EUSKO JAURLARITZA GOBIERNO VASCO

AURRERA!

68. zk.

2019ko ekaina

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

AURKIBIDEA

Denbora handia daramagu Administrazio Elektronikoari buruzko gaia lantzen, eta Administrazioari berari eta herritarrei ekar diezazkiekeen onura handiak ere aipatu ditugu. Baina, hainbeste lan egin eta gero, benetan dakigu nolako egoeran gauden? Lehen artikuluari *«Administrazio Elektronikoa aurrera doa Euskadin»* deitu diogu, eta bertan azaldu dugu lan handi horren emaitza zein den. Ernst & Young aholkularitza-enpresak egin duen konparazio-azterlaneko datuetan oinarrituta dago.

Bigarrenean, *«Segurtasunaren Eskema Nazionalaren esparruko arriskuen analisia»* landu dugu. Gai oso erakargarria iruditu ez arren, funtsezkoa da Administrazio Elektronikoak zerbitzu ona eman dezan. Zehatz-mehatz, gure inguruneko arriskubideak eta arriskuak aztertzean datza, baina, batez ere, arrisku horiek zuzen kudeatzean, Administrazioak herritarrei informazio-zerbitzuen bidez zerbitzu egokia eman diezaien.

Alboan izeneko atalean zenbait artikulu (edo «informazio-pilulak») bildu ditugu, Windows10 eta Office365 sistemei buruz, gure lantokietan pixkanaka instalatzen ari dira eta. Plataforma horretan nobedade ugari daude; hortaz, egoki iritzi diogu haien funtzionalitate batzuk eta hemendik aurrera gure lan egiteko moduan egin beharko ditugun aldaketa batzuk azaltzeari. Ale honetan, besteak beste, «hodeia», «fitxategiak partekatzea»ren abantailak eta «dokumentuen bertsio-antolaketa» jorratu ditugu, Eusko Jaurlaritzako langile guztientzat baliagarria izango delakoan.

Azken atalean, labur bada ere, *«Ziberespazioko desinformazio»*ak herrialdeei arrisku handia ekar diezaiekeela azaldu dugu; eta, horri lotuta, Kriptologia Zentro Nazionalak berriki argitaratu duen txostena ere aztertu dugu.

Amaitzeko, nabarmendu nahi izan dugu Deustuko Unibertsitateak Extremadurako Unibertsitateko Alicia Monje Micharet doktoreari Ada Byron 2019 saria eman ziola, duela aste batzuk. Micharet doktoreak robotak ikertzen ditu.

Administrazio Elektronikoa aurrera doa Euskadin

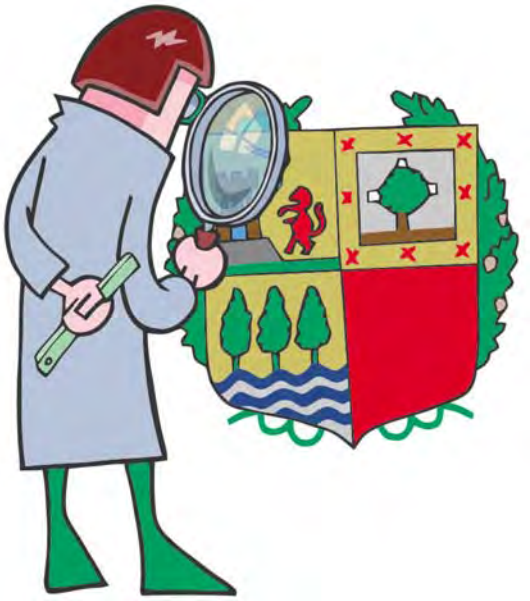
Administrazio publikoek urte asko eman dute «Administrazio elektronikoa» edo «eAdministrazioa» lantzen. Duela gutxi azterlan bat argitaratu da, eta haren bidez jakin dezakegu administrazioen gaur egungo egoera zein den.

Bi arau garrantzitsu onartu ziren 2015eko urrian, eta administrazio publikoen funtzionamenduan eragin handia izan dute, batez ere, herritarrei zerbitzua emateko moduan. Jakina denez, bata Administrazio Publikoen Administrazio Prozedura Erkidearen **39/2015 Legea** da; eta bestea, Sektore Publikoaren Araubide Juridikoaren **40/2015 Legea**[1].

Bi lege horien bidez sartu diren aldaketek bultzada handia eman diote administrazioaren digitalizazioari, eta, horrek, funtsean, onura handia ekartzen die herritarrei eta enpresei, baita Administrazioari berari ere.

TXOSTENA

Ernst & Young (EY[2]) enpresa espezializatua da aholkularitza- eta auditoria-proiektuetan. Guztira, 90 administrazio publikotan aztertu du bi arau horien betetze-maila. Txostena egiteko erreferentziatzat hartu dute pertsonen pertzepzioa, lineako izapide bat administrazioarekin egin behar dutenean.



Lan horren emaitzak *«La Administración Digital en España. Desde la perspectiva del ciudadano y de la empresa»* [Espainiako Estatuko Administrazio Digitala, herritarren eta enpresen ikuspegitik aztertua] txostenean bildu dituzte. Txostena iragan den martxoan argitaratu zuten.

Ernst & Young enpresaren txostenaren azala. Izenburua: *«La Administración Digital en España. Desde la perspectiva del ciudadano y de la empresa» [Espainiako Estatuko Administrazio Digitala, herritarren eta enpresen ikuspegitik aztertua]*

Txostenak 48 orri ditu, eta Espainiako administrazio publikoen **heldutasun digitalaren egoera** aztertu du. Azterlan hori egiteko, 39/2015 Legean eta 40/2015 Legean jasotako oinarrizko betekizun guztiak aztertu dituzte.

[1] **Araudia:**

Administrazio Publikoen Administrazio Prozedura Erkidearen **39/2015 Legea** (2015eko urriaren 2ko BOEn argitaratua, 236. zenbakikoan).
https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565

Sektore Publikoaren Araubide Juridikoaren **40/2015 Legea** (2015eko urriaren 2ko BOEn argitaratua, 236. zenbakikoan).
https://www.boe.es/buscar/act.php?id=BOE-A-2015-10566

[2] **Ernst & Young:** enpresa bat da, eta XIX. mendean sortu zuten Arthur Young-ek eta Alwin C. Ernst-ek.

