55. zk.
2016ko martxoa

Aurrera!

Berrikuntzaren eta Teknologia Berrien dibulgaziozko aldizkaria

Bulego Teknologikoak argitaratua
Informatika eta Telekomunikazioetako Zuzendaritza

AURKIBIDEA

Gaur egun, Artxibo Elektronikoa funtsezkoa da edozein administraziorentzat. Dagoeneko hainbat legek eta arauk horren funtzionamendua jaso eta arautzen dute. Bada Artxibo Elektronikoari hertsiki lotua dagoen gai bat, organismo eta erakunde publiko guztiek eratu behar dutena: «*Dokumentu Elektronikoak Kudeatzeko Politika*» (DEKP).

DEKPa edozein administraziorentzako hain garrantzitsua denez, aldizkari honen lehenengo artikuluan azalduko dizuegu alor horretan Eusko Jaurlaritzak egin dituen izapideak, aplikatu beharreko legedia eta haren harremana elkarreragingarritasunarekin.

Aldizkariaren bigarren gaian azken hilabeteetan gorantz ari den mehatxu berri bati buruz arituko gara, *ransomware*ari buruz, hain zuzen ere. Gure ordenagailuei mehatxu egiten dieten gero eta etsai gehiago dago. Horiei defentsa egiteko gauzarik onena informatuta egotea denez, artikulu honetan zehar mehatxu horren jatorria, funtzionamendua eta aldaerak zehaztuko ditugu; eta, batez ere, eraso mota hori saihesteko eta erasoaren ostean berrezartzeko modurik onena adieraziko dugu.

«*Alboan*» atalaren bidez, gure Eustateko kideek lortu duten kasu arrakastatsu baten berri eman nahi dizuegu: beren Informazio Sistemetako sailerako ISO9001 ziurtagiria lortu dute. Lorpen hori zenbait urteko lanaren ondorioa da, eta, beren prozesuak etengabe hobetzeari dagokionez, beste lorpen gogoangarri bat da.

«*Berri laburrak*» atalean, txartel mota berri bat aurkeztuko dizuegu, eSIM izenekoa. Berriki Bartzelonan izandako *Mobile World Congress*ean aurreratu dutenez, etorkizun hurbilean telefono mugikorrek txartel hori ekarriko dute barruan.

Halaber, «*Berri laburrak*» atalaren bidez, jakinaraziko dizuegu Eusko Jaurlaritzaren Software Librea Sustatzeko Bulego Teknikoak, SALE izenarekin ezaguna denak, bere webgune berria aurkeztu berri duela.

Artxibo Elektronikoaren garrantzia

Euskadiko administrazio publikoak espediente asko izapidetzen ditu egunero. Espediente horiek hainbat dokumentuz osatuta daude, eta, normalean, dokumentu horiek gure administrazioko leihatiletara paper-formatuan iristen dira. Baina gero eta ohikoagoa da dokumentu horiek formatu elektronikoan edo digitalean jasotzea.

HIZTEGIA

[1] **Espediente elektronikoa**: prozedura administratibo baten instantzia bati dagokion dokumentu elektronikoen multzoa da.

Dokumentu elektronikoa, bere aldetik, modu elektronikoan jasota dagoen edozein eratako informazioa da; euskarri elektronikoan artxibatuta dago, formatu jakin batean, eta identifikatu egin daiteke eta tratamendu berezitua izan dezake.

[Iturria: 11/2007 Legea, ekainaren 22koa, Herritarrek Zerbitzu Publikoetan Sarbide Elektronikoa izateari buruzkoa]

[2] **EEN**: (Elkarreragingarritasuneko Eskema Nazionala).

4/2010 Errege Dekretua, urtarrilaren 8koa, Administrazio Elektronikoaren esparruan Elkarreragingarritasun Eskema Nazionala arautzen duena.

Azken urteen buruan, Eusko Jaurlaritzak baliabide asko, giza-baliabideak zein ekonomikoak, erabili ditu espedienteen izapide elektronikoa ezartzeko[1].

Denok dakigunez, espedienteek hasiera eta amaiera bat dute. Hala ere, pertsona askok uste dute espediente bat ixtean haren kudeaketa ere amaitzen dela, baita haren dokumentu erantsiena ere. Bada, espedienteen (eta espedienteei lotutako dokumentuen) «benetako bizitza» haratago doa; izan ere, bai paperez izapidetuak bai elektronikoak **artxibatu** behar dira.

Orain arte dokumentu elektronikoen kudeaketak **izapidetze-fasea** bakarrik hartu du bere gain, nagusiki berehalako arazoak konpontzeko dugun joera dela-eta. Hori dela eta, garatzen joan diren administrazio elektronikoko sistema askok espedientearen izapidetzea baino ez zuten bere gain hartzen; espedientearen bukaerako artxibatzea ez zuten bere gain hartzen. Kasu horietan, sail horietako arduradunek gai hori aurrerago egiteko uzten zuten.

Baina horrek arazo larria sor dezake. Izan ere, bizi ziklo osoa ez badugu egiten, dokumentu-ondarearen zati handi bat gal dezakegu. Artxibatu gabeko dokumentu horiek iraganean, **Elkarreragingarritasuneko Eskema Nazionala (EEN)**[2] egokitu baino lehen, egin diren izapide elektronikoen funts berreskuraezinean txertatuko lirateke. Espediente baten bizi ziklo osoak **artxibatze elektronikoarekin** du amaiera, hau da, dokumentuaren kontserbazioarekin. Kontserbazio-prozesuak zenbait baldintza bete behar ditu, dokumentuen berreskuratzea (irakurketa), osotasuna, egiazkotasuna, eskuragarritasuna eta baliotasuna bermatzeko.

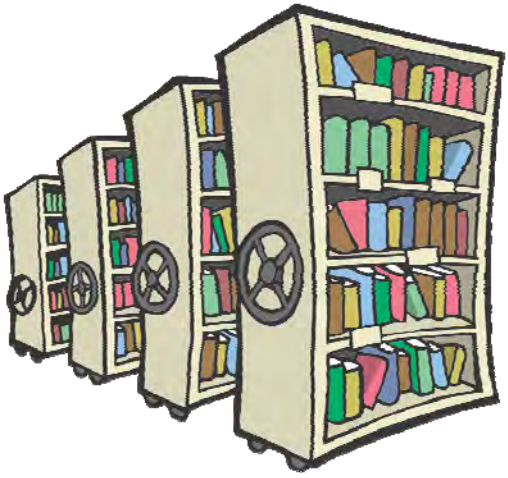
Gaur egun, espediente baten ARTXIBO ELEKTRONIKOA, beraz, funtsezkoa da administrazio elektronikoarentzat. Horren adierazle da azken urteetan sortu diren araudi eta legeek gero eta garrantzi handiagoa ematen diotela horri.

ARTXIBO ELEKTRONIKOA

Administrazio Publikoen Administrazio Prozedura Erkidearen urriaren 1eko **39/2015 Legea**ren 17. artikuluak honako hau adierazten du:

«17. artikulua. Dokumentuen artxiboa.

