EUSKO JAURLARITZA GOBIERNO VASCO

ARURRERA! 60

2017ko ekaina

Berrikuntza eta Teknologia Berrien dibulgaziozko aldizkaria
Bulego Teknologikoak argitaratua
Informatika eta Telekomunikazio Zuzendaritza

AURKIBIDEA

Entitate batek bezeroei eskaintzen dien zerbitzua hobetzeko daukan modu bakarra dauzkan prozesuak aztertzea da. Horretarako, lehenik eta behin, ezinbestekoa du jakitea zein prozedura dauzkan eta, baita ere, nola dauzkan antolatuta prozedura horiek. Eusko Jaurlaritzak ere helburu hori du, eta, horregatik, sail eta organismo autonomo guztietan Kudeaketa Publiko Aurreratuaren Eredu bat ezartzen ari da, *Aurrerabide* izenaz ezagutzen dena.

Metodologia horren bidez lortu nahi dena da sailen zuzendaritza eta zerbitzuek tresna bat izan dezatela, euren egoera zein den jakiten lagunduko diena, hobetu daitezkeen alderdiak optimizatu ahal izateko. Eta horri guztiari esker, herritarrei zerbitzu hobea eskaini ahal izango zaie. Lehendabiziko gaian, beraz, metodologia horri buruzko sarrera bat egingo dugu.

Bigarren gaian («*Prestakuntza, Segurtasunaren Eskema Nazionalaren ikuspegitik*»), adieraziko dizuegu prestakuntzako zer eduki lantzen ari den Eusko Jaurlaritza segurtasun informatikoaren eremuan. Langile guztientzako ikastaro batzuk dira, laguntzen digutenak, batetik, eraso informatikoak gutxitzen, eta, bestetik, jakiten zergatik den horren garrantzitsua sail eta organismo autonomoetako pertsona guztiak kontzientziatzea.

«Alboan» atalean, kasu honetan, Eusko Jaurlaritzako estandar teknologikoez jardungo gara, funtsezko pieza diren aldetik Euskadiko Administrazio Elektronikoaren azpiegitura horizontalaren ezaugarri teknikoak, lanpostuak eta abar definitzeko.

Azkenik, «*Wanna Cry*» malwarearen eraginez gertatu berri diren erasoek oihartzun handia izan dutenez bai zibersegurtasunaren arduradunen artean, bai oro har herritarren artean, segurtasun informatikoarekin zuzenean lotuta dauden bi gai ekarri nahi izan ditugu «*Berri laburrak*» atalean. Lehenik, «*CONAN mobile*» aplikazioaren bertsio berri bat aurkeztuko dugu, eta, bigarrenik, hizpide izango dugu zibersegurtasuna emakumearekin lotzen duen alderdi berritzaile bat, hots, Incibe Institutuak antolatutako «*Generoaren eta Zibersegurtasunaren Nazioarteko I. Foroa*»-n berriki aztertutako ikuspegi berri bat.

Aurrerabide ekimena

Erakunde orok etengabe aldatu behar ditu dauzkan prozesuak, egunero-egunero bezeroei zerbitzu hobe bat eman ahal izateko eta gainerako enpresekiko lehiakor izaten jarraitzeko. Administrazio Publikoen kasuan, gauza bera gertatzen da, horiek ere barne-prozesuak berrikusi behar baitituzte, beraien gizarteari zerbitzu hobe bat eskaini ahal izateko.

Askotan, Administrazio Publikoak nola funtzionatzen duen deskribatzerakoan, esaten da ez duela efikaziaz eta efizientziaz funtzionatzen, malgutasun txikia duela eta geldi egokitzen dela herritarrek eskatutako aldaketetara.

EUSKO JAURLARITZAREN
KUDEAKETA PUBLIKO
AURRERATUKO EREDUA

Eusko Jaurlaritzaren Berrikuntza Publikoaren Planean (BPP), zeina Herritarrak Hartzeko eta Administrazioa Berritzeko eta Hobetzeko Zuzendaritzak landu baitzuen, adierazi zen jada honako hau:

«*Administrazio Publikoa funtsezko pieza bat da gizarte aurreratu batean. Administrazio Publiko moderno, azkar eta efiziente bat erabakigarria da ongizate eta bizitza-kalitate handiagoko gizarte bat lortzeko. Beharbeharrezkoa dugu, beraz, Administrazio Publiko bat, gure gizarte konplexu, aldakor eta askotarikoak une oro egiten dizkion eskakizunei efikaziaz erantzuteko gai izango dena*».

Euskal gizarteari eskaintzen zaizkion zerbitzu publikoak hobetze aldera, BPPan ardatz bat sartu zen, helburu zuena Eusko Jaurlaritzan eta bere organismo autonomoetan **Kudeaketa Aurreratuaren Eredu bat** ezartzea, «Aurrerabide» izena hartu zuena.

Hasierako plangintzaren arabera, aurreikusita zegoen hiru urteko epean (2014ko otsailetik 2017ko urtarrilera) Jaurlaritzako zuzendaritza guztiek egingo zutela prestakuntza/ekintza.

Une honetan, Eusko Jaurlaritzako sail eta organismo autonomo guztiak ari dira parte hartzen.

Erreferentzia bat emateko, adierazi behar da 2014, 2015 eta 2016ko deialdietan, guztira, 110 zuzendaritza, organismo autonomo edo ordezkaritza izan direla parte hartu dutenak. 685 izan dira prozesuan zuzenean parte hartu duten zuzendari, ordezkari, zerbitzuko arduradun edo arloko arduradunak, eta 1.000tik gora dira prozesuan zeharka inplikatuta daudenak.

Funtzio Publikoko Sailburuordetzaren ekimen hau (2014-2016 BPPan sartuta dago) Eusko Jaurlaritzarako proiektu estrategiko bat da[1], jarraipena duena Gobernantza eta Berrikuntza Publikoaren 2020 Plan Estrategiko berrian.

NOLA FUNTZIONATZEN DU AURRERABIDEK?

Aurrerabideren ezaugarri nagusietako bat da **eredu propio** bat dela, Jaurlaritzako pertsonek berariaz diseinatua eta garatua, gure Administrazioarentzat asmatua, eta prozesuaren beraren hobekuntzan arreta gehiago jartzen duena bere alderdi formalean baino.

