu zertarako nahi dituzten datuak. Adibidez, beharrezkoa da web batek gure lan-helbidea zein den jakitea, baldin eta erosketa pertsonala egin nahi badugu? Edo, bestela, gure datuak enpresaren zerbitzarietan gordeko dituzte edo hirugarren enpresei lagako dizkiete mezuak bidal diezazkiguten?

Enpresa Europar Batasunekoa bada, araudi jakin batzuk bete beharko ditu, hala nola Datuak Babesteko Erregelamendu Orokorra (DBEO, edo ingelesez, GPRD). Weba Europar Batasunetik kanpo badago, kokatuta dagoen herrialdeko araudia berrikusi beharko da, lagatzen ditugun datu pertsonalen gainean zer eskubide dugun jakiteko.

Beste erosketa-politika batzuk

Pribatutasunaz gain, dendaren beste politika batzuk ere berrikusi behar ditugu erabiltzaileok, geure produktuaren erosketan eragin handia izan dezakete eta. Adibidez, zer berme du produktuak? Non aplikatzen da bermea? Nor arduratzen da garraio-gastuez? Barne hartzen dira aduana-kostuak nazioarteko salmenta bada? Zenbat denboraz atzeratu daiteke bidalketa erreklamazioa egin aurretik? Legezko erreklamaziorik egonez gero, zein lege eta auzitegiri lotzen zaio erabiltzailea?

Oro har, erabiltzaileek honako alderdi hauek hartu behar dituzte kontuan erosketak egiteko:

- **Bidaltzeko moduak:** garraio mota, enbalajea, entregatzeko lekua eta abar.
- **Bermea:** berme mota (osorik berriro ematea, frankiziarik gabeko konponketa, frankizia bidezko konponketa, berrerosketa-bonua eta abar) eta aplikazio-aldia.
- **Erosketan atzera egitea:** zenbat denboraz uko egin diezaiokegun erosketari, atzera egitearen kostua eta abar.
- **Erreklamazioak:** erreklamazio-aldia, -lekua eta -modua.
- **Garraioa:** kostuak, epeak, tasa gehigarriak.
- **Zerbitzu gehigarriak:** konponketa- eta garraio-aseguruak, eguneraketak, saldu ostekoa eta abar.

Atal horiek aztertuta, ezkutuko prezioak ager daitezke, produktuaren hasierako prezioan agertzen ez direnak.

Entregatzeko metodoak

Entregak egiteko formatu ugari daude. Horietako bakoitzak prozedura desberdina du, kostu desberdinekin eta datuen pribatutasun-inplikazio desberdinekin ere bai, kasu bakoitzean.

Entregari dagokionez, hiru motatakoak izaten dira:

- **Etxean entregatzea:** logistika-enpresak etxean entregatzen du produktua (edo bezeroak adierazitako lekuan). Horretarako, datu pertsonal asko behar ditu: izena, abizenak, NANa eta etxebizitzaren helbidea. Pribatutasun-maila txikieneko mekanismoa da.
- **Correosen edo hari lotutako denda batean entregatzea:** produktua Correosen edo hari lotutako denda batean uzten da, eta erabiltzailea leku horietara joaten da produktua jasotzera. Enpresak bezeroaren zenbait datu pertsonal ezagutu behar ditu, jasotzea baimendu ahal izateko, baina ez du jakin behar helbidea edo beste datu pertsonalik.
- **Jasotze-puntu batean entregatzea:** produktua kutxatila seguru batean entregatzen da, eta erabiltzaileak konbinazio bakar batekin hura ireki eta produktua jaso dezake. Kasu horretan, enpresak ez du kokapenari edo helbideari buruzko datu pertsonalik. Pribatutasun-maila handieneko entrega mota da.

Ordainketa-metodoak

Gure banku-datuak pribatutasunari buruzko datu pertsonalik kritikoenetako bat dira. Beraz, arreta berezia eskaini behar diegu ordainketa-metodoei.

Horiei dagokienez, hainbat aukera daude:

- **Banku-transferentzia:** pribatutasun-maila txikieneko mekanismoa da, banku-kontuaren kode osoa eman behar delako, eta horrek zordunketa okerrak izateko segurtasun eza dakar.
- **Kreditu-txartelarekin ordaintzea:** bezeroak kreditu-txartelaren datuak ematen ditu, eta pasabide seguru baten bidez egiten da zordunketa txartelean. Banku-erakunde jakin batzuetan, bigarren segurtasun-maila bat aktiba dezakezu, non zordunketa horretarako baimena eman behar duzun banku-aplikazioen bidez. Horrek segurtasun-maila gehigarria ematen du, ezin baitute zordunketa gehiagorik egin bezeroaren baimenik gabe.

- **Diru-zorro elektronikoarekin/aurreordainketa-txartelarekin ordaintzea:** ordainketa-prozedura txartel bidezko ordainketarena bera da, baina erabiltzen den txartelean kargatzen da ordaindu nahi den kostua. Horrela, kasurik okerrenean, erasotzaileak txartel horretan dagoen eskudirua baino ez luke erabiliko, zordunketa gehiagorik egiteko aukera izan gabe. Pribatutasun-maila handiagoa da, ez baitago erabiltzailearen banku-kontuari lotutako txartelik.
- **PayPal, Google Pay edo antzekoen bidez ordaintzea:** PayPal enpresak (Apple, Google edo antzeko beste batzuk) zure izenean egiten du ordainketa, erabiltzaileari kostua haren kontu korrontean edo aldez aurretik hark erregistratutako banku-txartel batean kargatuta. Sistemarik seguruenetako bat da, erabiltzaileak ez baitio banku-daturik eman behar dendari, eta horrek pribatutasun handiagoa dakar.
- **Jasotzean ordaintzea:** erabiltzaileak garraiolariari ordaintzen dio produktua jasotzen duenean. Garraio-asegurua estaltzeko nolabaiteko gainkostua izan ohi du. Pribatutasun handieneko metodoetako bat da, entregatzeko lekua eta erabiltzailearen izena baino ez baitira ematen.

