IKTen Gerenteordetzaren gomendio praktikoak segurtasun informatikoa kudeaketa lanetan aplikatzeko, SENen eta DPBLOren aplikaziotik eratorrita.

1 Sarrera

Bistan da bitarteko elektronikoak gero eta gehiago erabiltzen direla unibertsitatean. Gertaera hori 2012-2017 Plan Estrategikoaren ondorio zuzena da, eta, horren bidez erantzun eraginkor bat eman nahi zaio UPV/EHUk bete behar duen eta zerbitzu elektronikoen arloan gero eta ugariagoa den araudiari.

Nolanahi ere, bitarteko elektroniko horien erabilerak betebehar bat ezartzen dio UPV/EHUri, erabilera hori konfiantzaz egiteko baldintzak sor ditzan sistemen, datuen, komunikazioen eta zerbitzu elektronikoen segurtasuna bermatzeko neurriak aplikatuta; hartara, bitarteko horien bidez, unibertsitateko kideek beren eskubideak erabili eta betebeharrak beteko dituzte, beharrezkoak diren bermeekin.

Dokumentu honen xedea da informazioaren segurtasun kontzeptuak langileei hurbiltzea, lanpostuen eginkizunei lotuta. Horri begira IKTen Gerenteordetzak eginiko hainbat gomendio aurkezten dira, langile guztiek segurtasun informatikoa kudeaketa lanetan zuzen aplika dezaten.

Aplikatu beharreko segurtasun neurriak ez daude bakarrik teknologiaren menpe; haatik, beharrezkoa da zerbitzuak ematen eta datuak erabiltzen dituzten langileek behar bezala prestatuta egotea eta horri buruzko prestakuntza espezifiko bat jasotzea, unibertsitateko sistema eta zerbitzuetan aplikagarriak diren informazioaren teknologiak segurtasunez erabiliko direla bermatzeko.

Hori dela eta, dokumentu honek biltzen ditu, batetik, datu pertsonalen babesaren eta informazioaren segurtasunaren arloko lege betebeharrei buruzko oinarrizko kontzeptuak, eta, bestetik, segurtasun neurrien aplikazio praktikorako hainbat gomendio, langile guztiek erabili beharrekoak eguneroko lanean. Neurri horiek lotuta daude, besteak beste, lanpostuan eduki beharreko portaerari, informazioaren erabilera zuzenari eta hura gordetzeko gailu mugikorren eta euskarrien erabilerari.

1.1 Oinarrizko kontzeptuak

Informazioaren segurtasuna da kontzeptu nagusia, eta beste guztiak horren inguruan dabiltza. Halere, kontzeptu horren bi terminoak bereizita aztertzea komeni da, kontzeptuaren esanahiaz osorik jabetzeko.

RAEren (Espainiako Errege Akademia) arabera, **segurtasuna** arriskurik edo kalterik eza da. Segurtasunaren definizio horretatik ondoriozta dezakegu, beraz, arrisku kontzeptuak lotura estua duela segurtasunarekin.

RAEren arabera, **informazioa** ezagutzen multzo bat da, gai jakin baten inguruan ditugun ezagutzak zehaztea edo areagotzea ahalbidetzen duena. Dena den, badago beste definizio bat, guretzako erabilgarriagoa izan daitekeena, eta, horren arabera, informazioa datu prozesatuen multzo antolatu bat da, subjektu edo sistema hartzailearen ezagutza egoera aldatzen duen mezu bat osatzen duena.

Datu pertsonalaren –pertsona fisiko identifikatu edo identifikagarriei buruzko informazio oro– kontzeptua aztertzen badugu, bistan da datu pertsonalak informazioaren azpimultzo bat baino ez direla; beraz, informazioaren segurtasunean aplikagarriak diren kontzeptu guztiak halakoak izango dira ere datu pertsonalen segurtasunari buruz ari garenean.

Informazioaren segurtasun kontzeptua honela definitzen da: nolabaiteko konfiantza mailaz eusteko gaitasuna, informazioaren eskuragarritasuna, benekotasuna, trazabilitatea, osotasuna eta/edo konfidentzialtasuna arriskuan jar dezaketen istripuen aurrean eta legez kanpo edo asmo txarrez egindako ekintzen aurrean. Ikus dezakegunez, definizio horretan, arriskua askoz ere zehaztuagoa geratzen da (istripuak edo legez kanpo edo asmo txarrez eginiko ekintzak), segurtasun kontzeptua bere horretan geratzen da (nolabaiteko konfiantza mailaz eusteko gaitasuna) eta informazioak jasan dezakeen kaltea zehazten da: haren eskuragarritasuna, osotasuna, konfidentzialtasuna, benekotasuna eta/edo trazabilitatea arriskuan egotea.

Kontzeptu horrek **segurtasunaren 5 dimentsioak edo ezaugarriak** biltzen ditu:

- **Eskuragarritasuna:** Erabiltzaile baimenduek, hala behar dutenean, informazioa eta horri elkartutako aktiboak eskuratuko dituztela ziurtatzea.
- **Osotasuna:** Informazioaren eta hura prozesatzeko metodoen zehaztasuna eta osotasuna bermatzea.
- **Konfidentzialtasuna:** Informazioa hura eskuratzeko baimena duten pertsonek bakarrik eskuratuko dutela ziurtatzea.
- **Benetakotasuna:** Identitatea edo jatorria ziurtatzea.
- **Trazabilitatea:** Une oro nork zer eta noiz egin duen zehaztu daitekeela ziurtatzea.

Informazioaren segurtasun kontzeptutik haren gauzapena ere eratortzen da. Hala, helburua mehatxu jakin batzuei eusteko gaitasuna edukitzea bada, eusteko modua (segurtasuna) neurri zehatzak aplikatzea izango da, erresistentzia hori lortzeko.

Segurtasun neurri horiek arlo askotan aplika daitezke:

- **Antolakuntza:** Segurtasuna aplikatzean rolak eta erantzukizunak zehaztea.
- **Araudia:** Segurtatu beharreko informazioa erabiltzen duten langileen betebeharrak definitzea.
- **Operatiboa:** Pertsonen jarduteko modua prozeduren bidez arautzea, informazioa eta hura prozesatzen duten bitartekoak –informatikoak gehienetan– segurtasunez erabil ditzaten.
- **Kontraktuala:** Unibertsitatez haragoko betebeharrak ezartzea, azpikontratatutako enpresek eta beren langileek bete beharreko baldintzak zehaztuta eta unibertsitatearen erantzukizunak bere arlora mugatuta.

- **Teknologikoa:** Konponbide teknologikoak aplikatzea, ezarritako betebeharretan eta prozeduretan pertsonen ez-betetzeak saihesteko eta, modu horretan, haien jardun segurua bermatzeko. Neurri horietako asko informatikoak diren arren, neurri teknologikoak ere aplikatzen dira segurtasun fisikoaren gainean (sarrailak, sarbide txartelak, etab.).

1.2 Informazioaren segurtasuna arautzen duten legeak

1.2.1 Segurtasuneko Eskema Nazionala

Segurtasuneko Eskema Nazionala edo **SEN** arau hauek eratzen dute: 3/2010 Errege Dekretuak, urtarrilaren 8koak, administrazio elektronikoaren arloan segurtasuneko eskema nazionala arautzen duenak, eta dekretu hori aldatzen duen urriaren 23ko 951/2015 Errege Dekretuak.

