IKTen Gerenteordetzaren gomendio praktikoak segurtasun informatikoa kudeaketa lanetan aplikatzeko

SENen eta DPBLOren aplikaziotik eratorrita

IKT Gerenteordetza – Vicegerencia TIC
V1.0 (2016)

Universidad del País Vasco Euskal Herriko Unibertsitatea

NAZIOARTEKO BIKAINTASUN CAMPUSA
CAMPUS DE EXCELENCIA INTERNACIONAL

Aurkibidea

- Sarrera
- Segurtasuna kudeatzea
- Segurtasuna aplikatzea
  - Informazioa babestea
  - Euskarriak babestea
  - Lanpostua babestea
  - Gailu mugikorrak babestea
- Ondorioak

2

Aurkibidea

- Sarrera
- Segurtasuna kudeatzea
- Segurtasuna aplikatzea
  - Informazioa babestea
  - Euskarriak babestea
  - Lanpostua babestea
  - Gailu mugikorrak babestea
- Ondorioak

3

Definizioak

- **Segurtasuna:**
  - Arriskurik edo kalterik eza (RAE).
- **Informazioa:**
  - Ezagutzen multzo bat, gai jakin baten inguruan ditugun ezagutzak areagotzea edo zehaztea ahalbidetzen diguna (RAE).
  - Datu prozesatuen multzo antolatu bat, subjektu edo sistema hartzailearen ezagutza egoera aldatzen duen mezu bat osatzen duena (Wikipedia).
- **Informazioaren segurtasuna:**
  - 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.

4

Definizioak – Segurtasunaren Dimentsioak

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

5

Segurtasun neurriak

- **Jarduera eremuak:**
- Antolakuntza
  - Rolak eta erantzukizunak
- Araudia
  - Betebeharrak
- Operatiboa
  - Prozedurak
    - Orokorrak / teknikoak
- Kontraktuala
  - Baldintzak (aurreko edozein arlotan aplika daitekeena)
  - Erantzukizunak mugatzea
- Teknologikoa
  - Aurrekoak betetzen direla bermatzea
  - Fisikoa / logikoa
    - Ez dokumentalak

6

Segurtasuneko Eskema Nazionala

- 3/2010 Errege Dekretua, urtarrilaren 8koa, administrazio elektronikoaren arloan segurtasuneko eskema nazionala arautzen duena.
- 951/2015 Errege Dekretua, urriaren 23koa, 3/2010 Errege Dekretua aldatzen duena.
- Helburuak:
- Bitarteko elektronikoen erabileran beharrezkoak diren konfiantza baldintzak sortzea
  - Neurriak ezarriko dira sistema, datu, komunikazio eta zerbitzu elektronikoen segurtasuna bermatzeko.
- Bitarteko horien bidez, herritarrek eta administrazio publikoek beren eskubideak erabili eta betebeharrak beteko dituzte
- Aplikatzen zaie:
- Zerbitzu elektronikoei
- Bitarteko elektronikoei
- Zerbitzu edo/eta bitarteko horiek tratatutako informazioari

7

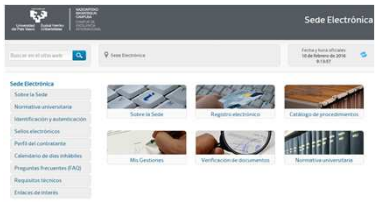
Segurtasuneko Eskema Nazionala

- Erakunde publiko batek informazioaren segurtasun arloan bete beharreko eskakizunak zehazten ditu.
- Segurtasun arloko erabakietan kontuan hartu beharreko oinarrizko printzipioak ezartzen ditu.
- Informazioa egoki babesteko errespetatu beharreko gutxieneko eskakizunak zehazten ditu.
- Oinarrizko printzipioak eta gutxieneko eskakizunak betetzeko mekanismo bat definitzen du.
  - Segurtasun neurri proportzionalak hartzea, informazioaren, sistemen eta babestu beharreko zerbitzuen nolakotasuna aintzat hartuta.
- Aplikatu beharreko segurtasun neurrien katalogo bat egiten du.
  - Antolakuntzakoak
  - Jardunekoak
  - Teknologikoak

8

Segurtasuneko Eskema Nazionala

- **SENen aplikazioaren adibideak**
- **Egoitza elektronikoa**
  - **Ataria**
  - **Sarrera erregistro elektronikoa**
  - **Nire kudeaketak**
  - **…**
- **AZPkoentzako zerbitzuak / AZPkoek emandakoak**
  - **GAUR**
  - **EHUDoku**
  - **Langileen ataria**
  - **…**
- **Zerbitzuak emateko erabilitako bitartekoak**
  - **Lanpostua**
  - **PCa**
  - **Zerbitzariak**
  - **Komunikazioak**



Datu Pertsonalak Babestea

- **15/1999 Lege Organikoa, irailaren 13koa, Datu Pertsonalak Babesteari buruzkoa.**
- **1720/2007 Errege Dekretua, abenduaren 21ekoa, 15/1999 Lege Organikoa garatzeko araudia onartzen duena.**
- **Helburuak:**
- **Datu pertsonalen trataeran pertsona fisikoen askatasun publikoak eta oinarrizko eskubideak babestea eta bermatzea, bereziki haien ohoreari eta norberaren nahiz familiaren intimitateari dagokienez.**
- **Datu pertsonalak biltzeak eta tratatzeak pertsonaren eskubideei ekar diezaieketen arriskuei aurre egitea.**
- **Aplikatzen zaie:**
- **Datu pertsonalei, haiek erabiltzeko modua edozein delarik**
- **Euskarri fisikoei eta/edo elektronikoei**

Datu Pertsonalak Babestea

- **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
  - Datuen komunikazioa (Hirugarrenei uztea eta haien kabuz eginiko trataerak)
- Eraginpeko pertsonen oinarrizko eskubideak zehazten ditu (sartzeko, zuzentzeko, ezeztatzeko eta aurka egiteko eskubideak).
- Datu pertsonalen datu fitxategien arduradunen betebeharrak definitzen ditu.
- Datu pertsonalen trataeran aplikatu beharreko segurtasun neurriak ezartzen ditu.
  - Fitxategi eta trataera automatizatuetarako (elektronikoak)
  - Fitxategi eta trataera ez automatizatuetarako (paperean)
  - Mailak bereizten dira (Baxua/Ertaina/Altua), datu moten arabera
    - Maila altuko datuak: ideologia, sindikatu afiliazio, erlijio, sinesmen, arraza, osasun edo bizitza sexualari buruzkoak, eraginpeko pertsonen onespenik gabe polizia xedeekin bildutakoak, eta genero indarkeriari lotutakoak