1. **Administrazio bakoitzak** bukatutako prozedurei dagozkien dokumentu elektronikoen **Artxibo Elektroniko bakar bat mantendu beharko du**, aplikatu behar den araudiak ezarritako terminoei jarraituz.



2. *Dokumentu elektronikoak dokumentuaren **egiazkotasuna, osotasuna eta kontserbazioa ahalbidetzen dituen formatu batean kontserbatu beharko dira.** Horiez gain, dokumentua kontsultatzea ere ahalbidetu beharko du, dokumentua egin zenetik igarotako denbora alde batera utzita. Era berean, ziurtatu egingo da datuak beste formatu eta euskarri batzuetara bidaltzeko aukera, aplikazio desberdinetatik sartzeko aukera bermatuz. Dokumentu horiek ezabatzeko, aplikatu behar den araudiak xedatutakoaren arabera baimendu beharko da.*

3. *Dokumentuak gordetzeko erabiltzen diren bitarteko edo euskarriek segurtasun-neurriak, **Segurtasuneko Eskema Nazionalean xedatutakoaren araberakoak**, izan beharko dituzte, jasotako agirien osotasuna, egiazkotasuna, konfidentzialtasuna, kalitatea, babesa eta kontserbazioa bermatzeko. Batez ere, erabiltzaileen identifikazioa eta sarbideen kontrola ziurtatuko dituzte, bai eta datuak babesteko legedian ezarritako bermeak betetzen direla ere».*

Elkarreragingarritasuneko Eskema Nazionala (EEN) arautzen duen 4/2010 Errege Dekretuak ezartzen duenez, **Gordailu elektronikoa** fitxategi zentralizatu bat da, eta, bertan, datuak eta dokumentu elektronikoak zein horien metadatuak[3] biltzen eta administratzen dira.

Indarrean dagoen legediaren arabera, 2017an erakunde guztiek bukatutako prozedurei dagozkien dokumentuetarako fitxategi elektroniko bat izan beharko dute. Horren harira, Eusko Jaurlaritzak bere Dokumentuak Kudeatzeko Sistema propioa du, **dokusi**[4] izenekoa. Sistemak dokumentuen ziklo osoa betetzen du, artxibatzea barne.

Artxibo Elektroniko bakarra abiatzeko, zenbait taldek ahalegin handia egin behar dute (teknologian adituak diren pertsonak, administrazioa, kudeaketa, artxibistika, araudia, zerbitzu juridikoak...).

Jarraian, Ogasuneko eta Administrazio Publikoetako Ministerioaren ustez dokumentu elektroniko bat arrakastaz kudeatzeko landu behar diren alderdirik garrantzitsuenak zehaztuko ditugu (2015eko uztailean Administrazio Elektronikoko Behatokiak osatutako «*Artxibo Elektronikoa dokumentu elektronikoaren azken fasea da*» dokumentuan jasota daude):

- Fitxategian eta teknologia berrietan adituak diren **diziplina anitzeko** adituen **kolaborazioa** behar da. Horrez gain, artxibozainak, teknologia berrietako alorreko profesionalak eta kudeatzaileak barne hartzen dituen administrazio-tratamendu koordinatua ere beharrezkoa da.

- Dokumentuak eta espedienteak kudeatzeko **aldez aurretiko tresnaz** osatutako agertokia aztertzea eta ordenatzea beharrezkoa da, baita tresna horiek erakundean jadanik existitu daitezkeen beste tresna batzuei atxikitzea ere.
- Beharrezkoa da **langileak** dokumentuak kudeatzeko **prestatzea** eta dokumentu-ondarearen garrantziaz jabetzea bultzatzea.
- **Espediente mistoen** (papera eta elektronikoa) tratamendu azkar bat aukeratu behar da.
- **Dokumentu elektronikoak kudeatzeko politika** bat izan behar da. Puntu hori prozesu osoaren gakoetako bat da.

Beraz, abiapuntua Dokumentu Elektronikoak Kudeatzeko Politika (DEKP) hori eratzea da.

DOKUMENTU ELEKTRONIKOAK KUDEATZEKO POLITIKA

Indarreko legediak ezartzen du organismo edo erakunde guztiek «*dokumentu elektronikoak kudeatzeko politika*» bat **izan behar dutela**. Hala ere, gaur egun guztiz garatutako benetako **adibide** gutxi daude. Izan ere, horietako batzuk politika osoak izan behar duenaren hurbilketatzat jo daitezke. Adibide gisa honako hauek aipatuko ditugu: unibertsitate-eremuan (Murtzia, Nafarroa,

HIZTEGIA

[3] **Metadatuak:** beste datu batzuk deskribatzen dituzten datuak dira, eta dokumentuak identifikatzeko, egiaztatzeko eta testuinguruan jartzeko balio dute. Dokumentu eta espediente elektronikoek gutxieneko metadatu batzuk dituzte, eta metadatu osagarriak izan ditzakete.

[4] **Dokusi:** (*Dokumentu Kudeaketako Sistema Integrala*) Eusko Jaurlaritzaren proiektua da, korporazioko dokumentuak kudeatzekoa eta **Artxibo Digitala** duena. Adierazi beharra dago EAEko Administrazio Publikoaren artxibatze-sisteman jadanik espediente eta dokumentu elektronikoak —antolatuak— kontserbatzen direla, eta horiek eskuratu daitezkeela, AKS/SGA (S54b aplikazioa) edo Artxiboa kudeatzeko sistema informatikoaren bidez.

Informazio gehiago dago «***dokusi*: *dokumentuak kudeatzeko sistema berria***» artikuluan (2008ko irailaren Aurrera buletina).

HIZTEGIA

[5] **Euskadi**: 2014ko apirilean, Euskal Herriko Unibertsitateak (UPV-EHU) dokumentu bat argitaratu zuen, unibertsitatearen «*Dokumentuak gestionatu eta artxibatzeko politika*» ezartzen zuena. Dokumentua honako webgunean kontsultatu daiteke:

https://www.ehu.eus/eu/web/idazkaritza-nagusia/dokumentuak-gestionatu-eta-artxibatzeko-politika

Beste alde batetik, informazio gehigarri gisa, aipatuko dugu Eusko Jaurlaritzak, bere aldetik, 2003. urtean 174/2003 Dekretua argitaratu zuela, uztailaren 22koa, Euskal Autonomia Erkidegoko Administrazio Publikoaren artxibo-sistemaren antolamenduari eta funtzionamenduari buruzkoa.

[163 zenbakiko EHAA, 2003ko abuztuaren 22koa]

Euskal Autonomia Erkidegoa[5]), toki-administrazioa (Cartagena, Bartzelonako Aldundia, Arganda del Rey, Valentziako Aldundia), erkidego-administrazioa (Katalunia, Kanariak) eta Estatuko Administrazio Orokorra (Ogasuneko eta Administrazio Publikoetako Ministerioa, Hezkuntzako, Kulturako eta Kiroletako Ministerioa).