Informatika eta Telekomunikazioetako Zuzendaritzak (ITZ), beste hainbat zuzendaritzek bezala, parte hartu du Aurrerabide ekimenean. Jarraian, ITZk ekimen honetan izan duen esperientziaren eta egin dituen

[1] **Proiektu estrategikoa:** Eusko Jaurlaritzak araudi hau argitaratu du, Aurrerabideri lotuta:

- Gobernu Kontseiluaren Erabakia, 2014-2016 BPPari buruzkoa (2014ko ekainaren 17a)
- Gobernu Kontseiluaren Erabakia, Aurrerabideri buruzkoa (2014ko urriaren 14a)
- Gobernu Kontseiluaren Erabakia, Ebaluazioei, Finkatze eta Hobetze Planei eta Kolaboratzaileen Sareari buruzkoa (2016ko ekainaren 7a)
- Lege Proiektua, Euskal Sektore Publikoaren Antolamendu eta Funtzionamenduri buruzkoa

lanen berri emango dugu, baliagarria izango delakoan.

Lehen pausoa izan da, PDCA[2] motako etengabeko hobekuntzako prozesu orotan gertatzen den bezala, **autoebaluazio** bat

egitea, jakiteko zein den gure egoera oinarri gisa darabilgun Kudeaketa Aurreratuaren Ereduarekiko: identifikatu behar ditugu indarguneak, ahulguneak, aukera posibleak, bai eta aurre egin beharko diegun mehatxuak ere. Halaber, beste dokumentu batzuekin batera, gure Zuzendaritzako Zerbitzu Katalogoa landu da. Horren guztiaren helburua izan da zehaztea zeintzuk izango diren konpromiso espezifikoak, gerora garatu beharko direnak.

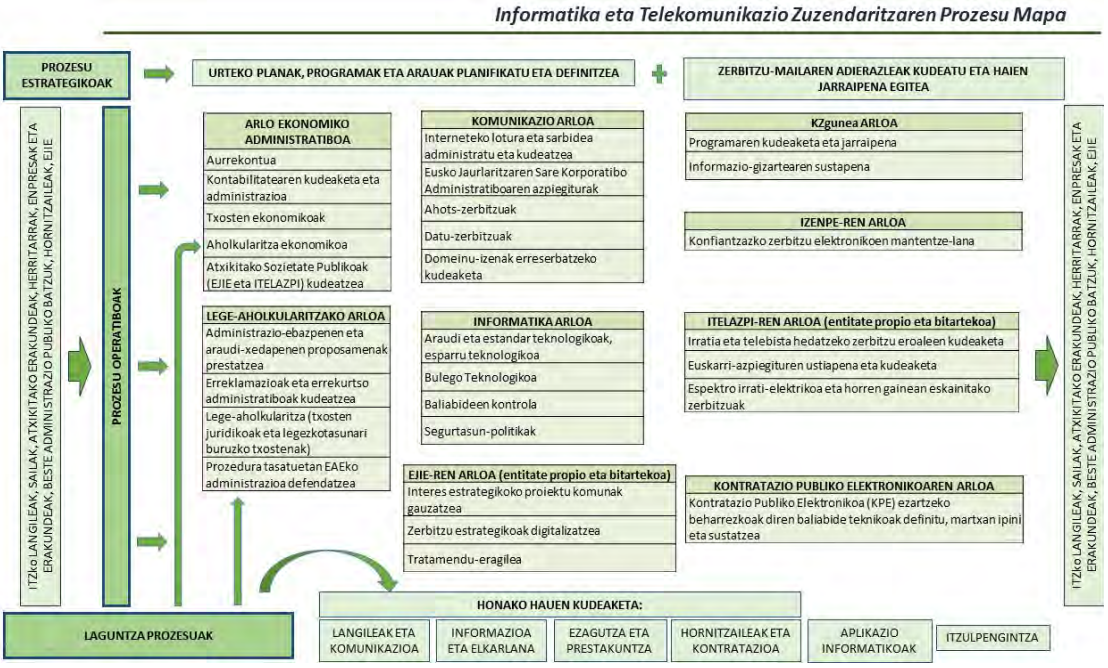
Proiektua, behin onartuta, faseka gauzatuko litzateke.

ZERTARAKO BALIO DU?

Metodologiako saioetan azaldutako gaiak lantzen badira, herritarren gustuko administrazio bilakatu ahal izango gara: gardenagoa, hurbilekoa, malgua, erantzunkidea, parte-hartzailea, berritzailea, ebaluatuak izango diren helburuekin lan egingo duena, eta efizienteagoa, hots, baliabide publikoak hobeto erabiliko dituena.

Horretarako, Ereduak arreta berezia eskaintzen die alderdi hauekin lotutako gaiei:

1. **Estrategia**: helburuen plangintza, Jaurlaritzaren estrategia globalaren bide beretik.
2. **Zerbitzuak**: zerbitzuak kudeatzea, herritarrek eskatzen dutenari erantzuteko.
3. **Pertsonak**: pertsonen kudeaketa, haien konpromisoa sustatzera bideratua.
4. **Berrikuntza**: testuingurua sortzea, berritzeko eta ideia eta proiektu berritzaileak kudeatzeko.
5. **Gizartea**: gobernu ona, etika publikoa eta elkarlana sustatzea eta erantzukizuna hartzea jasangarritasunarekiko, berdin-



[2] **PDCA:** Deming-en zikloa (Edwards Deming), PDCA zirkulu gisa (ingelesez, *Plan-Do-Check-Act*, hau da, Planifikatu-Egin-Egiaztatu-Jardun) edo etengabeko hobekuntzako espiral gisa ezagutzen dena, kalitatearen etengabeko hobekuntzarako estrategia bat da, lau pausoz osatua eta Walter A. Sheshartek asmatutako kontzeptu batean oinarritzen dena.

[iturria: Wikipedia]

tasunarekiko eta euskararen erabileraren normalizazioarekiko.

6. **Emaitzak**: emaitzen jarraipena egitea, ardatz bakoitzari dagokionez.