Enpresaren izena sortu zen Ernst & Whinney eta Arthur Young 1989an era globalean batu zirenean.

Enpresaren web-orria:
https://www.ey.com/es

Eta, xede horretarako, EY aholkularitza-enpresak autonomia-erkidego guztiak (17), aldundiak eta kabildoak (52) eta Espainiako udal nagusiak (21) aztertu ditu.

«Txostenak 48 orri ditu, eta Espainiako administrazio publikoen heldutasun digitalaren egoera aztertzeko egin da»

Ikus ditzagun txostenaren ondorio nagusiak...

DATUAK

Txostena egiteko, 39/2015 eta 40/2015 legeetako 132 betekizun zehaztu dira, eta gaien arabera taldekatu.

Adierazle aukeratuen betetze-maila ezagutze aldera, hainbat informazio-iturri eta komunikazio-kanal erabili dira. Kanal horiek administrazio publikoek zabaldu dituzte, erabiltzaileek izapideak egin ditzaten (enpresak barne):

1. Web ataria
2. Egoitza elektronikoa
3. Identitate digitala eta sinadura elektronikoa
4. Erregistro elektronikoa eta ordezkaritza
5. Herritarrei eta enpresei laguntzea
6. Herritarrei komunikazioak eta jakinarazpenak egitea
7. Espedientea, dokumentua eta fitxategi elektronikoa

Hala bada, Ernst & Young txosteneko datuen arabera, **Euskadi** autonomia-erkidegorik aurreratuena da funtzionamendu digitalaren arloan: betekizun horien % 94,7 betetzen du; ondoren, Galizia dago (% 94,2); Katalunia (% 93,5); Asturias (% 90,2) eta Madril (% 89,5).

Dena den, azterlanaren emaitzak irakurrita, egiaztatu egin da administrazio publiko batek ere ez dituela betetzen 39/2015 eta 40/2015 legeetan ezarritako betekizun guztiak. Horren harira, aipatzekoa da 2018an moratoria bat onartu zela, eta, horren ondorioz, betekizun batzuk 2020an indarrean jarriko direla. Honako hauek dira: ahalordetzeen erregistro elektronikoa, erregistro elektronikoa, enplegatu publiko baimenduen erregistroa, administrazioaren sarbide-puntu nagusi elektronikoa eta fitxategi elektroniko bakarra.

Bestalde, txostenean adierazitakoaren arabera, honako gai hauek dira administrazio publikoek gehien landu behar dituztenak: herritarrei komunikazioak eta jakinarazpenak egitea, erregistro elektronikoa eta ordezkaritza.

EY enpresak gaineratu du Administrazio Digitalak nabarmen aldatzen duela edozein administrazio publikoren funtzionamendua eta, hartara, erronka handia dela administrazio askotarako.

Gobernantza eta Berrikuntza Publikoko 2020 Plan Estrategikoa

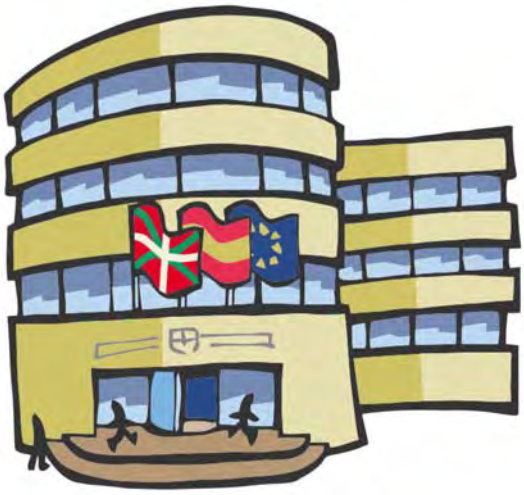
Hori dela eta, EY enpresak administrazioei gomendatzen die eraldaketa digitala urte batzuetako epean gauzatzeko plan bat aurrez egitea, Administrazio Digitala bermeekin ezartzeko eta zerbitzuak hobetzeko. Ildo horretatik, Eusko Jaurlaritzak PEGIP2020[3] («*Gobernantza eta Berrikuntza Publikoko Plan Estrategikoa*») egin du. Besteak beste, honako helburu estrategiko hauek ditu: administrazio elektronikoa gure eremuan zabaltzea, zerbitzu elektronikoen eskaintza

[3] **PEGIP2020:** *«Gobernantza eta Berrikuntza Publikoko Plan Estrategikoa»* adierazteko siglak dira, gaztelaniazko izenaren arabera. Honako webgune honetan informazio gehiago eskuragarri duzue:

www.euskadi.eus/blog/pegip2020/

PLATEA da Eusko Jaurlaritzako Administrazio Elektronikoaren pieza nagusi bat. Hitz horren bidez, *«Eusko Jaurlaritzaren e-Administrazioko Plataforma Teknologikoa»* adierazten dugu. Zenbait moduluz osatuta dago, eta sailek eta erakunde autonomoek erabiltzen dituzte aplikazioak garatzeko, elementu erkidegoen garapenaz eta mantentze-lanaz arduratu beharrik gabe.

osatzea eta herritarrek zerbitzuak erabil ditzaten sustatzea.