Segurtasun Eskema Nazionalaren helburua da bitarteko elektronikoen erabileran beharrezkoak diren konfiantza baldintzak sortzea. Horretarako, sistema, datu, komunikazio eta zerbitzu elektronikoen segurtasuna bermatzeko neurriak ezarriko dira, bitarteko horien bidez herritarrek eta administrazio publikoek beren eskubideak erabili eta betebeharrak bete ditzaten.

Segurtasuneko Eskema Nazionala unibertsitatearen zerbitzu elektronikoei, horiek emateko beharrezkoak diren bitarteko elektronikoei eta zerbitzu eta/edo bitarteko horiek erabilitako informazioari aplikatzen zaie.

SENek erakunde publiko batek informazioaren segurtasun arloan bete beharreko eskakizunak zehazten ditu. Horretarako, segurtasun arloko erabakietan kontuan hartu beharreko oinarrizko printzipioak ezartzen ditu; informazioa egoki babesteko errespetatu behar diren gutxieneko eskakizunak zehazten ditu; eta, oinarrizko printzipioak eta gutxieneko eskakizunak betetzeko mekanismo bat definitzen du. Sistema horren bidez, segurtasun neurri proportzionalak hartzen dira, informazioaren, sistemen eta babestu beharreko zerbitzuen nolakotasuna aintzat hartuta. Horrela, Segurtasuneko Eskema Nazionalak aplikatu beharreko segurtasun sistemen katalogo bat egiten du antolakuntza neurriak, jardun neurriak eta neurri teknologikoak bereizita.

Hortaz, Segurtasun Eskema Nazionala aplikatuko zaio unibertsitatearen zerbitzuek eta horiei eusteko bitarteko elektronikoek tratatutako informazioari:

- Egoitza Elektronikoa: Ataria, sarrera erregistro elektronikoa, nire kudeaketak…
- APZkoentzako zerbitzuak / AZPkoek emandakoak: GAUR, EHUDoku, Langileen Ataria…
- Zerbitzuak emateko erabilitako bitartekoak: Lanpostua, PCa, zerbitzariak, komunikazioak…

1.2.2 Datu Pertsonalak Babesteko Lege Organikoa

Datu pertsonalen babesaren arloko lege nagusiak honako hauek dira: 15/1999 Lege Organikoa, abenduaren 13koa, Datu Pertsonalak Babesteari buruzkoa, eta 1720/2007 Errege Dekretua, abenduaren 21ekoa, 15/1999 Lege Organikoa garatzeko araudia onartzen duena.

Datu pertsonalak (pertsona bat identifikatzeko edo pertsona horri lotutako datu oro, hala nola izena, abizenak, NAN, helbidea, jaiotza data, argazkia, helbide elektronikoa …) babesteari buruzko legeen helburua datu pertsonalen trataeran pertsona fisikoen askatasun publikoak eta oinarrizko eskubideak babestea eta bermatzea da, bereziki haien ohoreari eta norberaren nahiz familiaren intimitateari dagokienez, baita datu pertsonalak biltzeak eta tratatzeak pertsonaren eskubideei ekar diezaieketen arriskuei aurre egitea ere.

Datu pertsonalen babesari buruzko legeak datu pertsonalei aplikatzen zaizkie, haiek erabiltzeko modua edozein delarik, bai euskarri fisikoetan (papera) bai euskarri elektronikoetan.

Datu pertsonalen babesaren arloko legediak erakunde publiko batek datu pertsonalak babesteko bete behar dituen eskakizunak definitzen ditu. Datuen babeserako printzipioak ezartzen ditu (datuen kalitatea, informazio betebeharra eta onarpena, datuen segurtasuna eta sekretu betebeharra, eta datuen komunikazioa –hirugarrenei uztea eta haien kabuz tratatzea–); eraginpeko pertsonen oinarrizko eskubideak zehazten ditu (sartzeko, zuzentzeko, ezeztatzeko eta aurka egiteko eskubideak); datu pertsonalen datu fitxategien arduradunen betebeharrak definitzen ditu; eta, datu pertsonalen trataeran aplikatu beharreko segurtasun neurriak ezartzen ditu, hala formatu elektronikoen nola paperean emandako informaziorako. Segurtasun neurri horiek mailatan (baxua/ertaina/altua) antolatzen dira, datu moten arabera. Hala, maila altua datu hauei ematen zaie: ideologia, sindikatu afiliazio, erlijio, sinesmen, arraza, osasun edo bizitza sexualari buruzkoak, eraginpeko pertsonen onespenik gabe polizia xedeekin bildutakoei edo horrelakoak dituztenei, eta genero indarkeriako ekintzetatik eratorritakoei.

Horrenbestez, datu pertsonalak babestearen arloko legeria aplikatuko zaio unibertsitateko zerbitzuetan eta horietan erabilitako bitarteko elektronikoetan tratatutako informazio pertsonalari, hots:

- Egoitza elektronikoan tratatutako datu pertsonalak: Nire kudeaketak…
- AZPko langileen datu pertsonalak: Langileen ataria…
- AZPko langileek tratatutako datu pertsonalak: GAUR…
- Datu pertsonalak tratatzeko erabilitako bitartekoak: Lanpostua, PCa, zerbitzariak, komunikazioak…

Horrela, egiaztatu daitekeenez, aplikatutako araudi espezifikoa zein den alde batera utzita, informazioaren segurtasuna kontuan hartu beharreko elementu bat da beti, unibertsitateko langileek edozein informazio mota erabiltzen duten ia egoera guztietan.

2 Segurtasuna kudeatzea

2.1 Segurtasunaren araudia

Unibertsitateak informazioaren segurtasuna arautzen du arauzko eta laneko segurtasun neurriak ezarrita, unibertsitatearen funtzionamendua legedira egokitzeko, legedi horren inguruko zalantzak eta interpretazio akatsak saihesteko, eta erabiltzaileei beren lana segurtasun maila egokian egiten laguntzeko, eguneroko lanerako jardun ildoak finkatuta.

Segurtasun neurri horiek hainbat dokumentu motatan jaso dira, eta dokumentu horietan jasotakoak eraginpeko pertsonek bete eta aplikatu behar dituzte. Dokumentuak honako hauek dira:

- Segurtasun Politika. Unibertsitateak kritikotzat jotzen dituen zerbitzuak eta informazioa kudeatzeko eta babesteko modua arautzen duten jarraibideen multzo bat da. URL honetan aurki daiteke: https://egoitza.ehu.eus/es/informazioaren-segurtasun-politika
- Segurtasun Arauak. Dokumentu hauetan ekipoen, zerbitzuen eta instalazioen erabilera zuzena deskribatzen da, erabilera desegokia zer den esaten da, eta arauak betetzen ez direnean langileen erantzukizuna zein den deskribatzen da, indarrean dagoen legediarekin bat etorrita.
- Segurtasun Prozedurak. Dokumentu hauetan adierazten da nola egin behar diren eguneroko lanak, nor arduratzen den lan bakoitzaz, eta nola identifikatzen eta jasotzen diren portaera anomaloak.
- Segurtasun Gidak. Dokumentu hauetan zeregin jakin batzuk egiteko modu egokiak deskribatzen dira, eta deskribatutako zereginak egiteko modu onenak gomendatzen dira.

