SEGURTASUN-ESKULIBURUA

Izapidetze Telematikoko Aplikazioak (Platea)

Fitxategiaren izena: Segurtasun-eskuliburua - 2.1 bertsioa.doc		
Orrialdeak: 69		
Egilea: ITZ	***Nork berrikusia:***	***Nork onartua:***
Eguna: 2010-09-10	***Eguna:***	***Eguna:***

Bertsioa	**Data**	**Oharrak**
1.0	2009-06-04	Lehen zirriborroa
2.0	2009-06-25	Berrikusitako bertsioa
2.1	2010-09-10	Zuzenketa

Edukiak

0. Sarrera

Segurtasun-eskuliburua Izapidetze Telematikoko Zerbitzu Komunetan (ITZK) dago oinarrituta, hau da, Administrazio elektronikoa (e-Administrazioa) garatzeko azpiegitura teknikoa du oinarri, eta nahitaez erabili behar da izapidetze telematikoaren euskarri diren aplikazio informatiko guztietan.
Segurtasun-eskuliburu honek azpiegitura horri behar duen homogeneotasuna ematen dio izaera orokorreko segurtasun-neurriak, baita arlo teknikokoak eta antolakuntzakoak ere, ezartzen dituen heinean. Helburua da benetakotasuna, osotasuna, konfidentzialtasuna, erabilgarritasuna, informazioaren babesa eta trazabilitatea bermatzen direla ziurtatzea.

Segurtasun-eskuliburua bi zatitan banatzen da:

- **Segurtasun-politika.** Zerbitzu publikoak ematean erabilitako baliabide elektroniko, informatiko eta telematikoen segurtasunaren kudeaketari ekiteko asmoz, Euskal Autonomia Erkidegoko Administrazio Orokorraren eta bere Erakunde Autonomoen aldetik, helburu, ildo eta hartutako konpromisoari buruzko maila altuko adierazpena da.
- **Segurtasunari buruzko araudia**. Nahitaez bete beharreko segurtasun-neurriak. Informazioaren segurtasun-politikak jasotzen dituen helburuen oinarri diren arauen multzoaren bilduma da. Maila honetan segurtasun-helburuak zehazten dira, eta erabili beharreko arau orokorrak aurreratzen dira. Atal hori da, hain zuzen, dokumentu honen azken helburua.

1. Sarrera

Euskal Autonomia Erkidegoko (hemendik aurrera EAE) Administrazio Orokorraren eta bere Erakunde Autonomoen aktibo baliotsuenetako bat herritarrei zerbitzuak eskaintzeko erabiltzen duen informazio administratiboa da. Segurtasun-eskuliburu honen xedea EAEko Administrazio Orokorraren eta bere Erakunde Autonomoen informazioaren segurtasuna ziurtatzea da. Seguruak izan behar dira bai informazioaren prozesu telematikoa bera, bai informazioa tratatzen duten elementuak eurak: **izapidetze telematikoaren (e-Administrazioaren) euskarri diren aplikazio informatikoak**.

Aplikazio-esparru horren barruan, dokumentu hau segurtasunari buruzkoa da ikuspegi orokor batetik begiratuta, eta informazioaz gain, beste alderdi batzuk ere kontuan hartzen ditu, hala nola hardwarea, softwarea, sareak, datuak eta Izapidetze Telematikoaren Azpiegitura (hemendik aurrera, ITA) erabiltzen duten langileak.

Informazioa hiru egoera nagusitan egon daiteke: transmititzen, biltegiratuta edo prozesatzen egon daiteke, eta behar bezala babestu behar da, edozein dela ere dagoen egoera, edo egoera horietan erabiltzen diren baliabideak direnak direla.

Halaber, segurtasuna dela-eta, informazioak honako ezaugarriak ditu (hauek dira, edozein informazio edo dokumenturi dagokionez, baliabide elektroniko, informatiko eta telematikoak ─aurrerantzean, EIT Baliabideak─ erabiliz gero, zaindu behar diren bermeak:

- **Konfidentzialtasuna**: Ezaugarri horren bidez galarazten da informazioa baimenik gabeko norbanakoen, erakundeen edo prozesuen esku jartzea, edo horiei komunikatzea edo horien artean zabaltzea.
- **Osotasuna**: Ezaugarri horren bitartez bermatzen da informazioa prozesatu, garraiatu edo biltegiratu bitartean, ez dela baimenik gabe aldatu edo eraldatu. Aldaketarik egon bada, oso erraza da antzematea.
- **Erabilgarritasuna**: Ezaugarri horren bitartez, baimena duten erabiltzaileek informaziorako sarbidea dute behar dutenean, eta erabilera baimendua ukatzeko saiakuntzak galarazten ditu.
- **Benetakotasuna:** Ezaugarri horrek informazioa sortu duen erabiltzailearen nortasuna bermatzen du. Bidea ematen du ziurtasun osoz jakiteko nork bidali edo sortu duen informazio jakin bat.**Informazioaren babesa:** Zentzu zabalean, dokumentuak hondatu ez daitezen, haiek egonkortzeko eta babesteko erabiltzen diren prozesu eta eragiketen multzoa da. Baliabide digitalen kudeaketaz ari garenean, edozein dela ere baliabideen forma edo funtzioa, aintzat hartu behar dira dokumentuen bizitza-zikloa osatzen duten fase guztiak, dokumentuak zaintzeko neurriak ahalik eta agudoen ezartzeko. Beraz, informazioaren beraren ezaugarri bati buruz baino, informazioaren bizitza-zikloaren kudeaketaz ari gara hemen.
- **Trazabilitatea**: Ezaugarri horren bidez, informazioa sortzeko, aldatzeko eta kontsultatzeko eragiketetan gertatzen diren alderdi garrantzitsuak jakin daitezke, hala nola: Nork egin zuen eragiketa? Noiz egin zen eragiketa? Zeintzuk izan ziren eragiketaren emaitzak?