11

Datu Pertsonalak Babestea

- **DPBLOren aplikazioaren adibideak**
- 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

12

Aurkibidea

- Sarrera
- Segurtasuna kudeatzea
- Segurtasuna aplikatzea
  - Informazioa babestea
  - Euskarriak babestea
  - Lanpostua babestea
  - Gailu mugikorrak babestea
- Ondorioak

13

Segurtasuna arautzea

- Unibertsitateak informazioaren segurtasuna arautzen du.
  - Politika, arauak, prozedurak eta gidak ezartzen ditu horretarako
    - Pertsona guztiek bete eta aplikatu behar dituzte.
  - Zertarako:
    - Unibertsitatearen funtzionamendua legedira egokitzeko.
    - Araudiaren inguruko zalantzak eta interpretazio akatsak saihesteko.
    - Erabiltzaileei beren lana segurtasun maila egokian egiten laguntzeko.
      - Eguneroko lanerako jardun ildoak.
- Segurtasun Politika:
  - Jarraibideen multzo bat, unibertsitateak kritikotzat jotzen dituen informazioa eta zerbitzuak kudeatzeko eta babesteko modua arautzen duena.
  - https://egoitza.ehu.eus/es/informazioaren-segurtasun-politika

- Politika
- Araudia
- Prozedurak
- Gidak

14

Segurtasuna arautzea

- **Segurtasun Arauak:**
  - Deskribatzen dute:
    - Ekipo, zerbitzuen eta instalazioen erabilera zuzena.
    - Erabilera desegokitzat jotzen dena.
    - Langileen erantzukizuna, arau horiek betetzen ez direnean.
      - Indarrean dagoen legediarekin bat etorrita.
- **Segurtasun Prozedurak:**
  - Zehazten dute:
    - Nola egin eguneroko lanak.
    - Nork egin behar duen lan bakoitza.
    - Nola identifikatu eta jakinarazi portaera anomaloak.
- **Segurtasun Gidak:**
  - Zeregin jakin batzuk egiteko modu egokiak deskribatzen dira.
  - Deskribatutako zereginak egiteko modu onenak gomendatzen dira.

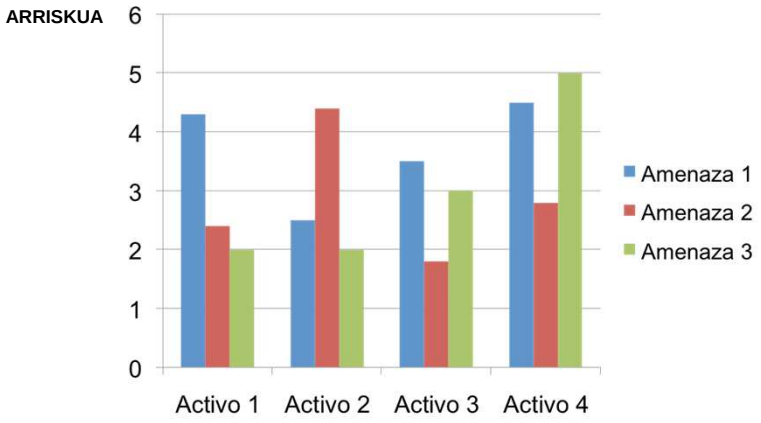
15

Segurtasun arriskuak kudeatzea

- **Helburua: aplikatutako segurtasun neurriek arriskuekiko proportzionalak izatea.**
  - Arriskua zenbat eta handiagoa izan, orduan eta segurtasun handiagoa beharko da.
- **Adibidea: Lurrikara Vs Birus informatikoa**
  - Lurrikara: arrisku ertain-baxua: oso probabilitate gutxi, inpaktu handia (pertsona guztiei eragiten die)
  - Birus informatikoa: Arrisku altua: probabilitate handia, inpaktu handia (ezabatzen ez bada eta zabaltzen bada, jende guztiaren lanari eragiten dio)

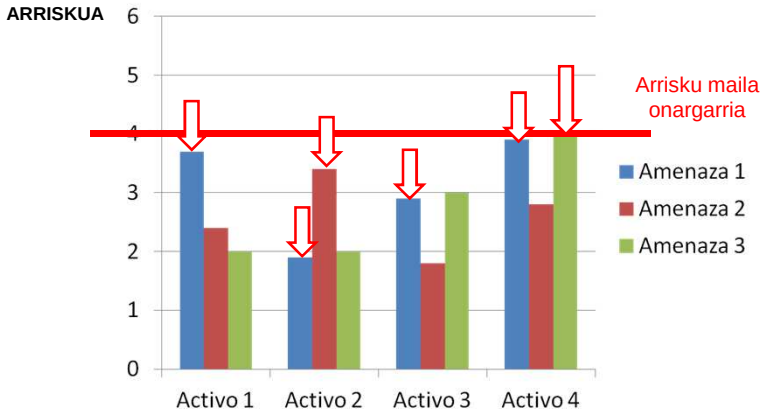
16

Arriskuen analisia:



17

Arriskuak kudeatzea:



18

Segurtasuneko gorabeherak kudeatzea

- **Segurtasuneko gorabehera**
- Ezusteko eta nahi gabeko gertakaria, aktiboen segurtasunean (segurtasun dimentsioren batean) eragin negatiboa duena.
- Adb.: aplikazioan datu okerrak agertzea, informazioa behar ez den lekuan agertzea, ordenagailuak gauza oso "arraroak" egitea, etab.
- **Segurtasuneko gorabeherak kudeatzea:**
- Gorabeherak artatzeko ekintza plan bat egitea. Konpontzeaz gainera, plan horrek neurketa bitartekoak eduki behar ditu, babes sistemaren kalitatea ezagutzeko eta joerak hautemateko, arazo handiak izatera iritsi aurretik (SEN).
- **Segurtasuneko gorabeherak kudeatzeko pausoak:**
- Gorabehera hautematea
- Gorabehera jakinaraztea:
  - Gorabehera berehala jakinaraztea Erabiltzaileentzako Zerbitzuari eta zerbitzu edo arloko arduradunari
- Tratatzea eta konpontzea

19

Aurkibidea

- Sarrera
- Segurtasuna kudeatzea
- Segurtasuna aplikatzea
  - Informazioa babestea
  - Euskarriak babestea
  - Lanpostua babestea
  - Gailu mugikorrak babestea
- Ondorioak

