EUSKO JAURLARITZA
GOBIERNO VASCO

43. zk.
2013ko martxoa

Aurrera!

Berrikuntzaren eta Teknologia Berrien dibulgaziozko buletina

Bulego Teknologikoak argitaratua
Informatika eta Telekomunikazioetako Zuzendaritza

AURKIBIDEA

Ziur asko, gure irakurle asko **BYOD**ekoak dira, baina oraindik ez dakite. Zertan datzan eta zer abantaila edo eragozpen dituen jakin nahi baduzu… Aurrera! aldizkariaren ale berri honetarako prestatu dugun lehen artikulua irakurtzea gomendatzen dizugu.

Bigarren artikuluan segurtasunaren gaira itzuli gara, baina erabili beharreko gailu edo teknologia berriak aintzat hartu beharrik gabe, oraingo honetan. Egia da askoren ustez segurtasuna *a posteriori* landu beharreko gaia dela, hau da, bezeroak eskatutako sistema edo aplikazio informatikoa diseinatu ondoren. Prestatu dugun artikulu honetan alderantzizko kontzeptu edo filosofia aurkeztu dugu, *Privacy by design* (**Pribatutasuna diseinutik**) izenekoa. Hain zuzen ere, filosofia honek azpimarratu nahi du zer nolako garrantzia duen (eta zer nolako onurak ekar ditzakeen) segurtasun-eskakizunak edozein proiektu egiten hasten den unean bertan txertatzeak, hau da, analisi- eta diseinu-faseetatik bertatik. Gainera, nabarmentzekoa da Europar Batasunak **Datuak Babesteko Araudi Orokorraren proposamena** egin duela (2012ko urtarrila), eta araudi horrek pribatutasunaren gaineko inpaktuaren analisia egiteko beharra jasotzen duela.

"*Alboan*" atalean, Eusko Jaurlaritzak EIJIEren laguntzaz gauzatuko duen informatika-proiektuaren berri emango dizuegu. Proiektu horri **Lanpostu korporatiboaren migrazioa** deritzo. 2013an Sare Korporatiboa osatzen duten pertsona guztiei eragingo dien proiektu horri esker, aplikazio hauek guztiak instalatuko dira: Windows7 sistema eragilea, Office2010 eta LibreOffice pakete ofimatikoak eta Internet Explorer 9 eta Mozilla Firefox nabigatzaileak.

"*Berri laburrak*" atalaren barruan, lehenik, Europar Batasuna garatzen ari den satelite bidezko nabigazio-sistema, GALILEO, osatzen duten sateliteei erantsi zaizkien funtzionalitate berriei buruz arituko gara: **bilaketa- eta salbamendu-zerbitzuak**, batik bat. Bigarrenik, **bosgarren WIFI belaunaldiaren** ezaugarri nagusiak laburbilduko ditugu: IEEE 802.11ac izenez ezagutzen den **WIFI estandar berria** prest egongo da 2013ko amaieran eta nabarmen hobetuko du, beste alderdi batzuen artean, hari gabeko konexioen datu-emaria. Gogorarazi behar da lehenengo WIFI belaunaldia 1997koa dela, eta 2 Mbps-ko datu-emaria (abiaduraren kontzeptuarekin nahastu behar ez dena) zuela.

Bazatoz BYODera?

Geroz eta ohikoagoa da goi-zuzendaritzak eta enpresetako gainerako langileek beren gailuak erabiltzea lanerako. Izan ere, abantaila asko eskaintzen dizkio langileari zein enpresari (erosotasun eta mugikortasun handiagoak, besteak beste). Badaude, ordea, kontuan hartu beharreko traba batzuk ere.

HIZTEGIA

[1] **BYOD:** "*Bring Your Own Device*" inglesezko esapidearen siglak dira (euskaraz, "*Ekarri zure gailua*").

BYOD, laburbilduz, enpresen politika bat da. Horren bidez, langileek beren gailu propioak eramaten dituzte enpresako baliabideetara sartzeko, esaterako, posta-elektronikoa, datu-basea eta fitxategiak, datuak eta aplikazio pertsonalak barne. Askotan "*Bring your own technology*" (ekarri zure teknologia) izena erabiltzen da. Horrek eremu askoz zabalagoa onartzen du, tresna (hardwarea) zein softwarea bere barne hartzen duena.

Kuriositate moduan, esan behar dugu BYOD deitutako sistema 70. hamarkadan jaio zela. Garai hartan, hainbat **ostalarik** bezeroek beren ardo propioa (botila) eramateko ekimena martxan ipini zuten; kasu horretan, bezeroek kortxoa kentzeagatik ordaintzen zuten bakarrik.

Enpresetako azpiegitura informatikoek duela asko "ireki" zizkieten ateak beren langileen, kolaboratzaileen zein bisitarien erabilera pertsonaleko ordenagailuei, batez ere 90eko hamarkadatik aurrera, ordenagailu eramangarrien gorakada gertatu zenean. Une hartatik aurrera ohiko bilakatu zen barne-saretik kanpoko edozein tokitatik, hau da, enpresako lantokietako ordenagailuez bestelakoetatik, enpresako sistema eta aplikazioetara konektatzea.

KANAL BERRIAK

Orain arte, enpresen helburua 24 ordu eskuragarri egongo ziren **aplikazio** eta **zerbitzuak** eskaintzea zen. Aurrerantzean, ordea, edozein **gailutatik** eskuragarri egotea ere izango da helburua.

Langile askok beren erabilerarako erosten dituzten *smartphone* eta *tablet*ak gai dira **edozein aplikazio** korporatibo **erabiltzeko**. Horri esker, langileek terminal bera erabiltzen dute bai beren gauzak zein lanekoak kudeatzeko; hala, bada, enpresa asko geroz eta serioago pentsatzen ari dira "nork bere gailua ekar dezala" estrategia, hau da, BYOD[1] deritzon joera bereganatzeaz.

Hitz berri horrek laburbiltzen du eremu korporatiboan **norberaren gailu mugikorrak** erabiltzeko joera, non eta erabiltzaileek (eta ez enpresek, gaur arte gertatu izan den bezala) jartzen dituzten baliabide teknologikoak.

Askok enpresarentzako arriskutsua dela pentsatzen duten arren, beste aditu askok uste dute gailu pertsonalak "lantoki" gisa erabiltzeak ez duela ordenagailu eramangarriekin edo USB memoriekin lan egiteak baino arrisku gehiago ekartzen, hala nola: gailua galtzeko arriskua, komunikazioak bidean antzematekoa edota informazio konfidentzialak ihes egitekoa. Aditu guztiak bat datoz, ordea, enpresaren jabetzakoak ez diren eta kontrolpean ez dituzten gailuen gainean **segurtasun korporatiboko politikak** aplikatzeko premiari dagokionez.

Hainbat ikerketen arabera, neurri eta sektore ezberdinetako enpresa askotan ari dira jasotzen, beren langileen aldetik, baliabide korporatiboak langileen jabetzako gailuetara (*smartphone* eta *tablet*ak, batik bat) ekarri, eta horien bidez baliabideok erabili eta eskuratzeko eskariak.