Pribatutasuna erosketan

Erosketak Internet bidez egiten ditugunean, arrastoak utz diezazkiekegu balizko erasotzaileei, gure pribatutasuna inbaditzeko aprobetxa ditzaketenak. Gure pribatutasunari eraso egitea saihesteko edo, gutxienez, mugatzeko aukerak ezagutzea komeni da.

Erabiltzailea webean erregistratzea

Ohikoa da denda elektroniko guztiek beren sisteman erregistratzea eskatzea. Erregistro horri esker, eskaerak berreskura ditzakegu, erosketa-prozesuarekin jarrai dezakegu, banku-txartelak gehi ditzakegu ordainketa-mekanismoa bizkortzeko eta abar.
Baliteke, ordea, abantaila horiek interesgarriak ez izatea

erosketa bakar eta puntual bat egin behar bada web jakin batean. Datu pertsonal asko ematen dizkiogu, eta horrek pribatutasuna galtzea dakar. Erosketa egiteko, zenbait datu eman beharko ditugu, geuk hautatutako entrega-prozeduraren eta ordainketa-metodoaren arabera.

Denda batzuek aukera ematen dute erosketak **gonbidatu** gisa egiteko, erregistrorik egin beharrik gabe, eta erosketa egiteko behar-beharrezkoak diren datu pertsonalak baino ez eskatuta. Baina web gehienek erregistroa eskatzen dute erosketak egiteko, eta askotan mezu elektroniko bat eskatzen dute.

Kasu horietan, gure helbide elektroniko pertsonala eman beharrik ez izateko, erosketak egiteko soilik erabiliko ditugun bigarren mailako beste helbide elektroniko batzuk sor ditzakegu. Hartara, gure helbide elektroniko pertsonala eta erosketetakoa bereiziko ditugu. Arrazoiren batengatik erosketa-webean segurtasun-akatsen bat edo hackeatzeren bat gertatuko balitz, ez genuke gure helbide elektroniko pertsonalerako sarbiderik emango.

SAREAN ETA SARE SOZIALETAN DATUAK PARTEKATZEN (INFORMAZIOA, FORMULARIOAK, FITXATEGIAK, ARGAZKIAK ETA ABAR).

Sarean informazioa partekatzeko hainbat modu ikusi.
e.digitall.org.es/A4C42C1V07

Beste aukera bat da posta elektronikoaren ezizena erabiltzea. Jatorrizko helbide elektroniko beraren hainbat ezizen sortzen dira; hala, ezizenera bidalitako mezu elektronikoak jatorrizko helbide elektronikoaren posta-karpetan jasotzen dira. Harrera-iragazkiak gehitu ohi dira, eta ezizen baten emaila jaso ahala, azpikarpeta batera bidaltzen da. Kasu horretan, aurrekoan bezala, erasotzaileak ezingo luke posta nagusira sartu, eta kontraneurriak erraz inplementa litezke, besterik gabe ezizen hori deuseztatuta.

Azkenik, gure posta nagusian etiketak eransteko aukera ematen duten zerbitzariak daude: horrekin, posta elektronikoko identifikatzailea aldatzen da, baina mezu elektronikoak jatorrizkoaren karpeta berean entregatzen dira. Gmailekin egin daiteke hori.

Informazio gehiago

Gmail gai da erabiltzaile-izenaren ondoren eta @gmail.com baino lehen + ikurra erantsita helbide elektronikoak sortzeko. Mezu elektroniko guztiak erabiltzailearen sarrerako ontzi berera iritsiko dira, baina etiketa-iragazki baten bidez hobeto kudeatu ahal izango dira webguneei ematen zaizkien posta elektronikoak.

Adibidez, maria@gmail.com erabiltzailearentzat posta elektroniko gehigarriak sor ditzakezu:

maria+webCompra@gmail.com
maria+amazon@gmail.com
maria+spam@gmail.com

Mezu elektroniko guztiak iritsiko dira maria@gmail.com-eko sarrerako karpetara, baina bakoitzak etiketa desberdina du.

Gailu seguruak

Internet bidezko erosketa-prozesua nabigazioarekin hasten da, nahi duzun produktua webgune batean aurkitu arte. Hortik aurrera, ikusi dugun bezala, erosketa digitaleko prozedura guztia gertatzen da. Beraz, ezinbestekoa da nabigatzeko gailu informatiko bat erabiltzea.

Hainbat gailu erabil daitezke Interneten nabigatzeko: smartphoneak, tabletak, ordenagailu eramangarriak, mahai gaineko ordenagailuak eta abar. Horiek guztiek nabigatzaile bat behar dute erosketak egiteko denden webak arakatzeko: Chrome, Firefox, Edge eta abar.

Gomendio nagusia da gailu pertsonal bat erabiltzea, beste inorekin partekatu gabea. Gailua partekatua bada, baliteke nabigazioaren eta erosketaren ondoren fitxategiak uztea, eta beste erabiltzaile batzuek azter ditzakete haiek, horrek dakarren pribatutasun-arrakalarekin.

Gailu partekatu bat erabiliz gero, erabiltzaile bakoitzak bere profila pasahitzarekin babestuta izatea gomendagarria da, gainerako erabiltzaileek profil horretara sartzeko modurik izan ez dezaten.

Ezin bada pasahitz bidez babestutako profil propiorik izan, nabigatzaileen ezkutuko modua edo nabigazio pribatua erabiltzea gomendagarria da, saioa amaitutakoan nabigatzaileak berak sortutako fitxategi guztiak ezaba daitezen.

Sare seguruetan nabigatzea

Webak oso seguruak izan daitezke eta pribatutasun handia berma dezakete, baina segurua ez den hari gabeko sare bat erabiltzen ari bazara, edozein erasotzailek zer egiten ari zaren ikusteko aukera ematen ari zara.

Lehenengo aholkua sare publikoak ez erabiltzea da. Establezimenduek, kafetegiek edo beste saltoki batzuek doan eskaintzen dituzten WiFi sareak ere ez dira seguruak. Horiek sare seguruak erabiltzen dituzte, baina gakoa publikoa da, eta beraz, edonork ezagutu dezake eta sar daiteke sare horretara.