EUSKADI

Euskadiri buruz, zehazki, honako **indargune** hauek azpimarratu ditu EY aholkularitza-enpresak:

- ✓ Web-atari bat erabilgarri edukitzea, eta atal batean herritarren eskaerak, proposamenak, Gobernuaren erantzunak eta Legebiltzarreko galderak jasotzea.
- ✓ Liderra izatea egoitza elektronikoari[4] buruzko betekizunak betetzen: besteak beste, herritarrei zerbitzu eraginkorra eta bizkorra, nabigazioa eta zerbitzu-zorro handia eskaintzen dizkielako.
- ✓ Herritarrei komunikazioak eta jakinarazpenak egiteko atalean, herritarrei jakinarazpenak egiteko baliabide elektronikoak erabiltzea, baldin eta herritarrek jakinarazpen-modu hori hautatu badute. Horrez gain, beste aurrerapauso bat ere egin dute, alegia, «*Herritarren karpeta*»[5] edo jakinarazpenak jasotzeko postontzia. Jardunbide horretan Euskadi eta Galizia erreferenteak dira.
- ✓ Estatuko jardunbide egokienetako bat izatea, herritarrei eta enpresei baliabide elektronikoen bitartez arreta emateko.
- ✓ Erregistro elektronikoaren eta ordezkaritzaren arloan, Euskal Autonomia Erkidegoak, Galiziarekin batera, puntuaziorik onena lortu du, nahiz eta betetze-maila % 83 baino handiagoa ez izan. (EY enpresak adierazi du autonomia-erkidego guztiek atal horretan dutela hobekuntza-tarterik handiena).

BESTE DATU BATZUK

Foru-aldundiek (edo baliokideek) eta **udalek** ematen dituzten zerbitzuei erreparatzen badiegu, honako hauek dira datu esanguratsuenak:

- ➢ Betetze-mailaren batezbestekoa % 64 ingurukoa da aldundi guztietan. Datuen arabera, aldundi batek ere ez ditu betetzen aipatutako lege horietako betekizun guztiak. Gipuzkoako Foru Aldundia da oinarrizko betetze-eredua gehien betetzen duena, zehazki, % 96,5; ondoren, Sevillakoa dator (ezarritako indizearen % 84,7).
- ➢ Azterlanaren datuetan oinarrituta, foru-aldundiek honako arlo hauetan izaten dituzte zailtasun handienak: ordezkaritzan, erregistro elektronikoan eta herritarrei komunikazioak eta jakinarazpenak egitean.
- ➢ Bestalde, Bizkaiko eta Arabako foru-aldundiek beste arlo batzuetan ematen dituzten zerbitzuak ere nabarmentzen dira.

[4] **Egoitza elektronikoa:** Interneteko gune bat da, alegia, web bat. Erabiltzaileak han sar daitezke, eta izapideak era seguruan egin ditzakete. Web horrek bermatzen du bertako informazio eta zerbitzuak osoak, errealak eta eguneratuak izatea.

Hauxe da Euskal Autonomia Erkidegoko Administrazioaren egoitza elektronikoa:

https://www.euskadi.eus

[5] **Herritarren karpeta:** lineako karpeta bat da. Erabiltzaileak administrazioarekin harremanetan jar daitezke, bulegoetara fisikoki joan beharrik gabe. «*Herritarren karpeta*»k administrazio digitaleko zerbitzuak eskaintzen dizkie herritarrei: informazio publikoa eskuratzea, formularioak deskargatzea, datu pertsonalak kontsultatzea eta abar. Gainera, aukera dago karpetaren bidez harreman telematiko seguruak ezartzeko eta bideratzeko; bestela, interesdunek fisikoki soilik egin beharko lituzkete izapideak.

- Aztertu diren udalen artean, betetze-mailaren batezbestekoa % 64,5 da. Gainera, egiaztatu egin da udal batek ere ez dituela betetzen aipatutako lege horietako betekizun guztiak.

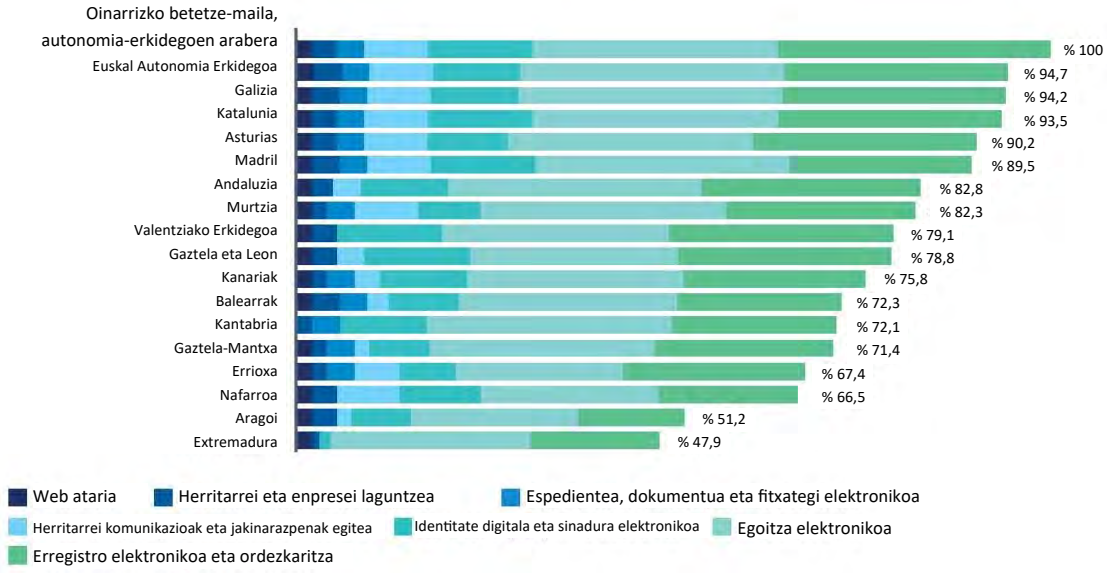
«Ernst & Young enpresak bildutako datuen arabera, Euskadi autonomia-erkidegorik aurreratuena da funtzionamendu digitalaren arloan»

- Udal aztertuen % 33k baino ez ditu betetzen legeak ezartzen dituen sinadura elektronikoaren arloko betekizunak. Honako hauek nabarmentzen dira, betetzen dituztenen artean: Malagakoa, Bilbokoa eta Palma Mallorcakoa, besteak beste.
- Vitoria-Gasteizko, Malagako eta Valentziako udalek identifikazioaren eta ordezkaritzaren arloko behar bezalako laguntza ematen diete administrazioarekin baliabide elektronikoen bitartez komunikatzera behartuta dauden pertsonei.