2.2 Segurtasun arriskuak kudeatzea

Arriskuen kudeaketa segurtasunaren kudeaketaren muina da. Horren helburua aplikatutako segurtasun neurriak arriskuekiko proportzionalak izatea da; hartara, arriskua zenbat eta handiagoa izan, orduan eta segurtasun handiagoa beharko da.

Arriskuen kudeaketa bi fasetan bereizten da. Lehenengoa **arriskuen analisia** da. Horretarako, lehenik eta behin, zerbitzuetan esku hartzen duten **aktibo guztiak identifikatzen dira** (zerbitzuak, informazioa, datu pertsonalak, bitarteko elektronikoak, pertsonak, etab.), eta gero **aktibo horien garrantzia baloratzen da**, horien segurtasuna "galtzeak" zenbateko larritasuna duen zehaztuta. Balorazioa aktibo bakoitzaren arduradunak egin behar du, berak baitu garrantzi hori modu egokian ebaluatzeko gaitasuna.

Aktiboak identifikatu eta baloratu direnean, aktibo bakoitzari eragiten dioten **mehatxuak ebaluatzen dira**, mehatxu horiek eragin dezaketen "kaltea" (inpaktua) zenbatuta; horrela, mehatxu bakoitzari lotutako arriskua ebaluatu nahi da.

Arriskuen kudeaketaren bigarren fasea arriskuak arintzea da; horretarako, aktibo bakoitzean aplikatu beharreko segurtasun neurriak zehaztu behar dira, mehatxu bakoitzak aktiboari egin diezaiokeen "kaltea" arintzeko; modu horretan, arriskua gutxituko da unibertsitateak onargarri jotzen dituen mailetara.

Hortaz, unibertsitateak, ziur asko, lehenago aplikatuko ditu segurtasun neurriak birus informatiko bati aurre egiteko, non arriskua handia den (nahiko gertagarria eta inpaktu handikoa; izan ere, ezabatzen ez bada eta zabaltzen bada, jende guztiaren lanari eragiten dio), lurrikara bati aurre egiteko baino, non arriskua ertain-baxua den (probabilitate oso gutxi daude, baina inpaktua handia da, pertsona guztiei eragiten baitie).

2.3 Segurtasuneko gorabeherak kudeatzea

Zoritxarrez, segurtasun neurriak ez dira hutsezinak. Dela haien aplikazioa pertsonen baitan dagoelako dela neurri teknologikoek ere huts egiten dutelako, egoera jakin batzuetan segurtasuneko gorabeherak gertatzen dira; hau da, inork nahi ez dituen ezusteko gertakariak, aktiboen segurtasunean (segurtasun dimentsioren batean) eragin negatiboa dutenak. Segurtasuneko gorabehera horiek, praktikan, egoerak dira, hala nola aplikazio batean datu okerrak agertzea, informazio jakin bat behar ez den lekuan agertzea (eduki behar ez lituzkeen pertsonarengana iritsitako paperezko dokumentuak), ordenagailuak gauza "oso arraroak" egitea, etab.

Segurtasuneko gorabeherak saihetsezinak direnez, informazioaren segurtasunaren oinarrizko faktoreetako bat segurtasun gorabeheren kudeaketa da, gerta daitezkeen segurtasuneko gorabeherak artatzeko jarduera planen garapen gisa ulertuta. Plan horiek, gorabeherak konpontzeaz gainera, neurketa mekanismoak ere izango dituzte, segurtasun neurrien kalitatea ezagutzeko eta joerak hautemateko, arazo handiak izatera iritsi aurretik.

Gorabeheren kudeaketan, pertsona guztien menpe dauden oinarrizko bi pauso daude: segurtasuneko gorabehera hautematea eta jakinaraztea. Horrek esan nahi du langile guztiek segurtasuneko gorabehera bat den edo izan daitekeen egoera mota oro identifikatzeko ardura dutela, baita hura Erabiltzaileentzako Zerbitzuari edo delako zerbitzu zein arloari lehenbailehen jakinarazteko ardura ere. Hortik abiatuta, unibertsitateak izendatutako pertsonak arduratuko dira segurtasuneko gorabehera tratatzeaz eta konpontzeaz, aurreikusitako prozeduren arabera.

3 Segurtasuna aplikatzea

Unibertsitateak segurtasun neurri asko bermatzen baditu ere, beste neurri batzuk, arauzkoak edo lanekoak direlako, unibertsitateko langileek eta erabiltzaileek modu egokian eta azkarrean aplikatu behar dituzte. Hori dela eta, kudeaketa lanetan kontuan hartu beharreko segurtasun neurri guztiak definitzen ditugu jarraian.

3.1 Informazioa babestea

Informazioari zuzenean aplikatzen zaizkion segurtasun neurriak dira eraginkorrenak, haren babes zuzena bermatzen dutelako.

3.1.1 Informazioa sailkatzea

Informazioari aplikatutako lehen segurtasun neurria bere sailkapena da, segurtasunaren ikuspuntutik. Horretarako, hainbat alderdi hartu beharko genituzke kontuan, hala nola informazio aktiboa baloratzea (arriskuen analisiaren atalean azaldu den moduan),

segurtasuneko gorabehera batek informazio horretan izan dezakeen eragina aintzat hartzea, eta informazioaren nolakotasuna zehaztea, besteak beste, legezko irizpide aplikagarriak aintzat hartuta (DPBLO, datu pertsonalak izatekotan, edo beste batzuk).

Informazioa sailkatzeko hainbat maila aplikatzen dira, eta horretarako, eskuarki, haren konfidentzialtasunari erreparatzen zaio; hartara, informazio publikoa batere konfidentzialtasunik ez duen informazioa da, eta informazio sentikorra edo erreserbatua, konfidentzialtasun mailaren bat duena, horren arabera hainbat maila ezarrita (hainbat kontzeptu erabil daitezke, hala nola barne erabilerako informazioa, isilpekoa, mugatua, etab.).

Informazioa sailkatzearen xedea sailkapen horrekiko proportzionalak izango diren segurtasun neurriak aplikatu ahal izatea da; hala, konfidentzialtasun maila apaleko informazioa malgutasun handiagoz erabili ahal izango da, eta informazioa erabiltzeko murrizketak soilik aplikatuko dira, konfidentzialtasunak hala eskatzen duenean. Modu horretan, informazioa tratatzeko irizpideak aplikatuko dira unibertsitateak hainbat jardueratarako ezarritako prozedurekin bat etorrita, jarduerak horiek izanik, besteak beste, sarbide kontrola, biltegiratzea, kopiak egitea, kanpoko biltegiratze euskarriak erabiltzea, transmisio telematikoa, etab.