Hobe da gure sare propioa segurtasunez eta sarbide-kontrolarekin erabiltzea, sare horretan gu espia gaitzakeen erasotzailerik ez dagoela bermatzeko.

Hala ere, gure sare propioa erabili ezin badugu, baditugu zenbait aukera segurua ez den WiFi sare bat erabiltzeko arazoa saihesteko.

1 | Zeure telefono mugikorreko datuetatik abiatuta WiFi bat sortzea: zeure smartphonea erabiliz, WiFi sare bat sor dezakezu, zeuk bakarrik jakingo duzun gako batekin, eta smartphonea bera erabil dezakezu Internetera sartzeko, beste ezein gailuk WiFi hori erabiliko ez duela bermatuta.

2 | VPN bat erabiltzea: sare pribatu birtualek (VPN, ingelesezko siglen arabera) aukera ematen dute sare publiko baten barruan konexio seguruak sortzeko, urruneko zerbitzari batekiko konexio enkriptatu baten bidez. Zerbitzari horrek izapidetuko ditu egiten ditugun eskaerak.

Informazio gehiago

Ordainketa-metodoak eta haien segurtasuna. *e.digitall.org.es/pago-seguridad*

Ordainketa segururako metodoak. *e.digitall.org.es/metodos-pago*

Orri bat erosteko fidagarria den edo iruzurra den detektatzen du. *e.digitall.org.es/detectar-estafas*

TRUSTe® Privacy Certification. *e.digitall.org.es/truste*

DigitAll

Segurtasuna

4.3

OSASUNAREN ETA ONGIZATEAREN BABESA

Segurtasuna

C1 maila 4.3 Osasunaren eta ongizatearen babesa

Erabiltzaileak eta mezuak blokeatzeko gida bisuala. Osasunaren ikuspegia

Erabiltzaileak eta mezuak blokeatzeko gida bisuala. Osasunaren ikuspegia

Dokumentu honetan, erabiltzaileak eta jaso nahi ez ditugun mezuak blokeatzeko gida bisual bat erakutsiko da. Ildo horretatik, gailu mugikorretako eta sare sozialetako blokeoak aurkeztuko dira.

Sarean erabiltzaileak eta mezuak blokeatzea

Ordenagailuek eta gailu mugikorrek sarbide azkarra eta erraza ematen diete komunikazio-modu ugariri, hala nola deiei, mezuei edo sare sozialei. Horrek abantaila ugari ekarri dizkio harremanari, baina arrisku batzuk ere eragin ditu, hala nola ziberjazarpena edo flaminga. Maila honetako bideoetako batean kontzeptu horiek azaldu dira eta horiek detektatzeko eta babesteko jarraibide batzuk eman dira.

ZIBERJAZARPENA ETA FLAMINGA: NOLA DETEKTATU ETA BABESTU?

Bideo honetan ziberjazarpenaren eta flamingaren kontzeptuetan sakontzen da. Era berean, egoera horiek saihesteko eta detektatzeko zenbait metodo ematen dira.
e.digitall.org.es/A4C43C1V02

Dokumentu honek gailu teknologikoen eta sare sozialen konfigurazioa du ardatz. Zehazki, sarean erabiltzaileak eta mezuak blokeatzeko hainbat aukera aurkezten ditu.

OHARRA

Ordenagailuak etxeetara iritsi izanak, gailu mugikor eskuragarrietarako sarbideak eta Interneten hedapenak aldaketa sakona eragin dute pertsonek harremanak izateko moduan.

Gaur egun, ia mundu guztiak du Interneterako sarbidea duen telefono mugikor bat. Horrek hainbat komunikazio-modu ahalbidetzen ditu: deiak, bideodeiak, testu-mezuak edo sare sozialetako elkarreraginak.

Abantailak argiak dira. Gaur egun, ia edozein lekutatik dei bat egin daiteke, egiten ari den jardueraren argazki bat atera eta berehala bidali daiteke, edo ekitaldi bati buruz denbora errealean eztabaidatu daiteke.
Hala ere, horrelako komunikazioek zenbait arrisku ekar ditzakete, hala nola ziberjazarpena edo flaminga. Arrisku horietako batzuk mundu errealean ere gerta daitezke; dena dela, bitarteko digital baten bidez gertatzeak eragin handiagoa izan dezake jazarpen mota jakin batzuetan, mezuak oso erraz zabal daitezkeelako.

Horrelako egoerek sufrimendu handia eragin diezaiokete biktimari, eta horrek osasun mentalean izan dezake eragina.

Horrelako egoera batean neurriak har daitezke gailu teknologikoetan eta sare sozialetan, gertatutakoa agintariei jakinarazteaz eta osasun mentaleko espezialista batengana jotzeko aukera baloratzeaz gain. Hurrengo azpiataletan, erabiltzaile jakin bat sarean blokeatzeko moduak azalduko dira, baita gailu mugikorretan deiak eta mezuak jasotzea mugatzeko moduak ere.

Deiak eta mezuak blokeatzea gailu mugikorretan

Gailu teknologikoak erabiliz jazartzeko modu ohikoenetako bat telefono bidezkoa da. Jazarpen mota horrek behin eta berriz deiak egitea edo testu-mezuak bidaltzea dakar berekin. Gainera, askotan, dei horiek mehatxuak edo irainak izaten dituzte. Horrek guztiak beldurra, antsietatea edo estresa eragin diezaioke biktimari, eta ondorio nabariak izan ditzake haren osasun mentalean.

Informazio gehiago

Telefono bidezko jazarpena jazarpen mota bat da, eta, beraz, Espainiako Zigor Kodean jasotako delitua da. 172 ter artikuluak honako hau ezartzen du:

Hiru hilabetetik bi urterako espetxealdiaz edo seitik 24 hilabeterako isunaz zigortuko da pertsona bati behin eta berriro jazartzen zaiona, legez baimenduta egon gabe honako jokaera hauetako bat izaten badu, eta jokaera horrek haren eguneroko bizitza era larrian nahasten badu.

e.digitall.org.es/acoso-telefonico

Telefono bidezko jazarpen-egoera baten aurrean, agintariei jakinarazteaz gain, neurriak har daitezke gailu mugikorra konfiguratzeko menuaren bidez.