ONDORIOAK

Ernst & Young enpresak egin duen txostena aztertuta, txostenaren arabera, EAE lehen postuan dago Estatuan, Administrazio Digitalaren arloan, zehazki, egindako lan handiarengatik. Hala eta guztiz ere, oraindik ere bidea dago egiteko; hortaz, Eusko Jaurlaritzan inbertsioak eta antolaketak egiten jarraituko dugu, administrazio elektronikoaren arloko lege-betekizunak ahalik eta lasterren betetzeko eta, ondorioz, gure zerbitzuak erabiltzen dituzten pertsonen premiei erantzuteko. ❑

Autonomia-erkidegoen heldutasun-indizearen analisia



TXOSTENA

Ernst & Young enpresaren *«La Administración Digital en España. Desde la perspectiva del ciudadano y de la empresa»* izeneko txostena eskuragarri dago helbide honetan:

https://www.ey.com/Publication/vwLUAssets/ey-la-administracion-digital-en-espana/$FILE/ey-la-administracion-digital-en-espana.pdf

Ernst & Young txostenaren azalaren argazkia

Segurtasunaren Eskema Nazionalaren esparruko arriskuen analisia

Metodologia bat da, erasoek Administrazioaren informazioan eragin ditzaketen arriskuak prebenitzeko eta haien aurka borrokatzeko. Ikus dezagun Eusko Jaurlaritzak nola antolatzen duen.

Eusko Jaurlaritzaren «Informazioaren Segurtasuna» deritzon prozesua Informatika eta Telekomunikazio Zuzendaritzak zuzentzen du, **Segurtasunaren Eskema Nazionalaren**[6] esparruan. Prozesu horretan, derrigorrez egin beharreko honako zeregin hau aldizka egiten du: **arriskuen analisia**.

Segurtasunaren Eskema Nazionala urtarrilaren 8ko 3/2010 Errege Dekretuak arautzen du, Herritarrek Zerbitzu Publikoetan Sarbide Elektronikoa izateari buruzko ekainaren 22ko 11/2007 Legearen 42. artikuluak ezartzen du, eta 951/2015 Errege Dekretuak aldatu du. Hauxe ezartzen da manu horietan:

> *«Segurtasunaren Eskema Nazionalaren bidez ziurtatu nahi da informazio-sistemek zerbitzuak beren espezifikazioen arabera ematea, bai eta informazioa zaintzea ere. Gainera, ziurtatu behar da kontrolik gabeko etenik edo aldaketarik ez gertatzea eta baimenik gabeko pertsonek informazio hori ez eskuratzea. Zerbitzuak bilakatu ahala, informazio-zerbitzuak ere hobetuz joango dira, zerbitzuen betekizunen oinarri diren betekizunak eta azpiegiturak finkatzen diren heinean»*

Laburbilduz, Segurtasunaren Eskema Nazionalak pertsonen konfiantza areagotu nahi du administrazio publikoekin ekintza elektronikoak egin behar dituztenean.

HELBURUA

Hauxe da Segurtasunaren Eskema Nazionalaren esparruko arriskuen analisiaren helburua:

- ✓ Eusko Jaurlaritzan zer informazio eta zer sistema erabiltzen diren jakitea
- ✓ Benetako arduraduna nor den jakitea
- ✓ Erabilgarri egongo ez balira, zer inpaktu eragingo litzatekeen jakitea
- ✓ Zer mehatxu dauden jakitea
- ✓ Zer arrisku dagoen halakorik gertatzeko
- ✓ Zer estaldura-neurri dagoen jakitea

Eusko Jaurlaritzak arriskuen analisi korporatiboa egitea erabaki du. Hona hemen helburuak:

- ✓ Erakundea arrisku nagusiez jabetzea lortzea
- ✓ Erakundearen zaurgarritasun-iturri nagusiak zehaztea
- ✓ Jarduteko lehentasunak metodologia globalaren arabera zehaztea
- ✓ Arriskuak minimizatzea lortzen duten ekintzak gauzatzea, erakundearen segurtasuna areagotzeko
- ✓ Erakundearen irudia babestea.

Hori guztia gauzatzeko, beharrezkoa da zerbitzu elektroniko aztertuen erantzukizuna duten sailetako eta erakunde autonomoetako arduradunak ere elkarlanean aritzea. Elkarlan hori **inkesta baten bidez** gauzatzen da. Inkesta bidaltzen zaie, eta beren erantzukizunaren mendeko zerbitzuetan bost segurtasun-dimentsioren inpaktua baloratu behar dute (dimentsiook aurrerago azaldu ditugu).

«Inkesta» **GlobalSuite**[7] izeneko tresna baten bidez egiten da. Ondoren, inkesta betetzeko urratsak azalduko ditugu.

[6] **SEN:** Segurtasunaren Eskema Nazionalaren siglak dira, eta eskema hori Administrazio Elektronikoaren esparruko Segurtasunaren Eskema Nazionala arautzen duen urtarrilaren 8ko 3/2010 Errege Dekretuak arautzen du.

(2010eko urtarrilaren 29ko BOEn argitaratu da, 25. zenbakian)

https://www.boe.es/buscar/doc.php?id=BOE-A-2010-1330

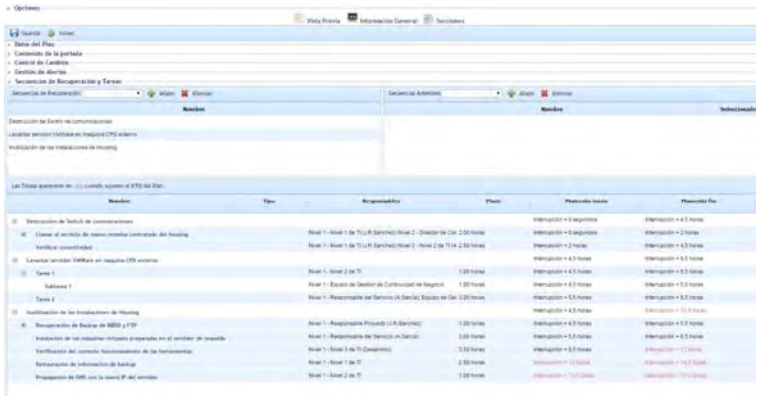
SENen xedea baliabide elektronikoak Administrazio Elektronikoan konfiantzaz erabiltzeko behar diren baldintzak sortzea da; horretarako, oinarrizko printzipioak eta gutxieneko eskakizunak ezartzen ditu segurtasunaren arloan.