Edonola ere, dokumentu elektronikoak kudeatzeko politika legeak eskatzen duen eta bete behar den baldintza bat baino gehiago da. Oinarrian, ezinbesteko tresnatzat har dezakegu, erakunde baten barruan dokumentu elektronikoen kudeaketa egoki garatzeko, beti EENek ezarritakoari jarraituz.

Baina, zer da dokumentu elektronikoak kudeatzeko politika zehazki? Laburbilduz, esango dugu erakunde baten **irizpide multzoa** dela, benetako dokumentu fidagarriak eta denboran zehar eskuragarri egongo direnak sortzeko eta kudeatzeko aukera emango digun irizpide multzoa.

Beraz, dokumentu honetan **zehaztapen teknikoak** eta irizpide eta gomendioak ezartzen dira, administrazioan sor daitezkeen dokumentu eta espediente elektronikoen elkarreragingarritasuna, berreskuratzea eta kontserbazioa bermatzeko beharrezkoak direnak.

Politika hori mailarik altuenean onartu behar da, erakundearen barruan, eta **erantzukizun** batzuk egozten ditu, dokumentuak beren bizi-ziklo osoan zehar tratatzeko programaren koordinazio, aplikazio, gainbegiratze eta kudeaketari dagokienez.

Gainera, dokumentu elektronikoak kudeatzeko politikak **Elkarreragingarritasuneko Eskema Nazionalak (EEN)** ezarritakoa betetzen dela bermatu behar du, ezinbestean bete behar den Elkarreragingarritasuneko Arau Teknikoan eta hari dagokion aplikazio-gidan xedatutakoari jarraituz.

Horretarako, ezarri da administrazio-espediente baten parte diren eta administrazioko ekintzetan erabiltzen diren dokumentu elektroniko guztiak euskarri elektronikoan kontserbatu behar direla. Herritarren eta administrazioaren arteko harremanak egiaztatzen dituzten dokumentuak, aldiz, jatorrizko formatuan edo dokumentuaren osotasuna ziurtatzen duen beste edozein formatutan kontserbatu behar dira.

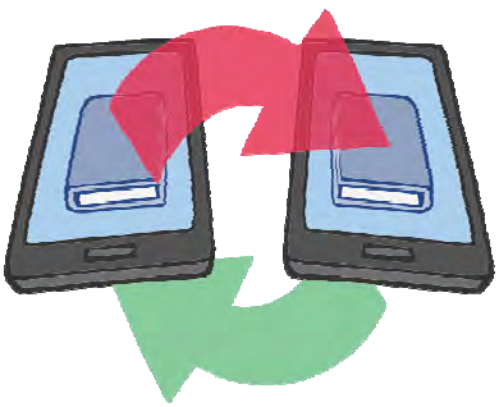
2013. urtetik **dokusi**-ko batzorde teknikoak bere DEKPko proposamena eratu du, oraindik Eusko Jaurlaritzak onetsi behar duena. Proposamenaren bitartez, EAEko Administrazio Publikoak eragin dezakeen dokumentuen kudeaketa, izapidetzea, antolaketa eta artxibatzea normalizatu eta hobetu nahi da, dokumentu elektronikoak kudeatzeko Elkarreragingarritasuneko Arau Teknikoan xedatutakoa errespetatuz.

«Artxibo Elektronikoa funtsezkoa da administrazio elektronikoarentzat»

ELKARREREGINGARRITASUNA

Gaur eguneko lege-markoan oinarrituz, gainera, administrazio bakoitzak interesdunei buruzko datuak eskuratzeko modua eman beharko die gainerako administrazio publikoei, datu horiek bere esku eta euskarri elektronikoan daudenean. Horretarako, **elkarreragingarritasunaz** baliatuko da.

Hain zuzen ere, behar hori Europarako Agenda Digitalean jasota zegoen, Europa 2020 Estrategiaren ekimen adierazgarrien barruan. Hain da garrantzitsua, ezen aditu askoren aburuz, «*elkarreragingarritasunik gabe ezin da administrazio elektronikorik egon*». Horrez gain, gehi genezakeen elkarreragingarritasuna ez litzatekeela existituko Dokumentu eta Artxibo Elektronikorik gabe.



Hain garrantzitsua denez, **EEN**ak Elkarreragingarritasuneko Arau Tekniko multzo bat ezarri duela. Administrazio publikoek nahitaez bete behar dituzten arau horiek administrazioen eta herritarren arteko elkarreragingarritasuneko alderdi jakin batzuk garatzen dituzte. Arauak honako hauek dira:

1. Estandarren katalogoa
2. Dokumentu elektronikoa
3. Dokumentuen digitalizazioa
4. Espediente elektronikoa
5. Sinadura elektronikoaren politika eta administrazioaren ziurtagiriak
6. Datuen bitartekotza-protokoloak
7. Datu-ereduen zerrenda
8. Dokumentu elektronikoak kudeatzeko politika
9. Espainiako administrazio publikoen komunikazio-sarera konektatzeko baldintzak
10. Benetako kopiaketako eta bihurketako prozedurak, dokumentu elektronikoen artean zein paperetik edo beste euskarri fisikotik formatu elektronikoetara
11. Erregistro-erakundeen artean erregistroak trukatzeko datu-eredua
12. Informazio-baliabideak berriz erabiltzea
13. Teknologia berriz erabiltzea eta transferitzea
14. Elkarreragingarritasuneko Eskema Nazionalarekin adostasun-adierazpena
15. XML-eskemen URLak

«Dokumentu Elektronikoa kudeatzeko, diziplina anitzeko adituen kolaborazioa behar da, hain zuzen ere, kudeaketako, artxibistikako eta teknologia berrietako adituen kolaborazioa»

Konprobatu daitekeenez, horietako asko hertsiki lotuak daude Dokumentuekin, Espedienteekin eta Artxibo Elektronikoarekin. Hortaz, elementu guzti horiek oinarrizkoak dira administrazioarentzat. ❑

LEGEDIA

Jarraian, Artxibo Elektronikoen funtzionamenduari eragiten dion araudiaren bilketa bat jasotzen da.

- ✓ **1164/2002 Errege Dekretua**, azaroaren 8koa; haren bidez, balio historikoa duen ondare dokumentala kontserbatzea, Estatuko Administrazio Orokorreko beste agiri batzuk deuseztatzearen gaineko kontrola eta dokumentu administratiboak jatorrizkoa ez den bestelako euskarri batean kontserbatzea arautzen da.
- ✓ **11/2007 Legea,** ekainaren 22koa, herritarrek zerbitzu publikoetan sarbide elektronikoa izateari buruzkoa. [31. artikulua. Agiriak elektronikoki artxibatzea]
- ✓ **4/2010 Errege Dekretua**, urtarrilaren 8koa, administrazio elektronikoaren esparruan Elkarreragingarritasunerako Eskema Nazionala arautzen duena. [X. kapitulua, 21. artikulua]
- ✓ **1708/2011 Errege Dekretua**, azaroaren 18koa, Espainiako Artxibo Sistema ezartzen duena eta Estatuaren Administrazio Orokorraren eta haren erakunde publikoen Artxibo Sistema eta bertan sartzeko araubidea arautzen dituena. [4. atala. Dokumentu elektronikoak eta babeste digitala]
- ✓ **21/2012 Dekretua**, otsailaren 21ekoa, administrazio elektronikoari buruzkoa. (50. zenbakiko EHAA, 2012ko martxoaren 9a]
- ✓ **39/2015 Legea**, urriaren 1ekoa, Administrazio Publikoen Administrazio Prozedura Erkidearena. [17. artikulua. Dokumentuak artxibatzea]
- ✓ **40/2015 Legea**, urriaren 1ekoa, Sektore Publikoko Araubide Juridikoari buruzkoa. [46. artikulua. Agiriak elektronikoki artxibatzea]

COVASAD

Esan behar da Euskadiko administrazioaren esparruan Euskal Autonomia Erkidegoko Administrazio Publikoaren Dokumentazioa Baloratzeko, Hautatzeko eta Balioztatzeko Batzordea dagoela, **COVASAD** siglekin ezaguna dena.