Gaur egun, ia ekipo guztiek dituzte telefono-zenbakiak blokeatzeko aukerak, marka edo modeloa edozein dela ere. Horrek zenbaki jakin batetik datozen deiak edo mezuak eragozteko aukera ematen du.

> **OHARRA**
>
> Batzuetan, jazarpen-egoera ez da pertsona jakin batena, bezeroak erakartzen saiatzen ari den konpainia batena baizik. Adierazitako gomendioez gain, oso aukera interesgarria dago: Robinson Zerrenda. Zerbitzu bat da, horretarako berariazko baimenik eman ez zaien erakunde edo enpresen publizitaterik ez jasotzeko.
>
> *listarobinson.es*

Ondoren, Android-gailu batean telefono-zenbaki bat nola blokeatu adieraziko da. Hala ere, prozedura oso antzekoa da iOS-terminaletan.

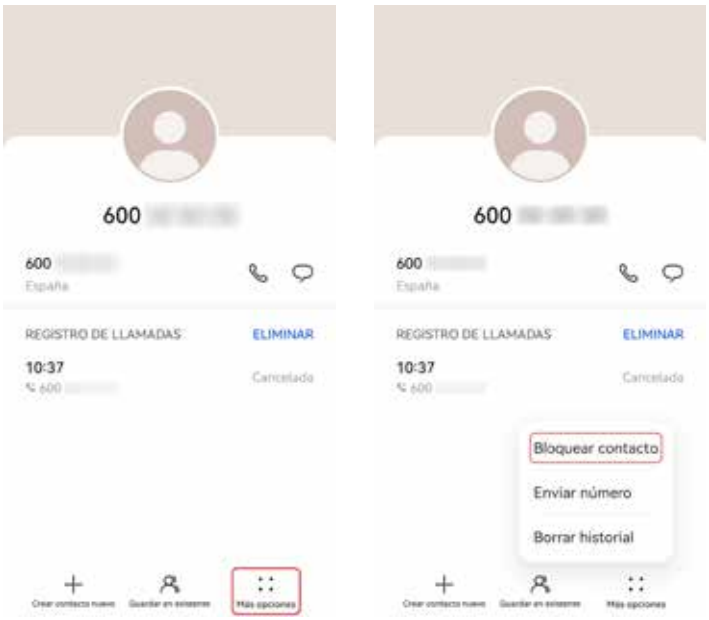
- Zenbaki bat blokeatzeko modurik errazena "**Telefonoa**" aplikazioa irekitzea da. Normalean, ekintza hori egiten denean, deien historia bistaratzen da; bestela, "**Berriak"** edo "**Deien historia"** aukera hautatu beharko da, gailuaren arabera.

Iturria: Geuk egina.

- Jasotako azken deiak bistaratu ondoren, blokeatu nahi den zenbakia aurkitu eta ikonoa sakatu behar da.

Iturria: Geuk egina.

- Ondoren, "**Aukerak"**-i dagokion ikonoa hautatu behar da, eta "**Blokeatu kontaktua**" botoian klik egin.



Iturria: Geuk egina.

- Horrela, zenbakia blokeatuta geratuko da, eta ez da zenbaki horretatik datorren deirik edo mezurik jasoko.

Iturria: Geuk egina.

Blokeatu nahi den zenbakia kontaktu gisa gordeta badago gailuaren agendan, prozedura ia berdina da. Besterik gabe, "**Kontaktuak**" aplikazioa ireki behar da, blokeatu nahi den kontaktua hautatu, eta aurretik azaldutako prozesua egin.

Informazio gehiago

Zenbaki jakin bat blokeatzeko ez ezik, gailuek zenbaki ezezagunak blokeatzeko iragazkiak konfiguratzeko aukera ere ematen dute, hau da, terminalean kontaktu gisa gordeta ez dagoen guztia blokeatzekoa. Era berean, identifikatuta ez dauden deiak ere blokeatu daitezke, hau da, telefono-zenbakia ezkutatzen dutenak.

Androiden web-esteka: *e.digitall.org.es/bloquear-telefono-android*
iOSen web-esteka: *e.digitall.org.es/bloquear-telefono-ios*

Erabiltzaileak eta mezuak blokeatzea sare sozialetan

Sare sozialen erabilerak gora egin du neurri handi batean azken urteotan, eta beraz, pertsonen artean komunikatzeko modu nagusietako bat bihurtu dira horiek. Horrek ziberjazarpen-bitarteko gisa erabiltzea ere ekarri du. Jazarpen-modu posible batzuk lotuta daude mezu, irudi edo bideo mingarriak, edo mehatxua ekar dezaketenak, behin eta berriz bidaltzearekin, gezurrak zabaltzearekin edo biktimaren identitatea ordeztuta mezuak bidaltzearekin.

Informazio gehiago

Unicefek dokumentu oso bat du bere webgunean, ziberjazarpenari buruzko galdera ohikoenetako batzuei erantzuteko, eta horri aurre egiteko moduari buruzko zenbait aholku ere ematen ditu.

e.digitall.org.es/ciberacoso

Munduan gehien erabiltzen diren sare sozialen artean, nabarmentzekoak dira Facebook, YouTube, WhatsApp edo Instagram. Horien guztien bidez ziberjazarpen-egoerak gerta daitezke; horregatik, erabiltzaileak eta mezuak blokeatzeko zer aukera eskaintzen dituzten jakitea garrantzitsua da.

Oro har, erabiltzaile bat blokeatzeak berekin dakar harengandik datorren mezurik edo edukirik ez jasotzea. Bestalde, blokeatutako erabiltzaileak ezingo du beste pertsonaren edukia ikusi, ezta harekin jardun ere, besteak beste.

Jarraian, erabiltzaile bat aipatutako sare sozialetan nola blokeatu azalduko da. Nolanahi ere, sare sozial guztiek blokeo-aukerak izan ohi dituzte.