Edonola ere, informazioaren tratamenduari lotutako oinarrizko printzipio batzuk aintzat hartu beharko dira; esate baterako, erabiltzaileak aplikatutako segurtasun neurriek neurritsuak izan beharko dute, eta kontuan hartu beharko dute, alde batetik, informazio horren erabilera inguruaren segurtasuna (unibertsitatekoa kanpokoa baino ingurune fidagarriagoa dela kontuan hartuta, kanpoan zorroztasun handiagoz aplikatu beharko dira neurriak), eta, bestetik, informazioaren konfidentzialtasun maila, kontuan hartuta, betiere, informazio korporatiboak zerbitzu korporatiboetan egon behar duela, informazio korporatiboa aldi baterako maila lokalean erabil daitekeen arren. Nolanahi ere, aldi baterako trataera horretarako kontuan hartu beharko dira informazioa, euskarriak, lanpostua eta/edo ondoren adierazitako gailu mugikorrak babesteko neurriak.

3.1.2 Zifratzea

Informazioa zifratzea segurtasun bitarteko ahaltsua da, baina kontuan hartu behar da oso prozesu sentikorra eta arriskutsua dela; izan ere, pasahitza galtzen edo informazioa zifratzeko erabilitako ziurtagiria baliogabetzen bada, ezin izango dugu berreskuratu zifratutako informazioa. Beraz, zifratzea soilik erabiliko dugu konfidentzialtasun maila goreneko informazioarekin eta DPBLOren arabera maila altua duen informazioarekin.

Informazioa biltegiratzean era askotan aplika daiteke zifratzea, aplikazio eremuaren arabera:

- Fitxategiak zifratzea, programen (pdf, Office, etab.) berezko tresnen bidez, baita karpeta osoak ere, zifratzeko tresna berezien bidez. Horrelakorik eduki ezean, eskaera bat egin daiteke Erabiltzaileentzako Zerbitzuan.

- Pen-driveak, CDak, DVDak eta antzekoak zifratzea; horrelakoetan, maila horri dagokion informazioa daukaten fitxategiak grabatzen dira, zifratze tresna espezifikoen bidez. Edonola ere, aukera bat da bitarteko horietan jasotako fitxategiak ere zifratzea, bitartekoak zifratu beharrean. Zifratzeko tresnak eduki ezean, eskaera bat egin daiteke Erabiltzaileentzako Zerbitzuan.

Zifratzearen aplikazioa kontuan hartu behar da ere informazioa transmititzean. Horrelakoetan, zifratzeko bitartekoak ere askotarikoak dira, aplikazio eremuaren arabera:

- Informazio hori daukaten posta elektronikoetan erantsitako fitxategiak zifratzea, eta informazioa erantsiari transferitzea, zifratu beharreko edukia izango balitz bezala (eta zifratze pasahitza komunikatzea posta elektronikoa ez den beste bitarteko batez).
- VPNak erabiltzea, transmisio zifratua eskatzen duen informazioa duten sistema eta/edo zerbitzuetara unibertsitatearen kanpotik sartzeko.

Era berean, pertsonek ziurtatu beharko lukete konfidentzialtasun maila goreneko informazioa daukaten web zerbitzuak zerbitzu zifratuak direla; hots, https zerbitzuak. Horretarako, nahikoa izango da erabiltzaileak nabigatzailearen helbide barran giltzarrapo bat agertzen dela egiaztatzea.

3.1.3 Sinadura elektronikoa

Sinadura elektronikoa informazioaren jatorriaren eta osotasunaren egiazkotasuna bermatzeko erabilitako segurtasun neurria da.

Unibertsitatean, horren erabilera ohikoenak hauek dira: sinadura elektronikoa beharrezkoa duten PDF dokumentuetan, ziurtagiri korporatiboa erabilita (unibertsitate txartelean sartuta dagoena), eta beharrezkoa duten (izapide elektronikoa/erregistro elektronikoa) egintza administratiboen sinadura elektronikoa, oraingoan ere ziurtagiri korporatiboa erabilita.

Sinadura elektronikoa erabiltzen da, halaber, informazioaren jatorria eta osotasuna egiaztatzeko, hala behar duten dokumentu elektronikoak zuzen sinatu direla egiaztatuta PDF dokumentuaren segurtasun propietateetan.

Sinadura elektronikoari lotutako kasu espezifiko bat elektronikoki sinatutako dokumentu elektronikoen inprimaketa da. Garrantzitsua da jakitea inprimatutako dokumentu horiek ez direla baliozkoak, non eta EKS (Egiaztapenerako Kode Segurua) duten. Kode hori dokumentu elektroniko ofizial bat modu bakarrean identifikatzen duen digitu multzo batek osatzen du, eta dokumentuaren orrialde guztietan agertzen da. EKS hori baliagarria da jatorrian elektronikoa den dokumentu baten benekotasuna eta osotasuna egiaztatzeko eta haren sinadura baliozkotzeko. Horretarako kode hori sartu behar dugu dokumentuaren igorleari dagokion egoitza elektronikoaren atalean, eta ikusten den dokumentu elektronikoa egiaztatzen ari garen dokumentu bera dela egiaztatu behar dugu.

3.1.4 Metadatuak

Metadatuak fitxategien ezaugarriak definitzen edo deskribatzen dituzten datuak dira, eta automatikoki sortzen dira, erabiltzaileak kontrolatu gabe. Metadatuak dira, esate baterako, honako hauek:

- Fitxategiaren sorreraren data eta ordua.
- Fitxategiaren sorreraren kokaleku geografikoa.
- Ekipo informatikoaren izena eta/edo haren IP helbidea
- Dokumentuaren edizioan parte hartu duten pertsonen, sistemen eta/edo erakundeen izenak eta txertatutako iruzkinak.

Metadatuek nahi baino informazio gehiago eman dezakete pertsonei edo erakundeari buruz, eta informazio hori erasoak egiteko erabil daiteke; batez ere, dokumentua asko zabaltzen denean, esate baterako, publikoari eskaintzen zaionean web zerbitzari batean edo bestelako informazio biltegiren batean. Hori dela eta, informazio hori minimizatu egin behar da.

Planteamendu horrekin bat etorrita, dokumentuak garbitzeko prozesu bat aplikatu beharko litzateke, ezkutuko eremuetan gordetako informazio osagarria, metadatuak, iruzkinak edo aurreko berrikuspenak kentzeko, non eta informazio hori hartzailearentzat esanguratsua den.

Dokumentuak garbitzeko prozedura desberdina izango da, fitxategi motaren eta horri lotutako aplikazioaren arabera.

3.1.5 Segurtasun kopiak

Unibertsitateak zerbitzu korporatibo guztien segurtasun kopiak egiten ditu aldian behin, eta horien bidez nahita edo nahi gabe galdutako datuak berreskuratu daitezke, antzinatasun jakin batez. Halere, erabiltzaileek beren ekipoetan bertan gordetako informazioaren segurtasun kopia egin beharko lukete, unibertsitateak ez baitu informazio hori zaintzen.

Ordenagailuan bertan gordetako informazioaren segurtasun kopiak egiteko kanpo euskarriak erabili beharko dira (Pen-drive, USB, CD, DVD, etab.). Kopia horiek, gutxienez, jatorrizko datuen segurtasun maila berbera eduki behar dute. Hala, segurtasun kopiaren (backup) babesa bermatzeko, informazioa, gutxienez, konprimatu eta zifratu beharko da (ZIP). Horrez gain, beharrezkoa izango da ere erabiltzaileek maiztasun batez egiaztatzea segurtasun kopiak berreskuratu daitezkeela, ordenagailu batek kanpoko euskarri horiek eta horien edukia irakur ditzakeela egiaztatuta.