Batzorde horren lana, beste batzuen artean, dokumentazioa **kontserbatzeko egutegiak** zehazteko prozesuan zentratzen da.

Informazio gehiago lor daiteke 174/2003 Dekretuan, uztailaren 22koan, Euskal Autonomia Erkidegoko Administrazio Publikoaren artxibo-sistemaren antolamenduari eta funtzionamenduari buruzkoan.

(13. artikuluak eta hurrengoek funtzionamenduaren inguruko funtzioak, osaera eta gainerako alderdiak garatuko dituzte).

Ransomware: gorantz ari den mehatxua

Malware[6] mota hori gaur egun Interneten dauden mehatxu handienetako bat bihurtzen ari da. Herritarrek «ordenagailu-bahiketa» izenarekin ezagutzen dute. Ekintza horren bidez, ziberkriminalek lortu nahi duten helburu bakarra dirua lortzea da —legetik kanpo, noski—. Horretarako, pertsona bati eraso egin eta diru-bahisari bat (*ransom*) ordaintzeko agintzen diote.

HIZTEGIA

[6] **Malware**: informazio-sistema bati kalteak eragiteko edo bertan infiltratzeko helburua duen software gaiztoa da.

[7] **Scareware:** erabiltzaileari beldurra ematea.

Zer da *RANSOMWARE* bat?

«Intentzio txarreko programa informatikoa da, eta kutsatutako sistemaren zati edo fitxategi jakin batzuetara sarbidea mugatzen du. Mugatzea kentzearen truke, bahisaria ordaintzeko eskatzen du. Ransomware mota batzuek sistema eragileko fitxategiak enkriptatzen dituzte, eta, ondorioz, gailua erabilezin bihurtzen dute eta erabiltzea bahisaria ordaintzera bortxatzen dute» (iturria: Wikipedia). Erasotzaileei ematen dizkien diru kopuruak direla eta, *malware* mota hori zabaldu egin da. Beste *malware* mota batzuek informazioa lortzeko xedea dute, baina *ransomware*ak, aldiz, dirua azkar lortzeko helburua du.

Zer egin behar da *malware* mota horrekin erasotzen badigute?

Orokorrean, ziberkriminalei **ez zaie INOIZ ordaindu behar** delitu-ekintza horiengatik. Izan ere, alde batetik, inoiz ez dugu ziurtasunez jakingo ezarri diguten murrizketa (kasu batzuetan erasoa jaso duen pertsonaren disko gogorreko fitxategien enkriptazioa) konponduko denik, eta, beste alde batetik, eraso mota horiek indartuko genituzke.

Zoritxarrez, gero eta handiagoa den mehatxu hau Ekialdeko Europatik Mendebaldeko Europara, Amerikako Estatu Batuetara eta Kanadara hedatu da; beste era batera esanda, kriminalak dirua dagoen lekuetara doaz. *Malware* horrek oso etekin handiak ekartzen dizkiete kriminalei eta delitu-erakundeei; izan ere, erasoa jasotzen duten pertsonen ia %3k eskatzen zaien ordainketa egiten dute.

DENBORAN ZEHARREKO ALDAKETAK

Laburki azalduko ditugu eraso mota horrek denbora zehar izan dituen aldaketak:

Hasierako aldagarriak: SMS Ransomware

Erabiltzailearen ordenagailua blokeatzen da, eta zenbaki jakin bati SMS (*Short Message Service*, mezu laburren zerbitzua, edo telefono mugikorretan erabilgarri dagoen testu-mezua) bat bidaltzeko adierazten duen ohar bat agertzen da. Ekintza hori egiten bada, desblokeatzeko kode bat jasotzen da eta ordenagailua libratzea lortzen da. Egiten den ordainketa bidalitako SMS-mezuaren tarifa altua da (SMS-mezua bidaltzea zenbaki *premium*ei). *Malware* mota hori sortzaileak azkar konturatu ziren antibirus-enpresek arazo horri aurre egiteko konponbideak arin eskaini zituztela, *premium*-mezua ordaindu behar izan gabe. Hori dela eta, eraso mota hori garatu eta ordainketa elektronikoko zerbitzuak erabiltzen hasi ziren (*online*-ordainketa).

Aurreneko bilakaera-maila: Winlockers-ak

SMS *Ransomware*aren kasuan gertatzen den bezala, erasoa jasotzen duen pertsonaren ordenagailua blokeatzen da. Baina zuzenean ordaintzeko eskatu beharrean, gizarte-ingeniaritzako teknikak erabiltzen ditu. Hau da, oldartua izan den pertsona engainatzen dute (*scareware*[7]). Horretarako, legeren bat hautsi duela azaltzen diote, jabetza intelektualeko Legea, esaterako, eta esaten diote, horren ondorioz isun bat ordaindu behar duela *online*-ordainketako sistema bat erabiliz. Ordaindu beharreko

zenbatekoa SMS *premium*aren kostua baino askoz handiagoa da, eta zenbait kasutan, 19 digitutako kode bat bidali behar zen, aldez aurretik ordainagiri gisa jasotzen zena. *Ramsomware*aren aldagai hori Errusian eta errusiera hitz egiten den herrialdeetan ikusi zen lehen aldiz, 2009. urtean.

*Ransomware*ak erabiltzailearen pantaila baino ez du blokeatzen, pantaila osoa okupatzen duen *banner*[8] baten bidez. *Banner* horrek beste programa batzuk exekutatzea eragozten du, eta, haren bitartez, estortsio-mezua ikus daiteke. *Malware* mota horren adibiderik ezagunenak «poliziaren birusa» eta «FBIaren birusa» dira, duela urte batzuk oihartzun handia izan zutenak.