Facebook

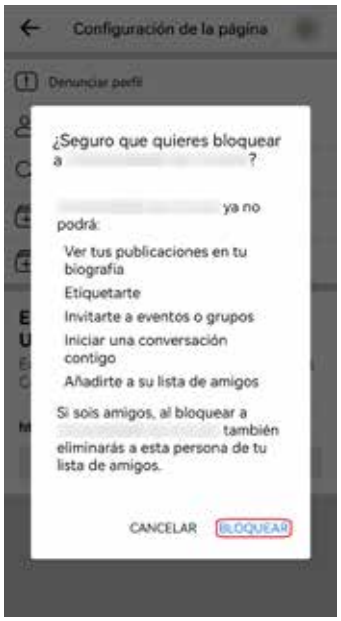
Facebooken norbaiten profila blokeatzen bada, hark ezingo du blokeoa egin duen pertsona etiketatu, ezta haren argitalpenak kontsultatu ere, besteak beste.

Facebooken profil bat blokeatzeko, urrats hauek egin behar dira:

1 | Bilatu blokeatu nahi den pertsonaren profila eta egin klik ikonoan.

Iturria: Geuk egina.

2 | Ondoren, mezu bat agertuko da, profila behin blokeatuta hark egin ezingo dituen ekintzak erakutsiko dituena. Prozesuarekin jarraitzeko, klik egin behar da "Blokeatu" aukeran.



Iturria: Geuk egina.

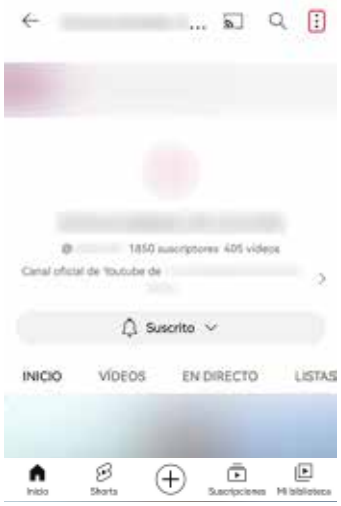
3 | Azkenik, mezu batek adieraziko du profila behar bezala blokeatu dela.

Iturria: Geuk egina.

Youtube

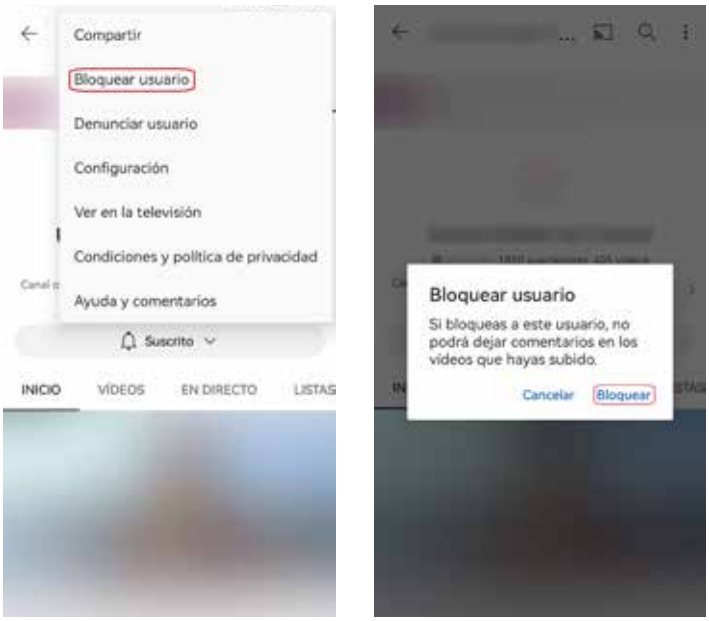
YouTube plataforma bat da, non erabiltzaileek bideoak parteka ditzaketen. Beraz, bere helburu nagusia ez da mezuak bidaltzea. Hala ere, bideoetan iruzkinak utzi daitezke, eta hori argitalpenaren egilea edo gainerako erabiltzaileak gogaitzea edo jazartzea helburu duten mezuak argitaratzeko bitarteko bat izan daiteke.

1 | Aurkitu blokeatu nahi den erabiltzailearen kanala eta hautatu ikonoa. ⋮



Iturria: Geuk egina.

2 | Egin klik “Blokeatu erabiltzailea” aukeran eta berretsi ekintza. Une horretatik aurrera, blokeatutako erabiltzaileak ezingo du iruzkinik utzi blokeoa eskatu duen pertsonaren bideoetan.



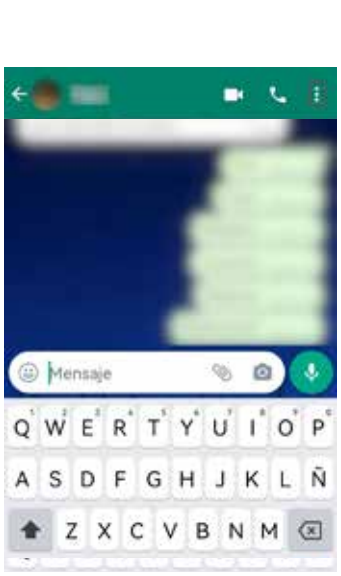
Iturria: Geuk egina.

WhatsApp

WhatsApp da, zalantzarik gabe, sareko komunikazio-plataforma nagusietako bat, eta, beraz, ziberjazarpen-egoeretako bitarteko nagusietako bat ere bada.