«Eusko Jaurlaritzak herritarrei eskaintzen dizkien zerbitzuak hobeto kudeatzeko eredu edo programa bat izan nahi du Aurrerabidek»

EGITEN IKASI

Esan dugun bezala, Aurrerabidek ahalik eta praktikoena izan nahi du. Horretarako, prestakuntza/ekintzako prozesu batean oinarritzen da, etengabeko laguntza emanez Kudeaketa Ereduaren oinarrizko elementuak zuzendaritza edo zerbitzu parte-hartzaile bakoitzean ezartzerakoan, eta «*Egiten Ikasi*» proiektuaren bidez egiten du hori.

Prozesu horren xedea da egiteko modu egokiei buruz taldean pentsatzen eta idazten laguntzea, gero gainerako kideekin aplikatu ahal izateko. Eta horrekin, lankidetzan diseinatzea bultzatzen da.

Horregatik, bere garaian, «*Egiten Ikasi*» proiektua diseinatzeko lantalde bat eratu zen, eta bertan, Herritarrak Hartzeko eta Administrazioa Berritzeko eta Hobetzeko Zuzendaritzako (DACIMA), Herri Arduralaritzaren Euskal Erakundeko (HAEE/IVAP) eta Funtzio Publikoko Zuzendaritzako ordezkariek parte hartu zuten. EUSKALIT[3]ek, berriz, prestakuntza/ekintzako *KnowInn* ikastaroak antolatzen eta garatzen daukan esperientzia eskaini zuen.

Geroago, egitura eta edukia kontrastatu zen zerbitzu-zuzendaritzekin, zerbitzu-arduradunekin eta teknikariekin; haien ekarpenak baliagarriak izan ziren hasierako proposamena hobetzeko.

Informatika eta Telekomunikazioetako Zuzendaritzak, gainerako zuzendaritza parte-hartzaileek bezala, ikaskuntza partekatuan oinarritutako prestakuntza batean eta tailer praktiko batzuetan parte hartu du. Horrela, urtebetean 10 saio egin dira (bakoitza 5 ordukoa), zuzendariekin eta zerbitzu bakoideak koordinatuta, sarean lan egiten dute prozesuak antolakuntza-unitateetan (zuzendaritzak, zerbitzuak...) eta Eusko Jaurlaritzako gainerako guneetan kudeatzeko kultura berri hori babesteko eta zabaltzeko. Era berean, beste kide batzuekin lankidetzan aritzen dira beste sail eta organismo batzuetako antolakuntza-unitateetan kudeaketa-ebaluazioak egiteko eta kontrastatzeko.

KOLABORATZAILEEN SAREA

«*Kolaboratzaile*» gisa jarduten dutenak Kudeaketa Eredu honen funtsezko pieza dira, ekimen hau arrakastatsua izateko behar den aldaketa kulturala bultzatzeko eragile aktibo baitira.

Nabarmentzekoa da kolektibo hori Eusko Jaurlaritzako bertako pertsonek osatzen dutela, eta Funtzio Publikoko Sailburuordetzako Aurrerabide Tal-

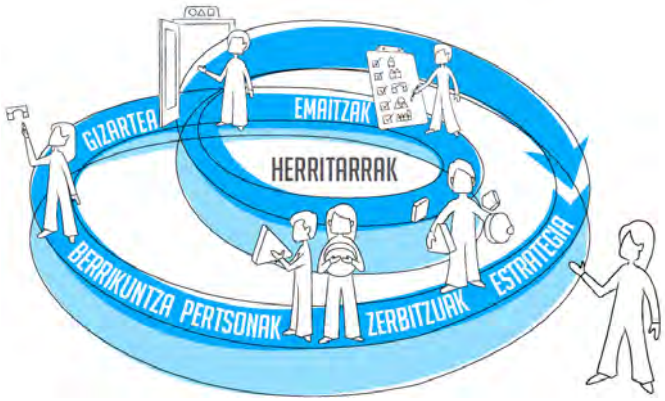
[3] **Euskalit**: Kalitatearen Sustapenerako Euskal Fundazioa da, 1992ko abenduaren 15ean sortua.

Eusko Jaurlaritzak bultzatutako fundazio bat da, helburu duena euskal erakundeetan Kudeaketa Aurreratua sustatzea eta horiek lehiakorragoak izan daitezen laguntzea.

EUSKALIT

http://www.euskalit.net

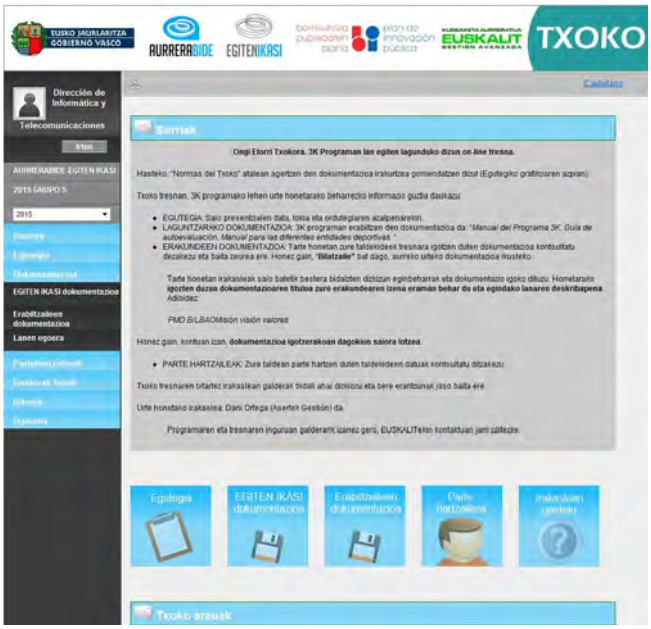
tzeko arduradunekin, zeintzuekin aditu bat egon baita «*entrenatzaile*» modura.



Saio horietan:

- Ereduaren ezaugarriak zeintzuk diren adierazi da.
- Kudeaketa onarekin lotutako tresnen erabilerari buruzko trebakuntza eman da.
- Esperientzia arrakastatsuen berri eman da.
- Estandar batzuk eman dira.
- Tutoretza-laguntza eman zaie saio batetik bestera zuzendaritza bakoitzean oinarrizko dokumentazioa prestatzeko, gerora egin beharreko lanean balia dezaten. Dokumentazio hori, besteak beste, «*entregagarri*» hauek osatzen dute: zerbitzuen katalogoa, prozesuen mapa, prozesu operatiboen fitxak eta bi urterako oinarrizko plangintza.