Gomendagarria izango litzateke, informazio lokalaren segurtasun kopien alternatiba gisa, informazio lokal hori biltegiratze zerbitzu korporatiboetara eramatea (gorde, gordetalde, EHUDoku –kontuan hartuta gordetalde eta EHUDoku bitarteko partekatuak direla–, etab.).

3.1.6 Informazioa ezabatzea

Lokalean bildutako informazio korporatiboa aldi baterako erabili beharko litzateke, eta, beraz, aldi baterako erabilera hori igarotzean ezabatu egin beharko litzateke. Nolanahi ere,

informazioa zerbitzu edo/eta gordailu korporatiboetan gorde beharko litzateke, lokaletik ezabatu aurretik.

Lokalean biltegiratutako informazio korporatibo guztia ezabatu beharko litzateke, eta, horrez gain, segurtasunez ezabatu beharko lirateke haien kopiak kanpo euskarrietatik, bai paperean inprimatutako aldi baterako kopiak suntsituta bai kopia elektronikoak dituzten euskarriak maila baxuan formateatuta (edo suntsituta, formateatu ezin bada), dagokion atalean adierazitakoaren arabera.

3.2 Euskarriak babestea

Atal honetan kontuan hartzen dira kanpoko informazio euskarri elektronikoak, bitarteko erauzgarri gisa ere ezagunak, hau da: Pen-Driveak, USBak, CDak, DVDak edo antzeko beste batzuk. Telefono mugikorrak, smartphoneak, tabletak eta antzekoak ez dira hartzen kanpoko informazio euskarritzat. Horrelakoak gailu mugikorren kategorian sartzen dira, eta horien segurtasun neurriak dagokion atalean zehazten dira.

Kanpoko informazio euskarri guztiek identifikatuta (etiketatuak) egon beharko lukete, gordetako informazioaren segurtasun maila gorena adierazita, baina haren edukia ezagutzera eman gabe. Erabiltzaileek identifikazio edo etiketa hori interpretatzeko moduren bat eduki beharko lukete, baina interpretazio hori ez litzateke egin beharko ikuste hutsarekin; haatik, beharrezkoa izan beharko luke hura azaltzeko erreferentzia edo utilitateren bat edukitzeak.
Erabiltzaileek beren ardurapean dauden informazio euskarriekin behar bezalako prestutasunez jokatu, eta haien gaineko kontrola eduki beharko lukete. Horretarako, arreta neurri hauek aplikatu beharko lituzkete, gutxienez:

- Fabrikatzailearen baldintzak errespetatzea, tenperaturari, hezetasunari eta ingurumenaren beste erasotzaile batzuei dagokienez.
- Horietara soilik langile baimenduak sar daitezkeela bermatzea.
- Euskarri horien bidalketak eta/edo harrerak erregistratzea, baita mugimendu horien baimentzailea ere.
- Edukia zifratzea, dagokion atalean adierazitakoarekin bat etorrita.

Informazio euskarriak bidaltzen badira, erabiltzaileek irteera eta euskarria jaso duen garraiolaria erregistratu behar ditu, bidalketa dagokion harrerarekin erkatu beharko du (euskarriaren harrera egiaztatzea) eta, egiaztapen horrek kale eginez gero, dagokion segurtasuneko gorabehera jakinaraziko du. Horrelakoetan, zifratze pasahitza bestelako bitarteko batez jakinarazi beharko litzaioke bidalketaren hartzaileari.

Informazio euskarriak jasotzen badira, erabiltzaileek harrera aurreikusita zegoela ziurtatu behar dute, eta horren jatorria egiaztatuko dute; kontrakorik gertatzen bada, beharrezkoak diren arreta neurri guztiak hartuko ditu. Horrez gain, sarrera eta euskarria entregatu dituen garraiolaria erregistratu, harrera dagokion bidalketarekin erkatu, eta, erkaketak huts eginez gero, dagokion segurtasuneko gorabehera jakinarazi beharko dute.

Amaitzeko, erabiltzaileek euskarriak maila baxuan formateatu behar dituzte, baldin eta beste informazio bat biltzeko berrerabiliko badira edo beste erakunde baterako liberatuko badira.

Gainerako kasu guztietan, euskarriak suntsitu egin beharko lirateke. Suntsitu beharko lirateke ere, hori eskatzen duen prozedura espezifikoren bat baldin balego.

3.3 Lanpostua babestea

Lanpostua da segurtasun neurriak aplikatzeko gune nagusietako bat; izan ere, alde batetik, gune horretan egiten dira informazioa tratatzeko eragiketa gehienak, eta, bestetik, segurtasun neurri gehienak ere lanpostuan aplika daitezke, ordenagailu pertsonalak segurtasun neurri teknologikoak aplikatzeko dituen ahalmenak direla eta.

3.3.1 Lanpostua

Lanpostuak, lanerako espazio fisiko gisa ulertuta (mahaia eta ordenagailua), garbi egon beharko luke, une-unean egiten ari den lanerako beharrezkoak diren euskarriak eta informazioa bakarrik edukita mahai gainean, baimendu gabeko pertsona batek eskuratu beharko ez lukeen informazioa eskuratzeko arriskua ahal bezain beste gutxitze aldera.

Hori dela eta, informazio erreserbatuak (publikoa ez dena) ez luke eskuratzeko moduan egon beharko erabiltzen ari ez denean. Hortaz, paperean dauden dokumentuak leku itxi batean gorde beharko lirateke, erabiltzen ari ez badira, eta ordenagailuaren pantailak ez luke erakutsi beharko informazio erreserbatuta, halakorik erabiltzen ari ez bada.

3.3.2 Ordenagailu korporatiboa

Ordenagailuek lanerako prest egon beharko lukete une oro. Premisa hori betetzeko, ahalmen hori kalte dezaketen ordenagailu pertsonaletan nahasmenak sor ditzaketen arriskuak gutxitzeko ahaleginak egiten dira.

Horregatik, erabiltzaile bakar batek ere ez luke eduki beharko ekipoa administratzeko baimenik. Modu horretan, jarduera okerrak, malwareak edo operatibotasun hori larriki kalte dezakeen funtzionamendu anomaloak saihestuko ditugu. Era berean, erabiltzaile bakar batek ere ez luke baimenik gabeko softwarerik instalatu beharko, ekipoaren funtzionamenduan edo errendimenduan kalteak saihesteko.

Horrez gain, kontuan hartu behar da ordenagailu korporatiboa eta horri lotutako bitarteko elektroniko (posta elektronikoa, nabigazioa, etab.) guztiak soilik lanerako erabili beharko liratekeela; hortaz, ez lirateke erabili beharko xede partikularretarako; izan ere, horrelako erabilerak, nekez kontrola daitezkeenez, nabarmen areagotu dezake arriskua. Gainera, bitarteko elektroniko korporatiboak erabiltzen direnean, garrantzitsua da kontuan hartzea erabilera unibertsitatearen identitateari dagoela lotuta (unibertsitatetik nabigatzen da, posta elektronikoa unibertsitatearen domeinuari dago lotuta, etab.); beraz, egindako jarduera oro unibertsitateko jardueratzat hartzen da beti.