BYOD sistema erakundeetan edukitzeak izan dezakeen inpaktua erakunde horren inguruabar berezien mende dago, hein handi batean, baita azken urteetan segurtasun korporatiboa kudeatzeko izan duen moduaren mende ere. BYOD sistema inflexio-puntua da ohiko estrategiei dagokienez, orain arte **negozio**-ereduaren eta **segurtasun**-premien arteko oreka bat bilatzen baitzen erabakiak hartzeko orduan.

HARTU BEHARREKO ESTRATEGIA

Duela zenbait urtera arte, enpresek beren langileak ordenagailuez (*smartphone*ak, *notebook*ak, etab.) hornitzea zen ohikoa. Halakoetan, enpresak ordenagailuak erosten zituen (edo, zenbaitetan, *leasing/renting* sistemak

aplikatzen zituen, horrek zekarren kostuarekin) eta, gainera, barne-softwarea jartzen zuen, lizentzia korporatiboak erosten zituen, lapurreta-, ebasketa- eta desagerpen-aseguruak estaltzen zituen, eta ordenagailuen matxurak edo teknologiaren zaharkitzea deritzona bere gain hartzen zituen.

Berrikiago, ordea, enpresa batzuk kalkuluak egiten hasi dira eta egiaztatu dute berreskuratzen ez den diru asko beren langileen azpiegitura teknologikotik datorrela, hain justu. Hori dela eta, zenbait enpresa hasi dira dagoeneko langileekin beren ordenagailu pertsonalak erabiltzea adosten (erabileraren kostua enpresek hartzen dute beren gain).

BYOD berriki sortutako fenomenoa dela pentsa daitekeen arren, hasi da dagoeneko negozioen munduan aldaketa handiak eragiten, sektore horretako langileen %90ek (herrialde garatuetan) beren gailuak erabiltzen baitituzte enpresako informaziora jotzeko. Aditu batzuek baieztatzen dute BYOD sistemak langileen produktibitatea igotzen laguntzen duela, enpresaren barruan behar duten malgutasuna ematen dielako, funtsean.

Baditu desabantaila batzuk, hala ere, premiazko kontrolak ezarri ezean sistema honek erakundeari kalte egin baitiezaioke: arrakalak ireki daitezke (eta informazio konfidentzialak horietatik ihes egin dezake), edo aplikazio gaiztoek sarera sartzeko balia dezaketen ate bilaka daiteke. Adibidez: langile batek enpresaren barne-sarera sartzeko *smartphone* bat erabiltzen badu, eta telefono hori galtzen badu, hor gordetako datu konfidentzial guztiak egokiak ez diren pertsonengana irits daitezke.

AINTZAT HARTU BEHARREKO ALDERDIAK

Joera berri horrek, beste edozein teknologia edo konponbidek bezala, alderdi onak eta txarrak ditu, beraz. Berrikus ditzagun horietako batzuk:

- **Malgutasuna**. Beren gailuak erabiltzean, enplegatuek telelana[2] egiteko aukera gehiago dute, edozein unetan eta edozein tokitatik balia baititzakete. Hala eta guztiz ere, eskuragarritasun-kontrolerako politika berriak abian jartzea eskatzen dio horrek enpresari, eta gailu-kopuru handiago baten (bakoitza bere sistema operatiboarekin eta bere aplikazioekin) konexioei eutsiko dieten sareko baliabide nahikoak edukitzea.
- **Kostuak murriztea**. Enplegatuek beren gailuak jartzen badituzte, enpresek ordenagailuetan (hardwarea) egin beharreko inbertsioaren zati bat aurrezten dute. Aldi berean, enpresak bere gain hartzen ditu telekomunikazio-zerbitzuak eta, horri esker, langileek ez dute ezer ordaindu behar, gailuak beren erabilera pertsonalerako ere erabiltzen dituzten arren.
- **Eraginkortasuna**. Enplegatuek berehala kudea ditzakete premiazko gaiak, edozein tokitik, gogoko dituzten eta ondo ezagutzen dituzten gailuak erabilita.
- **Produktibitatea.** Oro har, langileen produktibitatea areagotzea da informazioaren teknologietako adituek BYOD erabiltzean ikusten duten abantaila nagusia (izan ere, langileek ohikotasunez erabiltzen dituzten aplikazioak dauzkate eta, horrela, erosoago egin dezakete lan, aplikazio berrien erabilerak ikasteko beharrik gabe, esate baterako). Alderdi hau garrantzitsua da, askok uste baitute enplegatuek beren eduki eta aplikazioekin arreta gal dezaketela (sare sozialak erabiliz, jolasekin, baimendu gabeko orrietan sartuz, etab.)

HIZTEGIA

[2] **Telelana:** 2012/92 Dekretua, maiatzaren 29koa, Euskal Autonomia Erkidegoko Administrazio Orokorreko eta bere erakunde autonomiadunetako enplegatu publikoek zerbitzua telelanaren bidez modalitate ez-presentzialean nola eman arautuko duen Akordioa onartzeko dena.

(EHAA, 11. zk, 2012ko ekainaren 7koa)

Langileentzako desabantailetako bat da berez dagozkiena baino ordu gehiago lan egiten buka dezaketela (asko une oro konektatuta daude, beren posta elektronikoa berrikusten eta beren lanorduetatik kanpo lan egiten).

ETA SEGURTASUNA?

Garrantzi handieneko alderdia da hori.

BYOD abian jarri nahi duten edo horretan pentsatzen ari diren erakundeek ziurtatu behar dute enpresako informazioarekin kontaktua izango duten gailu guztiak **babestu** dituztela. Helburu nagusia, hortaz, **informazioak ihes egitea** saihestea da. Babestu beharreko gailuak ugari eta askotarikoak izateak lan hori zailtzen du eta, aldi berean, babesaren kostua igoarazten du.

Aintzat hartu beharreko beste alderdi bat da langile batek gure enpresan lan egiteari uzten badio zer gertatuko den hark bere gailuan gordeta duen informazioarekin, informazio pertsonala ez ezik enpresarena ere edukiko baitu. Azken arazo hori ekiditeko, enpresa batzuek konfidentzialtasun -klausulak sinarazi dizkiete langileei; klausula horietan, langileek enpresaren esku jartzen dute beren gailuetan gordetako informazio guztia (baita informazio pribatua ere).

"Estatu Batuak dira munduko liderrak BYOD sistema baliatzean; Asiako eta Latinoamerikako enpresek sistema hori erabiltzea sustatzen dute; Europa, aldiz, zuhurragoa da."

ESKAKIZUN BERRIAK

BYOD fenomenoari esker, erakunde asko konturatu dira beren hari gabeko WIFI sarea zaharkituta dagoela, duela zenbait urteko eskakizunei primeran erantzuten bazien ere, ez baitira gai egungoei erantzuteko.