Halaber, Informatika eta Telekomunikazioetako Zuzendaritzak plataforma informatiko bat erabili du («*Aurrerabideren txokoa*»), edukiak (dokumentuak) kargatzen eta deskargatzen laguntzeko, laguntzen jardun duenak zalantzak argitzeko eta gainerako parte-hartzaileekin harremanetan jartzeko.



FASEAK ETA GARAPENA

Etengabeko prozesu bat denez, metodologiaren barruan zenbait fase eta zeregin sartzen dira; besteak beste, honako hauek:

- ✓ «***Eginez Gara***» **Memoria** lantzea eta eguneratzea. Memoria horretan, egindako lanaren azken dokumentu guztiak bilduko dira.
- ✓ Autoebaluazioa (antolakuntza-unitateko langileek)
- ✓ Ebaluazio-galdetegiak betetzea
- ✓ Lehenespena, sendotu eta hobetu beharreko alderdiak zehazteko
- ✓ Finkatze eta Hobekuntza Plana lantzea

GERORA BEGIRA

Aurrerabidek gerora begira dituen helburuetako bat da bere Kudeaketa Eredua zabaltzea hezkuntzaren eta osasunaren sektoreko administraziora, gainerako administrazio instituzionalera eta sektore publikoko administraziora, baita hala eskatzen duten gainerako administrazio publikoetara ere.

Gaur egun, Aurrerabideko arduradunak eta kolaboratzaile-taldea harremanetan daude beste entitatebatzuekin[4] (Gipuzkoa eta Bizkaiko Foru Aldundiak, Euskal Udalen Elkartea [EUDEL], Gasteizko Udala eta Q-epea), eredua zabaltzen jarraitzeko.

Eusko Jaurlaritzak herritarrei eskaintzen dizkien zerbitzuak hobeto kudeatzeko eredu edo programa bat izan nahi du, azken finean, Aurrerabidek, eta hobekuntzarako beste edozein ereduk bezala, etengabeko prozesu bat eskatzen du, gure barne-prozesuak hobetzen jarraitu ahal izateko. ❑

[4] **Entitateak:**

- Gipuzkoako Foru Aldundia www.gipuzkoa.eus
- Bizkaiko Foru Aldundia www.bizkaia.eus
- EUDEL—Euskadiko Udalen Elkartea www.eudel.eus
- Vitoria-Gasteizko Udala www.vitoria-gasteiz.org

Informazio gehiago nahi izanez gero, jarri harremanetan Aurrerabideren Lantaldearekin (Funtzio Publikoaren Sailburuordetza), helbide elektroniko honen bidez: aurrerabide@euskadi.eus

Edo, bestela, kontsultatu proiektuaren web-gunean argitaratzen den informazioa: http://www.euskadi.eus/eusko-jaurlaritza/berrikuntza-publikoa-administrazioaren-hobekuntza/aurrerabide-kudeaketa-aurreratua/hasiera/

Prestakuntza, Segurtasunaren Eskema Nazionalaren ikuspegitik

Segurtasunaren Eskema Nazionala (SEN) Errege Dekretu bat da (3/2010 ED, urtarrilaren 8koa), administrazio publikoetako langileak prestakuntza egoki bat izatera behartzen dituena, Informazio Sistemek erabiltzen dituzten informazio-teknologien segurtasuna bermatzeko, eta, hartara, teknologia horiek babestuta egoteko.

[5] **ELZ/CAU:** Eusko Jaurlaritzako Informazio Sistemen Erabiltzaileen Laguntzarako Zentroa (440 telefonoa).

[6] **Ransomware:** (*ransom*, ingelesez erreskatea, eta *ware* atzizkia, softwarea dela adierazteko). Software edo programa informatiko bat da (*malware* motakoa); fitxategi edo karpeta zenbait zifratzen ditu, erabili ezinda uzteko. *Malware* horren helburua da dirua lortzea ordainketa elektroniko baten bidez; normalean *bitcoin*-etan ordaindu behar izaten da (diru birtualaren bidez), baina ordaindu arren, ez dago bermatuta fitxategi horiek berreskuratuko ditugunik.

[7] **GureSeK:** Eusko Jaurlaritzaren Informazioaren Segurtasuna Kudeatzeko Sistema (ISKS). ISKSak informazioaren segurtasuna zaintzeko prozesu-multzoak dira; erakundeak izan litzakeen arriskuak oinarri hartuta, informazioaren segurtasuna ezarri, inplementatu, mantendu eta etengabe hobetzeko erabiltzen dira. (Iturria: «*Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad*», AENOR ediciones)

Errege Dekretu horren 15. artikuluak («*Profesionaltasuna*»), bigarren zenbakian, honela dio: «*administrazio publikoetako langileek Administrazioaren sistema eta zerbitzuei aplikatzen zaizkien informazio-teknologien segurtasuna bermatzeko* ***beharrezko prestakuntza espezifikoa*** *jasoko dute*».

KONTZIENTZIAZIOA ETA PRESTAKUNTZA

Garbi dago berebiziko garrantzia duela administrazio publikoetan lan egiten dutenen **kontzientziazioak eta prestakuntzak**, erabiltzen diren sistema, zerbitzu eta datuen segurtasuna bermatzeko, eta, beraz, herritarrekiko eta enpresekiko konfiantza sortzeko, administrazioekin egin beharreko gestioetan bitarteko telematikoen erabilera sustatu dadin.

Aditu guztiak bat datoz: segurtasunaren eremuko babesak (suebakiak, birusen kontrako softwarea, *antispam* iragazkiak, bidegabeko sartzeak atzemateko eta prebenitzeko sistemak...) ez dira nahikoa giza akatsei aurre egiteko. Aurrera aldizkariaren azken alean adierazi zen bezala (59. zk., 2017ko martxoa), «***kontzientziatzea, praktika onak baliatzea*** *eta* ***zentzuz jokatzea*** *dira armarik onenak izaten ditugun erasoetatik babesteko (gaizkile zibernetikoek ingeniaritza sozialeko teknikak erabiltzen dituzte beren erasoetarako)*». Eta aipatutako «arma» horiei **prestakuntza** egoki bat gehitzen badiegu, lortuko dugun babesa ere egokia izango da.