20

Informazioa sailkatzea

- **Informazioa sailkatu beharko litzateke, alderdi hauek kontuan hartuta:**
  - **Segurtasuneko gorabehera batek informazio horretan izan dezakeen eragina**
- **Informazioaren nolakotasuna**
  - **Legez ezarritakoaren arabera (DPBLO, beste batzuk).**
- **Unibertsitatearen balizko sailkapen mailak (konfidentzialtasuna):**
  - **Publikoa**
  - **Erreserbatua (hainbat konfidentzialtasun mailatan: barne erabilera, konfidentziala…).**
- **Sailkapen horri dagozkion segurtasun neurriak aplikatu beharko lirateke.**
- **Informazioa tratatuko da, informazio horri lotutako edozein jardueratarako ezarritako prozedurekin bat etorrita, barnean sartuta:**
  - **Haren sarbide kontrola.**
  - **Haren zifratzea / sinadura elektronikoa.**
  - **Metadatuen kudeaketa.**
  - **Kopiak egitea.**
  - **Informazioa ezabatzea.**
  - **Euskarri/PC/bitarteko mugikorren erabilera.**

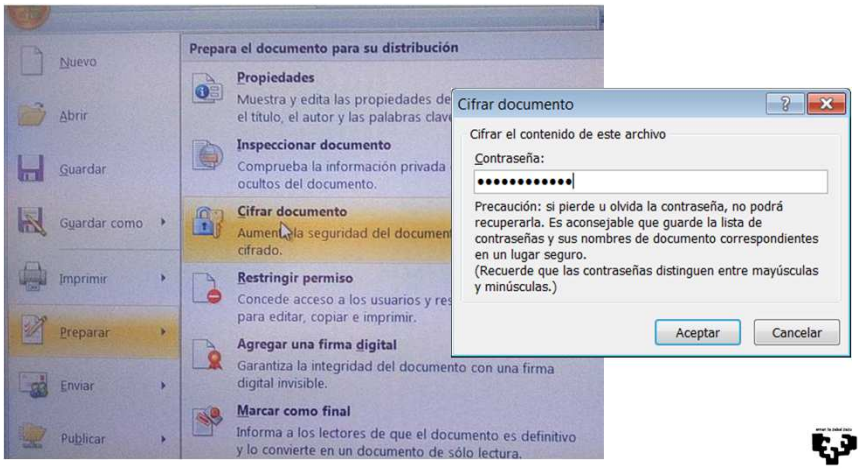
Informazioa sailkatzea

- **Informazioa tratatzeko oinarrizko printzipioak:**
- **Erabiltzaileak aplikatutako segurtasun neurriek proportzionalak izan beharko lukete alderdi hauekiko**
  - **Informazioa tratatzeko ingurunearen segurtasuna (unibertsitatea / kanpoa)**
  - **Informazioaren konfidentzialtasun maila**
- **Informazio korporatiboak zerbitzu korporatiboetan egon behar du**
- **Informazio korporatiboa aldi baterako erabil daiteke maila lokalean**
  - **Egoki babestuko da, dagokion konfidentzialtasun mailaren arabera**
    - **Informazioa babesteko neurriak aplikatuta**
    - **Euskarriak babesteko neurriak aplikatuta**
    - **Lanpostua babesteko neurriak aplikatuta**
    - **Gailu mugikorrak babesteko neurriak aplikatuta**

- **Informazioa zifratzea oso prozesu sentikorra da, eta arrisku handikoa.**
- **Pasahitza galdu edo ziurtagiria baliogabetuko balitz, ezinezkoa izango litzateke zifratutako informazioaren DEUS ERE bilatzea.**
- **Konfidentzialtasun maila goreneko informazioa (eta DPBLOren arabera maila ALTUKOA) zifratuko da.**
- **Gordetzen denean**
  - **Zifratu fitxategiak, programen (PDF, Office, etab.) berezko tresnen bidez, gako batez babestuta.**
  - **Babestu fitxategiak edo karpetak ZIP baten barruan, gako batez.**
  - **Zifratu karpeta osoak, zifratze tresna espezifikoen bidez.**
    - **Halakorik izan ezean, eskatu Erabiltzaileentzako Zerbitzuan.**
  - **Zifratu pen-driveak, CDak, DVDak eta antzekoak. Horrelakoetan, maila horretako informazioa duten fitxategiak grabatzen dira, Erabiltzaileentzako Zerbitzuak emandako tresnen bidez.**
  - **Adibideak:**
    - **Zifratzea 7-Zip-ekin (zip)**
    - **Microsoft Word (docx)**
    - **Adobe Acrobat Pro (pdf)**

23

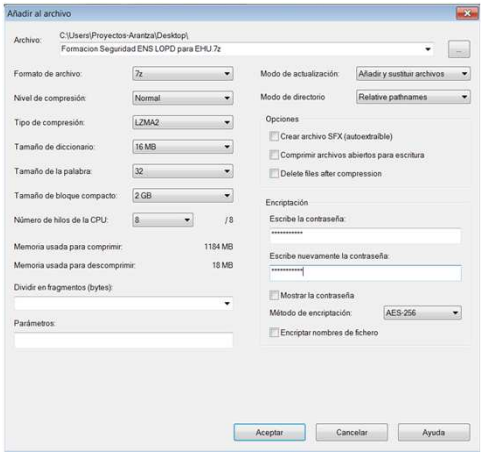
- **Docx zifratzea Microsoft Wordekin:**
- **Office-ren botoia → Prestatu → Zifratu dokumentua → Sartu zifratze pasahitza**



24

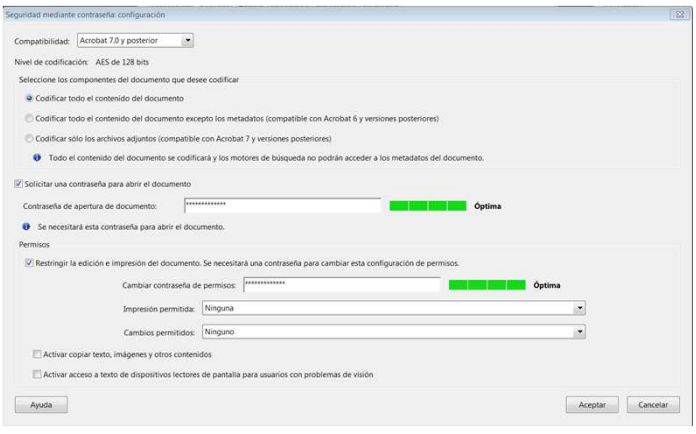
Zip zifratzea 7-Zip-rekin:

- **Klikatu eskuineko botoia fitxategiaren gainean → 7-Zip → Gehitu fitxategiari → Sartu pasahitza "Enkriptatzea" atalean**