Argi dago informazioaren teknologiekin (IT) lotutako saila dela, gaur egun, "natibo digitalek[3]" enpresara ekarri ohi dituzten gailu eramangarri pertsonalen etorrerak gehien eragindakoa. Sail horretan sartu behar dira ITko arduraduna, sistemen eta komunikazioen arduraduna, laguntza teknikokoa edota segurtasunekoa.

ESTATISTIKAK

Egunez egun egiazta dezakegun bezala, geroz eta erabiltzaile gehiagok erosten dituzte, mundu osoan, beren erabilera pertsonalerako gailu eramangarriak.

Hona hemen *smartphone* eta *tablet*ak enpresetan **txertatzeari** buruzko zifrarik adierazgarrienen laburpena, 2012. urteari dagokionez:

- ✓ *Smartphone*n txertatze-maila:
  Estatu Batuak %44; Kanada %33; Erresuma Batua %51; Frantzia %38; Alemania %29; Errusia %25 (2011ko datuak); Txina %33; India %23 (2011ko datuak); Mexiko %20 eta Brasil %14.
  (iturria: *Google/IPSOS*)
- ✓ *Tablet*en txertatze-maila:
  Estatu Batuak %42; Kanada %22; Erresuma Batua %28; Alemania %12; Frantzia %19; Errusia %3; Txina %3; India %2; Mexiko %3 eta Brasil %4.
  (iturria: *Strategy Analytics*)

Espainian arreta jarrita, esan behar da Estatuko enpresa gehienek interesa dutela BYOD izeneko joera berri honetan. Hala eta guztiz ere, enpresa horien %18k bakarrik garatu du BYOD ezartzeko moduari buruzko estrategia bat; are gehiago dena, enpresen % 40k ez du gailu pertsonalen erabilera baimendu ere egiten laneko jardunetarako.
(iturria: @asLAN)

HIZTEGIA

[3] **Natibo digitalak:** "Natibo digital" edo "*homo sapiens* digital" deritze XX. mendeko 80ko eta 90eko hamarkadetan edo horien ondoren jaiotako pertsonei, teknologia digitala sortu ondorengoak baitira. Horrela, "etorkin digital" terminoa sortu da 80ko hamarkada baino lehen jaio badira ere teknologia-aldaketaren prozesu osoa bizi izan duten pertsonak izendatzeko.

Natibo digitalak lan munduan sartzeak eragin du BYOD errealitate bilakatzea eta, gaur egun, erabiltzaileak erabakitzen du bere komunikazioetarako zein gailu erabili nahi duen. Ez hori bakarrik, *downgrade* bat onartu eta erabiltzaile-esperientzia osatugabe baten aurrean (informazioaren teknologiako segurtasun -prozesu zurrunen ondorioz) amore eman ordez, nahiago dute bi gailu erabiltzea, bat erabilera pertsonalerako eta beste bat lanerako.

Baina, ITko sailaz gainera, finantzen sailari, giza baliabideen sailari eta juridikoari ere eragiten dio, horiek guztiek batera parte hartu behar baitute zenbait erabaki garrantzitsutan: langilearen gailuan jarri beharreko aplikazioak zein izango diren, zer baimen emango zaizkion edota aplikazio horiek nork eta zer baldintzatan (ekonomikoak, lanekoak eta ordutegiari dagozkionak) erabiliko dituen erabakitzean, besteak beste.

"*Natibo digitalak* lan munduan sartzeak eragin du BYOD errealitate bilakatzea eta, gaur egun, erabiltzaileak erabakitzen du zein gailu erabili nahi duen bere komunikazioetarako."

Apurka-apurka haziz joango den joera berri horren aurrean (belaunaldi gazteak beren bizitzan gailu adimendunak erabiltzen ohituta baitaude, eta ez diete horiei uko egin nahi), enpresak segurtasuna hobetzeko neurri batzuk hartzen hasi dira:

1. Informaziora jotzeko pribatutasun- eta segurtasun-**politikak eta -protokoloak** sortzea. Aditu askoren ustez, BYOD sistemaren arazo nagusia da kontrola enplegatuen esku uzten dela, eta azken horiek sarritan ez direla segurtasunaz arduratzen, beranduegi den arte.
2. **Web-aplikazioak** erabiltzea. Horrela, datuak zein aplikazioak web-zerbitzari seguru batean daude, erabiltzailearen ordenagailuan ezer utzi gabe.
3. **MDM**a[4] (*Mobile Device Management)* erabiltzea. Horrek ziurtatzen digu segurtasun- eta konexio -politikak enpresan gauzatuko direla. (PCen munduan oso erraza da diziplina homogeneoari eustea, ez, ordea, *tablet* eta *smartphone*n arloan, kudeaketa korapilatsuagoa baita).

Berriki egindako azterlanen arabera, Estatu Batuak dira munduko liderrak BYOD politika garatu eta baliatzeari dagokionez; Asiako eta Latinoamerikako enpresek ere sostengua ematen diote filosofia berri hori erabiltzeari (baita erabilera sustatu ere); Europa, aldiz, zuhurragoa da eta muga gehiago jarri dizkio. [ikus, aurreko orrialdean, "Estatistikak" taula]

Bukatu baino lehen, eta artikulua irakurri ondoren: orain bazatoz BYODera? ❑

ADIBIDE BATZUK

Berriki argitaratutako azterlanek erakutsi dute haziz doala urrutitik lan egiten duten eta horretarako beren gailu pertsonalak erabiltzen dituzten langileen kopurua.

Cisco Systems teknologia-enpresak, adibidez, egiaztatu du bere BYOD programa %52 hazi dela 12 hilabetetan, enplegatuek 8.144 iPad eta 20.581 iPhone baitituzte.

Amerisource-Bergen farmazia-enpresak duela gutxi jaurti du mila enplegatu ingururi zerbitzua emateko BYOD programa.

Cespa konpainia espainiarrak, berriz, BYOD joerari erantzuna emateko helburuarekin, 500 sarbide-punturen bidez hari gabeko estaldura ematen duen sarea zabaldu du.

Adibide horiek gorabehera, enpresa gehienak BYOD sistema ezartzeko prozesuaren lehenengo faseetan daude oraindik.

Urte hau fenomeno horren hedapenarena izango den ala ez ikusteke gaudelarik (hala diote aholkulariek), toki batzuetan BYOD enpresen mugak gainditzen ari da eta beste arlo batzuetara zabaltzen ari da, hala nola, **hezkuntzara.** Forsyth County eskola-eskualdea (Georgia, Estatu Batuak) osatzen duten 35 ikastetxek, adibidez, sistema hori bereganatu dute dagoeneko, BYOT (*Bring Your Own Technology* edo "Ekarri zure teknologia") izendapenarekin.