SENen ezarritakoa betetze aldera, Euskal Autonomia Erkidegoko Gobernu Kontseiluak, 2015eko ekainaren 30ean egindako bileran, Eusko Jaurlaritzako Administrazio Elektronikorako egituraketa eta segurtasun-rolen esleipena onartzea erabaki zuen.

Eusko Jaurlaritzaren zerbitzu elektronikoen arduradunek mezu elektroniko bat jasotzen dute (Alertas GlobalSUITE bidez), eta haren bidez jakinarazten zaie hainbat balorazio egin behar dituztela.

Arduradunak bere zerbitzu elektroniko esleituen zerrenda ikusten du, inkesta eskuratzen duenean. Zerbitzu bakoitzaren kritikotasuna baloratu behar da, Segurtasunaren Eskema Nazionalak ezarri dituen bost segurtasun-dimentsioen ikuspegitik. Hona hemen dimentsiook:

- **Eskuragarritasuna** [E]: zer inpaktu eragingo litzatekeen, zerbitzua erabilgarri egongo ez balitz, edo zerbitzuan sartzea ezinezkoa izango balitz. Aipatzekoa da zerbitzu guztiak ez daudela egunero erabilgarri 24 orduz. Haietako batzuk bulego-orduetan eta astelehenetik ostiralera bitartean baino ez daude erabilgarriak.

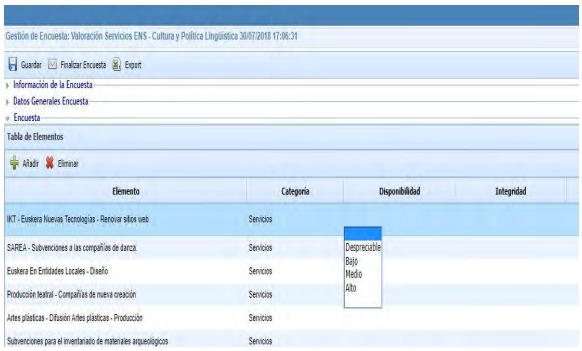


- **Osotasuna** [O]: kontuan hartzen da zer inpaktu eragingo litzatekeen, baldin eta, erabiltzaile baten akats batengatik, informazioaren aurka nahita egindako ekintza batengatik, edo baimenik gabeko pertsona batek egindako aldaketa batengatik, zerbitzuari lotutako informazio edo daturen bat aldatuko balitz eta, ondorioz, zerbitzuko informazioa zuzena izango ez balitz.
- **Konfidentzialtasuna** [K]: dimentsio horrek erakutsi behar du zer inpaktu eragingo litzatekeen, baimenik gabeko erabiltzaile batek zerbitzu zehatz bateko informazioa eskuratuko balu, edo informazio hori bidegabe argitaratuko balitz.
- **Benetakotasuna** [B]: zer inpaktu eragingo litzatekeen, erabiltzaile identifikatuak gezurra esan eta beste pertsona baten lekua hartuko balu. Dimentsio horri dagokionez, identitatea faltsutzea da errazen balora litekeen egoera, bereziki, arduradunek zerbitzuen kudeaketa edo tratamendua egiteko gaitasun edo espezializazio bereziak behar dituzten zerbitzuetan.
- **Trazabilitatea** [T]: jardueraren gaineko informaziorik ez izateak zer ondorio ekarriko lukeen (zer egin den, nork egin duen edo noiz izan den ez jakitea). Zerbitzu elektroniko baten trazabilitatearen inpaktuaren adibide gisa aipa daiteke izapide bat epe barruan egin den ala ez erakusteko betebeharra. Jardueraren arrastoa galtzen bada, edo ez badago arrastorik, zaila izango litzateke frogatzea epeak ez direla bete.

[7] **Global Suite:** informatika-programa bat da, eta Eusko Jaurlaritzak arriskuen ziklo osoa —arriskuen identifikazioa, analisia eta ebaluazioa— kudeatzeko hautatu du, Arriskuen Kudeaketarako ISO 31000 arauarekin bat etorrita.

Web-orria: www.globalsuite.es

Dimentsioen azterketan ez dago mendekotasun-harremanik, hau da, haietako baten maila handia izateak ez du zertan eraginik izan beste batzuen balorazioan. Adibide gisa laguntza-programa batzuk aipa



ditzakegu: programa horietan bildutako datuen konfidentzialtasuna kritikoa da; eta, erabilgarritasuna, ordea, askoz ere txikiagoa da, eskaera egiteko epea handia delako.

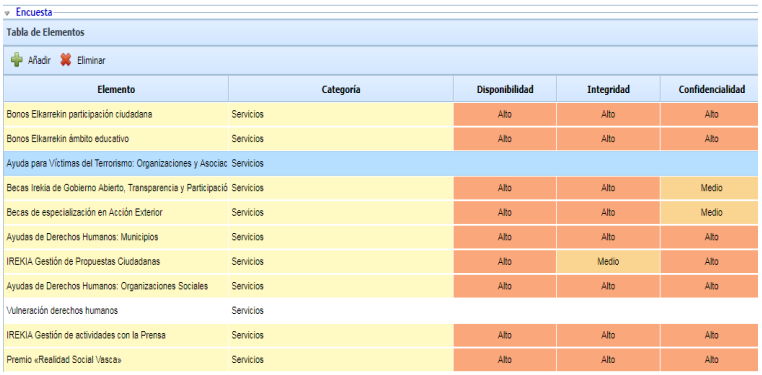
Zerbitzu bakoitza dimentsio horietako bakoitzaren arabera ebaluatzen da. Lau inpaktu-maila bereizi ditugu:

- **Oso txikia**: ez da topatu erakundearen funtzioak kaltetu ditzakeen ondoriorik.
- **Txikia**: ondorioek kalte mugatua egingo liekete erakundearen funtzioei edo zerbitzuei (erakundean agerikoa izango litzateke betebehar arruntak betetzeko gaitasunaren murrizketa, nahiz eta betebeharrak gauzatzen jarraitu).
- **Ertaina**: ondorioek kalte larria egingo liekete erakundearen funtzioei edo zerbitzuei (erakundean nabarmen murriztuko litzateke funtsezko betebeharrak eraginkortasunez betetzeko gaitasuna, nahiz eta betebeharrak gauzatzen jarraitu).
- **Handia**: ondorioek kalte oso larria egingo liekete erakundearen funtzioei edo zerbitzuei (erakundeak funtsezko betebeharren bat gauzatzeko gai ez izatea, eta zerbitzuek edo funtzioek ez lukete aurrera jarraituko).