Pdf zifratzea Adobe Acrobat Pro-rekin:

- **Fitxategia → Propietateak → Segurtasun Sistema → Hautatu Segurtasuna pasahitzaren bidez**



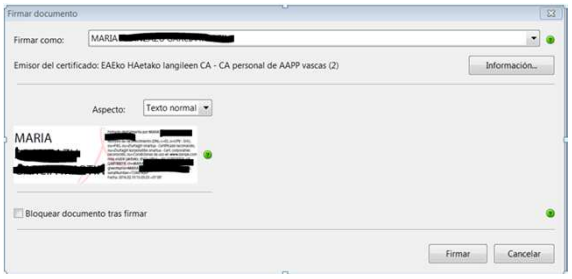
Informazioa babestea

- **Konfidentzialtasun maila goreneko informazio guztia (eta maia ALTUKOA DPBLOren arabera) zifratuko da:**
- **Komunikatzean:**
  - **Zifratu fitxategi erantsiak, informazio hori daukaten posta elektronikoetan.**
    - **Atxikiari informazioa transferituta, hala behar bada.**
    - **Zifratze pasahitza komunikatuta, beste bitarteko batez.**
  - **Erabili VPNak, maila horretako (dagokion atalean adierazitakoaren arabera) informazioa duten sistema eta/edo zerbitzuetara sartzeko unibertsitatearen kanpotik.**
- **Pertsonek konfidentzialtasun maila goreneko informazioa daukaten web zerbitzuak https zerbitzuak direla ziurtatu beharko lukete (nabigatzailearen helbide barran giltzarrapo bat ageri dela egiaztatzea).**

27

Sinadura elektronikoa

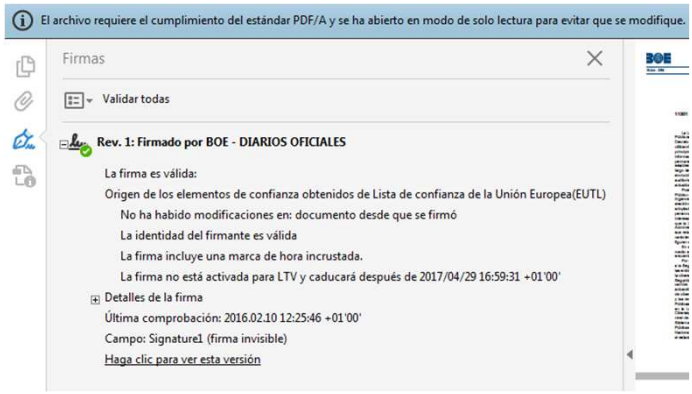
- **Sinadura elektronikoa erabiliko da, informazioaren jatorriaren eta osotasunaren egiazkotasuna bermatzeko:**
- **Beharrezkoa duten (izapidetze elektronikoa/ erregistro elektronikoa) egintza administratiboak sinatuko dira, ziurtagiri korporatiboa erabilita**
- **Beharrezkoa duten PDF dokumentuak sinatuko dira (programa zuzen konfiguratuta eta pertsonalizatuta badago), ziurtagiri korporatiboa erabilita (unibertsitate txartelean sartuta dagoena)**
  - **Ver → Rellenar y Firmar → Colocar firma → Arrastrar nuevo rectángulo de firma → Seleccionar certificado a utilizar → Firmar**



28

Sinadura elektronikoa

- **Informazioaren jatorria eta osotasuna benetakoak direla egiaztatuko da, horren sinadura elektronikoa egiaztatuta:**
- **Hala behar duten dokumentu elektronikoak zuzen sinatu direla egiaztatuko da**



29

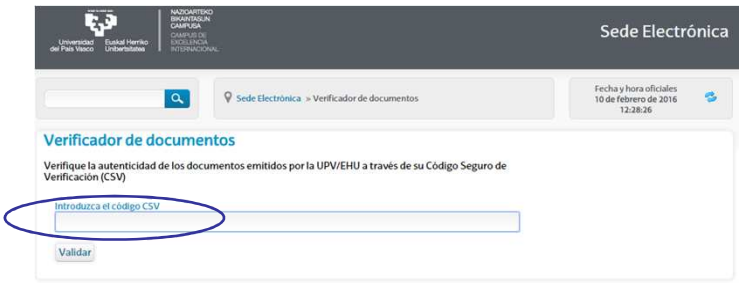
Sinadura elektronikoa

- **Sinatutako dokumentuak inprimatzea:**
- **Ez du baliorik, non eta EKS (Egiaztapenerako Kode Segurua) duten.**
  - **EKS kode bat da, dokumentu elektroniko ofizial bat modu bakarrean identifikatzen duen digitu multzo batek osatutakoa.**
    - **Egoitza elektronikoak eta erlazionatutako tresnek automatikoki sortzen dute.**
    - **Dokumentuaren orrialde guztietan ageri da.**
  - **Baliagarria da jatorriz elektronikoa den dokumentu baten benekotasuna eta osotasuna**

30

Sinadura elektronikoa

- **EKS dokumentuak egiaztatzea:**
- Dokumentua sortu duen erakundearen egoitza elektronikoan



31

Dokumentuak eta 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 informatikoen 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 erakundeei buruz.**
- 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.

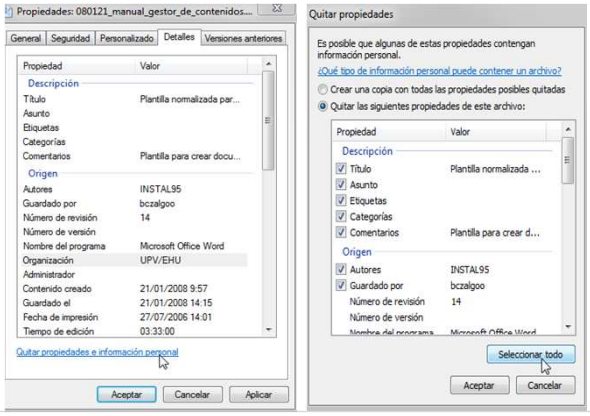
32

Dokumentuak eta metadatuak

- **Dokumentuak garbitzeko prozesu bat aplikatu beharko litzateke, ezkutuko eremuetan gordetako informazio osagarria, metadatuak, iruzkinak edo aurreko berrikuspenak kentzeko.**
- **Informazio hori hartzailearentzat esanguratsua denean izan ezik.**
- **Dokumentuak garbitzeko prozedura desberdina izango da, fitxategi motaren eta horri lotutako aplikazioaren arabera. Esate baterako:**
  - **Metadatuak ezabatzea Windows 7n**
  - **Metadatu ezkutatuak ezabatzea Microsoft Office-n**
  - **Metadatuak ezabatzea Adobe Acrobat Pro-n**