HIZTEGIA

[4] **MDM:** *Mobile Device Management* ingelesezko esapidearen siglak dira. **Software** mota bat da, gailu mugikorrak segurtatu, monitorizatu eta administratzeko bidea ematen duena, telefono-operadorea edo zerbitzuen hornitzailea zein den axola gabe. MDM gehienek funtzionalitate ugari dituzte: aplikazioak instalatzea, ordenagailuak kokatu eta horien aztarnari jarraitzea, fitxategiak sinkronizatzea edota datuak eta gailuetarako sarbidea ematea; hori guztia urrunetik, noski. Aplikazio-mota horiek onarpen handia izan dute enpresetan eta oso azkar hazi dira, *smartphone*ak enpresetan asko ugaritu direlako, batik bat.

http://es.wikipedia.org/wiki/Mobile_device_management

Pribatutasuna diseinutik (*Privacy by design*)

Oro har, proiektu-, zerbitzu- eta aplikazio-garatzaileek oztopotzat hartzen dute Datu Pertsonalen Babesa, eta itxurak atxikitzeko izapide bat dela pentsatzen dute. Horregatik, proiektuaren azken faseetan baino ez da kontuan hartzen. Horri dagokionez, "**Privacy by design**"-ek paradigma berria dakar; eta ondorengo lerroetan azalduko dizuegu zertan datzan.

HIZTEGIA

[5] **DBEB:** Datuak Babesteko Euskal Bulegoa zuzenbide publikoko entea da, nortasun juridiko propioa eta gaitasun publiko eta pribatu erabatekoa dituena. Herri-administrazioekiko inongo loturarik gabe betetzen ditu bere eginkizunak. (www.avpd.euskadi.net)

[6] **PIA:** *Privacy Impact Assessment* kontzeptuaren laburdura da, edo euskaraz Inpaktuaren Ebaluazioa Pribatutasunean. Tresna bat da, eta haren bidez jakin ahal da nolako ezaugarriak dituen zerbitzu edo produktu batek datu pertsonalen babesari dagokionez.

[7] **PET:** *Privacy Enhancement Techniques* kontzeptuaren laburdura da (euskaraz, intimitatearen eskubidea babesteko teknologiak). Neurri koherenteez osatutako sistema bat da, eta intimitatearen eskubidea babesteko erabiltzen da. Horretarako, datu pertsonalak ezabatzen ditu edota haien kopurua murriztu, edota haien kudeaketa ez-beharrezkoa edo nahi gabekoa saihestu, hori bai, informazio sistemen funtzionalitatea kaltetu gabe.

2011ko maiatzean entzun nuen lehenengoz "***Privacy by design***" kontzeptua, "*euskal securiTIConference*" ekitaldian, hain zuzen. Baina lehendik ere bazen jorratua; izan ere, 2009an hitz egin zuten kontzeptu honi buruz Madrilen egin zuten Datuak babesteko eta Pribatutasunari buruzko 31. nazioarteko hitzaldiaren 5. bilkuran (ikus "Neurri proaktiboak" koadroa, orriaren behealdean); bertan, honelako galderak plazaratu ziren: aplikazio baten diseinuaren zein momentutan izan behar dugu kontuan bizitza pribatua?, zer metodologia jarraitu behar dugu?, existitzen diren arauak, nahikoak al dira?, nola mugiarazi ditzakegu profesionalak?, eta pribatutasuna errespetatzen duen diseinua enpresen kulturan sartu behar dugu? Eta hurrengo urtean, 2010ean, Jerusalem-en egindako 32. Hitzaldian gai honi buruzko ebazpen bat sinatu zen. Bestalde, "euskal securiTIConference" hartan (Informazioaren segurtasunari buruzko Euskal kongresuan), Euskadiko Informatika Ingeniarien Elkargo Ofizialak (EIIEO) eta Industria, Berrikuntza, Komertzio eta Turismo Sailak antolatua, Pedro Alberto González-ek, Datuak Babesteko Euskal Bulegoko (DBEB[5]) Datuak Babesteko Erregistroa eta Teknologia Berriak Unitatearen arduradunak, hitzaldi bat egin zuen eta bere izenburua honakoa zen: "*Privacy by design: Lehen diseinutik pribatutasuna bermatzen duten aplikazioak garatzen*" (http://www.slideshare.net/pagonzalez/presentacin-pagonzalez-en-euskalsecuritic). Hitzaldi hartan azpimarratu zuen, besteak beste, pribatutasuna eskubide bat dela eta kontuan izan behar dela modu proaktiboan. Halaber, **PIA**[6] (*Privacy Impact Assessment- Inpaktuaren Ebaluazioa Pribatutasunean*) eta **PET**[7] (*Privacy Enhancement Techniques- intimitatearen eskubidea babesteko teknologiak*) kontzeptuak azaldu zituen.

2012ko urtarrilean aurkeztu zen, Europan, **Datuak Babesteko Araudi Orokorrerako proposamena**. Araudi horrek pribatutasunaren gaineko eraginaren analisia (PIA; ingelesezko sigletan) egiteko aukera jasotzen du, eta Europako herrialde batzuek gomendio gisara jaso dute, dagoeneko, datuak babesteari buruzko legeetan. Analisi-mota horrek barne hartu beharko du, beste

NEURRI PROAKTIBOAK

Datuak babesteko eta Pribatutasunari buruzko 31. Nazioarteko Konferentziak "*Datuak babesteko eta Pribatutasunari buruzko nazioarteko estandarrak*" deitutako ebazpena idatzi zuen. Konferentziak neurri proaktiboei kapitulu bat eskaintzen die, **betetze** eta **gainbegiratze** atalean, hain zuzen. Eta neurri horien guztien artean, ondorengo bi hauek ditugu nabarmendu beharrekoak:

- *Datu pertsonalak kudeatzeko erabiltzen diren sistemen edota informazio teknologiak egokitzea pribatutasuna babesteko dagokion araudiari; bereziki, xehetasun teknikoei eta bere garapenari edo ezarpenei buruz erabaki behar denean.*
- *Sistema berriak edota datu pertsonalak kudeatzeko informazio-teknologiak ezarri baino lehen, ikerketak martxan jartzea, pribatutasunean nolako eragina izango duten aztertzeko. Modu berean, praktikan jarri behar dira datu pertsonalak kudeatzeko eredu berriak edo aldaketa nabariak egin jada egiten diren kudeaketetan.*

gauza batzuen artean, interesatuen eskubide eta askatasunentzat egon daitezkeen arriskuen ebaluazioa.

JATORRIA

Ontarioko (Kanadako probintzia) Informazio eta Pribatutasun Mandatariak, **Ann Cavoukian** doktoreak, "*Privacy by design*" kontzeptua 90eko hamarkadaren hasieran asmatu zuen. Orduz geroztik, kontzeptua zabaltzen joan da doktorea. Kontzeptu hau filosofia eta ikuspuntu berri bat da, eta pribatutasuna zenbait teknologiaren diseinuen xehetasunetan kontuan izatean datza.