Bilakaera aurreratua: fitxategien enkriptatzailea (*fyle encryptors*)

Aldagai horretan, *malware*ak erabiltzailean fitxategiak enkriptatzen ditu, enkriptazio-algoritmo konplexuak erabiliz. Erabiltzaileari diru kopuru bat eskatzen zaio, bere ordenagailua aske uztearen truke. Printzipioz, ordainduz gero enkriptatutako fitxategiak berreskuratu ahal izango ditu (desenkriptazio-kode baten bidez). Ordainketa elektronikoko bitartekoen bidez ordaindu behar da, *ransomware Winlockers*aren kasuan bezala. Kasu horietan, enkriptazio-eragiketen konplexutasuna *ransomware*-motaren araberakoa da: batzuek kodean bertan dagoen enkriptazio-tresnak erabiltzen dituzte, eta beste batzuek, aldiz, beste batzuen enkriptazio-tresnak erabiltzen dituzte, adibidez, GPG, WinRAR...

ENTREGATZEKO ETA HEDATZEKO MEKANISMOAK

Entregatzeko eta hedatzeko mekanismoak honako ekintza-forma hauetan oinarritzen dira nagusiki:

- **Spam moduko posta elektronikoetan atxikita**

*Ransomware*a zaborra diren posta elektronikoen (*spam*) bidez iristen da, eta fitxategi gaiztoak dakartza erantsita. Jasotzen den posta elektronikoak itxura normala izan dezake, eta erabiltzaileari erantsitako fitxategia zabaltzeko eskatzen dio. Fitxategi hori .zip luzapeneko fitxategi konprimitua izan daiteke, adibidez. Fitxategi konprimitu hori zabaltzean, .ziparen barruko fitxategi bitarra (zero eta bat zenbakiez enkriptatutako informazioa duen fitxategia) exekutatzen da, eta *malware*a sisteman instalatzen da. Horrek ordenagailua *C&C server*[9] batekin harremanetan jartzen du. Bertatik pantaila blokeatzeko irudia jaisten da (geo-lokalizazioko sistemetan oinarrituz, hainbatetan jarduten ari den lekuko hizkuntzara egokitzen da irudia), eta, horrez gain, enkriptatzeko kodea bidaltzen da bertara.

- ***Exploit*[10] *kits* edo *exploit pack***

Esploratzen duten tresna multzoak dira (*pakete* izenekoak), eta, ahal izatekotan, erasotzen dituzten makinetan instalatutako softwarean (adibidez, Java softwarean, Adoberen softwarean oldarkorragoak direnak, saihesten laguntzeko eta kudeatzeko zenbait jarraibide eta gomendio ezagutzera ematen ditu.

2015. urtean soilik, Gobernuko CERT Nazionaleko Interneten Alerta Goiztiarreko Sistemak (SAT-INET) eraso mota horrekin erlazionatutako 500 gertakari baino gehiago kudeatu zituen (2014an 200 izan ziren).

Txostenera sarbidea:

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

CCN-CERTen webgunea:

www.ccn-cert.cni.es

CCN-CERT IA-01/16 Mehatxu-txostena

Ransomwarearen aurkako segurtasun-neurriak

CCN-CERT-a Zentro Kriptologiko Nazionaleko (CCN) informazioak jasandako segurtasun-gertakariei erantzuna emateko gaitasuna da. CCN-CERTak sailkatutako sistemek eta administrazio publikoen eta interes estrategikoko enpresen eta erakundeen sistemek jasotako ziber-erasoen gaineko erantzukizunak ditu. **IA-01/16 Mehatxu-txostena — Ransomwarearen aurkako segurtasun-neurriak** argitaratu du. Haren bitartez, mota horretako gertakariak, gero eta ugariagoak eta

HIZTEGIA

[8] **Banner:** Web-orrietan gehitzen den Interneteko iragarpen-formatua da.

[9] **C&C server:** *Command and Control Server*, komandoko eta kontroleko zerbitzaria, makina zentralizatuak dira, eta komandoak bidaltzeko (jarrai-bideak) eta *botnet* (robot-sarea) baten parte diren ekipoen irteerak jasotzeko gai dira.

[10] **Exploit**: informazio-sisteman instalatutako aplikazioek eta sistemek dituzten ahuleziez baliatzen den software- edo kode-programa da. Bi mota egon ohi dira: ezagunak eta ezezagunak («*zero eguna*» ere deitzen zaie).

—PDF—, nabigatzaileetan, instalatutako *plugin*etan[11]...) aurkitutako segurtasun-hutsuneak «ustiatzen» dituzte beren etekinerako. Tresna mota horiek erasotzaileen (ziber-kriminalak) partez eros dezakete, eta azken erabiltzaileari entregatu nahi dioten *malware*a barne har dezakete. Zenbait eratan instalatu daitezke: ezkutuko deskargen bidez, webgunearen urrakortasunaren bidez, ofimatikako fitxategietako makroen bidez... Erabiltzaile batek konprometitutako webgune batetik (webgunearen ahulezia batez baliatuz ziber-delitugile batek instalatu duen ezkutuko *iFrame*[12] bat duen webgune batetik, esate baterako) nabigatzen duenean, ezkutuko *iFrame*ak *exploit* bat duen beste webgune batera bidaliko dio. *Exploit*ak erabiltzaileren makinan bere lana egingo du, deskargatu eta exekutatu denean. Jarduteko modu bat da *banner*ak erabiltzea, adibidez. Normalean ziber-kriminalek ordaintzen dituzte iragarki horiek (orokorrean pornografiako web-orrietan txertatzen dira), eta kode bat txertatzen zaie, erabiltzailea bigarren webgune batera bidal dezaten. Webgune horretatik *exploit kit* bat deskargatzen eta exekutatzen da pertsona horren ordenagailuan.

Horregatik, aurrerantzean aipatuko dugun bezala, prebentziozko neurririk garrantzitsuenetako bat da **sistema eguneratuta mantentzea, azkeneko segurtasun-adabakiekin**.

- **Urruneko mahaigaineko zerbitzuak (RDP, *Remote Desktop Protocol*)**

Hainbatetan, zerbitzu horiek ez dira oso ziurrak sarbide-pasahitzei dagokienez. Hori dela eta, hiztegi bidezko erasoak gelditzeko ahulak dira (sarbide-hitz sorta bat era automatizatuan erabiltzea legez kanpoko sarbidea izateko).

- **Beste *malware* baten bidez**

Software gaizto jakin batez kutsatutako sistema bat *ransomware*a deskargatzeko eta exekutatzeko erabil daiteke.

*RANSOMWARE*AREN BIDEZKO ERASO BAT SAIHESTEKO NEURRIAK

Prebentziozko neurriak ***Ransomware*aren kontrako segurtasun-neurriak** izeneko **CCN-CERT IA-01/16 Mehatxuen txostenean** (ikus «*Mehatxu-txostena*» taula):

1. Garrantzitsuak diren datuen aldizkako **segurtasun-kopiak** (*backups*) mantentzea: kopiak **isolatuak** eta beste sistema batzuekiko **konektibitaterik gabe** mantendu behar dira (*ransomware*ak eragindako ordenagailuari konektatutako sistema guztiei eragin diezaieke; adibidez, **CryptoLocker** izenaz ezagutzen den *ransomware*ak ordenagailuan muntatutako unitate guztietan barrena ibiltzeko eta zerrendatzeko gaitasuna du, USBak edo sare-unitateak direla). Horrez gain, zerbitzu jakinetara sartzeko metodo gisa, VPN (*Virtual Private Network*) erabiltzeko gomendatzen da; izan ere, lehen esan bezala, *ransomware*ko kutsadura asko urruneko mahaigaineko zerbitzuen bidez sartzeagatik sortzen dira.
2. **Sistema eguneratuta** mantentzea (sistema eragilea gehi instalatutako programak)

Microsoften EMET tresnak

EMET (*Enhanced Mitigation Experience Toolkit*) tresna multzo bat da, eta softwarean segurtasun-ahuleziak ustiatzea saihesteko erabiltzen da.