Kasu erreal bat: pertsona baten helbide elektroniko korporatibora mezu bat iritsi da, bidaltzaile ezezagunekoa eta mezua jaso duen pertsonarekin zerikusirik ez duen gai baten ingurukoa; esteka bat (*link*) edo fitxategi erantsiak dauzka mezuak, eta gaizki idatzita dago, edo akats ortografikoekin. Mezuaren gaia honelako zerbait izan daiteke: «*sari bat irabazi duzu...*», «*faktura bat daukazu: sakatu esteka hau...*», «*pakete bat jaso duzu posta bidez...*», etab. Zentzuak **esaten digu ez dela komeni** era horretako mezuak irekitzea eta, gutxiago, hor jartzen dituzten esteketara joatea edo fitxategi erantsiak irekitzea. Mota horretako mezuren bat edo susmagarria den besteren bat jasotzen dugunean, egokiena da gure informatika-zerbitzua edo Erabiltzailearen Laguntza Zentroa (ELZ/CAU[5]) jakinaren gainean jartzea, esku hartu dezan eta arazoa segurtasun-gorabehera gisa bideratua izan dadin. *Ransomware*[6]-erasoak mezu elektronikoen bidez hasten dira zabaltzen erakundeetan (adierazi berri dugun hori bezalako mezuen bidez).

PRESTAKUNTZA-PROGRAMA PROPIOA

GureSeK[7] (*Gure Segurtasun Kudeaketa*, Eusko Jaurlaritzaren informazioaren segurtasuna kudeatzeko prozesua) programa bat defi-

nitzen eta idazten ari da, *Eusko Jaurlaritzaren Informazioaren Segurtasuna Kudeatzeko Sistemaren Prestakuntza Programa* izenekoa. Dokumentu bat da, IVAPeko[8] prestakuntza arautuarekin lotua dagoena, eta ezartzen duena zer ildo jarraitu behar diren Eusko Jaurlaritzako langileen prestakuntza- eta trebakuntza-ekintzak arautzeko, erakundearen segurtasuna kudeatzeko prozesuari dagokionez.

Jarraian, prestakuntza horren ezaugarri nagusiak zeintzuk diren azalduko dugu (**prestakuntza-ekintzak formalki onartuak izan behar dira** Eusko Jaurlaritzaren segurtasunaren antolaketari buruz Gobernu Kontseiluak —2015eko ekainaren 30ean— onartutako Erabakiaren[9] bidez sortutako **batzordeetan**: «*Erabaki-proposamena, zeinaren bidez onartzen den Eusko Jaurlaritzaren Administrazio Elektronikorako antolakuntza-egitura eta segurtasun-rolen esleipena.*»).

GURESEK PRESTAKUNTZAREN IRISMENA ETA HELBURUAK

Programa honetako prestakuntza Eusko Jaurlaritzako sail eta organismo autonomo guztietako langileei dagokie.

Hauek dira prestakuntza-programa honen helburu espezifikoak:

- Ezagutzera ematea Segurtasunaren Eskema Nazionalean jasotako bitarteko elektronikoen erabilerari dagozkion segurtasun-politikekin zerikusia duten alderdi guztiak.
- Eusko Jaurlaritzako erabiltzaileek zer obligazio orokor dituzten ezagutaraztea eta horietaz kontzientziatzea.
- Informazio-sistema batek izan ditzakeen arriskuak identifikatzen ikastea (arduradunek egin dituzte jada zerbitzu elektronikoen balorazioak).
- Segurtasunaren kudeaketari lotutako oinarrizko alderdiak ezagutzea eta segurtasun-gorabeherei erantzuna ematea.
- Gure jardute-eremuari dagozkion segurtasun-rolak ezagutzea.

ESKAINITAKO PRESTAKUNTZA-MODULUAK

Hiru prestakuntza-modulu izango ditugu:

- Segurtasuna (sarrera)
- Segurtasunaren arloko oinarrizko prestakuntza.
- Segurtasunaren arloko prestakuntza aurreratua.

SEGURTASUNAREN SARRERAKO MODULUA

Hauek dira segurtasunaren sarrerako moduluaren helburuak:

- Segurtasunaren arloko esparru arautzailea ezagutzea.
- Informazioaren segurtasunari dagokionez, lanpostuan erabiltzaile gisa errespetatu eta onartu behar diren printzipio orokorrak (arauak) ezagutzea («*Eusko Jaurlaritzako erabiltzaileen obligazio orokorrak*» dokumentuan jasota daude, eta datu pertsonalen babesaren arloan [DBLOED] eta zerbitzu elektronikoen segurtasunaren arloan [SEN eta MSPLATEA] aplikatzekoak diren legezko obligazioen ondoriozkoak dira)

Hauek dira ikastaro honen edukiak:

- Segurtasuna (sarrera). informazioaren segurtasuna, **EOKBT** segurtasun-bermeak

[8] **HAEE/IVAP:** Herri Arduralaritzaren Euskal Erakundea da, Eusko Jaurlaritzako egungo Gobernantza Publiko eta Autogobernu Sailari atxikitako organismo autonomoa, zeinaren sorrera, egitura eta funtzioak uztailaren 27ko 16/1983 Legean ezarrita baitaude. Erakundearen jardute-eremurik handienetako bat da euskal Administrazioko langileen hautaketa eta prestakuntza.

Informazio gehiagorako: www.ivap.euskadi.eus

[9] **Gobernu Kontseiluaren Erabakia, Eusko Jaurlaritzaren segurtasuna antolatzeari buruzkoa:** erakunde gisa informazioaren segurtasunaren eremuan ditugun obligazioak zeintzuk diren, prestatu behar dugun dokumentazioa zein den eta Eusko Jaurlaritzan segurtasuna nola antolatuta dagoen jakin nahi izanez gero, Aurrera aldizkaria kontsulta dezakezue, 56. zk., (2016ko ekainean argitaratua), eta, zehazki, «*Informazioaren Segurtasun Politika (ISP)*» izeneko artikulua.