Dokumentu honetan garatutako Segurtasun-eskuliburuaren helburua benetako babes eraginkorra lortzeko oinarrizko arau iraunkorrak ezartzea da, eta horretarako EAEko Administrazio Orokorraren eta bere Erakunde Autonomoen informazioa erabiltzeko moduak prebentiboa, antzemangarria, erreaktiboa eta dinamikoa behar du izan. Hori da bide bakarra

herritarren informazioa zaintzeko, aipatutako bermeak ezartzeko, eta informazioaren tratamenduari eragiten dioten legeak betetzeko.

Hori guztia proportzionaltasun-printzipioa aplikatuta eta jarraituta garatuko da, eta, beraz, bakarrik izapide eta jardunbide bakoitzaren izaerari eta inguruabarrei egokitutako bermeak eta segurtasun-neurriak eskatuko dira. Halaber, herritarrei bakarrik eskatuko zaizkie eskatu diren xederako derrigorrezkoak diren datuak.

2. Aplikazio-eremua

Eusko Jaurlaritzak, berrikuntzaren eta administrazio elektronikoaren ereduaren barruan, e-Administrazio korporatibo eta komunerako azpiegitura bat ezartzea, abian jartzea, hobetzea, eta etorkizunari begira, garatzea erabaki du, herritarrek eta Eusko Jaurlaritzak erabiltzeko, baita Administrazioaren beraren informazioa, eta herritarrek eta herritarrentzat sortutako informazioa tratatzeko, Administrazioak bultzatutako beste ekimen batzuek erabiltzeko ere.

Erakundea horrela definitzea, hau da, herritarrei zerbitzuak emateko erakundea izatea, eta herritarrekiko harremanetarako teknologia berriak erabiltzea, erronka handia da EAEko Administrazio Orokorrarentzat eta bere Erakunde Autonomoentzat, batez ere, informazioaren erabilera partekatuari dagokionez, eta jakina, informazio horren segurtasunari dagokionez.

Arlo honetan erronka bikoitza da, alde batetik, Administrazioak herritarren informazioa babesteko betebeharra duelako, eta beste alde batetik, informazioaren teknologien erabilera baldintzatzen duten legeak bete behar dituelako – Datu Pertsonalak Babesteari buruzko Lege Organikoa, Informazio Gizartearen Zerbitzuen Legea, Sinadura Elektronikoari buruzko Legea, Herritarrek zerbitzu publikoetara jotzeko bide elektronikoak erabiltzeari buruzko Legea eta EIT baliabideen Dekretua–.

Horrenbestez, hau da dokumentu honen aplikazio-esparrua:

- e-Administrazioaren inguruneko aplikazioak (dokumentu honetan ulertzen den bezala). Zehazkiago, PLATEA azpiegitura teknologikoa, hura behar bezala erabiltzeko nahitaezkoak diren osagaiak (sare-elementuak, zerbitzuak, erabiltzaileen ekipoak, periferikoak, oinarrizko aplikazioak), eta plataforma hori erabiltzen duten aplikazioak. Dokumentu honetan zehar, aplikazio, osagai eta egitura multzo horri ITA esango zaio.
- ITAk tratatuko duen informazioa guztia. Hau da, EAEko Administrazio Orokorraren eta bere Erakunde Autonomoen langilek erabiltzen, zaintzen edo sortzen duten informazio guztia, euskarri magnetikoetan, optikoetan, paperean edo bestelako euskarrietan dagoena, bai beren lanpostuetan bertan dagoena, bai erabiltzaile anitzeko zerbitzarietan dagoena, azken hauek bertako instalazioetan egon ala ez.
- EAEko Administrazio Orokorraren eta bere Erakunde Autonomoen langileei eragingo dieten antolakuntza-prozesuak, ITAren aplikazioak erabiltzeari eta ezartzeari buruzkoak.
- Segurtasun-eskuliburu honen hartzaile objektiboak, ikuspegi funtzional batetik, honakoak dira:
    - ITA erabiltzen duten EAEko Administrazio Orokorreko eta bere Erakunde Autonomoetako funtzionarioak.
    - e-Administrazioaren euskarri diren aplikazioen garatzaileak. Garatzailea da e-Administrazioaren aplikazioa edo aplikazioen azpiegitura sortzeko prozesuan parte hartu duen edo erantzukizuna duen edozein pertsona. Garatzaileak erakundekoak bertakoak edo kanpokoak izan daitezke.
    - e-Administrazioaren euskarri diren baliabideen administratzaileak. Administratzailea e-Administrazioaren aplikazioa edo azpiegitura ondo funtzionatzeko parte hartzen duen edo erantzukizunak dituen edozein pertsona da. Administratzaileak erakundekoak bertakoak edo kanpokoak izan daitezke

  - e-Administrazioaren aplikazioei, informazioari, azpiegiturari, sareei edo inguruei eragiten dien funtzioren bat betetzen duten beste batzuk. Adibidez, inguru seguruetako mantentze-lanetako pertsonak.