Hori lortzeko, segurtasuna arintzeko teknologiak erabiltzen ditu EMETek. Teknologia horiek erasotzaileak softwarearen ahuleziez baliatzeko saihestu behar dituen oztopoak eta babes bereziak dira. Segurtasuna arintzeko teknologia horiek ez dute bermatzen segurtasunaren ahuleziak ezin direla ustiatu. Baina beren helburua da ustiatzea **ahal bezain beste zailtzea**.

Horrez gain, EMETek SSL/TLS ziurtagiriak finkatzeko konfigura daitekeen ezaugarri bat eskaintzen du, *Certificate Trust* izenekoa (konfiantzazko ziurtagiriak). Ezaugarri hori gako publikodun azpiegiturez (PKI, *Public Key Infrastructure*) baliatzen diren bitartekarien erasoak hautemateko (eta gelditzeko, EMET 5.0rekin) diseinatua dago.

EMETek Microsoft .NET Framework 4.0 behar du.

https://support.microsoft.com/es-es/kb/2458544

HIZTEGIA

[11] **Plugin-ak**: konektoreak, luzapenak, aplikazioak edo programak dira, eta beste aplikazio edo programa batekin harremanetan jartzen dira, funtzionalitate jakin bat emateko. Orokorrean oso espezifikoak izaten dira funtzionalitate horiek.

[12] **iFrame**: txertatutako markoa, HTML-dokumentu bat (*HyperText Markup Language*, hipertestuko marka-hizkuntza, markatze-lengoaiari egiten dio erreferentzia, web-orriak osatzeko) beste HTML-dokumentu baten barruan eransteko aukera ematen du.

segurtasun-adabakiekin: JAVA makina birtualeko, Flasheko edo Adobeko eguneratu gabeko bertsioak dira kutsatzeko bide nagusietako bat (lehen esan bezala, *exploit kits*ek instalatutako softwarearen segurtasun-hutsuneak ustiatzen dituzte).

3. **Antibirus-programak eguneratuta** mantentzea (kode kaltegarriko azken sinadurekin) eta suebakia ondo konfiguratzea aplikazio mailan (zerrenda zuriko aplikazioetan oinarrituta —*white listing*—, sistema eragilea baimenik ez duten eta kaltegarriak diren programetatik babesten duena).
4. **Posta elektronikoko zerbitzuak *anti-spam* sistemak izatea** (zabor-postaren aurkakoa), kutsatzeko bide ohikoenetako bat zabor-postari erantsitako dokumentua da eta.
5. **Segurtasun-politikak ezartzea**, *ransomware*ak erabilitako direktorioetatik fitxategiak zabaltzea ezinezkoa izan dadin, adibidez, honako hauetatik: App Data, Local App, etab. Politikak ezartzeko tresnak daude, halanola, CryptoLocker Prevention Kit eta AppLocker.
6. **Kode kaltegarriaren eta C&C Serveraren arteko komunikazioa ekiditea** (dagoeneko entregatzeko eta hedatzeko mekanismoen barruan komando- eta kontrol-zerbitzariak duen funtzioa azaldu dugu), domeinu eta zerbitzari bidezko trafikoa IDS/IPS[13]-ak erabiliz blokeatuz.
7. **EMET motako** edo antzeko **tresnak erabiltzeko** gomendatzen da (ikus «*Microsoften EMET tresnak*»), nabigatzailea eta ofimatikako aplikazioak babesteko.
8. **Administratzaile-pribilegioak dituen kontuak ez erabiltzea** erabat beharrezkoa ez bada. Horrela, *ransomware*-ekintza baten eragina murriztuko dugu; izan ere, administratzaile-kontu batetik mota guztietako ekintza kaltegarriak egin daitezke.
9. **Sarbide-kontroleko zerrendak mantentzea sarean mapatutako unitateentzat**. Era horretan, kutsadura egotekotan sare-unitateak enkriptatu ahal izatea saihestuko dugu (unitate horietan idazketa-pribilegioak mugatuz).
10. **Javascript-eko[14] blokeatzaileak erabiltzea nabigatzailean**
11. **Luzapenak erakustea ezagunak diren fitxategi mota guztietarako**. Neurri hau hartzearen arrazoia da *ransomware* batzuek bi luzapeneko fitxategi kaltegarriak erabiltzen dituztela, exekutatu daitezkeen fitxategi kaltegarriak direla ezkutatzeko (adibidez: .PDF.EXE; horrela, erabiltzaileak .PDF luzapenarekin bukatzen den fitxategi-izen bat ikusten du soilik).
12. **«Anti-Ransom»[15] tresna instalatzeko gomendatzen da**, *ransomware* motako kutsadurak sortutako eragina arin dezakeena. Tresna hori *honeypot* (*ezti-poto*) kontzeptuan oinarritzen da, hau da, gertatzen diren erasoak erakartzen eta aztertzen ditu, kontrolpeko ingurune batean: erabiltzaile-karpeta bat sortzen da, eta erabilgarriak eta *ransomware*ak enkripta ditzakeen dokumentuak uzten dira bertan (*honeyfiles* izenarekin ezagutzen dira), orduan, karpeta horretako fitxategiek izaten ditzaketen aldaketak aztertzen ditu; aldaketa horiek gertatzen badira, aldaketak egin dituen prozesua hautematen du, prozesuaren memoria iraultzen du enkriptazioaren kodea aurkitzeko eta prozesua «hiltzen» du.
13. **Makina birtualak erabiltzea**. Teknikoki, ingurune birtual batean zailagoa da *ransomware* eraso bat gauzatzea.

ZER EGIN BEHAR DA ERASO BAT GERTATZEN DENEAN?

Ransomware erasoetako asko gizarte-ingeniaritzan oinarritzen dira (iruzurrean oinarrituta dagoena). Eraso horiek egiteko, posta elektronikoa darabilte, eta, horren bidez, posta elektronikoa jaso duen pertsonak webgune jakin bat zabaltzea edo fitxategi konkretu bat exekutatzea lortu nahi dute. Horregatik, eraso mota horiek saihesteko, oso garrantzitsua da azkeneko erabiltzaileek jasotzen duten **kontzientziazioa** eta **prestakuntza**.