(Erabilgarritasuna, Osotasuna, Konfidentzialtasuna, Benetakotasuna eta Trazabilitatea), Segurtasunaren Eskema Nazionala, datu pertsonalen babesari buruzko legedia, mehatxuak...

«Programa honetako prestakuntza Eusko Jaurlaritzako langile guztiei dagokie»

- Informazioaren segurtasunaren gaineko politika.
- Informazioaren kanpoko euskarriak: USB gailuak, kanpoko beste gailu batzuk, paperaren erabilera, funtzioanitzeko gailuak.
- Lanpostua: mahaigain garbiaren politika, pasahitzen politika (SARgune[10]), metadatuen garbiketa...

SEGURTASUNEKO OINARRIZKO PRESTAKUNTZARI BURUZKO MODULUA

Langileei dagokienez, hauek dira modulu honen helburuak:

- Informazioaren segurtasunaren arloan aplikatzekoa den esparru arautzaileari buruzko oinarrizko ezagutza batzuk jakitera ematea.
- Langileek segurtasunari buruzko gutxieneko funtzio batzuk bereganatzea, beste ohiko zeregin bat izango balitz bezala.
- GureSeK-en egitura eta funtzionamendua ezagutzea.
- GureseK-ek lanpostuan dituen ondorioez jabetzea.

[10] **SARgune**: Sare Korporatibora sartzeko sistema da. Helburua: segurtasuna eta kalitatea hobetzea, eta, era berean, Sare Korporatiboaren zerbitzuetarako sarbidea erraztea (posta elektronikoa, aplikazioak, sistemak...) Pasahitzen politika sendo bat darama inplizituki sistemak, ekipoetara sartzeko erabiliko dena.

Segurtasunaren sarrerako modulua: segurtasun-dimentsioak (EOKBT)

Segurtasun-dimentsioak, segurtasun-berme ere deituak, hauek dira:

- **Erabilgarritasuna**: erakunde edo prozesu baimenduek sarbidea dute hala behar dutenean.
- **Osotasuna**: informazioa ez da baimenik gabe aldatu.
- **Konfidentzialtasuna**: baimenik ez duten pertsonei, erakundeei eta prozesuei ez zaie informazioa eskuragarri jartzen, ez eta jakinarazten.
- **Benetakotasuna**: entitate batek adierazitako identitatea egiazkoa da edo datuen iturria bermatzen da.
- **Trazabilitatea**: entitate baten jarduerak entitate horri baino ez dakizkioke egotzi.

Aipatutako segurtasun-dimentsioak aztertzen dira zerbitzu bakoitzarentzat, eta dimentsio horietako bakoitzari maila bat esleituko zaio: **TXIKIA**, **ERTAINA** edo **HANDIA**.

- **TXIKIA**: segurtasun-gorabeheraren kaltea **ARINA** da (ohiko obligazioei erantzuteko gaitasun operatiboa pixka bat murriztea, erakundearen aktiboei kalte txikia eragitea, lege edo araudiren bat formalki ez betetzea, norbaiti kalte txikiren bat eragitea...)
- **ERTAINA**: segurtasun-gorabeheraren kaltea **LARRIA** da (ohiko obligazioei erantzuteko gaitasun operatiboa nabarmen murriztea, erakundearen aktiboei kalte nabarmena eragitea, lege edo araudiren bat materialki ez betetzea, norbaiti kalte nabarmen bat eragitea...)
- **HANDIA**: segurtasun-gorabeheraren kaltea **OSO LARRIA** da (OINARRIZKO obligazioei erantzuteko gaitasun operatiboa GALTZEA, erakundearen aktiboei kalte OSO HANDIA EDO KONPONEZINA eragitea, lege edo araudiren baten ez-betetze larria, norbaiti kalte handiren bat eragitea, konponbide zailekoa edo konponezina dena...)

Oinarrizko prestakuntzako modulu honen eta sarrerako lehen moduluaren hartzaileak Eusko Jaurlaritzako langile GUZTIAK dira, zeintzuk behartuta baitaude bi moduluak egitera. Horretarako, IVAPek, urteko prestakuntza-ikastaroen katalogo orokorraren bidez, eta, betiere, erakunde horrek bidezkotzat jotzen duen aldizkakotasunez, *on-line* prestakuntza bat jarriko du eskuragarri Eusko Jaurlaritzako sail eta organismo autonomoei atxikitako langileentzat, Eusko Jaurlaritzako langile guztiek izan dezaten aukera eta obligazioa prestakuntza hori jasotzeko. Oinarrizko prestakuntzako modulu hori eginda badago baina ikastaroaren edukiak nabarmen aldatu badira, berriz egin beharko da ikastaroa.

SEGURTASUNEKO PRESTAKUNTZA AURRERATUARI BURUZKO MODULUA

Hauek dira ikastaro honen edukiak:

- ✓ Sarrera. Segurtasuneko oinarrizko moduluaren edukien laburpena.
- ✓ GureSeK. Eusko Jaurlaritzako segurtasun-prozesua: prozesuaren rolak, funtzioak eta erantzukizunak; prozesuaren jarduerak; prozesuaren ebaluazioa eta jarraipena.
- ✓ GureSeK. Aplikazio praktikoa: segurtasunaren kudeaketa (GureseK mantentze-programa, arriskuak analizatzeko eta kudeatzeko metodologia, kudeaketa dokumentalaren prozedura, segurtasun-gorabeherak kudeatzeko prozedura, auditoretza-prozedura, etengabeko hobekuntzako sistematika...) eta segurtasun teknologikoa (segurtasun-arkitekturaren gutxieneko baldintzak, azpiegiturak eguneratzeko politika, bidegabeko sartzeak atzemateko eta prebenitzeko politikak, jarraipen-plana...).

Prestakuntza-modulu hau aurrez aurrekoa izango da: azalpen teoriko-praktiko bat emango da, ikus-entzunezko euskarri baten bidez.