- Kontratuaren ikuspegitik:
  - **Enplegatuak:** funtzionarioak, lan-kontratuko langileak eta behin-behineko langileak
  - **Kanpokoak**: beste erakunde batzuetako langileak dira. Harreman bereziak direla medio, hala nola, zerbitzu-kontratuak, asistentzia teknikokoak, eta aholkularitza-kontratuak, besteak beste, EAEko Administrazio Orokorrak eta bere Erakunde Autonomoek baliatzen dituzte.
- Segurtasun-neurri bakoitzaren hartzailea adierazteko lehen sailkapena erabiliko da (ikuspegi funtzionala). Bigarren sailkapena (kontratuaren ikuspegia) segurtasun-neurriak garatzean erabiliko da.

3. Segurtasun-politika

Eusko Jaurlaritzaren segurtasun-politikaren jarraibideak ***ISO/IEC 27002:2005***[1] estandarraren arabera zehaztu dira, segurtasunari buruzko erreferentzia-esparru bat, nazioartean babestuta eta onartuta dagoena. Segurtasunari buruzko teknologia-, antolamendu- eta prozedura-esparru horren oinarria informazio-aktiboak babesteko arauen edo neurrien, estandarren prozeduren eta segurtasun-tresnen multzoa izango da.

Ondoren, segurtasun-politikak eta segurtasunari buruzko araudiak barne hartzen dituzten segurtasun-domeinuak azaltzen dira:

3.1. Segurtasun-politika

Domeinu honek informazioaren segurtasuna kudeatzeko eta babesteko jarraibide orokorrak ematen ditu, herritarrei eman beharreko zerbitzuen betekizunekin eta indarrean dagoen araudiarekin bat etorriz. Zuzendaritzak politikaren ildoak argi ezarriko ditu zerbitzuaren helburuen arabera, eta informazioaren segurtasunarekin duen konpromisoa erakusteko, informazioaren segurtasun-politika argitaratuko eta mantenduko du. Informazioaren segurtasunaren gaineko jarrera orokorreko domeinua denez, sarreran aipatutako berme guztiak hartu behar ditu kontuan: konfidentzialtasuna, osotasuna, erabilgarritasuna, benetakotasuna, babesa eta trazabilitatea.

Informatika eta Telekomunikazioen Zuzendaritzak (aurrerantzean, ITZ), Berrikuntzaren eta Administrazio Elektronikoaren Zuzendaritzarekin eta Herritarrei Arreta Emateko Zuzendaritzarekin batera, e-Administrazioko esparruko Segurtasun-eskuliburua egiteko ardura du. Tramitazio telematikoaren oinarri diren aplikazio informatikoen esparruan segurtasuna aplikatzeko esparrua zehazteko helburuarekin, segurtasun-bermeak –osotasuna, benetakotasuna, erabilgarritasuna konfidentzialtasuna, babesa eta trazabilitatea– betetzen direla ziurtatzen duten politikek, araudiek, estandarrek eta prozedurek osatzen dute Segurtasun-eskuliburu hori. Segurtasun-politika honek Segurtasun-eskuliburuaren ataletan zehaztu behar diren segurtasunari buruzko ildo nagusiak ezartzen ditu.

ITZ-k, Segurtasun-eskuliburua egiteko ardura duen aldetik, hura sortzeko, aldiro-aldiro berrikusteko, egokitzeko eta Eusko Jaurlaritzaren plan estrategikoekin bat etortzeko erantzukizuna hartzen du bere gain. Horrez gain, Segurtasun-eskuliburua eguneratu egin behar da honakoak kontuan hartuta: indarrean dagoen araudian egondako aldaketak, auditoretzen edo arrisku-azterketen emaitza nabarmenak, Segurtasun-eskuliburua hobetzeko iradokizunak, etab.

3.2. Informazioaren segurtasuna. Antolakuntzako alderdiak

Domeinu honek segurtasuneko bi helburu dauzka: (1) Informazioaren segurtasuna kudeatzea Administrazioaren barruan eta (2) kanpokoek eskura ditzaketen baliabideen eta informazio-aktiboen segurtasuna zaintzea. Lehenengo helburua lortzeko, funtsezkoa da Eusko Jaurlaritzak informazioaren segurtasun-politika onartzea, segurtasun-rolak esleitzea, eta Administrazio osoan segurtasuna ezarri dela berrikustea eta koordinatzea. Bigarren helburua lortzeko, funtsezkoa da kanpokoek ITAra egindako edozein sarrera, eta prozesatutako eta ezagutzera emandako informazioa kontrolatzea.

---

[1] 'Information technology – Code of practice for information security management', ISO/IEC 27002:2005 arauari dagokiona.

Segurtasun-politika mantentzearen eta ezarri ondoko jarraipena egitearen gaineko zaintzeari eta kontrolatzeari buruzko domeinu bat denez, sarreran aipatutako segurtasun-bermeak aintzat hartuko ditu: konfidentzialtasuna, osotasuna, erabilgarritasuna, benetakotasuna, babesa eta trazabilitatea.

Eusko Jaurlaritzak, EAEko Administrazio Orokorrean eta bere Erakunde Autonomoetan informazioaren segurtasunari buruzko helburuak ezartzen hasteko, lortzeko eta mantentzeko antolakuntza-baliabide batzuk eskaintzen ditu.

Antolamendu-egitura hori abenduaren 18ko 232/2007 Dekretuan identifikatutako arduradunek osatuko dute.

- Justizia eta Herri Administrazio Saileko titularrari dagokio dokumentu hau onartzea. Dokumentuak informazioaren segurtasunerako baliabideen erabilgarritasuna ziurtatzen du, eta izapidetze telematikoaren euskarri diren aplikazio informatikoetan ezarritako segurtasun-maila zehazten du.
- ITZren betebeharra da, EIT baliabideen Dekretuaren arabera, segurtasun-eskuliburua egitea, azaldutako aplikazio-eremuaren barruan.