Kalteak baloratzen direnean, honako hauek kontuan hartu behar dira: pertsona baten, pertsona-talde baten edo erakunde bat edo batzuen kalte ekonomikoa; zerbitzu elektronikoaren sail edo erakunde autonomo erantzulearen irudi publikoaren gaineko kaltea; edota Eusko Jaurlaritzak har dezakeen kaltea, arauak ez betetzeagatik. Adibidez, datuen babesaren arloko betekizunak urratzen badira, eta informazioa galtzen bada, ondorio kaltegarriak kateatu litezke, eta, besteak beste, diru-zehapenak eta publizitate negatiboa ekarriko lizkioke erakundeari, betebeharrak ez betetzeagatik.

SENen esparruko zerbitzu elektronikoez arduratzen diren sail eta erakunde autonomoetako ordezkariek beren balorazioak adierazten dituzte inkestetan; ondoren, balorazio horiek finkatzen dira, eta arriskuen analisia osatzen da.

Azken zikloko arriskuen analisiaren emaitzen arabera, Eusko Jaurlaritzak xedatu du maila HANDIko zerbitzuak daudenean, zerbitzu horiei euskarri ematen dieten informazio-sistema guztiek ere MAILA handiko kategoriakoak izan behar dutela. Eusko Jaurlaritzak ziurtatu behar du sistema horiek betetzen dituztela Segurtasunaren Eskema Nazionalean maila handietarako ezarrita dauden neurriak. Bestela, zerbitzuak



egokitzeko plan bat ezarri behar du, betetzen ez badituzte. Xedea Eusko Jaurlaritzak berak ematen dituen zerbitzuen kalitatea zaintzea da, herritarrek informazioa erabiltzen dutenean, edota enpresek zerbitzuak erabiltzen dituztenean.

DEFINIZIOAK

Aktiboa

Erakundearentzat balioa duen osagai, funtzio edo bitarteko bat da: esaterako, informazioa, datuak, zerbitzuak, aplikazioak, ekipamenduak, komunikazioak, administrazio-baliabideak, baliabide fisikoak edota giza baliabideak.

Mehatxua

Istripua gertatzeko eta informazio-sisteman edo erakundean kalte egiteko balizko arriskua. Mehatxuak beti egoten dira, baina prebenitu daitezke; edo haien ondorioak arindu daitezke, gauzatzen baldin badira.

Arriskuen analisia

Informazio-sistema batek izan ditzakeen mehatxuak, ahulguneak, arriskuak eta eraginak aztertzeko prozesua, kontuan hartuta jada ezarrita dauden segurtasun-neurriak. Abiapuntutzat hartzen da segurtasun-neurrien eraginkortasuna eta kostua hobetzeko alderdiak zehazteko.

ONDORIOAK

Komeni da, beraz, Eusko Jaurlaritzako pertsona guztiei gogoratzea Informazioaren Segurtasuna (eta horrek barne hartzen du Segurtasunaren Eskema Nazionala) **prozesu integrala** dela, eta baliabide teknikoak, giza baliabideak, baliabide materialak eta antolaketa-baliabideak eskatzen dituela.

Baliabideok arrisku-maila ebaluatzeko, aztertzeko, kudeatzeko eta zehaztutako balioen artean mantentzeko gaitasuna eduki behar dute.

Eusko Jaurlaritzan **GureSeK**[9] segurtasunaren kudeaketa-prozesua dugu. Prozesu horren bitartez, sailek eta erakunde autonomoek herritarrei ematen dizkieten zerbitzu elektronikoen segurtasuna kudeatzen da, eta haren bidez antolatzen dira zereginak (besteak beste, arriskuen analisia).

EAEko Administrazio Publikoko langile guztiek bete behar dituzte segurtasun-arauak

Segurtasun-politikan langile guztiek, hau da, bai Eusko Jaurlaritzako langileek, baita Euskal Autonomia Erkidegoko Administrazio Publikoak azpikontratatzen dituen langileek ere, betebehar batzuk bete behar dituzte, zerbitzu elektronikoak zuzenean nahiz zeharka ematen dituztenean. Halaxe jasota dago 3.8 atalean («*Erabiltzaileen betebehar orokorrak*»).

Era berean, informazioaren segurtasunaren arloko gidalerro batzuk bete behar dira, Euskal Autonomia Erkidegoko Administrazio Orokorrak eta haren erakunde autonomoek zerbitzu elektronikoak emateko zenbait produktu erosi edo zerbitzu batzuk kontratatu behar dituztenean. ❑

[9] **GureSeK:** hitz horrek informazioaren segurtasuna kudeatzeko sistema definitzen du. Sistema horri, ingelesez, *Information Security Management System* (ISMS) esaten diote; eta euskaraz, *«Gure Segurtasun Kudeaketa»* esaten diogu.

GureSeK da Eusko Jaurlaritzak herritarrei ematen dizkien zerbitzu elektronikoen segurtasuna kudeatzeko prozesua. Prozesuak bermatzen du zerbitzu elektroniko horietan aplikatzen diren segurtasun-neurriek indarreko lege-eskakizunak betetzea. Era berean, neurriok ziurtatu behar dituzte informaziorako sarbidea eta informazioaren osotasuna, eskuragarritasuna, benetakotasuna, konfidentzialtasuna, trazabilitatea eta kontserbazioa.

AZKEN INKESTAREN ONDORIOZKO DATUAK

2017ko otsailean, Eusko Jaurlaritzak lehen auditoria egin zuen, bere arloko segurtasun-neurriak zenbateraino betetzen diren ezagutzeko.