Ransomware baten erasoa jaso dugula baldin badakigu, sare-ingurune batean egin behar dugun lehenengo gauza da sarearen kablea deskonektatzea, edo hari gabeko sarea (Wi-Fi) desgaitzea. Jarraian, gertakaria jakinarazi behar diogu informatikako larrialdietako erantzun-taldeari, erabiltzaileari arreta emateko gure zentroari (Eusko Jaurlaritzako Sare Korporatiboaren erabiltzailea izatekotan, Erabiltzailearen Laguntza Zentroari —ELZ/CAU— deitu beharko zaio), eta abarri; izan ere, haiek balioztatuko dituzte gertakariak eta egon daitezkeen konponbideak, erasoa jaso duen pertsonak emandako informazioaren arabera. ❑

HIZTEGIA

[13] **IDS/IPS**: ingelesez *Intrusion Detection System* (IDS) eta *Intrusion Prevention System* (IPS), hautemate-sistemak eta intrusioak saihesteko sistemak. Intrusio bat erabiltzaile edo prozesu gaizto batek eragindako ekintza-segida da, ekipo edo sistema batean baimenik gabe sartzea xede duena.

[14] **Javascript:** Programazioko lengoaia interpretatua da (erabiltzailearen web-nabigatzailean exekutatzen da), eta objektuei zuzenduta dago. Testua, animazioak, eta abar agertzen diren webgune dinamikoak sortzeko erabiltzen da. Web-orrietan berariazko funtzionalitateak sortzeko aukera ematen du.

[15] **Ransom-aren aurkako tresna:** «ezti-poto» (*honeypot*) kontzeptuan oinarritutako tresna. Ikusi informazio gehiago eta tresnara sarbidea:

http://www.security-projects.com/?Anti_Ransom

ALBOAN:

Eustaten Informazio Sistemen sailak ISO9001 ziurtagiria jaso du

«Ziurtagiria lortzeak ez du esan nahi bukaera heldu dela. Prozesuak etengabe hobetzearen barruko lorpen bat gehiago baino ez da»

Artikulu honetan gure Eustateko kideek beren Informazio Sistemen sailerako **ISO9001 ziurtagiria** lortzeko egin duten ibilbidea azalduko dizuegu (zehazki, kalitatea kudeatzeko sistemarako).

Zalantzarik gabe, lorpen garrantzitsua da hori, eta horren helburua da, Informazio Sistemen sailak Eustateko gainerakoei eskaintzen dizkien zerbitzuak etengabe hobetzea, bai eta jadanik ezarrita dauden barneko kudeaketa-prozesu eta -sistemak hobetzea ere.

AURREKARIAK

Kalitate-sistema ezartzea (eta ondorengo ziurtagiria lortzea) zenbait urtetako lanaren ondorioa izan da, eta duela urte batzuk hasitako zenbait ekimen finkatuz lortu da. Ekimen guzti horiek prozesu informatikoen sistematizazioarekin eta etengabeko hobekuntzarekin erlazionatuta daude: «Besaide» bultzatzea («Métrica 3»-an oinarritutako eta Eustatentzako egokitutako informazio-sistemak kudeatzeko eta garatzeko metodologia), proiektuak kudeatzeko Prozesua eta adierazleekin kudeatutako jardueren Katalogoa.

Proiektu horri ekiteko erabakia hartu baino urte batzuk lehenago, Eustaten lan-kultura **kalitatean eta etengabe hobetzean** oinarritzen zen jadanik. Une horretara arte, prozesuen Mapa eta zerbitzuen Karta bezalako elementuak ezarrita zituzten.

2009an, IKTen alorreko erakundeek erabilitako metodologien eta kalitate-ereduen azterketa bat egin eta gero, uste izan zen ISO ziurtagiriak martxan zeuden ekimen guztiak bultzatzera lagunduko zuela.

Bada, 2010ean ekimenak sistematizatzeko eta lerrokatzeko neurrietan lan egiten hasi ziren, Eustaten «*Informatikako eta Telekomunikazioetako 2013-2016 plana*»-ren markoan ziurtagiri-prozesua lantzeko helburuz.

2013an ISO9001 ziurtagiri-proiektuari ekiteko behin betiko erabakia hartu zen, Eustaten **informatika-sailarentzat** eta hari lotutako lan-prozesuentzat. Lan hori 2014 eta 2015 artean gauzatu zen, fase ezberdinetan.

2014an, adibidez, proiektuaren irismena zehaztu zen, proiektuaren arduradunak izendatu ziren eta ISO9001 kalitate-sistemari buruzko dagokion prestakuntza egin zen.

Geroago, kalitate-sistema definitu zen eragindako sailetako bakoitzean: dokumentazioa kudeatzea, proiektuak kudeatzea (aplikazioak garatzea), sistema informatikoak kudeatzea (komunikazioak, segurtasuna), kontratazioa eta giza baliabideak.

FASEA	2009 ... 2013	2014	2015
Aldez aurretiko fasea			
1. fasea: Prestakuntza eta abiatzea			
2. fasea: Kalitate-sistema definitzea			
3. fasea: Sistema ezartzea			
4. fasea: Sistemaren funtzionamendua			
5. fasea: Kanpo-ikuskaritza			

Fase horretan misioaren, ikuspegiaren eta balioen eta Kalitate-sistemaren arteko koherentzia berrikusi zen, eta informatikako prozesuko Mapa egokitu zen.

2014. urte bukaera aldera, sistema behin betiko ezarri zen. Proiektuak kudeatzeko eta definitutako Besaide-araudia betetzeko tutorazioak egin ziren.

2015. urte hasieran sistema erabat ezarri zen. Proiektuen tutorazioarekin aurrera egin zen eta sistemaren lehen ikuskaritza egin zen. Aurrerago, garatutako prozesu guztiak finkatu eta gero, ikuskaritza 2015eko maiatzaren 19an izan zen, eta Eustatek **kalitate-ziurtagiria** lortu zuen.

LORPENAK

ISO ziurtagiriko proiektuak honako hauek lortzeko, besteak beste, aukera eman dio Eustati:

- ✓ Proiektuak kudeatzeko eta plangintza egiteko metodologia uniformea definitzea eta ezartzea, egindako jarduera eta proiektu guztientzat.
- ✓ Jardueraren plangintza egitea, hasierako plangintzaren eta egindako jardueraren artean egon daitezkeen desbideratzeak kontrolatuz.
- ✓ Proiektua kudeatzeko jarduerek eta Besaide-metodologiak ezarritako jarduera teknikoek eta dokumentazioak bat egitea.
- ✓ Baliabide-beharren azterketa eta horien barne-kudeaketarako edo azpikontratazioetarako aurreikuspena hobetzea.
- ✓ Adierazleen aginte-taula oso bat ezartzea, erakundearen estrategiarekin eta Eustaten Zerbitzu-Kartarekin lerrokatuta dagoena eta erakundea etengabe hobetzera zuzentzen duena.
- ✓ Barne-bezeroei zerbitzuak sistematizatzea (produkzio estatistikoa), zerbitzu-mailako hitzarmenen edo ANSren bidez.
- ✓ Ondorioak ateratzea, hobetzeko ekintzak xedatzea eta proiektuen itxieran ikasitako gaiak zabaltzea.
- ✓ Erakundeari metodoak eta tresnak ematea, erakundera gehitzen diren pertsona berriak prestatzea eta integratzea errazteko.
- ✓ Prozesu bidezko kudeaketan eta etengabe hobetzean oinarritutako ISO9001 ziurtagiria, beraz, EFQM enpresa-bikaintasuneko ereduarekin lerrokatuta dagoena.