EAEko Administrazio Orokorrak eta bere Erakunde Autonomoek egiten dituzten proiektuen bizitza-zikloan parte hartzeko, izapidetze telematikoaren euskarri diren aplikazio informatikoetan, jakintza-arlo askotako taldeak osatu beharko dira, **informazioaren segurtasuna bizitza-ziklo horretako fase guztietan har dadin kontuan.**

Aldian-aldian, dauden ahulguneen, horiekin lotutako arriskuen eta ezarritako kontrolen berrikuspenak egingo dira.

Funtzionalitate-, prezio-, errendimendu- edo gaitasun-betekizunez gain, kanpokoekin egindako zerbitzu-kontratuek segurtasunari buruzko berariazko baldintzak eduki behar dituzte, teknologiari buruzkoak eta hura instalatu, konfiguratu, mantentze-lanak egin edo ezabatzen duten langileen jarduerei buruzkoak.

Era berean, zerbitzuak kanpora ateratzeko kontratuek segurtasunari buruzko berariazko baldintzak eduki behar dituzte, teknologiari buruzkoak eta zerbitzu horiek ematen dituzten langileen jarduerei buruzkoak. Administrazioko langileen ardura da lana kanpora ateratzeak dakartzan arriskuez jabetzea, eta horiek eraginkortasunez kudeatzen direla ziurtatzea.

3.3. Aktiboen kudeaketa

Domeinu honek aktiboen babes egokia eskaintzen du (mantentze-lanak, inbentarioa eta sailkapena, barne). Aktiboen jabeak identifikatzen ditu. Horien ardura da aktiboen gainean eduki behar diren kontrolak mantentzea. Informazioa igortzen, biltegiratzen edo prozesatzen duten baliabide edo euskarri guztiak hartu behar dira kontuan. Adibidez: ordenagailu eramangarriak, komunikazio mugikorrak, eta PLATEAren osagaiak. Horiek guztiak sailkatu behar dira, ziurtatu behar delako informazioak babes-maila egokia duela. Informazioa sailkatu beharko litzateke, informazio hori erabiltzen denean, daukan premia, dauden lehentasunak eta espero den babes-maila adierazteko. Domeinu honek eragin berezia du konfidentzialtasun-bermeari dagokionez; halere, nabarmendu beharra dago, arduradunak aktibo bakoitzeko esleitzeak, eta arduradun horiek aktiboen gaineko segurtasun-politika bete behar izateak, domeinua horizontala izatea dakartela, sarreran zehaztutako segurtasun-bermeei dagokienez. Hona hemen berme horiek: konfidentzialtasuna, osotasuna, erabilgarritasuna, benetakotasuna eta informazioaren babesa.

Izapidetze telematikoaren euskarri diren aplikazio informatikoen informazio-aktiboen inbentarioa eduki behar da, eta aktibo bakoitzak bere arduraduna eta jagolea izan behar du. Inbentario hori aldian-aldian eguneratu behar da.

Informazioaren segurtasunaren eta hura tratatzeko moduaren maila egokia ezartzeko xedez, informazio-aktiboak e-Administrazioaren jarduerarako noraino diren kontu handikoak eta zenbateraino diren kritikoak kontuan hartuta sailkatu behar dira. Informazioa sailkatzeko gidak egin behar dira, eta sailkapenarekin lotutako babes-neurriak.

3.4. Giza baliabideak eta segurtasuna

Domeinu honen bidez, aipatutako aplikazio-eremuaren barruko inbentarioko aktiboetara jo ahal duen edozein pertsonak, hau da, enplegatu guztiek (Eusko Jaurlaritzakoek, azpikontratatutako enpresetakoek, tratamenduaz arduratzen direnek eta horiek azpikontratatutakoek), enplegatuaren bizitza-ziklo osoan zehar (kontratatu aurretik, kontratatuta dagoen bitartean eta lan-harremana bukatu ondoren), segurtasunari dagokionez, informazio-sistemei eta baliabideei buruzko erantzukizunak onartzen dituztela eta haietaz jabetuta daudela ziurtatu nahi da. Ziurtatu nahi den lehen bermea konfidentzialtasuna da, eta horretarako enplegatuaren betebeharrei eta erantzukizunei buruzko klausulak jarriko dira. Beste helburu bat da lapurreta egiteko, iruzur egiteko eta instalazioak eta baliabideak gaizki erabiltzeko arriskua gutxitzea.

Eusko Jaurlaritzak prestakuntza egokia emango die erabiltzaileei Segurtasun-eskuliburu honi dagokionez, segurtasun-betekizunak eta legezko erantzukizunak barne.

Eusko Jaurlaritzaren informazio-sistemetan segurtasunak duen garrantzia ondo ezagutu behar dute erabiltzaileek. Segurtasuna eraginkorra izateko, erabiltzaileek jakin behar dute zer espero den haiengandik eta zein diren euren erantzukizunak, eta horiekin konpromisoa hartu behar dute. Ezarrita dauden segurtasun-neurri fisikoak eta logikoak zergatik jarri diren jakin behar dute, baita segurtasun-neurriak hausteak dakartzan ondorioak ere.

Eusko Jaurlaritzak komunikazio-plana ezarri behar du, segurtasunari buruzko enplegatuentzako prestakuntza-saioak barne hartzen dituena. Saio horiek berariazkoak izan daitezke, edo gaiarekin lotutako beste bilera batzuetan sar daitezke. Saio horien ordez, bestelako prestakuntza-tresnak erabili ahalko dira, euskarri magnetikoan banatuta edo Intraneten bidez.