Irailaren 11ko atentatuaz geroztik, badirudi edozer gauza egin daitekeela segurtasuna bermatzeko, eta, askotan, pertsonen pribatutasuna bigarren mailan uzten da. Cavoukian doktoreak azpimarratzen du ez dugula segurtasuna eta pribatutasuna kontzeptuen artean hautatu behar (ikus beheko koadroan *Privacy by Design*-en oinarrizko 4. printzipioa). Esan nahi baita ez dugula pribatutasuna baztertu behar segurtasun-maila altuagoa lortzeko; aitzitik, bi kontzeptuak kontuan izan behar ditugula, betiere, pribatutasuna gure askatasun askoren oinarria

PbD[8]-ren OINARRIZKO 7 PRINTZIPIOAK

1. **Proaktiboa, ez-erreaktiboa; Prebentibo ez-zuzengarria**

Privacy by Design-ek (PbD) neurri prebentiboak erabiltzen ditu, ez erreaktiboak; pribatutasunaren kontrako gertaerak jazo baino lehen aurreikusten eta saihesten ditu. Ez da noiz zer gertatuko zain geratzen, eta ez du konponbiderik eskaintzen gertatutako pribatutasunaren kontrako arau-hausteak zehatzeko. Bere helburua da pribatutasunaren urraketei aurrea hartzea. Hau da, gertaera jazo baino lehen eskua hartzea, eta ez horren ostean.

2. **Lehenetsitako konfigurazioa: pribatutasuna**

Lehenetsitakoak agintzen du. Edozein sistematan eta edozein negoziotan datu pertsonalak automatikoki babestuta egon behar du. Ezer berezirik egin gabe, sistema eraiki behar dugu pribatutasuna berez babestuta egon dadin (gaur egun, Facebook-en gertatzen denaren kontrakoa).

3. **Diseinuan txertatutako pribatutasuna**

Pribatutasunak ardazten du eskaintzen den zerbitzua; alegia, sistemaren zati integrala da, aldez aurretik pentsatua, eta ez du funtzionalitatea gutxitzen.

4. **Erabateko funtzionalitatea - "Denak irabazle", eta ez "Batak irabazi, besteak galdu"**

Pribatutasuna versus Segurtasuna moduko bikote faltsuak saihesten ditu. Egiaztatzen du posible dela biak aldi berean izatea, "*batak irabazi, besteak galdu*" kontzeptura jo gabe.

5. **Alderik aldeko segurtasuna. Bizi-ziklo osoa babestu**

Informazioaren aurreneko elementua jaso baino lehen sisteman txertatu denez, *Privacy by Design* dagokien datuen bizi-ziklo osoan zabaltzen da segurtasun osoz; izan ere, segurtasun neurri sendoak beharrezkoak dira pribatutasuna bermatzeko, hasieratik bukatu arte. Horrek bermatzen du datu guztiak segurtasun osoz gordetzen direla, eta, ondoren, prozeduraren amaieran, datuak txikitzen direla, inolako atzerapenik gabe. Beraz, PbD-k bermatzen du informazioaren bizi-zikloaren kudeaketa segurua egiten dela, hasieratik amaieraraino, alderik alde.

6. **Ikusteko modukoa eta gardena – beti irekita**

PbD-k ziurtatu nahi du, negozioa edozein dela ere eta erabilitako teknologia edozein dela ere, egiten diren promesak eta iragarritako helburuak beteko direla, eta betetze hori modu independentean egiazta daitekeela; hots, osagarriak zein eragiketak ikusteko modukoak eta gardenak direla, bai erabiltzaileentzat bai hornitzaileentzat.

7. **Erabiltzaileen pribatutasuna errespetatu – Erabiltzaileak ardatz duen ikuspuntuari eutsi**

Gauza guztien gainetik, PbD-k eskatzen du arkitektoek eta operadoreek pertsonen interesak lehenestea; alegia, erabiltzailea lehentasunen ardatza izatea.

Jatorria: http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-spanish.pdf (*Information and Privacy Commissioner of Ontario*)

HIZTEGIA

[8] **PbD:** *Privacy by Design* kontzeptuaren laburdura da. Informazio gehiago irakurtzeko, bisitatu ondorengo helbidea: www.privacybydesign.ca

dela jakinda.

PBD EBAZPENA

Arestian esan bezala, "*Privacy by design*" nazioarteko estandar bihurtu zen Datuak babesteko eta Pribatutasunari buruzko 32. nazioarteko hitzaldian. Horretarako, etorkizunean informazioaren pribatutasuna sendotzea helburu duen ebazpena egin zen.

Gaur egun, datuen babesa eta pribatutasuna aztertzen dugunean, kudeaketa-arduradunek datu pertsonalak babesteko legea baino ez dute kontuan hartzen, lege-hausterik ez egiteko. Baina ez dute ikusten zer-nolako eragina izan dezaketen bildutako datuek pertsonen pribatutasunean. Horregatik, PbD[9] diseinu filosofia berriari buruz hitz egiten da.

"*Privacy by design*" ebazpenak "pribatutasun" kontzeptua teknologia berrietan eta erakundeetan zuzenean sartzea du helburu, hasiera-hasieratik, pribatutasunaren babesaren oinarrizko osagai bihurtu arte, ikuspuntu teknikotik zein antolakuntzaren ikuspuntutik. Beste modu batean esanda, teknologia berrien diseinuetan, enpresen praktiketan eta azpiegituretan pribatutasuna sartzea lortu nahi da, pribatutasuna modu proaktiboan kudeatzeko eta balio lehenetsia izateko, a posteriori ezarri beharrean; izan ere, indarrean dauden araudiak betetzeak ez du esan nahi pribatutasuna bermatzen denik.

Teknologia berriak, dakigunez, oso azkar garatzen dira, legeak baino askoz azkarrago. Horregatik, beharrezkoa da teknologia berri horiek, baita erakundeek ere, **lehenetsitako pribatutasun** printzipioa onartzea, betiere produktuen eta zerbitzuen hasierako azterketa faseetan, beste betebehar bat izango balitz bezala. Gaur egun, adibidez, segurtasuna, usagarritasuna, erabilerraztasuna... kontuan hartzen dira hasiera-hasieratik.

Kontzeptu hau gero eta gehiago erabiltzen ari da hainbat erakundetan, proaktiboa eta prebentiboa baita.

PBD ETA BERE TRILOGIA

Hasieran, Privacy by Design (PbD) teknologiara zuzenduta zegoen, bere lan-esparru nagusia baitzen. Dena den, gaur egun beste bi arlotan ere aplikatzen da. Beraz, ondorengo esparruetan lantzen dela esan dezakegu:

- ✓ IKT sistemak (Informatika eta Komunikazioetarako Teknologiak)
- ✓ Negozio-jarduera arduratsuak
- ✓ Diseinu fisikoa eta sareko azpiegitura

Teknologia izatez ez da pribatutasunaren kontrako mehatxu bat, arazoa da nola erabiltzen den. Pribatutasun-praktika onak erabiltzeak inbertsioaren itzulera dakar (*ROI*[10]), eta gainera erabiltzailearen konfiantza eta gogobetetzea ere areagotzen du. Beraz, ondoriozta dezakegu negozioentzat pribatutasuna ona dela.