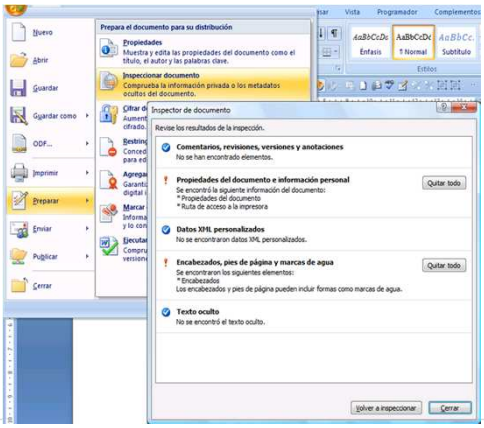
Dokumentuak eta metadatuak

- **Metadatuak ezabatzea (Windows 7):**
  - **Fitxategiaren propietateak (klikatu eskuinean) → Xehetasunak → Kendu propietateak eta informazio pertsonala → Hautatu "Kendu fitxategi honen propietate hauek"**
    - **1. aukera: "Hautatu dena" → Onartu**
    - **2. aukera: Hautatu ezabatu nahi diren propietateak → Onartu**



Dokumentuak eta metadatuak

- **Ezabatu metadatu ezkutatuak docx-en (Microsoft Office 2007 edo hortik gorakoa):**
  - **Office-ren botoia → Prestatu→ Hautatu "Ikuskatu dokumentua"**
  - **Sakatu "Ikuskatu" → Hautatu ezabatu nahi diren metadatuak → Sakatu "Kendu dena" dagokion atalean**



Dokumentuak eta metadatuak

- **Ezabatu metadatuak PDFn (Adobe Acrobat Pro):**
  - **Fitxategian → Propietateak → Deskribapena → Ezabatu nahi dituzun metadatuak → Sakatu metadatu osagarriak → Ezabatu nahi dituzun metadatuak**

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.**
- **Erabiltzaileek beren ekipoetan bertan gordetako informazioaren segurtasun kopia egin beharko lukete.**
  - **Segurtasun kopiak egitea, kanpo euskarrietan (Pen-drive, USB, CD, DVD, etab.).**
- **Kopia horiek, gutxienez, jatorrizko datuen segurtasun maila berbera eduki beharko lukete.**
  - **Segurtasun kopiaren (backup) babesa bermatzeko, informazioa, gutxienez, konprimatu eta zifratu beharko da (ZIP).**
  - **Segurtasun kopiak berreskuratu daitezkeela egiaztatu beharko da.**
- **Gomendagarria izango litzateke informazio lokal hori biltegiratze zerbitzu korporatiboetara eramatea (gorde, gordetalde, EHUDoku, etc.).**
    - **Adi! Bitarteko batzuk partekatuak dira, esate baterako, gordetalde eta EHUDoku**

37

Informazioa ezabatzea

- **Informazio eta/edo dokumentazio korporatibo guztia zerbitzu eta/edo gordailu korporatiboetan gorde beharko litzateke, lokaletik (lanpostua) ezabatu baino lehen.**
- **Lokalean bildutako informazio korporatiboak aldi baterako erabili beharko litzateke, eta, beraz, aldi baterako erabilera amaitzean ezabatu egin beharko litzateke.**
- **Ezabatzeko mekanismoak izan daitezke:**
  - **Lokaletik informazioa ezabatzea.**
  - **Kopia elektronikoak dituzten (ikus dagokion atala) euskarriak maila baxuan formateatzea (edo suntsitzea, formateatu ezin bada).**
  - **Paperean inprimatutako aldi baterako kopiak ezabatzea.**

38

Aurkibidea

- Sarrera
- Segurtasuna kudeatzea
- Segurtasuna aplikatzea
  - Informazioa babestea
  - Euskarriak babestea
  - Lanpostua babestea
  - Gailu mugikorrak babestea
- Ondorioak

39

Kanpoko informazio euskarriak

- **Kanpoko informazio euskarritzat hartzen dira gailu erauzgarri guztiak (Pen-Driveak, USBak, CDak, DVDak edo antzeko beste batzuk).**
- Telefono mugikorrak, smartphoneak, tabletak eta antzekoak ez dira hartzen kanpoko informazio euskarritzat, gailu mugikorren kategorian sartzen baitira (ikus dagokion atala).
- **Kanpoko informazio euskarri guztiek identifikatuta egon beharko lukete, gordetako informazioaren segurtasun maila gorena adierazita, baina haren edukia ezagutzera eman gabe.**
- Erabiltzaileek identifikazio horren esanahia ulertu beharko lukete:
  - Hura azaltzen duen utilitate edo erreferentzia baten bidez.
  - Ikuste hutsarekin.

40

Kanpoko informazio euskarriak

- **Erabiltzaileek beren ardurapean dauden informazio euskarriekin behar bezalako prestutasunez jokatu, eta haien gaineko kontrola eduki beharko lukete, neurri hauen bidez:**
- 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.
- **Informazio euskarriak bidaltzen badira, erabiltzaileek:**
- Irteera eta euskarria jaso duen garraiolaria erregistratu behar dute.
- Bidalketa dagokion harrerarekin erkatu behar dute (harrera egiaztatzea).
- Erkaketak huts eginez gero, segurtasuneko gorabehera bat jakinarazi behar dute.

41

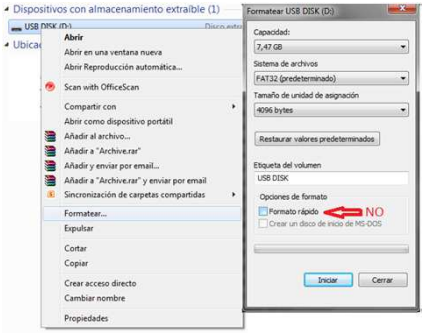
Kanpoko informazio euskarriak

- **Informazio euskarriak jasotzen badira, erabiltzaileek:**
- Harrera aurreikusita zegoela ziurtatu, eta haren jatorria egiaztatu behar dute.
  - Kontrakorik gertatzen bada, beharrezkoak diren arreta neurri guztiak hartuko dituzte.
- Sarrera eta euskarria eman duen garraiolaria erregistratu behar dituzte.
- Harrera dagokion bidalketarekin erkatu behar dute.
- Erkaketak huts eginez gero, segurtasuneko gorabehera bat jakinarazi behar dute.
- **Aplikatu beharreko zifratze bitartekoak informazioa babesteari buruzko atalean zehaztutakoak izango dira.**
- Zifratze pasahitza beste bitarteko batez jakinarazi behar zaio bidalketaren hartzaileari.