3.5. Segurtasun fisikoa eta ingurumenekoa

Domeinu honek aipatutako aktibo fisikoak (ukigarriak) ziurtatu nahi ditu, sarbidea kontrolatuta eta kanpoko (ingurumeneko) gorabeheren aurka babestuta. Domeinu honek honako hauek bermatzen ditu: informazioaren erabilgarritasuna, osotasuna, erabilgarritasuna eta konfidentzialtasuna.

Izapidetze telematikoaren euskarri diren aplikazio informatikoen azpiegitura, eta horiek erabiltzen dituzten biltegiratze-euskarriak, euren eraikinetan nahiz zerbitzu-hornitzaileenetan edo hirugarrenenetan egon, kalte fisikoaren edo lapurretaren aurka babestuta egon behar dira, eta horretarako fisikoki sartzen uzteko kontrol-mekanismoak erabiliko dira, bertara baimena duten langileak bakarrik sartu ahal direla ziurtatzeko.

Helburu horrekin, azpiegitura hori sarbide murriztuko eremuetan jarri behar da, segurtasun-maila desberdinekin, eta bertara behar den baimena duten langileak bakarrik sartu ahalko dira. Maila bakoitzera egindako sarrerak sarrera-kontroleko mekanismoek erregistratuko dituzte, eta gerora auditoretzak egin ahal izateko gordeko dira.

Sistemak eta horiek duten informazioa behar bezala babestuta egon behar dira mehatxu fisiko edo ingurumenekoen aurka, nahitakoak nahiz halabeharrezkoak izan.

3.6. Komunikazioak eta eragiketak kudeatzea

Domeinu honek azpiegituraren ustiaketa modu seguruan eta era kontrolatuan egiten dela, bere egoera ikuskatzen dela eta arazoen berri ematen dela ziurtatu nahi du. Horretarako kontrol-helburu batzuk zehazten ditu: eragiketekin zerikusirik duten prozedurak eta erantzukizunak, hirugarrenen zerbitzuen kudeaketa, sistemen planifikazioa eta onarpena, kode gaiztoaren aurkako babesa, babes-kopiak, sare-segurtasunaren kudeaketa, biltegiratze-gailuen kudeaketa, sozietateen arteko informazio-trukaketaren kontrola, merkataritza elektronikoko zerbitzuen kontrola eta sistemen monitorizazioa. Domeinu honek, aurreko domeinuekin alderatuta, antolakuntzakoak baino kontrol tekniko gehiago zehazten ditu. Honako hauek bermatzen ditu: erabilgarritasuna, konfidentzialtasuna, osotasuna eta informazioaren babesa.

Informazioa tratatzeko baliabide guztiak erabiltzeko eta kudeatzeko, erantzukizunak eta prozedurak ezarriko dira. Horren barruan sartzen da erabiltzeko (operatzeko) jarraibide egokiak eta intzidentzien aurrean erantzuteko prozedurak finkatzea.

Hala komeni denean, atazak bananduko dira, azpiegitura, nahita edo axolagabekeriaz, gaizki erabiltzeko arriskua gutxitzeko.

Arretaz ibili behar da software gaiztoa ez sartzeko, eta sartu bada, antzemateko. Softwarean eta informazioa tratatzeko baliabideetan erraz sar daiteke software gaiztoa, hala nola, birus informatikoak, sareko harrak, Troiako zaldiak eta bonba logikoak. Erabiltzaileek softwarea gaiztoak edo baimenik gabekoak dituen arriskuak ezagutu behar dituzte; eta lanpostuetan, zerbitzarietan eta sare publiko zein pribatuetarako konexio-pasabideetan kontrolak eta neurri bereziak ezarri beharko dira halakorik sar ez dadin, edo behin sartuta, berehala antzemateko, Eusko Jaurlaritzaren informazio-sistemak, birusekin edo bestelako software gaiztoarekin, kutsa ez daitezen. Bereziki, funtsezkoa da arreta handia jartzea ordenagailu pertsonaletan birus informatikoak ez sartzeko edo antzemateko. Birusen aurkako mekanismoak nahitaez eguneratu behar dira, aldizka, eta modu erregularrean, Eusko Jaurlaritza osoan.

Onartu den babes-kopien estrategia lortzeko, jarraitu beharreko prozedura batzuk ezarriko dira, hau da, babes-kopiak egingo dira, gero saiakuntzak egingo dira ikusteko berreskuratzeko balio duten, gertakariak edo hutsegiteak erregistratuko dira, eta hala dagokionean, ekipoen ingurunea monitorizatuko da.

Administrazioaren mugak zeharkatzen dituzten sareen segurtasunaren kudeaketak arreta berezia eskatzen du, zehazki, kontrol eta neurri gehigarriak, sare publikoetan zehar doazen kontu handiko datuak babesteko. Behar diren kontrolak ezarri behar dira igorlea ordezkatzea galarazteko, eta igorritako informazioa inork alda ez dezan edo gal ez dadin, bai barne-sareetan kokatutako sistemekiko komunikazioetan, bai kanpoko sistemekin egindakoetan, horien euskarri diren plataforma, protokolo edo aplikazioak edozein izanda ere.

Dokumentuak, euskarri informatikoak (diskoak, zintak, etab.), sarrera edo irteerako datuak eta sistemaren dokumentazioa kalteen, lapurreten eta baimenik gabeko sarreren aurka babesteko behar diren prozedurak ezarriko dira. Kontu handiko informazioa duen Eusko Jaurlaritzaren edozein informazio-aktibo biltegiratu, erabili, garraiatu, ezabatu edo botatzen denean, ziurtatu beharko da baimenik ez duen inork ezingo duela informazio horretara jo edo informazio hori berreskuratu.