ZAINTZA-TEKNOLOGIA INBADITZAILEAK

Badakigu, zaintza-teknologia inbaditzaileak existitzen direla; eta, gaur egun, asko erabiltzen ari direla. Hortaz, modu batean edo bestean, denok jasaten ditugu egunero, esaterako, irrati-frekuentzia bidezko identifikazio teknologiak (RFID[11]); identifikazio-, zaintza- eta kontrol-teknologiak (zaintza kamerak, publikoak zein pribatuak); datu biometrikoak erabiltzen dituzten teknologiak (sarbide- eta segurtasun-kontrola); gorputz-irudiak (gorputz osoko eskanerrak); sare-jarraipena eta monitorizazioa (Interneteko zerbitzu hornitzaileak -ISP-), identitate digitalen bilketarako sistemak, etab.

Askotan, segurtasun sistema horiek segurtasunari lehentasuna ematen diote, eta gure pribatutasunaren zati bati uko egiten diote. PbD printzipioak, berriz, produktuen eta zerbitzuen hasierako garapen faseetatik pribatutasuna kontuan izan behar dela aldarrikatzen du. Are gehiago, esaten du printzipio horiek kontuan hartu ahal direla datuen segurtasuna eta sistemaren funtzionalitatea gutxitu gabe. Ez dugu ahaztu behar datuen bizitza-ziklo osoan segurtasun-arriskuak izango ditugula. Horregatik, arriskuak murriztea izango da helburuetako bat.

Orain, hainbat teknologia edo adibide ikusiko ditugu pribatutasuna (PET) handitzeko:

HIZTEGIA

[9] **PbD diseinuaren filosofia:** sistemen/zerbitzuen diseinatzaile baten lana pertsonen pribatutasuna babestetik abiatu behar da. Horretarako, galdera hauek egingo dizkio bere buruari: datu pertsonalen bat jaso beharko dut?, hala bada, zein da beharrezko gutxienekoa?, nork eskuratu ahal izango ditu datu horiek?, nola kontrolatu ahalko dira datu horiek baimendutako pertsonek bakarrik ikus ahal ditzaten?...

[10] **ROI:** *return on investments*, inbertsioaren itzulera. Lortutako etekina edo funtzionalitatea konparatzen du egindako inbertsioarekin.

[11] **RFID:** *Radio Frequency Identification*, irrati-frekuentzia bidezko identifikazioa. RFID teknologiaren ideia eta barra-kodearena oso antzekoak dira. Bien arteko ezberdintasun handiena da barra-kodeak seinale optikoak erabiltzen dituela datuak igortzeko; eta, RFIDk, berriz, irrati-uhinak erabiltzen dituela. (ikus Aurrera aldizkariaren 42. alea, 2011ko ekainekoa, "*RFID teknologia*" artikulua)

•**Datu biometrikoak:** Kasu honetan, datu-base biometriko zentralizatuak eta handiak sortzea saihestu behar dugu. Halaber, gomendagarria da gordetzen eta transferitzen diren datu biometrikoak enkriptatzea.

•**RFID etiketak:** Zaintza- eta kontrol-sistema honi dagokionez, "*clipped tag*" izeneko teknologia existitzen da, IBMk garatua, eta kontsumitzaileei aukera ematen die automatikoki antena desgaitzeko. Adibidez, zigiluak orritik kentzen diren bezalaxe (puntu-lerroez) edo arraspatuz, loteria txartelak bezala.

•**Bideozaintza:** Teknologia honen bidez lortutako datuekin hainbat gauza egin ditzakegu, esaterako, bistaratu, gorde, indexatu, eta, azkenik, biltegiratu. Teknologia honek delinkuentzia saihesteko edota ebidentziak biltzeko balio dezake, betiere ondo erabiltzen bada. Dena den, kezka handia dago grabatutako datuak nola erabiliko diren jakiteko. Grabazio batean agertzen diren objektuak (gorputzak eta aurpegiak, esaterako) enkriptatzen duten teknologiak existitzen dira jada, eta bakarrik deskodetu egingo lirateke ikerketa bat egongo balitz.

•**Gorputzen irudiak:** Bidaiariak eskaneatzeko teknologiak gero eta ohikoagoak dira hainbat aireportutan, eta balizko segurtasun mehatxuak identifikatzeko erabiltzen dira. Arazoa da pertsonen intimitateari larri erasotzen diotela. Horregatik, enkriptatutako irudiak urruneko puntu batera bidaltzeko teknologiak erabiltzen ari dira. Bertan, eskaneatutako pertsonarekin inolako harreman fisikoa ez duen langile batek ikuskatzen ditu. Langileak ezin izango ditu jasotako irudiak gorde, bidali, ezta inprimatu ere. Are gehiago, irudia ezabatu beharko da ondorengo ikuskaritza egin baino lehen. Gainera, pribatutasun iragazki bat aplikatzen zaio irudiari, horrela, balizko mehatxuak baino ez dira ikusten; gorputzak eta aurpegiak lausotzen dira.

•**Sarearen jarraipena eta monitoretza:** Internet-eko zerbitzu hornitzaileek erabiltzaileen datu asko biltzen dituzte, esaterako, on-line egindako jarduerak. Hori arazo larria izan daiteke lapurreta bat izatekotan edota galtzen edo saltzen badira. Adibidez, Torontoko Unibertsitateak "bunker" izeneko sistema bat sortu du arazo horri aurre egiteko. Sistema horren bidez, zerbitzu hornitzaileak bereziki babestu beharreko datuak bildu ditzake eta, ondoren, leku seguru batean gorde. Sistemak debekatutako erabilerak saihesten ditu, alde batetik; eta txosten batzuk eskaintzen ditu, beste alde batetik. Horrela, norbaitek sistemari erasotzen diola antzematen bada, litekeena da bereziki babestu beharreko datuak suntsitzea erasotzaileak datuak jaso baino lehen.

•**Identitate digitalak:** Sarritan, Internet-en geure burua identifikatu behar dugu modu digitalean. Gaur egun, **identitatearen lapurreta** (ikus behealdeko koadroa) gaitz bat da, eta, horren ondorioz, erabiltzaileek Internet-en duten konfiantza gutxitzen doa. Gainera, ziurtagiri hauen bilketak pertsonen profil oso zehatzak eskaini ditzake. Hori guztia murrizteko, hainbat teknologiak datu pertsonalen bilketa eta erabilera ahalik eta gehien murrizten dute.