Auditoriaren emaitza nahikotzat jo zen. Segurtasunaren Eskema Nazionalera egokitzeko prozesu espezifiko bat aurrez egina zenez, eskemaren betekizun espezifiko gehienak bete ziren.

Informazio eta Telekomunikazio Zuzendaritzaren egokitze-maila % 80 da, aitortu zaion babes-mailaren araberako segurtasun-kontrolekin eta neurriekin bat etorrita. Babes-maila aitortua HANDIA da.

Segurtasun-neurriak betetzen diren ebaluatzeko, 3/2010 eta 951/2015 errege-dekretuen II. eranskinean ezarrita dauden segurtasun-neurrien kategoria edo dimentsio bakoitzaren araberako ebaluazioa egin da.

Azken hilabeteotan, Eusko Jaurlaritzak beste auditoria bat egin du, eta emaitzak laster jakinaraziko dizkiete sailei eta erakunde autonomoei.

ALBOAN:

Windows10 eta Office365 sistemei buruzko aholkuak: Sarrera

«Windows10 eta Office365 plataforma berriari esker, jada ez dago fitxategiak erantsi beharrik»

Gure lantokietara heldu dira jada Office365 eta Windows10. Segidan, lanabes horien ezaugarri esanguratsuenak eta aholku edo jardunbide batzuk azaldu dizkizuegu, guztiok lanabes berri horiei ahalik eta etekin handiena atera diezagun.

Has gaitezen...

HODEIAN

Argi eduki behar dugu hemendik aurrera dokumentu guztiak gure ordenagailuan egon beharrean, «*hodeian*» egongo direla, hau da, zerbitzarietan; eta gure ordenagailua dokumentuotan sartzeko eta haiekin lan egiteko baino ez dugula erabiliko.

Horren ondorioz, M, N eta gainerako sare-unitate ezagunak, orain arte erabili ohi ditugunak, karpeta batzuek ordeztuko dituzte, eta karpeta horiek SharePoint-en eta OneDrive-n egongo dira. Horrek abantaila handia ematen digu: dokumentu horietan beste ordenagailu batetik sar gaitezke, hau da, gurea ez den beste ordenagailu batetik edo edozein lekutatik (adibidez, gure etxeko ordenagailutik, KZgune batetik eta abarretatik); eta ez da beharrezkoa izango programa edo baimen bereziren bat edukitzea (VPN, OWA edo antzekorik).

Honako web-atari honen bitartez sartzen da plataforma horretara:

https://portal.office.com

ERRAZ PARTEKATZEA

Egun arte, gure eguneroko lanean, dokumentu bat idatzi eta gero, beste pertsona bati eranskin gisa bidali ohi diogu, pertsona horrek irakur zezan eta, beharrezkoa izanez gero, alda zezan; beraz, orain arte dokumentua mezuari atxiki diogu. Ondoren, pertsona horrek dokumentu hori itzultzen zigun, eta guk dokumentu horren azkeneko bertsioa lantzen jarraitzen genuen. Windows10 eta Office365 plataformaren bidez, ordea, eranskinak atxiki beharrean, dokumentuak **PARTEKATU** egiten dira, eta, hartara, hainbat pertsonaren arteko **LANKIDETZA** sustatzen da.

Horretarako, editatzen ari garen dokumentua hautatu, dokumentua partekatzeko aukera sakatu eta gure dokumentuaren hartzailea hautatu baino ez dugu egin beharko. Horren erraza da. Prozesu horrek ordezkatuko du orain artekoa: bidali nahi dugun dokumentua kopiatzea, posta elektronikoan sartzea, mezu elektronikoa idaztea, eranskina mezuari atxikitzea eta bidaltzea.

Gainera, Office365 berriak beste funtzionalitate batzuk dauzka, besteak beste, dokumentuaren sortzaileok **segurtasuna** eta **kontrola** izaten ditugu, dokumentuen gainean. Dokumentu bat partekatu nahi dugunean, adibidez, erabaki dezakegu nola

banatu nahi dugun, hau da, dokumentu horren gainean zer baimen eman nahi diogun beste pertsona horri. Hona hemen dokumentua partekatzeko modu batzuk:

- ✓ Dokumentuan sartzeko esteka duen edozein pertsonarekin
- ✓ Hainbat pertsonarekin, aldi berean (Eusko Jaurlaritzatik kanpoko langileekin ere bai)
- ✓ Pertsona zehatz batekin (gainerako pertsona guztiei sarbidea debekatuta)
- ✓ Pertsona batekin, baina epemuga zehatza ezarrita (hau da, iraungitze-data ezarrita)
- ✓ Pertsona batekin dokumentua partekatzea, dokumentua elkarrekin editatzeko (Office365 berriak aukera ematen digu beste pertsona batekin dokumentu bera aldi berean editatzeko; halaber, bi pertsonak edo gehiagok dokumentu baten edukia alda dezakete)

Office365 paketeak badauka beste ezaugarri garrantzitsu bat: **dokumentuen bertsioak kudeatzen ditu**. Plataforma berrian dokumentu beraren 500 bertsio arte gorde daitezke, eta, gainera, automatikoki gordetzen ditu, hau da, erabiltzaileak ez du ezer egin behar. Aukera horren bidez, erraz berreskura dezakegu dokumentuaren aurreko bertsioa (hau da, ez da izango beharrezkoa EJIEri eskatzea egun zehatz bateko segurtasun-kopia edo «*backup*»).

PRESTAKUNTZA

Plataforma berrian nobedade ugari daudenez, Informatika eta Telekomunikazio Zuzendaritzak, EJIErekin batera, hainbat ikastaro edo prestakuntza-saio programatu ditu, aldaketa erraz egiteko eta plataformaren aukera guztiak ezagutzeko.

Era berean, Jakina intranetean atal espezifiko bat sartu da, proiektu horri buruz. [Ikus taula hau: *«Laguntza behar baduzu...»*] ❑

«Office365 berriak funtzionalitate oso baliagarriak ditu, besteak beste, dokumentuen gaineko segurtasuna eta kontrola»

Office365 atari berrian sartzeko webgunea: https://portal.office.com

jakina

LAGUNTZA BEHAR BADUZU...