42

Kanpoko informazio euskarriak

- 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 behar dira.
- Suntsitu beharko dira ere hori eskatzen duen prozedura espezifikoren bat egonez gero.

43

Aurkibidea

- Sarrera
- Segurtasuna kudeatzea
- Segurtasuna aplikatzea
  - Informazioa babestea
  - Euskarriak babestea
  - Lanpostua babestea
  - Gailu mugikorrak babestea
- Ondorioak

44

Lanpostua

- **Lanpostuak garbi egon beharko luke, unean-unean egiten ari den lanerako beharrezkoak diren euskarriak eta informazioa bakarrik edukita mahai gainean.**
- **Informazio erreserbatua ez da eskuratzeko moduan egongo, erabiltzen ari ez denean.**
  - **Paperean dauden dokumentuak leku itxi batean gordeko dira, erabiltzen ari ez badira.**
  - **Pantailak ez du informazio erreserbatua erakutsiko, halakorik erabiltzen ari ez bada.**

45

Ordenagailu korporatiboa

- **Ordenagailuek lanerako prest egon behar dute une oro.**
  - **Erabiltzaile bakar batek ere ez du baimenik izango ekipoa administratzeko. Modu horretan, jarduera okerrak, malwareak edo operatibotasun hori larriki kalte dezaketen funtzionamendu anomaloak saihestuko ditugu.**
  - **Era berean, erabiltzaile bakar batek ere ez du instalatuko baimendu gabeko softwarerik, ekipoaren funtzionamenduan edo errendimenduan kalteak saihesteko.**
- **Ordenagailu korporatiboa eta horri lotutako bitarteko elektroniko guztiak (e-posta, nabigazioa, etab.) soilik lanerako erabili beharko lirateke.**
  - **Xede partikularretarako erabiltzeak nabarmen areagotu dezake arriskua.**
  - **Erabiltzaileen jarduera unibertsitateari lotuta dago.**

46

Erabiltzaileak identifikatzea

- **Pertsona bakoitza modu unibokoan identifikatuko da, dagokion kredentzialaren bidez, unibertsitateko informazio sistemen aurrean, hartara:**
  - **Jakin dezakegu zer pertsonak jaso duen identifikatzaile bakoitza eta zer sarbide eskubide jaso dituen.**
  - **Jakin dezakegu nork zer egin duen.**
- **Sartzeko kredentzialek erabiltzailearen kontrolpean egon behar dute bakarrik, eta soilik aktibatuko dira horrela daudenean.**
  - **Pertsona batek ezin ditu erabili beste baten sarbide kredentzialak.**

47

Egiaztatze bitartekoak eta sarbide kontrola

- **Erabiltzaileak onartuko du sarbide kredentzialak jaso dituela eta horrek dakarzkion betebeharrak ezagutzen eta onartzen dituela, hau da:**
  - **Zaintza arduratsuaren betebeharra**
  - **Konfidentzialtasuna babestearen betebeharra**
  - **Berehala informatzearen betebeharra, galduz gero.**
- **Informazio sistemetara sartzeko hainbat egiaztatze bitarteko erabil daitezke:**
  - **Kontu/Pasahitz korporatiboa**
    - **Egiaztatze sistema honen sendotasuna pasahitzean datza (pasahitzen politikan).**
  - **Txartel korporatiboa + PIN**
    - **Egiaztatze sistema sendoagoa da, eta etorkizunean unibertsitateak eskuratu beharko du.**

48

Egiaztatze bitartekoak eta sarbide kontrola

- **Informazio sistemetara sartzeko hainbat egiaztatze bitarteko erabil daitezke:**
  - **Beste egiaztatze bitarteko batzuk**
  - **Etorkizunean, egiaztatze sistema aurreratuen erabilera aurreikusten da (erabilera bakarreko pasahitzak, ontzi txartelak, etab.).**
- **Sartzen saiatzen ari denari ezinbesteko informazioa bakarrik eman behar zaio.**
- **Baimendutako saialdi kopurua mugatua izango da, eta, hainbat hutsegite segidan eginez gero, sartzeko aukera blokeatu egingo da.**
- **Sistemak, sartzeko eta egiaztatzeko prozesuan, bere betebeharrak jakinaraziko dizkio erabiltzaileari.**

49

Egiaztatze pasahitzak erabiltzea

- **Pasahitzak buruz ikasi beharko lirateke.**
  - **Bitarteko elektroniko batean gordetzen badira, pasahitzak fitxategi zifratu batean idatzi beharko dira.**
  - **Leku seguru batean gorde behar dira beti.**
- **Erabiltzaileak pasahitza aldatu behar du konektatzen den lehen aldian, baita administratzaileak edo sistemak pasahitza eman diotenean ere.**
- **Pasahitza aldatu behar da, beste pertsona batzuek ezagut dezaketela susmatzen bada.**
- **Pasahitza ez zaio inori esango (ezta nagusiei, lankideei edo informatika zerbitzuko langileei ere), inola ere.**

50

Pasahitzen politika

- Gutxieneko luzera: 8 karaktere
- Hiru karakterek, gutxienez, 4 mota hauetakoak izan beharko lukete:
  - Zenbakiak
  - Letra larriak
  - Letra xeheak
  - Karaktere bereziak: * . + $ & # @ - ! % ^ ; ( ) { } [ ] < > ? /_
- Ezingo du eduki karaktererik zurian.
- Ezingo da eratu soilik hiztegiko hitzez edo erraz iragarri edo erabiltzaileari lotuta egon daitezkeen karakterez (izenak, helbideak, matrikulak, etab.)

51

Pasahitzen politika

- Ezin dira erabili pasahitz gisa edo horren zati gisa erabiltzailearen kontuaren identifikatzailea, izena edo abizenak.
- Pasahitzak, gutxienez, sei (6) hilean behin aldatu behar dira.
  - Pasahitz baten erabilera denbora funtsezko faktore bat da, hura asmatzeari begira.
- Ez dira berriro erabili behar azken hamar (10) pasahitzak.

52

Ordenagailua blokeatzea

- **Ordenagailua blokeatu egin behar da, erabili gabe zentzuzko denbora bat igaroz gero.**
  - Erabiltzaileek eskuz blokeatu dezakete <Windows>+<L> teklak aldi berean sakatuta.
  - Funtsezkoa da, lanpostua utziz gero.
  - Ekipo korporatiboek blokeo automatikoa dute, erabili gabe daudenerako.
  - Saioa hasteko txartela korporatiboa erabiltzen bada, ekipo korporatiboa eskuz blokeatu daiteke, txartela kenduta.
  - Erabiltzailea berriro egiaztatu beharko da, saioa berriro hasteko.
- **Lanpostutik kanpo denbora luzez egon behar bada, ordenagailua itzaltzea gomendatzen dugu.**
  - Ekipoan hasita dagoen saio bat kalteberagoa da beti.