3.3.3 Erabiltzaileak identifikatzea

Pertsona bakoitza modu unibokoan identifikatu beharko litzateke, dagokion kredentzialaren bidez (erabiltzailearen identifikatzaile gisa ezaguna), unibertsitateko informazio sistemen aurrean; hartara, une oro jakin daiteke zer pertsonak jaso duen identifikatzaile bakoitza eta zer sarbide eskubide dituen, eta jakin daiteke ere nork zer egin duen.

Hori dela eta, sartzeko kredentzialek erabiltzailearen kontrolpean egon behar dute bakarrik, eta soilik aktibatuko dira horrela daudenean. Pertsona batek ezin ditu erabili beste baten sarbide kredentzialak (transferitu eta utzi ezin den informazio pertsonala).

3.3.3.1 Egiaztatze bitartekoak eta sarbide kontrola

Erabiltzaileak sartzeko kredentzialak jaso dituenean, kontuan hartu behar du hura edukitzeak hainbat erantzukizun dakarzkiola:

- Zaintza arduratsuaren betebeharra
- Konfidentzialtasuna babestearen betebeharra
- Berehala informatzearen betebeharra, galduz gero

Unibertsitateko informazio sistemetara sartzeko hainbat egiaztatze bitarteko erabil daitezke:

- **Kontu/pasahitz korporatiboa:** Egiaztatze sistema honen sendotasuna pasahitzean datza (aplikatutako pasahitzen politikan).
- **Txartel korporatiboa + PIN:** Egiaztatze sistema sendoagoa da, eta etorkizunean unibertsitateak eskuratu beharko luke.
- **Beste egiaztatze** bitarteko batzuk: Etorkizunean, egiaztatze aurreratuen erabilera aurreikusten da (erabilera bakarreko pasahitzak, ontzi txartelak, etab.).

Informazio sistemek prestatuta egon beharko lukete, egiaztatze prozesuan sartzen saiatzen ari denari emandako informazioa ezinbesteko gutxienekoa izateko; hori dela eta, ez litzateke inoiz adierazi beharko parametro okerra erabiltzailearen identifikatzailea (kontua) edo pasahitza den; hartara, balizko erasotzaile batek ez du jakingo erabiltzen ari den kontua edo pasahitza zuzena den.

Indarrezko erasoak saihesteko (hainbat pasahitza sartzea behin eta berriro pasahitza asmatzen saiatzeko), saialdi kopurua mugatua izango da, eta, hainbat hutsegite segidan eginez gero, sartzeko aukera blokeatuta geratuko da.

Horrez gain, informazio sistemek, sartzeko eta egiaztatzeko prozesuan, bere betebeharrak jakinaraziko dizkiote erabiltzaileari, sistema horietara sartzeko inplikazioez jabetu dadin.

3.3.3.2 Egiaztatze pasahitzak erabiltzea

Pasahitzak **buruz** ikasi beharko lirateke, eta ez da gomendagarria erregistratzea edo inon idaztea; hala eginez gero, erregistratuak izan diren lekura norbait sartzeko eta eskuratzeko

arriskua baitago. Pasahitzak bitarteko elektroniko batean apuntatzen badira, ohar hori fitxategi zifratu batean egin behar da, eta, edonola ere, leku seguruan gorde.

Erabiltzaileak **pasahitza aldatu** beharko luke konektatzen den lehen aldian, baita administratzaileak edo sistemak pasahitza eman dionean ere; horrela, erabiltzaileak bakarrik ezagutuko du. Horrez gain, pasahitza aldatu beharko litzateke, beste pertsona batzuek ezagut dezaketela susmatzen bada.

Pasahitza **ez litzaioke esan beharko inori** (ezta nagusiei, lankideei edo informatika zerbitzuko langileei ere), inola ere.

3.3.3.3 Pasahitzen politika

Pasahitzak erraz asmatzeko modukoak ez izateko edo horretarako diseinatutako mekanismo automatizatuen bidez urratuak ez izateko, pasahitzen politika hau bete beharko litzateke:

- **Gutxieneko luzera:**
  - Gutxienez 8 karaktereko luzera eduki beharko luke.
- **Konplexua:**
  - Hiru karakterek, gutxienez, 4 mota hauetakoak izan beharko lukete:
    - Zenbakiak
    - Letra larriak
    - Letra xeheak
    - Karaktere bereziak: * . + $ & # @ - ! % ^ ; ( ) { } [ ] < > ? /_
  - Ez luke eduki beharko karaktererik zurian.
- **Ez igartzeko modukoa:**
  - Ez litzateke eratu beharko soilik hiztegiko hitzez edo erraz iragarri edo erabiltzaileari lotuta egon daitezkeen karakterez (izenak, helbidea, matrikulak, etab.)
  - Ez litzateke inoiz erabili beharko pasahitz gisa edo horren zati gisa erabiltzailearen kontuaren identifikatzailea, izena edo abizenak.
- **Maiz berritzea:**
  - Pasahitzak, gutxienez, sei (6) hilean behin aldatu beharko lirateke.
  - Ez lirateke berriro erabili beharko azken hamar (10) pasahitzak.

3.3.4 Ordenagailua blokeatzea.

Ordenagailua bloketatu egin beharko litzateke, erabili gabe zentzuzko denbora igaroz gero. Blokeoak, gutxienez, automatikoa izan beharko luke, ekipo korporatiboak denbora batez erabili gabe egon ondoren gertatzen den moduan. Nolanahi ere, erabiltzaileek eskuz blokeatu beharko lukete, lanpostua uzten duten aldiro. Blokeo hori egin daiteke <Windows>+<L> teklak aldi berean sakatuta edo txartel kooperatiboa kenduta, betiere ekipo korporatibo batean saioa hasteko erabili bada.

Kasu batean nahiz bestean, erabiltzaileak berriro egiaztatu beharko du, jarduera berriro hasteko.

Lanpostutik kanpo denbora luzez egon behar bada, ordenagailua itzaltzea gomendatzen dugu; izan ere, ekipoan hasitako saio bat, blokeatuta egon arren, kalteberagoa da beti, saioak martxan egon baitaitezke (nabigazioa, aplikazioak, etab.).

3.3.5 Antibirusa

Ordenagailu guztiek eduki beharko lituzkete kode kaltegarriei aurre egiteko prebentzio eta erreakzio mekanismoak (antibirus gisa ezagutzen ditugunak). Ekipo korporatiboek antibirusa daukate, lehentasunez aktibatuta.

Malwarearen aurkako (antibirusa) software horrek oinarrizko bi premisa hauek bete beharko lituzke: beti gaitua egotea, eta birus sinaduren eredu eguneratu bat edukitzea. Horrela ez bada, erabiltzailea ez litzateke egongo babestuta azken birusen aurrean.

Software antibirusak malware bat hauteman baina ezabatu ez duela konturatuz gero, berehala jakinarazi beharko litzaioke Erabiltzaileentzako Zerbitzuari, unibertsitateak horretarako ezarritako prozedurekin bat etorrita.