Pribatutasuna sendotzeko erreminta eta teknologia hauetaz gain, kontuan izan behar ditugu pribatutasunaren aukera murriztaileak lehenetsita dituzten aplikazioak eta teknikak (*privacy by default*), eta baita datu pertsonalak elkartrukatzeko metadatu ereduak ere diseinatu, betiere araudiek ezarritakoa betetzeko; eta, azkenik, DLP[12] (*Data Loss Prevention*) teknologia erabiltzea. Sare-sozialen esparruan ere zaindu behar da pribatutasuna, horregatik Datuak Babesteko Agentziak informazioa prestatzen ari dira, eta formakuntza antolatzen dute erabiltzaileek erabilera arduratsua egin dezaten. ❑

IDENTITATEAK LAPURTZEA

Identitatea lapurtzea da erasotzaile batek, baliabide informatikoen bidez edo beste baliabide batzuen bidez, informazio pertsonala lortzea; gero modu ilegalean erabiltzeko. Munduan azkarren hazten ari den delitua da. Hainbat bide daude informazio pertsonala eskuratzeko:

- ***Phishing***[13] **eta posta faltsuen bidez**: erasotzaileak benetako erakundeen, banketxeen edo enpresen antza hartzen du.
- **Pertsonala**: erasotzaileak entzuten edo ikusten duen informazioaren bitartez hartzen du.
- **Eraso antolatua**: erasotzaileak enpresa, banketxe edo erakunde baten segurtasun-sistema apurtzen saiatzen dira bezeroen datuak lortzeko. (Jatorria: http://es.wikipedia.org)

HIZTEGIA

[12] **DLP:** ingelesez *Data Loss Prevention* esan nahi du, hau da, segurtasunari buruzko hainbat mekanismo eta prozeduren multzoa. Multzoaren helburua da ezkutupeko informazioaren edo bereziki babestu beharreko datuen galerak ekiditea.

(ikus Aurrera aldizkariaren 33. zkia., 2009ko martxokoa, "*Kanpoko gailu mugikorren segurtasuna*" artikulua)

[13] **Phishing:** ingelesezko *fishing* «arrantza» esapidetik eratorria. Modu gezurtian erabiltzaileak "arrantzatzeko" jarduerari deritzogu, betiere haien informazio ezkutua lortzeko. Dena den, batzuek diote «*password harvesting fishing*» (pasahitzen uzta eta arrantza) kontzeptuaren laburdura dela. 1996an erabili zen lehenengoz phishing hitza, eta "alt.2600" hacker-en albiste taldean izan zen.

(ikus Aurrera aldizkariaren 22. zkia., 2009ko martxokoa, "*Ciber-delituak*" artikulua)

ALBOAN:

Lanpostu korporatibo berrirako migrazioa

"2013an gauzatuko da Eusko Jaurlaritzako 6.000 ordenagailuen migrazioa."

Guztiok dakigu informatika etengabe bilakatzen ari dela. Hainbeste ezen, aldian-aldian, aplikazio berriak ezarri behar izaten ditugun, edo erabili ohi ditugun produktuen aldaera berrietara migratu behar izaten dugun. Gure erakundea, Eusko Jaurlaritza, ez dago gertaera-mota horietatik kanpo eta, historikoki, hainbat eguneraketa egin behar izan ditu dagoeneko (sistema eragileak, ofimatika-paketeak eta beste *backoffice* ingurune batzuk).

Bada, urte honetan zehar beste migrazio bati aurre egin beharko diogu. Hori dela eta, artikulu hau prestatu dugu aldaketa zehazki zer izango den eta zer urrats emango diren azaltzeko.

ARRAZOIAK

2012an hasi zituen Eusko Jaurlaritzak 2013 urte honetan PC korporatiboaren oinarrizko softwarea aldatzeko prestaketak. Proiektu horrek Eusko Jaurlaritzako Administrazio Sare Korporatiboan lan egiten duten pertsona guztiei eragingo die.

Proiektu berria, zehazki, egungo PC korporatiboa (Windows XP sistema eragilea, Internet Explorer 8 nabigatzailea eta MS Office 2003 ofimatika-paketea barne hartzen dituena) aldatzean datza, software berri hauek instalatzeko: Windows 7 sistema eragilea, Internet Explorer 9 eta Mozilla Firefox nabigatzaileak eta, ofimatika-multzo gisara, MS Office 2010 eta LibreOffice 3.

Hauek dira, besteak beste, migrazioa egitearen **arrazoiak**:

- Teknologiaren zaharkitzea: egungo sistemak eguneratu ezin direnez, babestuta egoteari utzi diote eta aldatu ezean segurtasun-arazo larriak gerta litezke.
- WindowsXP-SP3 euskarria: 2014ko apirilean bukatzen da Eusko Jaurlaritzak sistema eragile horrentzat duen euskarria.
- Arkitektura berria: PCaren arkitektura berri bat eduki nahi dugu, osatzen duten geruzen artean (hardwarea, sistema eragileak, aplikazioak eta datuak) independentzia handiagoa eskainiko duena.
- Funtzionalitateak: funtzionalitate gehiago eskura izateko premia dago (WiFia, USBak, etab.).
- Arrazoi ekonomikoak: zerbitzu hobea eskaini nahi bada, automatizazioa handiagotu eta eskuzko prozesuak murriztea (berrabiaraztean edo adabakitzean ematen den denbora) beharrezkoa da; eta egungo sistemek ez dute horretarako aukerarik ematen.

IRISMENA

PC korporatibo berria diseinatzea ez da egiteko erraza; aitzitik, EJIEko teknikarien aurretiazko hainbat lan eskatzen ditu proiektua arrakastatsua izan dadin edo, beste modu batean esanda, azken erabiltzaileei ahal bezain arazo gutxien eragin diezaieten. Hauek dira egiten ari diren lanetako batzuk:

- ✓ Beharrezko hedapen-**mekanismoak** ezartzea migrazio-eragiketa ahal bezain "gardena" izan dadin
- ✓ Erabiltzailearen **datuentzako** migrazio-prozesua diseinatzea (gorde beharreko datuen bolumena zenbat eta handiagoa izan, denbora gehiago beharko da)
- ✓ Ordenagailuaren **segurtasun**-maila egokia

ezartzea (profila, konfigurazioak, etab.)

- ✓ Sailen aplikazio guztien bateragarritasuna egiaztatzea

Egin beharreko lana are gehiago zailtzen da migrazioa Eusko Jaurlaritzako sail eta erakunde autonomo guztietara iristen dela aintzat hartzen badugu. Hala, bada, 6.000 ordenagailuz ariko ginateke, gutxi gorabehera. Horrez gainera, gorago aipatu bezala, dauden aplikazio korporatibo guztien (740, gutxi gorabehera, horietako 500 web-aplikazioak dira, eta 240 bezeroa/zerbitzaria motakoak) arteko bateragarritasuna egiaztatu behar da, baita erabili ohi den hardwarea (inprimagailuak, eskanerrak eta gainerako periferikoak) ondo dabilela aztertu ere.

Kontuan izan behar dira, orobat, Access datu-baseak erabiltzen dituzten aplikazioak, balitekeelako Office2010 softwarearekin ongi ez ibiltzea. Hori dela eta, EJIEk arreta berezia eman beharko dio alderdi horri.