ARRAKASTARAKO FAKTOREAK

Ziurtagiria lortzeko, honako faktore hauek funtsezkoak izan dira:

- Zuzendaritzaren lidergoa eta beharrezkoak ziren jarduerei lehentasuna ematea
- Kalitate-kudeaketako sistemako (KKSA) eta gainerako prozesuetarako arduradun bat izendatzea. Arduradunek sistemaren definizioan eta ezartzean aktiboki esku hartu dute.
- Kalitate-batzorde bat xedatzea, erantzukizuneko, azpi-zuzendaritzako, arloko burutzako eta kalitate-arduraduneko pertsonez osatua dagoena.
- Informatika-saileko langileak kalitate-sistema finkatzeko tartean sartzea.
- IKTen alorretik kanpoko erakundeek antzeko sistemak ezartzean, eta, zehazkiago, softwarea garatzean, duten aldez aurreko esperientzia kontrastatzea.
- Sistema definitzean parte hartuko duten pertsonak aldez aurretik prestatzea: Kalitate-batzordea eta Koordinatzaileak.
- Eta landu beharreko prozesu-alor ezberdinetan:
  - Informazioa biltzeko bilera, prozesuaren arduradunaren eta KKSAren esku-hartzearekin. Bertan, prozesuaren oinarrizko funtzionamendua, tartean dauden dokumentuak definitzen dira, eta horrela, prozesua kudeatzeko eta egokitzeko aukera ematen duten eragileak sortuko dira.
  - Eustaten langileak prozesuak balidatzea eta ezartzea, maila guztietan: prozesuaren arduraduna, KKSA eta goragoko arduradunekin edo kolaboratzaileekin konfirmatzea.
  - Sistema tutorizatzea: bilerak prozesuen arduradunekin, jarraipena egiteko.

HURRENGO URRATSAK

Eustaten ezarritako kalitate-sistema bizirik dago eta hobetzeko eta mantentzeko prozesu baten barruan dago. Ziurtagiria lortzeak ez du esan nahi bukaera heldu dela. **Prozesuak etengabe hobetzearen barruko lorpen bat gehiago baino ez da**.

Gaur egun, balioesten ari dira garapen arineko metodologiei, proiektuen etengabeko jarraipenari, metodologiak txertatzeari, IKTen (CMMi, ISO27000, ITIL, PMP...) berariazko ereduei eta adierazleak eta kalitate-erregistroak kudeatzeko automatizazioari lotutako hobekuntzak egitea. ❑

«ISO9001 arauaren helburu nagusia Informazio Sistemen sailak Eustateko gainerako sailei eskaintzen dizkien zerbitzuak etengabe hobetzea da»

[**Informazio gehiago**]:

Eustaten webgunea

www.eustat.eus

Eustat

ALBOAN

BERRI LABURRAK!!

55. zk.

2016ko martxoa

eSIM txartela

Aurreikusi da 2020 urtean munduan 10.500 milioi gailu mugikor konektatuta egongo direla. Gailu horiek oraingo txartel fisikoaz, SIMaz, (*Subscriber Identity Module*, abonatuaren identifikazio-modulua) askatzeak aukera berri bat ekarriko du, batez ere, urruneko makinen (M2M) eta kontsumo-elektronikoaren arteko komunikazioetarako.

SIM txartel fisikoa eSIM, SIM txertatua (murgildua edo inkrustatua), SIM elektronikoa, SIM birtuala edo SIM GSMA *Embedded* izenekin ezagutzen denarengatik trukatuko da; **fabrikan instalatuko da gailuan, hardware-elementu baten gisa** (plakan inplantatutako *txip* txikia). Telefono mugikorrei dagokienez, operadorez aldatzea sinpleago eta azkarrago bihurtuko du. Hala ere, gailu horietan ez dira 2017ko bukaera aldera arte instalatuko.

Operadoreak eta fabrikatzaileak ados jarri dira, hardwarean aldez aurretik instalatutako txartel birtual komun bat sortzeko estandar bat ateratzeko. Txartela edozein telefonia-enpresatako informazioarekin kargatu ahal izango da (elkarreragingarritasuneko profila), eta, ondorioz, gaur eguneko SIM txartela baztertuko da. 2016ko *Mobile World Congress*ean, telekomunikazioetako operadoreen munduko elkarteak (GSMA) eSIMaren ezaugarri teknikoak aurkeztu zituen.

Lehenengo esperientziak edo piloto-probak makinaz makinako (M2M) ekipamenduekin egingo dira, autoetan edo segurtasun-sistemetan eta erloju inteligenteetan instalatutakoak.

Gailu mugikor inteligenteetarako SIM mota berriaren abantailetako bat da **gailu bakarretik zenbait SIM administratu ahal izango direla** (SIM anitzeko gailuak). Halaber, herrialdetik ateratzen garenean, atzerriko operadoreetan alta emateko prozesua erraztuko du eSIMak. Horrek *roaming*aren kostuak arintzeko lagunduko du.

SALEren webgune berria

SALE (*Software Askea/Libre Euskadin*) Eusko Jaurlaritzaren software librea babesteko bulego teknikoa identifikatzen duen marka da. Jaurlaritzak 2010ean abiatu zuen ekimen hori, Informatikako eta Telekomunikazioetako Zuzendaritzaren bidez.

Ekimen horrek web-orri bat zuen, eta web-orri horren ingurune teknologikoa LAMP (Linux, Apache, MySQL, PHP) motako arkitektura batean zuen euskarria.

Aurten, webgune zaharreko eduki guztiak (informazioa, artikuluak/*post*, irudiak, estekak...) Eusko Jaurlaritzaren eduki korporatiboen kudeatzailera mugitu dira berriki, diseinua eguneratzeko eta euskadi.eus atari korporatiboko azpiegiturari probetxua ateratzeko.

Webgune berria erabilgarri dago jadanik, eta bere ezaugarri nagusia da *responsive design*a, hau da, edukia sartzen ari garen gailura egokitzen da, dela telefono mugikor bat, dela ordenagailu bat edo dela *tablet* bat.

Webgune berriak zenbait atal ditu:

- **Nabarmengarriak**: webgunearen goiko aldean SALEk egin eta argitaratu dituen azken hiru artikuluak edo iragarkiak nabarmentzen dira.
- **Deskribapena**: SALEri buruzko erreseina txiki bat gehitzen da, eta helburuak eta SALEk profila duen sare sozialen estekak aipatzen dira (*facebook*, *twitter*...).
- **Software librea**: atal horretan software librearen historia eta ezaugarri nagusiak zehazten dira, baita bere filosofia eta erreferentziarik garrantzitsuenak ere, beste alderdi batzuen artean.

SALEren webgunea: http://www.euskadi.eus/sale