3.3.6 Ordenagailu pertsonalaren suebakia

Ordenagailu pertsonalak sareko erasoei aurre egiteko babes bitartekoak ere eduki beharko lituzke (firewall edo suebaki gisa ezagunak). Ekipo korporatiboek ere badituzte, lehentasunez aktibatuta.

Suebakiaren erabilerak oinarrizko bi premisa hauek bete beharko lituzke: gaitua egon behar du beti, eta erabiltzaileak ez du sekula lehenetsitako konfigurazioa saihestu behar. Premisa horren ildotik, ez litzaioke inori baimenik eman beharko Internet bidez ekipora konektatzeko, non eta horren beharra justifikatuta dagoen eta dagokion baimena lortzen den.

Suebakiaren edozein ohartarazpen susmagarriren berri eman beharko litzaioke lehenbailehen Erabiltzaileentzako Zerbitzuari, unibertsitateak ezarritako prozedurekin bat etorrita.

3.3.7 Posta elektronikoa, SPAM eta phishing

Unibertsitateak posta elektronikoa erabiltzeko oinarrizko arauak ezarri ditu langileentzat:

https://www.euskadi.eus/r47-bopvapps/es/bopv2/datos/2015/03/1501146a.shtml

Halere, aipatutako arauez harago, segurtasunaren arloko beste alderdi batzuei ere erreparatu behar zaie, hala nola:

- Unibertsitateak emandako postontziak transferiezina izan beharko luke.

- Postaren helbidea foroetan edo posta zerrendetan sartzea saihestu beharko litzateke, non eta beharrezkoa den eta hornitzaileak konfiantzazkoak diren; izan ere, eraso asko helbide horietaz baliatzen dira.
- Postaren igortzailea ezezaguna bada eta/edo horren gaia arraroa bada, mezua beti ezabatu beharko litzateke ireki gabe (edo kuarentenan jarri, datu gehiago eduki arte), bereziki fitxategi atxikiak eta exekutagarriak baditu.
- Nahasita jasotako posta bat jaso izana igortzaileari jakinarazi behar zaio, eta posta ezabatu.

Posta elektroniko bat bidaltzeko unean, arreta berezia jarri beharko litzateke hartzaileengan, ongi idatzita daudela eta hartzaile zuzenak direla egiaztatuta (izan ere, auto-osatu bezalako funtzioek hartzaile okerrei egindako bidalketak eragin ditzakete, eta, horren ondorioz, aurreikusita ez zeuden hartzaileek behar ez den informazioa jasoko dute, behar besteko arreta ez jartzeagatik); kontuan hartu beharko litzateke ere bidalitako eta, batez ere, birbidalitako informazioaren konfidentzialtasun maila, postak hirugarren bati buruzko informazioa eduki baitezake, amaierako hartzaileak ezagutu beharko ez lukeena. Horrez gain, saihestu egin beharko litzateke, ahal den neurrian, konfidentzialtasun maila goreneko informazioa posta elektronikoz bidaltzea, eta, beharrezkoa izango balitz, informazioa zifratu beharko genuke.

Horrez gain, jardunbide jakin batzuk saihestu behar dira, hala nola:

- Gutun kateatuen zabalkundean parte hartzea, baita eskema piramidaletan edo antzekoetan ere.
- Mezuak bidaltzea edo erantzutea, horien bidez malwarea sar badaiteke edo arriskuak nahiz arazoak egon badaitezke unibertsitatearen sistema eta tresna informatikoetan eta teknologikoetan.
- Esteka susmagarrietan klik egitea.
- Fitxategi erantsi susmagarriak exekutatzea.

3.3.8 Web zerbitzuak, Internet eta sare sozialak erabiltzea

Internet, web zerbitzuak eta sare sozialak erabiltzean, jarraitu beharko genituzkeen gomendio eta jardunbide egokiak dira honako hauek:

- Bisitatutako orriaren segurtasuna eta benekotasuna egiaztatzea (HTTPS).
- Nabigatzailearen segurtasun mailak erabiltzea.
- Mugatzea, ahal bada, cookien erabilera nabigazioan.
- Informazio pribatua ezabatzea (historiala, cookiesak, pasahitzak, etab.) edo InPrivate (Internet Explorer) / Pribatu (Firefox) / Inkognito (Chrome) moduan nabigatzea.
- Applet-en eta Script-en exekuzioa mugatzea eta zaintzea.
- Fidagarriak ez diren edo susmagarriak diren orriak ez bisitatzea.
- Fidagarriak ez diren kode edo programa ez jaistea.
- Osagarri ezezagunak ez instalatzea.

Horrez gain, Internet, web zerbitzuak eta sare sozialak erabiltzean, hainbat jarduera saihestu behar dira, esate baterako:

- Legez kanpoko jarduerei lotutako webguneetara sartzea.
- "Hacking" guneetara edo segurtasunik gabekotzat ezagunak diren guneetara sartzea, informazioaren osotasuna eta konfidentzialtasuna arriskuan egon baitaiteke.
- Jabego eskubideari buruzko legeen bidez babestutako materiala (software barne) jaistea Internetetik, erabiltzeko eskubidea ematen duen baimena edo lizentzia eduki gabe.
- Unibertsitatearena den edozein informazio argitaratzea edo haren izenean argitaratzea, dagokion baimena izan gabe.
- Baimendu gabeko sarbidea lortzea edo lortzen saiatzea, unibertsitatearenak diren edo ez diren ekipo, zerbitzu, datu edo azpiegituretara sartzeko.
- Esteka susmagarrietan klik egitea.

Sare sozialen erabilera espezifikoari dagokionez, kontuan hartu beharko litzateke, modu osagarrian, bi irizpide orokor hauek: emandako informazio kopurua mugatzea eta, batez ere, "argitaratu aurretik pentsatzea"; izan ere, aztarna digitala ezabatzea ia ezinezkoa da, eta edozein argitalpen ia iraunkor bihurtzen da.

3.4 Gailu mugikorrak babestea

Gailu mugikorretan segurtasun neurri osagarriak aplikatu behar dira; izan ere, mugikortasun horri datxekion arrisku jakinak daude, berariaz tratatu beharrekoak.

3.4.1 Urruneko sarbidea eta VPN

Unibertsitateak emandako VPN (Virtual Private Network) soluzioek konfidentzialtasuna (zifratua) eta osotasuna ematen dute komunikazioan, baita benekotasuna ere erabiltzailearen identitatean. Zerbitzu hori URL honetan azaltzen da:

http://www.ehu.eus/es/web/ikt-tic/vpn

Interneten ez dauden zerbitzuak eskuratzeko erabiltzaileen urruneko sarbidea, hots, unibertsitatearen instalazioetatik kanpo hirugarrenen sareetatik (Internet) egindakoa, soilik egin beharko litzateke unibertsitateak jarritako VPN tresnen bidez. Debekatuta egon beharko luke, beraz, unibertsitatearen sistemen urruneko sarbide eta/edo kontrolerako tresna alternatiboen erabilerak.