WINDOWS7 BAINO ASKOZ GEHIAGO

Proiektua Windows7 Enterprise sistema eragilearen inguruan oinarritzen bada ere, proiektu hori baliatuko da, batetik, egungo direktorio aktibotik Windows Server 2008 R2ra igarotzeko eta, bestetik, egungo SMS2003 azpiegitura SCCM (*System Center Configuration Manager)* berrira aldatzeko.

Beste gai aipagarrienen artean dago, aurrez esan bezala, Microsoften ofimatika-paketearekin batera (Office2010) software askeko horren sistema baliokidea instalatuko dela, zehazki, **LibreOffice**n 3.5 aldaera.

Nabarmentzekoa da, baita ere, nahi duten erabiltzaileek modu erraz eta erosoagoan aukeratu ahalko dutela "Euskarazko profila" sistema eragileko eta ofimatika-paketeko interfazeen lan-hizkuntzatzat.

PROIEKTU PILOTUA

Eusko Jaurlaritzako Sare Korporatiboko ordenagailu guztietan **migrazio masiboa** gauzatu aurretik dena ondo ibiliko dela ziurtatzeko, proiektu pilotu bat egin da, 60 pertsona ingururekin, joan den abenduan eta urtarrilean.

Sail eta profil ezberdinetako pertsona horien ordenagailuetan oinarrizko software berria instalatu zaie, ahal bezain beste proba egin eta gerta zitekeen edozein arazo jakinarazteko.

Tarte horretan, pertsona horiek EJIEren laguntza eta sostengua jaso dute (Erabiltzailearen Laguntza Zentroaren bidez) sor zitezkeen arazoak konpontzeko.

Windows7 eta Office2010eko interfazea (menuak eta pantailak) egungo bertsioen aldean nabarmen aldatzen denez gero, une honetara arte horiekin lan egin ez duten pertsonek kontzientzatzeko/ikasteko fitxa batzuk ere izan dituzte eskura, beren eguneroko lanean sor dakizkiekeen zalantzak argitzeko.

Tarte hori bukatu eta gertatutako arazo guztien berri eman ondoren, EJIEko proiektu-arduradunak horiek aztertzen ari dira, berriro errepika ez daitezen.

Ezarritako plangintzaren arabera, 2013. urte honetan gauzatuko da Eusko Jaurlaritzako 6.000 ordenagailuen (mahai gaineko ordenagailuak eta eramangarriak) migrazioa.

Horrela, datozen hileetan proiektuaren bilakaerari buruzko berriak izango ditugu. ❑

"Joan den abenduan eta urtarrilean Proiektu Pilotua egin da, 60 pertsonen parte-hartzearekin."

[**info+**]:

EJIE (Eusko Jaurlaritzaren Informatika Elkartea):

http://www.ejie.net

BERRI LABURRAK!!

43. zk.

2013ko martxoa

GALILEO sateliteei erantsitako funtzionalitate berria

AURRERA aldizkariaren 8. zenbakian (2002ko ekaina) hitz egin zen lehen aldiz GALILEO sistemaz, hots, Europar Batasunak garatutako satelite bidezko sistema globalaz. Horren helburua da, besteak beste, gaur egun GPS (*Global Positioning System*) sistema amerikarrarekiko eta GLONASS sistema errusiarrarekiko dagoen mendekotasuna saihestea, bata zein bestea arlo militarrekoak baitira.

GALILEO sateliteen sistemak bost zerbitzu emango ditu:

1. **Zerbitzu irekia.** Pertsona guztiei bideratutako doaneko zerbitzua. GPSek eskaintzen dutena baino doitasun eta eskuragarritasun handiagoak.
2. **Aplikazio kritikoentzako zerbitzua.** Segurtasuna kritikoa den aplikazioetarako pentsatuta, hala nola, bidaiarien aireko garraiorako. Zerbitzu hori eman ahal izateko, frekuentzia bikoitzeko hargailu egiaztatuak erabiliko dira eta sistemak integritate-maila altua eskainiko du.
3. **Merkataritza-zerbitzua.** Ez da doanekoa izango, bistan denez, eta zerbitzu irekiak eskaintzen dituenak baino zerbitzu gehiago behar dituzten aplikazioentzat baliatuko da, zifratutako bi seinale erantsita.
4. **Zerbitzu publiko arautua**. Gobernu-aplikazioak erabiltzeko eskuragarri egongo den zerbitzua. Une oro eta edozein egoeratan egon beharko du martxan.
5. **Bilaketa- eta salbamendu-zerbitzua.** Eskainitako hobekuntzei esker munduko edozein tokitatik bidalitako sorospen-mezuak denbora errealean jaso eta zehaztasunez aurkitu ahalko dira, metro gutxiko errorearekin.

Azken zerbitzu horretarako, Bartzelonan egoitza duen MIER Comunicaciones enpresak fabrikatu eta diseinatu ditu Europako nabigazio-sistemari **bilaketa- eta salbamendu-funtzionalitatea** erantsiko dioten ekipamenduak. Ekipamendu horiek gai dira arriskuan dauden pertsonen sorospen-zeinuak jaso eta estazio-hartzaileetara igortzeko, azken horiek salbamendua antola dezaten.

Gaur egun, bukaeran egongo diren hogeita hamar sateliteetatik bost daude orbitan.

Bosgarren WIFI belaunaldia

IEEE 802.11n hari gabeko konexio estandarrak nabarmen hobetzen zuen **802.11b** eta **802.11g** aurreko estandarren transmisio-abiadura: zaharrek 54 Mbps-eko gehienezko emariak zituzten, eta berriagoak 600 Mbps-ekoa. Gainera, bi banda erabiltzen ditu aldi berean: 2,4 eta 5 GHz-koak, eta MIMO kontzeptua barneratzen du. Azken horrek hainbat sarrera eta irteera egoteko aukera ematen du (transmisio espaziala deritzona), eta gailu komertzialetan bi edo hiru espazio-jario onartzen ditu. Hala eta guztiz ere, 802.11n atzean gelditzen ari da **IEEE 802.11ac** estandar berriaren ondoan. Azken hori **bosgarren WIFI belaunaldia** izenez ezagutzen da, eta 2013ko bukaerarako amaituta egongo dela aurreikusten da, nahiz eta eros daitezkeen, jadanik, teknologia hori onartzen duten gailuak, hala nola, PCE-AC66 dual-band izeneko ASUS etxeko 802.11ac sareentzako egokigailuak, 1'3 Gbps-ra iristeko gai direnak.

Asmoa da 802.11 estandar guztiak egun daudenekin bateragarriak izatea, eta ezberdintasuna geruza fisikoan egotea soilik (seinale elektrikoak eta kableak).

IEEE 802.11 estandarraren beste bertsio bat, **IEEE 802.11ad** izenekoa, **hainbat Gigabit segundoko** emarietara iristeko gai izango da 60 GHz-ko bandaren gainean, baina arazo bat du: **oso distantzia laburretarako** bakarrik balio duela (metro gutxi batzuk); hori dela eta, 802.11n eta 802.11ac estandarrentzako osagarria izango da.

802.11ac espezifikazioaren azken bertsioa:

http://www.ieee802.org