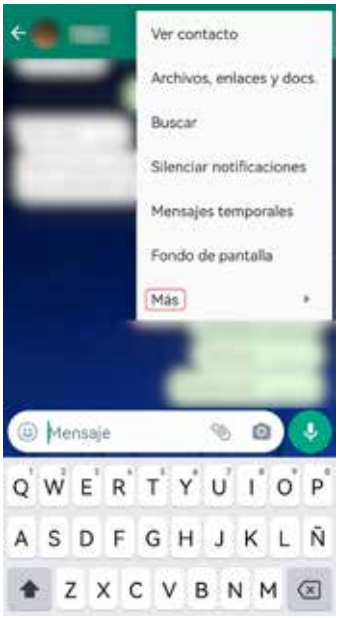
Hau da WhatsAppeko kontaktu bat blokeatzeko prozedura:

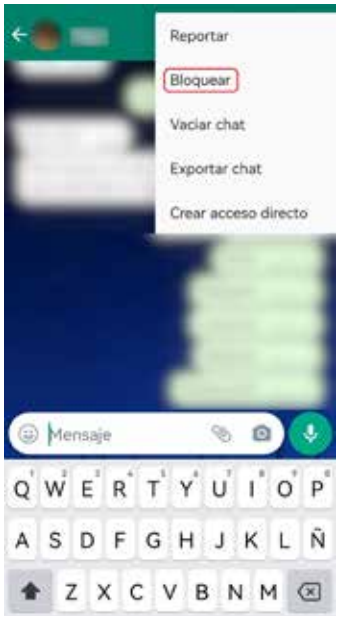
1 | Ireki kontaktuarekiko txata eta hautatu.



Iturria: Geuk egina.

2 | Agertzen den menuan, egin klik “Gehiago” aukeran eta, ondoren, “Blokeatu” aukeran.





Iturria: Geuk egina.

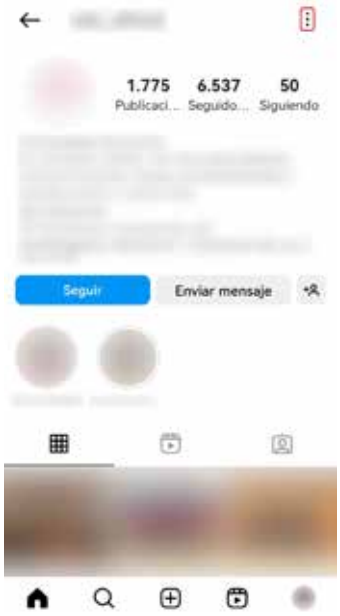
3 | Berretsi ekintza.

Iturria: Geuk egina.

Instagram

Instagram munduan gehien erabiltzen den sare sozialetako bat da. Sare horretako profil bat blokeatzeko jarraitu beharreko urratsak ikusitako gainerako plataformetakoen oso antzekoak dira. Jarraian, egin beharreko prozesua zehaztuko da:

1 | Aurkitu erabiltzailearen profila eta hautatu. ⋮



Iturria: Geuk egina.

2 | Egin klik “Blokeatu” aukeran.

Iturria: Geuk egina.

3 | Hautatu zer blokeatu nahi den: erabiltzailearen profil guztiak, edo etorkizunean sor litezkeenak, ala hautatutako profila bakarrik. Azkenik, egin klik “Blokeatu” aukeran.

Iturria: Geuk egina.

OHARRA

Sare sozial gehienek, erabiltzaileak blokeatzeko aukera emateaz gain, erabiltzaileak plataforman salatzeko aukera ere izaten dute. Horrela, sare sozialeko administratzaileek gertatutakoa ikertuko dute, eta, besteak beste, salatutako kontua eteteko neurriak har litzakete.

DigitAll

Segurtasuna

4.4 INGURUMENAREN BABESA

Segurtasuna

C1 maila 4.4 Ingurumenaren babesa

Ingurumen-jasangarritasunerako Big Data eta teknologia digitalak

Ingurumen-jasangarritasunerako Big Data eta teknologia digitalak

Dokumentu honetan terminoen glosarioa garatuko dugu, eta teknologia digitalen eta Big Dataren aplikazioekin lotutako kontzeptuak zabalduko ditugu, efizientzia energetikoari eta jasangarritasunari dagokienez, maila honetako bideoetan jasotakoak.

***"Teknologia digitalak, Big Data eta Ingurumen Jasangarritasuna"* A4C44C1V02 bideoan** ikusi dugun bezala, gaur egun, planetaren ingurumen-egoerarekin lotutako erronka oso garrantzitsuei aurre egin behar diegu. Erronka horiek gaur egungo geure bizitzako alderdi guztietan eragiten digute, eta aldatu egin behar ditugu haiek, etorkizuneko aldaketetara egokitu ahal izateko.

TEKNOLOGIA DIGITALAK, BIG DATA ETA INGURUMEN JASANGARRITASUNA

Teknologia digitalen erabilera masibotik datozen datuen fluxua aztertzeko ingurumen-aplikazioak, efizientzia energetikoa hobetzen eta jasangarritasunaren alde egiten laguntzen dutenak.
e.digitall.org.es/A4C44C1V02

Horretarako, gobernuak eta enpresa pribatuak, gaur egungo une erabakigarriaz jabetuta, erronka horiei aurre egiteko eta, ingurumenarekiko errespetua mantenduz, baliabide naturalak babesteko eta kontserbatzeko politikak garatzen hasi dira. Politika horiek garatzeko, Big Dataren analisia bezalako tresna efikazen erabileraren emaitzez baliatzen dira. Big Data funtsezko tresna bihurtu da erabakiak hartzeko, neurrien arrakasta edo porrota aztertu edo herritarren iritzia ezagutzeko bidea ematen baitute.

Egunero milioika datu digital sortzen dira mundu osoan, eta administrazioak edo enpresek datu horiek biltegiratzen dituzte gero erabiltzeko.

ADI

Datu horien aniztasuna hain da zabala, non giza jardueraren alderdi guztiak barne hartzen dituzten, baita planetako eremu guztietako erregistro naturalak ere. "Big Data" esaten zaio datuak eskala handian metatu, prozesatu, aztertu eta erabiltzeari. Datu horiek ingurumen-kudeaketarako eta garapen jasangarrirako erabiltzen badira, orduan "*Sustainable Data*" edo "Datu jasangarriak" esaten zaie.

Big Dataren jatorria

TEKNOLOGIA DIGITALAK, BIG DATA ETA INGURUMEN JASANGARRITASUNA

e.digitall.org.es/A4C44C1V02

Maila honetako "Teknologia digitalak, Big Data eta Ingurumen Jasangarritasuna" bideoan esaten denez, Big Data ari garela, hainbat galdera sortzen dira: zer dira?, nola sortzen dira? eta zertarako balio dute?, adibidez.

Big Data zer da?