Erakundeen arteko informazio- eta software-trukaketak kontrolatu egingo dira, eta indarrean dagoen legeria guztia bete beharko da. Hitzarmen formaletan oinarrituta egingo dira trukaketak. Batetik bestera doazen euskarriak babesteko prozedurak eta arauak ezarriko dira. Kontuan

hartuko dira merkataritza, posta eta datu elektronikoen trukaketarekin (EDI, elkarreragingarritasun-zerbitzuak) lotutako segurtasunaren aldeko ondorioak, baita segurtasun-neurri eta -kontrolen baldintzak ere.

Eusko Jaurlaritzaren eduki publikoen zehaztasuna, garrantzia eta egiazkotasuna ziurtatzeko, baita informazioa zabalkuntza handiko hedabideetan argitaratzeari buruz indarrean dagoen legeria betetzeko ere, edukiak argitaratzeko prozesuetan azpiegitura berezia egon behar da, argitaratu nahi diren edukiak onartzeko aukera emateko.

Segurtasuneko intzidentziak konpondu ahal izateko, diziplina anitzeko antolakuntza-egitura sortu behar da.

3.7. Sarbide-kontrola

Domeinu honek segurtasunari buruzko alderdi garrantzitsu eta nabarmenetako bat hartzen du bere baitan: informazio-sistemetara sartzeko kontrolaren problematika. Horretarako, kontrol-helburu hauek jartzen ditu: sarbide-kontrolerako negozio-betekizunak, erabiltzaileen sarrerak kudeatzea, erabiltzaileen erantzukizunak, sareko sarbide-kontrola, sistema eragilearen sarbide-kontrola, aplikazioetara eta informaziora sartzeko kontrola, eta telelana eta mugikortasuna, e-Administrazioaren esparruan. Domeinu honek honakoak bermatzen ditu: benetakotasuna eta konfidentzialtasuna. Trazabilitate ona bermatzen duen oinarrizko kontrola ere bada.

Sareetara, sistemetara eta horietan dagoen informaziora sartzeko baimenak emateko orduan, kontuan hartuko da erabiltzaileak bakarrik euren lana egiteko behar dituzten baliabideetara eta informaziora sartu ahal izatea.

Prozedura formalak ezarriko dira sistemetarako eta zerbitzuetarako sarbide-eskubideen esleipena kontrolatzeko. Prozedura horiek erabiltzailearen sarbide-zikloko fase guztiak hartu behar dituzte bere baitan, erabiltzaile berrien erregistroarekin hasi eta sistemetara eta zerbitzuetara sartu beharrik ez duten erabiltzaileen erregistroari baja eman arte. Arreta berezia eskatzen du sarbide-eskubide pribilegiatuak nori eman erabakitzeak, horrek ematen baitie erabiltzaileei sistemaren kontrolak gainditzeko aukera.

Izapidetze telematikoaren euskarri diren aplikazio informatikoetara sartzeko, erregistratutako erabiltzaileak identifikazio-, autentifikazio- eta baimentze-prozesua gainditu beharko ditu. Erregistro-mekanismoak eta sarrerak eta sistemen erabilera monitorizatzeko mekanismoak ezarriko dira.

Erabiltzaile bakoitzaren sarbide-kredentzialak pertsonalak eta besterenezinak izango dira. Erregistratuta dagoen eta sarbide-kredentzialak dituen pertsona bakoitzak horien konfidentzialtasuna bermatu beharko du, eta behar bezala erabiltzen direla ziurtatu beharko du. Sistemetan mekanismo egokiak ezarriko dira, beste inork kredentzialak ikusteko modurik izan ez dezan.

Babes eraginkorrak baimena duten erabiltzaileen arteko elkarlana eskatzen duenez, erabiltzaileek garbi izan behar dute zein diren euren erantzukizunak sarbide-kontroleko neurrien eraginkortasuna mantentzeko orduan, bereziki, pasahitzen erabilerari dagokionez eta euren eskura jarritako materialaren segurtasunari dagokionez.

Zerbitzuetarako sarrerak, kanpoko zein barruko sareetatik, kontrolatu egin behar dira, erabiltzaileak sareetara eta zerbitzuetara sartzen direnean ez dituztela zerbitzu horiek arriskuan jartzen bermatzeko. Horretarako hauek erabiliko dira:

- Interfaze egokiak EAEko Administrazio Orokorraren eta bere Erakunde Autonomoen sarearen eta beste Administrazioen eta/edo Erakunde batzuen sare publiko zein pribatuen artean.
- Autentifikazio-mekanismo egokiak erabiltzaileentzat eta ekipoentzat.
- Erabiltzaileek informazio-zerbitzuetara egindako sarrerak kontrolatzea.

Sare publikoetatik izapidetze telematikoaren euskarri diren aplikazio informatikoetarako urruneko sarbideak transmititzen den informazioaren konfidentzialtasuna bermatu behar du, baita urruneko sarbide-zerbitzua erabiltzeko baimena duten erabiltzaileen nortasuna ere, autentifikazio-mekanismo sendoen bidez.

Ordenagailuetarako sarbidea mugatu behar da, bakarrik baimendutako erabiltzaileak sar daitezen. Ordenagailua erabiltzaile batek baino gehiagok erabiltzen badu, gai izan beharko litzateke:

- Baimendutako erabiltzaile bakoitzaren nortasuna identifikatzeko eta egiaztatzeko (eta hala badagokio, terminala eta edo haren kokapen fisikoa).
- Pasahitzen kalitatea bermatze aldera, pasahitzak kudeatzeko mekanismoak eskaintzeko.
- Hala dagokionean, erabiltzaileen konexioak edo konektatzeko ordutegiak murrizteko.