53

Antibirusa

- **PC guztiek eduki beharko lituzkete kode kaltegarriei aurre egiteko prebentzio eta erreakzio sistemak (antibirus gisa ezagunak).**
  - Ekipo korporatiboek lehenetsita dauzkate.
- **Anti-malware (antibirusa) softwareak premisa hauek bete behar ditu:**
  - BETI gaitua egotea
  - Birus sinaduren eredu eguneratu bat edukitzea
- **Software antibirusak malware bat hauteman baina ezabatu ez duela konturatuz gero, berehala jakinarazi behar zaio Erabiltzaileentzako Zerbitzuari, unibertsitateak horretarako ezarritako prozedurekin bat etorrita.**

54

Lanpostuaren suebakia

- PCak sareko erasoei aurre egiteko bitartekoak eduki beharko lituzke (firewall edo suebakiak).
  - Ekipo korporatiboek lehenetsita dauzkate.
- Suebakiak premisa hauek bete beharko lituzke:
  - BETI gaitua egotea.
  - Lehenetsitako konfigurazioa saihestea EZINEZKOA izatea.
- Ez litzaioke inori baimenik eman beharko Internet bidez ekipora konektatzeko.
  - Salbuespena egingo da beharra justifikatuta dagoenean eta dagokion baimena eskuratzen denean.
- Suebakiaren edozein ohartarazpen susmagarriren berri eman behar zaio lehenbailehen Erabiltzaileentzako Zerbitzuari, unibertsitateak horretarako ezarritako prozedurekin bat etorrita.

55

Posta elektronikoa, SPAM eta phishing

- Posta elektronikoa erabiltzean langileek bete beharreko oinarrizko arauak ezarrita daude:
  - https://www.euskadi.eus/r47-bopvapps/es/bopv2/datos/2015/03/1501146a.shtml
- Ezarritako arauez gainera, beste alderdi batzuei ere erreparatu behar zaie, hala nola:
  - UPV/EHUk emandako postontziak transferiezina izan behar du.
  - Ez da postaren helbidea sartu behar foroetan edo Interneteko posta zerrendetan, 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 ezabatu beharko da 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.

56

Posta elektronikoa, SPAM eta phishing

- **Arreta berezia jarri behar da hartzaileengan**
  - Egiaztatu ongi idatzita daudela
  - Egiaztatu hartzaile zuzenak direla (erne auto-osatzeko aukerarekin)
  - Kontuan hartu bidalitako eta, batez ere, birbidalitako informazioaren konfidentzialtasun maila; saihestu, ahal den neurrian, konfidentzialtasun maila goreneko informazioa posta elektronikoz bidaltzea.
- **Ezarritako arauez gain, saihestu beharreko jarduerak dira:**
  - Gutun kateatuen zabalkundean parte hartzea, baita eskema piramidaletan edo antzekoetan ere.
  - Klik egitea esteka susmagarrietan.
  - Fitxategi erantsi susmagarriak exekutatzea.
  - UPV/EHUren sistemetan eta tresna informatiko eta teknologikoetan malwarea sartu, edo arrisku nahiz arazoak ekar ditzaketen mezuak bidaltzea edo horiei erantzutea.

57

Web zerbitzuak, Internet eta sare sozialak erabiltzea

- **Internet, web zerbitzuak eta sare sozialak erabiltzean, jarduera hauek saihestu beharko lirateke:**
  - Legez kanpoko jarduerei lotutako webguneetara sartzea.
  - "Hacking" guneetara edo segurtasunik gabekotzat ezagunak diren guneetara sartzea, horrelakoetan informazioaren osotasuna eta konfidentzialtasuna arriskuan egon baitaiteke.
  - Jabego eskubideari buruzko legeen bidez babestutako materiala (softwarea barne) jaistea Internetetik, erabiltzeko eskubidea ematen duen baimena edo lizentzia eduki gabe.
  - Klik egitea esteka susmagarrietan.
  - UPV/EHUrena den edozein informazio argitaratzea edo haren izenean argitaratzea, dagokion baimena izan gabe.
  - Baimendu gabeko sarbidea lortzea edo lortzen saiatzea, UPV/EHUrenak diren edo ez diren ekipo, zerbitzu, datu edo azpiegituretara sartzeko.

58

- **Internet, web zerbitzuak eta sare sozialak erabiltzean, jardunbide egoki hauei jarraitu behar zaie, ahal den neurrian:**
  - 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 nabigatzea InPrivate / Pribatu / Inkognito moduan.
  - Applet-en eta Script-en exekuzioa zaintzea eta mugatzea.
  - Fidagarriak ez diren edo susmagarriak diren orriak ez bisitatzea.
  - Fidagarriak ez diren kode edo programak ez jaistea.
  - Osagarri ezezagunak ez instalatzea.

- **Horrez gain, sare sozialak erabiltzean, kontuan hartu beharko lirateke jardunbide egoki hauek:**
  - **Emandako informazioa mugatzea**
  - **"Pentsatzea argitaratu aurretik"**
    - Edozein argitalpen ia iraunkor bihurtzen da.
    - Aztarna digitala ezabatzea ia ezinezkoa da.

Aurkibidea

- Sarrera
- Segurtasuna kudeatzea
- Segurtasuna aplikatzea
  - Informazioa babestea
  - Euskarriak babestea
  - Lanpostua babestea
  - Gailu mugikorrak babestea
- Ondorioak

61

Urruneko sarbidea eta VPN

- Unibertsitateak emandako VPN (Virtual Private Network) soluzioek konfidentzialtasuna (zifratua) eta osotasuna ematen dute komunikazioan, baita benekotasuna ere erabiltzailearen identitatean.
- 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 ahal izango da unibertsitateak emandako VPN tresnen bidez.
  - Debekatuta dago, beraz, bestelako urruneko sarbide eta/edo kontrol tresnak erabiltzea unibertsitateko sistemetara sartzeko.
- VPN konexioa ezarrita dagoenean, erabiltzaileek unibertsitatearen sarean aplikatutako egiaztatze prozesu berbera bete beharko dute.
  - VPN bidezko urruneko sarbideak, beraz, ez ditu emango sarbide pribilegio gehiago.