Big Data datu "gordin" ugari dira, eta berariazko programa informatikoen bidez prozesatzen dira, sektore jakin batzuei lagundu diezaiekeen informazioa lortzeko.

Big Data nola sortzen da?

Informazio-kantitate hori hainbat modutan bil daiteke. Sateliteen irudiak, estazio meteorologikoak, gailu mugikorrak, tenperatura-sentsoreak, hezetasun-sentsoreak edo argitasun-sentsoreak izan daitezke edo sare sozialetatik (Facebook, Instagram, Tik Tok...) eta datu-base publikoetatik ere lor daitezke. Hona hemen, laburbilduta, Big Dataren iturri nagusiak:

1 | **Pertsonek sortutakoak.** Lehen eskuko informazio-iturri handi bat sare sozialak dira, eta oso kalitate onekotzat jotzen dira. Sare horiek datuak, iritziak, edukiekiko erreakzioak eta erabiltzaileen beraien irudiak ere biltzen dituzte, gobernuentzat eta enpresentzat interesgarriak izan daitezkeen alderdiei buruzkoak. Adibidez, mezu elektroniko bat bidaltzea, Facebooken iruzkin bat idaztea, telefono bidezko inkesta bati erantzutea, kalkulu-orri batean informazioa sartzea, WhatsApp bati erantzutea, bezero baten harremanetarako datuak hartzea, Interneteko esteka batean klik egitea... Egunero egiten ditugun ekintza ugari datu-iturri izugarriak dira.

OHARRA

Big Dataren tamainaren adibide bat erabiltzaileek sare sozialetan sortzen dituzten datuak dira: Googlek egunero 3,5 mila milioi bilaketa-kontsulta baino gehiago prozesatzen ditu, egunero 350 milioi argazki kargatzen dira Facebooken, egunero 306,4 mila milioi mezu elektroniko bidaltzen dira eta 5 milioi txio egiten dira.

2 | Makinen arteko informazio-trukeak sortutakoak. Pertsonen arteko interkonexioaz gain, makinak ere interkonektatuta daude eta datuak zuzenean partekatzen dituzte: M2M izenaz ezagutzen da (ingelesezko "machine to machine"-tik dator). Hala, tenperatura kontrolatzeko sistemak, parkimetroak, lorategiak automatikoki ureztatzeko sistemak, ibilgailuen eta telefono mugikorren GPSa, zentro publiko eta pribatuetan dauden era guztietako salmenta-makinak edo etxebizitzetako elektrizitate-kontagailuak, makinek kontrolatutako beste sistema askoren artean, beste sistema batzuekin komunikatzen dira gailuen bitartez, eta jasotako datuak transmititzen dizkiete sistema horiei. Horiek guztiek komunikazio-metodoak erabiltzen dituzte interkonexioa gauzatzeko, hala nola Wifi, ADSL, zuntz optikoa edo Bluetooth.

3 | Biometrikoak. Datu horiek eguneroko bizitzan barrutietara sartzeko erabiltzen diren edo jarriak daramatzagun (ingelesez, *weareables*) sentsoreetatik datoz. Hona hemen adibide batzuk: telefono mugikorren hatz-marken sentsoreak, erretina-eskanerrak, DNA-irakurgailuak, aurpegia edo ahotsa ezagutzeko sentsoreak, jarduera-eskumuturrekoak, pultsometroak eta abar. Haien erabilera oso zabalduta dago segurtasun-arloan, aldaera guztietan (pribatua, korporatiboa, militarra, poliziakoa, inteligentzia-zerbitzuetakoa eta abar), bai eta kirol- eta medikuntza-teknologian ere.

4 | Web marketina. Merkataritza elektronikoaren eta online-salmentako atarien hazkundearen ondorioz, sareko gure mugimenduak era guztietako neurketen mende daude, eta horien helburua marketin-azterketak eta jokabide-azterketak egitea da. Adibidez, web bateko erabiltzaileen kurtsorearen mugimenduaren miaketan, orriaren posizioaren detekzioan edo orri horretako desplazamendu bertikalaren jarraipenean oinarritutako bero-mapak egiten direnean. Datu horiekin ondorioak ateratzen dira, hala nola orri bateko zer atalek erakartzen duten gehien erabiltzailea, edo zer produktu interesatzen zaizkion gehien (zer produktutan egiten duen klik edo zer eremutan pasatzen duen denbora gehien, alegia).

5.- Datuen babesa. Merkataritza elektronikoaren, banku-kontu batetik besterako datu-transferentzien, hegazkin-txartelen erreserben edo artikulu bat merkataritza elektronikoko atari bateko erosketa-orga birtual batean sartzearen hazkundea da adibideetako bat.

Big Datak zertarako balio du?

Gaur egun gehien egiten den galderetako bat da zertarako balio duen Big Datak edo zer onura dakarten, batez ere kontuan hartuta, oro har, nahiko kontzeptu berria dela jendearentzat. Erabilera eta onura ugari daude, eta honako hauek dira nabarmenenak:

1 | **Ekoizpen-kostuak murriztea eta baliabideak optimizatzea.** Datu-teknologia handiek eta hodeian oinarritutako analisiak abantaila handiak dakartzate kostuei dagokienez, datu ugari biltegiratu behar direnean eta baliabideak kudeatzeko modu efizienteagoak identifikatu behar direnean (azken horiek etekin ekonomiko, sozial edo teknologiko handiagoa emango duten jardueretara bideratzeko).

2 | **Iruzurrezko jokabidea edo egindako ekintzei buruzko** iritziak detektatzea. Gobernuek edo enpresek neurriak hartzen dituztenean edo produktuak jaurtitzen dituztenean, Big Data erabiltzen dute ekintza horien emaitza aztertzeko. Aztertutako eta egituratutako datu horiek informazio asko ematen dute ekintza horien jarraipena aldatu, hobetu edo ezeztatzeko.

3 | **Erabaki adimendunak hartzea eta horretarako denbora murriztea.** Analisiaren abiadurak, datu-iturri berriak aztertzeko gaitasunarekin uztartuta, aukera ematen du erakundeek ikasitakoan oinarritutako erabakiak hartzeko.