Informazio gehiago behar baduzue, kontuan izan Jakina intranetean (*«Prestakuntza»* atalaren barruan) *«Windows10 eta Office365»* izeneko atala duzuela, eta bertan laguntza-**dokumentuak** argitaratuko direla. Besteak beste, honako hauek:

- Windows, Word, Excel, Power Point eta Outlook sistemen zenbait funtzionalitateri buruzko bideoak; gaur egun, 50 bideo baino gehiago argitaratu dira. Gutxi gorabehera, 2 minutukoak dira.
- Gidaliburuak edo beste dokumentu interesgarri batzuk: esaterako, informatika-postuen migrazioaren gaineko informazioa eta abar.

Proiektu horretarako bi kanal espezifiko erabilgarri daude, **intzidentzia**k konpontzen laguntzeko, sortuz gero. Hauexek dira: o365era@ejie.eus helbide elektronikoa (*«EJIE, Office365 Kudeaketa»* postontzia); eta telefono-zenbakia, 72940.

Informazio gehiago behar baduzue, dokumentazio hau ere kontsulta dezakezue:

- ✓ *«Badator Office365 paketea»* artikulua, 62. zenbakiko *Aurrera* alean argitaratua (2017ko abenduan)
- ✓ *«Windows10 eta Office365»* artikulua, 63. zenbakiko *Aurrera* alean argitaratua (2018ko martxoan)

ALBOAN

Kontrazala!!

68. zk.
2019ko ekaina

IXTEKO

Ziberespazioko desinformazioa

Ziberespazioko desinformazioa bultzatzeko kanpainen aurka zer egin jakitea herrialdeen segurtasunaren arloko erronka handienetako bat da.

Interneti eta informazio digitala kontsumitzeko ohiturei buruzko zenbait azterlanek adierazten dute 16 eta 65 urte bitarteko biztanleen % 90 «**desinformazio-eraso bat**»en biktimak izan daitezkeela.

Kriptologia Zentro Nazionalak duela gutxi argitaratu du txosten hau: «*Informe de Buenas Prácticas, Desinformación en el ciberespacio*» [Jardunbide egokien txostena. Ziberespazioko desinformazioa]. Txostenean azaldu dituzte gaur egungo desinformazio-ekintzen ezaugarriak eta metodologia. Xedea herritarrei tresnak ematea da, informazioa modu kritikoan kontsumitu eta parteka dezaten, eta, aldi berean, herrialde baten interesen aurkako ekintzak nahigabe sustatu ez ditzaten; hortaz, desinformazio-ekintzetan bereizgarri diren komunikazio-produktuak eta -plataformak ezagutzeko baliabideak ematen dira.

Izatez, desinformazio-kanpaina baten biktimak ez izatea eragile baten baino gehiagoren erantzukizuna da. **Erakunde publikoek**, adibidez, gaitasunak garatu behar dituzte sistema publikoen aurkako eraso mota horiek prebenitzeko, detektatzeko eta neutralizatzeko; **enpresa pribatuek**, beren aldetik, lortu behar dute beren plataforma digitalak kanpaina gaiztoak gauzatzen laguntzeko tresnak ez bilakatzea; eta, azkenik, baliabide digitalak erabiltzen dituzten **herritarrek** arduratu behar dute desinformazio- eta manipulazio-kanpainak bereizteaz, txosten horretako «**dekalogo**»an aipatzen den bezala. Katalogo osoa hemen kontsulta dezakezue, eta informazio gehiago ere jaso dezakezue:

https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3552-ccn-cert-bp-13-desinformacion-en-el-ciberespacio-1/file.html

PROTAGONISTAK

Alicia Monje Micharet doktoreak Ada Byron saria irabazi du

Maiatzaren 16an, Deustuko Unibertsitateak Alicia Monje Micharet doktoreari eman zion Ada Byron 2019 saria.

Alicia Monje Micharetek Extremadurako Unibertsitatean eskuratu zuen doktore-titulua, 2006an. Doktoregoko Aparteko Saria irabazi zuen, eta Europar Doktoregoaren Aipamena ere jaso zuen. Gaur egun, Concepción Aliciak Madrilgo Carlos III.a Unibertsitateko RoboticsLab taldean jarduten du.

Concepción Alicia Monje

Ana Freire

TEO giza itxurako robotaren gaineko ikerlana egiten ari da. Laguntza-robota izateko pentsatuta dago, zehazki, pertsonen bizitzaren kalitatea hobetzeko. Haren lanak hainbat sari jaso ditu, besteak beste, Madrilgo Carlos III.a Unibertsitatearen Ikerketa Bikaintasun Saria eta Orange Fundazioaren Emakumea eta Teknologia Saria irabazi ditu (biak, 2018an).

Aurrekoaz gain, gaur egun, RoboCom++ europar proiektua zuzentzen duen lagunetako bat da. Proiektu horren helburua etorkizuneko laguntza-robota garatzea da.

Ada Byron Gaztea Saria

Bestalde, Ada Byron Gaztea Saria Ana Freirek irabazi du. Irabazlea Informatikako ingeniaria eta doktorea da. Bartzelonako Pompeu Fabra Unibertsitateko Ingeniaritza Eskolako ikerlaria eta irakaslea da, eta unibertsitate bereko jasangarritasunari buruzko zentroko zuzendaria ere bai (Centre d'Estudis sobre Sostenabilitat). 36 urte ditu, eta jada 40 argitalpen zientifiko eta hiru patenteko ekarpena egin du. Horrez gain, beraren lanak nazioarteko aintzatespena ere jaso du: *Google Anita BorgScholarship*, *Big Data Talent Award*, besteak beste. *Business Insider* aldizkarian aipatu dituzte iraultza teknologikoa lideratuko duten Espainiako 23 gazte, eta Ana Freire haietako bat da.

Datuak gizarte-xedeetarako aztertzean datza haien ikerketa. Esate baterako, gizarte-sareetako datuak burugaixotasunak detektatzeko nola erabili ari dira aztertzen.

Argibide gehiago: https://www.deusto.es