Susmagarriak edo ustekabekoak diren jokabideak antzemateko eta horiei aurre egiteko, jardueren erregistro-sistemak ezarri edo aktibatu behar dira, EAEko Administrazio Orokorraren eta bere Erakunde Autonomoen informazio-aktiboetan sistemek, aplikazioek eta erabiltzaileek egindako jarduerek sortutako datuak jasotzeko.

Sistema eramangarriak eta telelaneko urruneko sarbideak babesteko, araudiak, prozedurak eta berariazko teknikak ezarriko dira.

3.8. Informazio-sistemak eskuratzea, garatzea eta mantentze-lanak egitea

Domeinu honek segurtasuna informazio-sistemetan txertatuta dagoela ziurtatu nahi du. Horretarako, kontrol-helburu batzuk ezartzen ditu: informazio-sistemei (erositakoei edo garatutakoei) eragiten dieten segurtasun-baldintzak, aplikazioek behar bezala prozesatzea, kontrol kriptografikoak, segurtasuna fitxategi-sistemetan, segurtasuna garapen-prozesuetan eta laguntza teknikoko prozesuetan, eta ahulgune teknikoen kudeaketa. Domeinu honek honakoak bermatu nahi ditu: erabilgarritasuna, konfidentzialtasuna eta osotasuna.

Administrazioan hasten diren garapen-proiektuak, izapidetze telematikoaren euskarri diren aplikazio informatikoei zuzenean eragiten badiete, **segurtasuneko berariazko baldintzak beren bizitza-ziklo osoan** kontuan hartuta eraman behar dira aurrera.

Aplikazioak aipatutako eremuaren barruan garatzeko eta mantentzeko kontrolak eta erregistro egokiak jarri behar dira, segurtasuneko zehaztapenak behar bezala ezarri direla bermatzeko, eta hori programazioaren arloko segurtasuneko jardunbide egokiak kontuan hartuta egingo da.

Bereziki, arriskupeko informazioa babesteko, sistema eta teknika kriptografikoak erabiliko dira –zifratzea, sinadura digitala, nahitaez onartu beharra–, beste neurri eta kontrol batzuek babes egokia ematen ez dutenean.

Izapidetze telematikoaren euskarri diren aplikazio informatikoetan dagoen informazioa baimenik gabeko aldaketen aurka babestuta egon behar da, informazioaren osotasuna bermatuko duten mekanismoak erabilita.

Garapenaren bizitza-zikloko faseetan segurtasuna ezartzea errazteko, gidak, estandarrak, gomendioak eta prozedurak eskura jarri behar dira, hala nola kontrol kriptografikoak, gakoen kudeaketa, programazio segurua, etab.

Garapen informatikoko bizitza-zikloa osatzen duten inguruneak behar bezala bananduta edo segmentatuta egon behar dira, sistema bakoitzean eta guztietan. Halaber, inguruneetan dauden datuetara sartzea galarazteko edo datuak ez zabaltzeko, ekoizpen-ingurunearen eta gainerako inguruneen arteko datu errealen trukaketa kontrolatu behar da.

Garapen- edo proba inguruneetan, aplikazioentzat edo azpiegiturarentzat, probako datuen sortak eduki behar dira prestatuta, berariaz egindakoak, eta horietan datuen eta pertsonen arteko harremanak bananduta edo ezkutatuta egongo dira.

3.9. Informazioaren segurtasunari buruzko intzidentziak kudeatzea

Domeinu honek ITArekin eta e-Administrazioaren euskarri diren aplikazioekin lotutako gertakariak eta segurtasuneko ahulguneak jakinaraz daitezela bermatu nahi du, behar diren zuzenketa-ekintza egokiak egin ahal izateko. Domeinu honek, batez ere, hauek bermatu nahi ditu: erabilgarritasuna, konfidentzialtasuna eta osotasuna.

Gertakariak eta ahulguneak ahalik eta azkarren jakinaraz daitezela exijitu behar da (antzemandako edozein ahulgune edo susmo). Helburu hori lortzeko, prozedura eta bide egokiak ezarri behar dira (kudeaketa-kanal ezagunak); puntu hau 3.4 atalarekin dago lotuta (giza baliabideak eta segurtasuna). Informazioaren segurtasunaren gaineko kontzientziazio, prestakuntza eta trebakuntzari buruzko atala da.

Halaber, segurtasuneko intzidentziak kudeatzeko metodologia tinkoa aplikatzen dela bermatu behar da (erantzukizunak eta prozedurak ezartzea). Horrekin batera, etengabeko hobekuntzako prozesuak eta ebidentziak jasotzeko metodoak erabili behar dira.

Badago mekanismo bat segurtasuneko intzidentziak monitorizatzeko, horiekin lotutako kostuak kuantifikatzeko, eta ebidentziak jasotzeko.

Segurtasun-gertakariak jakinarazteko eta lehentasunak ezartzeko prozedura formalak ezarriko dira. Eragindako langile guztiek izapidetze telematikoaren euskarri diren aplikazio informatikoetan eragina izan dezaketen era guztietako gertakariak eta ahulguneak jakinarazteko prozedurak ezagutu beharko dituzte.

Segurtasun-gertakariak eta ahulguneak, behin jakinarazita, modu egokian kudeatzeko, erantzukizunak eta prozedura formalak ezarriko dira. Gainera, segurtasun-intzidentzien kudeaketa etengabe hobetzeko prozesu formal bat ezarriko da.

Intzidentzia bakoitzarentzat behar diren ebidentzia guztiak jasoko dira, indarrean dagoen legedia betetzeko.