4 | **Akatsen, arazoen eta hutsuneen sorburua zehaztea ia denbora errealean.**

5 | **Produktu berriak garatzea.** Bezeroen beharrak eta haien gogobetetzea ebaluatzeko gai izateak dakar haiek nahi dutena emateko ahalmena. Horrek esan nahi du item berriak sor daitezkeela eskakizun horiei erantzuteko.

6 | **Eskaintzak optimizatzea.** Big Datak aukera ematen du aurreikusteko, erosleen aurreko jokabideetan oinarrituta, haiek nola jokatuko duten etorkizunean eta, beraz, eskaintzak modu arrazoituan ezar daitezke eta dirua aurrez daiteke.

7 | Salmenta-puntuan bezeroentzako kupoiak sortzea, haien erosketa-ohituretan oinarrituta.
8 | Merkatua hobeto ezagutzea.
9 | Lehiakideei jarraipena egitea. Makrodatuek lehiakideak hobeto ezagutzen eta aurrea hartzen laguntzen dute.
10 | Informazioa denbora errealean eskuratzea. Informazio zaharkituak ez du balio aplikagarririk gaur egun, eta are gutxiago, etorkizunean; horregatik, teknologia horrek egunero ematen duen datu-bilketak berehalako feedbacka izatea ahalbidetzen du.

Big Data motak

Egituratuak

Formatu finkoan biltegiratu eta prozesa daitekeen eta sarbidea izan dezakeen edozein daturi "egituratutako" datu esaten zaio. Datuen tratamenduan erabili ohi direnak dira. Beren ezaugarri nagusiak hauek dira: tauletan gorde daitezke eta luzeraren eta formatuaren definizio argia dute.

Horietakoak dira, besteak beste, zenbakiak, karaktere-kateak eta datak. Informazio gehiago duten beste datu mota batzuk egon arren, horrek ez du esan nahi garrantzirik ez dutenik. Hala ere, gaur egun, arazoak daude datu horien tamainarekin, asko hazten ari baitira, eta zettabyte anitzen mailaren ohiko dimentsioetara iristen ari baitira.

Egituratu gabeak

Modu ezezagunean dagoen edo egitura egituratu gabeko datu gisa sailkatua duen edozein datu da. Tamaina aldetik izugarriak izateaz gain, egituratu gabeko datuek erronka ugari planteatzen dituzte haietatik balioa eratortzeko prozesamenduari dagokionez.

Jatorrizko formatuan dauden datuak dira; jaso ziren moduan daude, alegia. Ez dute modu tradizionalean biltegiratzeko aukera ematen duen formatu espezifikorik, haien informazioa ezin baita bereizi luzeran eta formatuan zehaztutako datu moten arabera. Horien artean ohikoak dira, adibidez, mezu elektronikoak, multimedia-aurkezpenak (powerpointak, esaterako), testu-prozesadoreen dokumentuak edo PDF formatuko fitxategiak.

Egituratu gabeko datuen ohiko adibide bat dira testu-fitxategi sinpleen, irudien eta bideoen -besteak beste- konbinazio bat duten datu-iturri heterogeneoak.

Gaur egun, erakundeek datu ugari dituzte eskuragarri. Baina, zoritxarrez, ez dakite nola eratorri balioa haietatik, modu gordinean edo formatu egituratu gabean daudelako datu horiek.

Erdiegituratuak

Datu erdiegituratuek bi datu mota horiek eduki ditzakete. Definitu daitekeen formatu bat izaten dute, baina erabiltzaileak ezin du erraz ulertu, eta horregatik, informazioaren pieza bakoitza nola irakurri zehazten lagunduko duten arau konplexuak erabili behar dira. Datu erdiegituratu baten adibide bat XML fitxategi batean erakutsitako datu bat da.

Egitura moduko bati jarraitzen diote, baina egitura hori ez da datu egituratu gisa kudeatzeko bezain erregularra. Eredu komun batzuk dituzte, deskribatu egiten dituztenak eta haien arteko erlazioei buruzko informazioa ematen dutenak. Adibidez, HTML, web-orriak egiteko lengoaia, non etiketa-sistemak jarraibide komun horiek detektatzeko aukera ematen duen.

Erabileraren adibideak

***"Teknologia digitalak, Big Data eta Ingurumen Jasangarritasuna"* A4C44C1V02** bideoan gai honi buruz erakutsitako adibideez gain, askoz adibide gehiago daude Big Data jasangarritasunerako erabiltzeari buruz, hala nola leonardo konpainiaren proiektua (*leonardo.com*). Konpainia hori Big Datan oinarritutako hainbat proiektu garatzen ari da sateliteetako informazioa erabiliz.

TEKNOLOGIA DIGITALAK, BIG DATA ETA INGURUMEN JASANGARRITASUNA

e.digitall.org.es/A4C44C1V02

Besteak beste, nabarmentzekoa da satelite-irudien erabilera: irudi horiek algoritmo indartsuekin prozesatzen dituzte, NBEren 2030 Agendako Garapen Jasangarrirako Helburuak (GJH) lortzen laguntzeko, hala nola lurzoruaren, ur-baliabideen, basoen eta hirien kudeaketa jasangarria. Sateliteek oso ekarpen garrantzitsua egiten dute; izan ere, behaketa-puntu bakar baten bidez, behatu nahi ditugun aldagai eta fenomenoen neurketa bat eskaintzen dute, hau da, globalak, objektiboak eta planetako puntu batetik bestera eraman daitezkeenak, jasangarritasun-adierazleekin erlazionatzeko.

Informazio gehiago

- *e.digitall.org.es/sustainable-data*
- *e.digitall.org.es/un-bigdata*
- *e.digitall.org.es/master-bigdata*
- *e.digitall.org.es/data-catalog*
- *e.digitall.org.es/fao*
- *e.digitall.org.es/bigdata-analysis*
- *lifeunderyourfeet.org*
- *e.digitall.org.es/bangladesh*
- *e.digitall.org.es/postgrado-bigdata*
- *e.digitall.org.es/youtube-bigdata*

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