Prestakuntza-modulu honetara joan behar dira langileak, baldin eta beren lanpostuak harreman zuzena badu administrazio elektronikoaren eremuko informazioaren segurtasunarekin. ❑

[11] **SCORM**: *Sharable Content Object Reference Model*, Internet bidezko ikaskuntzako (*elearning*) produktuentzako zehaztapen teknikoen multzo bat da. Edukien egitura eta portaera —eta eduki horiek ostatatu eta exekutatuko dituzten plataformena— definitzeko arauak zehazten ditu.

Prestakuntza, CCN-CERT bidez

Zentro Kriptologiko Nazionalaren (CCN) webgunean, bi ikastaro daude edonorentzat es-kuragarri, **alderdi publikoan**:

- **Segurtasunaren Eskema Nazionala:** bederatzi unitate edo modulu dira, erreferentziako dokumentazioz osatuak:
  1. Administrazio Elektronikoa eta Informazioaren Segurtasuna.
  2. Segurtasun Eskema Nazionala. Sarrera.
  3. Informazioaren Segurtasunaren gutxieneko baldintzak.
  4. Segurtasunaren Azpiegitura eta Tresnak.
  5. Segurtasun-auditoretzak eta gorabeherei erantzutea.
  6. Erreferentziako organoak eta organismoak.
  7. Sistemen eta Segurtasun Neurrien kategorizazioa.
  8. Ariketa praktikoa.
  9. ENSren CCN-STIC gidak eta informazio osagarria.
- **Informazio Sistemen Arriskuen Analisia eta Kudeaketa**: helburua da informazio-sistemetan dauden arriskuen kudeaketa eta analisiari lotutako alderdi teorikoak aztertzea (Sarrera, Arriskuen kudeaketa-prozesua, Arriskuen analisi baten elementuak, Aktiboak, Mehatxuak, Inpaktua eta arriskua, Operazioen jarraipena eta Ondorioak).

Alderdi pribatuan ere ikastaro batzuk ezarri dituzte, segurtasunarekin zerikusia dutenak.

CCN-CERT ikastaroak SCORM[11] zehaztapen teknikoen multzoaren barruan garatu dira.

https://www.ccn-cert.cni.es/

ALBOAN:

Eusko Jaurlaritzako estandar teknologikoak berrikustea eta eguneratzea

«Estandarrak definitzea ekimen estrategiko eta beharrezko bat da Eusko Jaurlaritzarentzat»

Eusko Jaurlaritzako Informatika eta Telekomunikazioetako Zuzendaritzaren eskumenetako bat da «*estandarren betetzeaz, kontrolaz eta jarraipenaz*» arduratzen den autoritate zentral moduan jardutea, otsailaren 18ko 35/1997 Dekretuan adierazten den bezala (35/1997 Dekretua, informazio eta telekomunikazio sistemen egitekoak eta kudeaketa-modalitateen planifikazioa, eraketa eta banaketa arautzen dituena).

Estandarrak definitzea **ekimen estrategiko eta beharrezkoa** da Eusko Jaurlaritzarentzat, zuzenean laguntzen baitu gure Administrazioaren helburu estrategikoak lortzen. Besteak beste, honako hauek:

- ✓ Herritarrei eta enpresei eskainitako zerbitzuen kalitatea areagotzea eta kalitate gorena bermatzea.
- ✓ Administrazioaren barne-prozesuetan, efikazia eta efizientzia handienerantz joatea.
- ✓ Instituzioen eta organismo publikoen arteko lankidetza-ingurune eta -sare bat zabaltzen laguntzea.

Eusko Jaurlaritzaren Estandar Teknologikoen Dokumentuan, euskal Administrazioak teknologia berrien eremuan zabaldutako zerbitzuei euskarri ematen dieten zehaztapen eta baldintza teknikoak jasotzen dira, betiere, Eusko Jaurlaritzak bere planen bidez ezarritako helburu estrategikoekin bat etorriz. Estandar horiek Eusko Jaurlaritzaren Informatika Elkarteak kudeatzen ditu (**EJIE**, S.A.).

Horretarako, Estandar Teknologikoen dokumentuan estandar edo produktu batzuk definitzen dira, korporatibotzat edo nagusitzat jotzen direnak, eta Eusko Jaurlaritzako sail/organismo autonomoen Informazio Sistemen oinarri izango direnak.

Euskal administrazio elektronikoaren azpiegituraren euskarri diren ingurune teknologikoen etengabeko bilakaera eta administrazioa osatzen duten sail eta organismo autonomoetan sortzen diren ekimenak direla-eta, beharrezkotzat jo da Eusko Jaurlaritzako estandar teknologikoen edukia berrikusteko eta eguneratzeko beharrezko zereginei heltzea, betiere, planteatzen diren behar guztiei erantzun egoki bat emateko osotasunaren, kalitatearen eta segurtasunaren ikuspegitik, eta, halaber, datozen urteetako esparru teknologikoa ezarri ahal izateko.

Horregatik, eta 35/1997 Dekretuan ezarritakoa betetze aldera, Informatika eta Telekomunikazioetako Zuzendaritzak ekimen bat bultzatu du, Eusko Jaurlaritzaren es-

tandar teknologikoak berrikusteko eta eguneratzeko.

DOKUMENTUTIK WEBERA

Orain arte, estandar teknologikoei buruzko informazio guztia «*Estandar teknologikoen dokumentua*» delakoan sartuta zegoen. Dokumentu hori honela egituratuta zegoen: dokumentu nagusi bat eta eranskin batzuk, haren osagarri. Eta Informatika eta Telekomunikazioetako Zuzendaritzaren webgunean zegoen guztia eskuragarri. Hauek ziren eranskin horiek:

1. Interkonexio-eredua (JASO eta SARA)
2. PLATEA estandar teknologikoak
3. Estandarren katalogoa, eAdministrazioaren eremuan
4. Sinadura eta Ziurtagiri Politika
5. Aldaketaren kudeaketaren metodologia
6. Garapenerako gidalerroak
7. Dokumentuen formatu onartuak
8. Produktu/teknologia definituen bertsio eguneratuak
9. Estandarrak, FLOSSaren eremuan

Aipatutako ekimen horren bidez, gaur egun estandar teknologiko moduan bildutako informazioa berrikusteko eta eguneratzeko eta web formatu batera egokitzeko beharrezkoak diren lanak egin dira.