62

Ordenagailu eramangarriak

- Pertsonek arretaz jokatu beharko lukete, ekipo horiek galtzeko edo lapurtzeko aukeren aurrean.
- Ekipo eramangarrien arduradunak identifikatuta egongo dira.
- Ekipo horiek galtzen badira edo lapurtzen badituzte, berehala jakinarazi beharko zaie Erabiltzaileentzako Zerbitzuari eta dagokion arduradunari.
  - Berariaz adierazi beharko da lapurtutako ekipoaren fitxategietan DPBLOren araberako maila ALTUKO informazioa ote dagoen.
- Saihestu behar da, ahal den neurrian, ekipo eramangarriak unibertsitatera urrunetik sartzeko kredentzialak edukitzea.
  - Urruneko sarbide kredentzialak honako hauek dira: unibertsitatearen beste ekipo batzuetara sartzeko gaitasuna ematen duten kredentzialak, hala nola VPN konexiorako pasahitzak, unibertsitateko zerbitzuetara sartzeko pasahitzak edo antzeko beste batzuk.

63

Ordenagailu eramangarriak

- Informazioa galtzeko edo lapurtzeko aukerak handiagoak direnez, arreta berezia jarri beharko da ordenagailu pertsonal batean aplikagarriak diren segurtasun neurri guztietan:
  - Informazioaren backupa egitea
  - Konfidentzialtasun maila goreneko informazioa (eta DPBLOren arabera maila ALTUA duten datu pertsonalak) zifratzea.
  - Pasahitzen politika
  - Antibirusak
  - Suebakiak
  - VPN eta urruneko sarbidea

64

Telefono mugikorrak eta BYOD

- **Telefono mugikorren, tableten eta antzeko gailuen berezko segurtasun neurri guztiak erabili beharko dira.**
  - **PIN / Eredua/ Aztarna / …**
  - **Eredua ez ikusteko moduan egongo da, metodo hori erabiliz gero**
  - **Zifratzea**
- **Ordenagailu eramangarrietarako zehaztutako segurtasun neurri guztiak aplikatuko dira, ahal bada.**
- **Horrelako gailuetan informazio sentikorra ahalik eta gutxien erabiliko da.**
- **Mugikorra korporatiboa bada:**
  - **Jakinarazi haren galera edo lapurreta**
  - **Haren matxura edo haustura Erabiltzaileentzako Zerbitzuak kudeatuko du.**

65

Telefono mugikorrak eta BYOD

- **Mugikor pertsonala eginkizun korporatiboetan erabiltzen baduzu (BYOD, Bring Your Own Device)**
  - **Aplikatu mugikor korporatiboetarako ezarritako neurri berberak.**
  - **Bereizi zer den pertsonala eta zer korporatiboa.**
    - **Bereizi eta isola ezazu, ahal duzun guztietan.**
    - **Ez partekatu informazio korporatiboa Internet zerbitzuekin (google, iTunes, etab.).**
  - **Jakinarazi haren galera edo lapurreta.**

66

Wifi publikoak edo hirugarrenen sareak

- **WiFi publikoak ingurune erabat EZ-SEGURUAK dira:**
  - **Edonor konektatu daiteke.**
  - **Edonork espiatu ditzake edonoren konexioak**
  - **Gakoa beharrezkoa izan arren (konektatuta dauden guztiek ezagutzen dute).**
  - **Unibertsitatean EDUROAM (eta ez EHU-wGuest) da WiFi seguru bakarra, komunikazioak ere zifratzen dituelako.**
- **Arreta neurriak hartu WiFi publikoak edo hirugarrenen sareak erabiltzean:**
  - **Ez sartu informazio sentikorrera (erreserbatua, pribatua).**
  - **Informazio sentikorra eskuratu behar baduzu, erabili bakarrik zerbitzu seguruak.**
  - **HTTPS / VPN zerbitzuak, unibertsitatearen zerbitzuetara sartzeko.**
  - **Ez zaitzala inork ikusi pasahitza sartzen.**
  - **Indartu gailu mugikorren segurtasun neurrien aplikazioa.**

67

Aurkibidea

- **Sarrera**
- **Segurtasuna kudeatzea**
- **Segurtasuna aplikatzea**
  - **Informazioa babestea**
  - **Euskarriak babestea**
  - **Lanpostua babestea**
  - **Gailu mugikorrak babestea**
- **Ondorioak**

68

Praktikan jarri ikasitakoa

- 1. Hautatu Word dokumentu bat zure PCtik.
- 2. Kendu metadatu guztiak.
- 3. Sortu hautatutako Wordaren PDFa.
- 4. Sinatu zure txartela korporatiboarekin, Adobe Acrobat Pro erabilita.
- 5. Zifratu 7zip bidez, pasahitz sendo bat erabilita.
- 6. Bidali e-postaz, erantsi gisa, ikastaroko kide bati.
- 7. Eman iezaiozu pasahitza, aurreko e-posta ez den beste bitarteko batez.

69

Praktikan jarri ikasitakoa

- 8. Jaso duzu erantsi zifratu bat duen e-posta bat? Ireki ezazu.
- 9. Uste duzu pasahitza sendoa zela? Hitz egin horri buruz bidaltzailearekin.
- 10. Sinatuta dago? Egiaztatu sinadura.
- 11. Web orrian argitaratu daitekeen dokumentu bat dela uste duzu? Uste duzu UPV/EHUko langile guztiek eskuratzeko moduan egon daitekeela? Uste duzu zifratua egon beharko lukeela beti? Hitz egin horri buruz bidaltzailearekin.

70

Ondorioak

- Segurtasuna guztion ardura da
  - Unibertsitatearena
  - Pertsonena
- Pertsonak segurtasunaren katebegirik ahulena gara
  - Ezezagutzagatik
  - Zuhurtziagabekeriagatik
  - Nagikeriagatik
  - Jarraikitasunik ezagatik
  - Baita utzikeriagatik ere
- Segurtasun arazoek guztioi eragiten digute

71

Ondorioak

- Segurtasun gaietan zalantzaren bat baduzu:
  - Kasu egin zure senari
  - "Gaizki esan sarri eta gehienetan igarri"
- Segurtasun arazoren bat dagoela uste baduzu:
  - JAKINARAZI
  - Erabiltzaileentzako Zerbitzuari eta zure arduradunari
  - Lehenbailehen
  - Ahalik eta informazio gehiena emanez
  - Galdetu
  - Erabiltzaileentzako Zerbitzuari eta zure arduradunari

72

Joseba Enjuto, Nextel S.A.

Informazioaren segurtasuna eta Unibertsitatearen irudi ona zure esku ere badaude