VPN konexioa ezarrita dagoenean, erabiltzaileek unibertsitatearen sarean aplikatutako egiaztatze prozesu berbera bete beharko lukete. Beraz, VPN bidezko urruneko sarbideak ez lituzke eman beharko sarbide pribilegio osagarriak.

3.4.2 Ordenagailu eramangarriak

Ekipo eramangarri bakoitzaren arduradunak identifikatuta egon beharko luke. Erabiltzaile horiek arreta espezifikoa jarri beharko lukete, ekipoak galtzeko edo lapurtzeko arriskuaren aurrean. Ekipo horiek galduko balira edo lapurtuko balituzkete, Erabiltzaileentzako Zerbitzuari eta dagokion arduradunari jakinarazi beharko litzaioke berehala, informazio sentikorra (konfidentzialtasun maila handikoa) eduki dezaketelako, eta berariaz adierazi beharko litzateke lapurtutako eramangarriak DPBLOren araberako maila ALTUKO informazioa zuten fitxategiak ote zituen.

Saihestu beharko litzateke, ahal den neurrian, ordenagailu eramangarriak unibertsitatera urrunetik sartzeko kredentzialak edukitzea, horrelakotzat ulertuta unibertsitatearen beste ekipo batzuetara sartzeko gaitasuna eman dezaketen kredentzialak, hala nola VPN konexiorako pasahitzak, unibertsitateko zerbitzuetara sartzeko pasahitzak edo antzeko beste batzuk.

Horrez gain, informazioa galtzeko edo lapurtzeko aukerak handiagoak direnez, arreta berezia jarri beharko litzateke ordenagailu pertsonal batean aplikagarriak diren segurtasun neurri guztietan eta, bereziki, honako hauetan: informazioaren backupak, konfidentzialtasun maila altuenetako informazioa (eta DPBLOren arabera maila ALTUA duten datu pertsonalak) zifratzea, pasahitzen politika, antibirusa, suebakia, VPN eta urruneko sarbidea.

3.4.3 Telefono mugikorrak

Telefono mugikorrak, tabletak eta antzeko gailuak segurtasunez erabiltzeko, gailu mota horiek berezkoak dituzten segurtasun neurri guztiak aplikatu beharko lirateke, horietan gordetako informazioa (konfidentzialtasun maila handia denean) egoki babeste aldera.

- Gailura sartzeko kontrola: PIN, Eredua, Aztarna edo antzekoa, ereduaren bisualizazioa ezkutatuta metodo hori erabiltzen bada.
- Zifratua.

Telefono mugikorrak eta antzekoak erabiltzeko oinarrizko segurtasun neurri gisa informazio sentikorraren erabilera mugatzea ere gomendagarria da. Horrez gain, ordenagailu eramangarrietarako zehaztutako segurtasun neurri guztiak aplikatu beharko lirateke, ahal izanez gero.

Gailu mugikor korporatiboen kasuan, funtsezkoa da haien galera edo lapurreta jakinaraztea, baita haien matxura edo haustura IKTen gerenteordetzaren Erabiltzaileentzako Zerbitzuaren bidez kudeatzea ere.

Mugikor pertsonala lan korporatiboak egiteko erabiliko balitz (BYOD, Bring Your Own Device), mugikor korporatiboetarako ezarritako neurri berberak aplikatu beharko lirateke, eta horien galera eta lapurreta ere jakinarazi beharko litzateke. Halere, kasu horretan, komenigarria izango litzateke segurtasun neurri osagarriak aplikatzea, hala nola pertsonala eta korporatiboa bereiztea, ahal den neurrian biak bereizita eta isolatuta, eta informazio korporatiboa ez partekatzea Interneteko zerbitzuekin (google, iTunes, etab.).

3.4.4 Wifi publikoak edo hirugarrenen sareak

Segurutzat har daitekeen WiFi sare bakarra unibertsitatearena da (eduroam). Sare horretaz harago, garrantzitsua da kontuan hartzea beti **WiFi publikoak** (pasahitzik gabekoak –irekiak– edo pasahitza partekatua dutenak –barnean sartuta, beraz, EHU-wGuest) ingurune erabat **ez-seguruak** direla; izan ere, edonor konektatu daiteke, eta, beraz, edonork espiatu ditzake edonoren konexioak. Hortaz, funtsezkoa da arreta neurriak hartzea, WiFi publikoak edo hirugarrenen sareak erabiltzen badira.

WiFi publikoak edo hirugarrenen sareak erabiltzen badira, hartu beharreko arreta neurri nagusiak honako hauek dira:

- Informazio sentikorrera ez sartzea (erreserbatua, pribatua).
- Zerbitzu seguruak bakarrik erabiltzea, informazio sentikorra eskuratu behar bada (https zerbitzuak eta/edo unibertsitatearen zerbitzuetara sartzeko VPNa).
- Beste pertsona batzuek pasahitzak nola sartzen diren ez ikustea.
- Gailu mugikorren segurtasun neurrien aplikazioa indartzea, gailura sartzeko kontrol mekanismoak maiztasunez berritu behar direla kontuan hartuta.

4 Ondorioak

Segurtasuna guztioi dagokigu. Unibertsitateak beharrezko segurtasun neurrien aplikazioa bermatu behar du, baina beti egongo dira pertsonen baitan dauden segurtasun neurriak. Horrez gain, segurtasunaz hitz egitea, kate bat bere katebegi ahulena bezain sendoa izatearen konparazioa erabili ohi dugu beti, eta, informazioaren segurtasunari buruz ari bagara, onartu beharko dugu pertsonak garela katebegirik ahulenak; izan ere, askotan ez ditugu betetzen zehaztutako segurtasun neurriak, askotariko arrazoiak direla eta (batzuetan ez ezagutzeagatik, askotan alferkeriagatik, ahaleginik ezagatik batzuetan, eta beste zenbaitetan utzikeriagatik).

Ezin dugu ahaztu segurtasun arazoek guztiongan dutela eragina. Pertsonek kalteak jasaten dituzte, eta egoera zailean geratzen dira; unibertsitatearen aktiboei kalte egiten zaie, eta ondorioak, azkenean, gizarte osoak jasan behar ditu. Beraz, segurtasuna zaintzeak guztion kontua izan behar du.

Hori guztia dela eta, garrantzitsua da aplikatu daitezkeen segurtasun neurriak zein diren jakitea, eta argi edukitzea segurtasun gaietan, zalantzaren aurrean, zentzuz jokatzea dela baliabide nagusietako bat portaera zuzena zein den jakiteko. "Gaizki esan sarri eta gehienetan igarri" esaera tresna eraginkorra izaten da segurtasunaren arloan jarraitu eta saihestu beharreko jarduerak identifikatzeko. Zalantzaren bat izanez gero, Erabiltzaileentzako Zerbitzuarengana edo arloko arduradunarengana jo daiteke. Edonola ere, argi eduki behar da beti, segurtasun arazo baten susmoa izanez gero, garrantzitsuena dela hura lehenbailehen jakinaraztea eta ahalik eta informazio gehiena ematea bai Erabiltzaileentzako Zerbitzuari bai arduradunari.

Azken finean, gogoratu beti honako hau: unibertsitatearen segurtasuna eta irudi ona zure esku daude.