Horretarako, Informatika eta Telekomunikazioetako Zuzendaritza, azken asteetan, dokumentu nagusiaren eta horren eranskinen edukiak berrikusteaz eta eguneratzeaz arduratu da, EJIEn gai bakoitzaren inguruan dauden arduradunekin lankidetzan.

Edizio berri honetan, estandar teknologikoek dakarten berritasun bat da alde batera utziko dugula «*DOKUMENTUA*»ren ideia, eta eduki guztiak «***FITXA***» formatu batera pasako ditugula (webgunean eskuragarri egongo dira), eta, hartara, «*web responsive*» diseinu bat izango dugu, edozein gailutatik sartu eta kontsultatzeko aukera emango duena (ordenagailua, *tableta*, *smartphone*-a,...). Gainera, fitxa bakoitzean sartuko diren «*link*» edo estekei esker, ikusi ahal izango dugu estandar baten eta bestearen arteko erlazioa zein den, nazioarteko arauekiko baliokidetasuna (ISO...), informazioa zein egunetan eguneratu den, etab.

LOGOTIPOA

Fitxen edukia edo informazioa eguneratu ondoren, estandar teknologikoak eta horien inguruko dokumentazio guztia identifikatzeko logotipo bat diseinatzeari ekin zitzaion.

Ezaugarri hauek dituen logotipoa hautatu zen azkenean:

- ✓ «**E**» letrak «*Euskadi*» eta «*Estandarrak*» adieraziko lituzke.
- ✓ Eduki desberdinen arteko integrazioa eta konexioa sinbolizatzen du (estandarrak eta produktuak).
- ✓ Edukien segurtasuna, sendotasuna eta batasuna adierazten du.
- ✓ Kolore iluna (gris iluna) normalean teknologiarekin lotzen da.
- ✓ Kolore urdinak, bestalde, segurtasuna eta fidagarritasuna adierazten du, eta, gainera, korporazioaren egungo webguneak daukan kolore urdinaren antzekoa da.

Eguneratzea amaitu bada ere, horrek ez du esan nahi argitaratzen den informazioa finkoa edo estatikoa denik; izan ere, eman zaion egiturari esker (fitxa bidezkoa) edozein datu eguneratu ahal izango da modu azkar eta malgu batean. ❑

«Edizio honetako berritasunetako bat da DOKUMENTU formatutik FITXA formatura pasa garela»

[**Informazio gehiago**]:

Eusko Jaurlaritzaren estandar teknologikoen webgunea

http://www.euskadi.eus/informatika

(atala: «*Estandar teknologikoak*»)

60
2017ko ekaina

BERRI LABURRAK!!

CONAN mobile

Zibersegurtasunaren Institutu Nazionaleko (Incibe) Internautaren Segurtasun Bulegoaren (erdaraz, OSI) helburuetako bat da pertsonek eremu digitalaren inguruan duten konfiantza areagotzea, zibersegurtasunaren prestakuntzaren bidez. Horregatik, publiko orokorrarentzat eskuragarri jarri du doako tresna bat, Android sistema operatiboa (2.2. bertsioa edo handiagoa) instalatuta duten gailu mugikorrak analizatzeko eta babesteko (*smartphone*-a, *tableta*...).

Tresna edo aplikazio hori (Aurrera aldizkariaren 49. alean eman genizuen lehen bertsioaren berri) *GooglePlay* dendatik deskarga daiteke, eta aukera ematen dizu zure Android gailuaren segurtasun-maila ezagutzeko, gailuaren analisi baten bidez (Interneterako sarbidea izan behar da).

Analisiaren emaitzak aditzera ematen du zein den aztertutako ekipoaren segurtasun-egoera orokorra: **ARRISKUAN**, **ARRETA ESKATZEN DU**, **ZUZENA** eta **BURUTU GABE**; eta bost atal ditu:

1. Konfigurazioa (arazoak dituen edo arreta eskatzen duen, sistema operatiboaren analisiaren emaitzen arabera).
2. Aplikazioak (instalatutako aplikazioen arriskugarritasunari buruzko analisia).
3. Baimenak (handiak, ertainak eta txikiak; instalatutako aplikazioei eman zaizkien baimenei lotuta).
4. Zerbitzu proaktiboa (instalatutako aplikazioen gertaera eta konexioei buruzko alerta: WiFi konexio ez-seguruak; deiak eta mezuak, tarifikazio bereziko zenbakietara...).
5. Internautaren Segurtasun Bulegoaren (OSI) aholkuak (terminal mugikorraren segurtasuna hobetzeko, Inciberen web-orrira konektatzen da zuzenean).

Webgunea: https://www.osi.es/es/conan-mobile

Generoa eta Zibersegurtasuna

Oihartzun handia izan du herrialde desberdinetako konpainiek eta instituzioek «*Wanna Cry*» *malware*aren eskutik jasandako eraso masiboak, eta jende asko ohartu da zeinen garrantzitsua den zibersegurtasuna.

Asko dira segurtasun informatikoarekin lotuta dauden alderdiak, kontuan hartu behar direnak mota horretako mehatxuen aurrean; adibidez, erakunde bateko erabiltzaileekin erasoak ekiditeko egin behar den kontzientziazio-lana, edo kontuan hartzea galera ekonomiko handia eragin dezakeela mota horretako birus edo *malware* batek.

Baina bada beste ikuspegi bat ere, kontuan hartzea komeni dena: Zibersegurtasunaren eta genero ikuspegiaren artean dagoen lotura.

Ildo horretatik, **Incibe**k (Zibersegurtasunaren Institutu Nazionala) «*Generoaren eta Zibersegurtasunaren Nazioarteko I. Foroa*» antolatu berri du, Leonen (ekainaren 5ean eta 6an egin da). Bertan, segurtasun informatikoaren eta generoaren hainbat alderdi aztertu dira; besteak beste, honako hauek: genero-aniztasunak teknologiaren eta zibersegurtasunaren eremuan duen garrantzia; genero-indarkeriaren aurkako ekintzak, eremu digitalean; edo sareko genero-delituak.

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Inciberen webgunean kontsulta daitezke parte-hartzaileen zerrenda eta hitzaldiak.

Web-orria: https://www.incibe.es