3.10. Zerbitzuaren jarraitutasuna kudeatzea

Domeinu honek, hondamendia gertatuz gero, e-Administrazioaren aplikazioen euskarri den ITAren erabilgarritasuna bermatu nahi du. Helburua da ekintza-plan bat zehaztea, hondamendi baten ondorioak gutxitzeko. Domeinu honek honako hauek bermatzen ditu: osotasuna eta informazioaren babesa. Helburua da jardunaren jarraitutasuna kudeatzeko prozesu bat ezartzea, hondamendia gertatuz gero, EAEko Administrazio Orokorraren eta bere Erakunde Autonomoen prozesu kritikoak berreskuratuko direla ziurtatzeko. Administrazioaren jardunaren ikuspuntutik begiratuta, azpiegitura erabiltzeko moduan ez dagoen denbora-tartea maila onargarrietara jaitsi behar da, eta horretarako antolamendu-, teknologia- eta prozedura-kontrol batzuk jarri behar dira, bai prebentiboak, bai berreskuratzekoak.

Prozesu hori Zerbitzu-jarraitutasun Plan baten bidez garatuko da. Plana aldizka eta modu erregularrean onartu behar da, eta une oro eguneratuta eduki behar da. Horretarako, Eusko Jaurlaritzaren jardunaren euskarri diren edo harekin zerikusirik duten informazio-sistemen jarraitutasun ezak eragin dezakeen arriskua eta horrek dakarren eragina aztertu behar dira.

3.11. Betetzea

Arau-esparrua, eta arau-esparru horrek agintzen duen segurtasuneko edozein betekizun, bete daitezela du helburu domeinu honek, eta horretarako informazio-sistemetan Segurtasun-eskuliburu honen bidez garatutako segurtasun-politikak eta -estandarrak bete behar dira. e-Administrazioaren azpiegituraren eta aplikazioen auditoretza-prozesua ahalik eta eraginkorrena izatea ere lortu nahi du. Domeinu hau horizontala da eta sarreran zehaztutakoak bermatzen ditu: konfidentzialtasuna, osotasuna, erabilgarritasuna, benetakotasuna eta informazioaren babesa.

Eusko Jaurlaritzak, herritarren aurrean, informazioaren segurtasunari buruz indarrean dagoen legedia betetzeko erantzukizuna hartzen du. e-Administrazioaren aplikazioen informazio-aktiboen segurtasunari, zuzenean zein zeharka, eragiten dieten araudiak, legeak eta kontratupeko baldintzak, informazioaren segurtasunari buruzkoak, identifikatu behar dira.

Arlo guztien erantzukizuna da beren jarduera-eremuan aplikatu beharreko legedia, indarrean dagoena, ezagutzea eta betetzea.

Bereziki, Datu Pertsonalak Babesteko Lege Organikoak eta harekin lotutako Segurtasun Neurrien Erregelamenduak zehazten dituzten mekanismoak eta prozedurak hartu behar dira kontuan, hori baita informazio pertsonalaren segurtasunari buruzko erreferentziazko legedia.

Eusko Jaurlaritzako langileek isilpekotasunaren betebeharra daukate, hau da, euren lan-jardunean eskuratutako inolako informaziorik ez zabaltzeko konpromisoa dute.

Izapidetze telematikoaren euskarri diren aplikazio informatikoei, aldiro-aldiro, auditoretza egin behar zaie. Helburua da segurtasunari buruzko araudia eta informazioaren segurtasunari buruz indarrean dauden prozedurak eta jarraibideak betetzen direla egiaztatzea.

Auditoretza-prozesuak epe laburrera planifikatutako segurtasun-ekimenak betetzen direla egiaztatu behar du, kontrolak zein mailataraino ezarri diren, eta segurtasunaren ikuspegitik zenbateraino diren eraginkorrak aldian-aldian berrikusi behar du. Auditoretza-prozesua Eusko Jaurlaritzak bere aldetik egiten dituen barne-egiaztapenetatik bereizita egon behar da.

Jarraipen- eta auditoretza-mekanismoak, ustekabean nahiz asmo txarrez, inork ez ditzan desaktibatu, behar diren neurriak ezarriko dira.

ITAren eta e-Administrazioaren aplikazioen segurtasuna dela-eta, ikuskapenak egingo dira, aldian-aldian.

3.12. Segurtasunaren kudeaketa

Aplikazio-eremuaren barruan, Informazioaren Segurtasuna Kudeatzeko Sistema (aurrerantzean, ISKS) ezarriko da, UNE-ISO/IEC 27001:2007 (ISO/IEC 27001:2005) estandarrean oinarrituta, segurtasuna etengabe hobetzeko prozesua ezartzeko helburuarekin.

Horretarako, aldian-aldian, berrikuspenak egingo dira, gutxienez urtean behin. Halakoetan, beste ekintza batzuen artean, ISKSren irismena berrikusiko da.

Berrikuspen horiek ISKSren irismenari eragin ahal dion edozein gertakariren aurrean erantzuteko ere egingo dira, adibidez:

- Legeria-aldaketak.
- Aldaketak antolakuntzan.

- Aldaketak ingurune teknikoan.
- ISKSren kudeaketari eragin ahal dioten intzidentziak.

Berrikuspen horien helburua honakoa izango da:

- Gertakariak ISKSren irismenari zein mailatan eragiten dion ezagutzea.
- Irismena aldatzea, hala badagokio.
- ISKS berria zehaztea eta ezartzea, hala badagokio.

Bilerak fisikoak edo birtualak izan ahalko dira, eta biltegi zentralizatu batean jasoko dira ISKSrekin zerikusia duten aktak, proposamenak eta erabakiak.

4. Araudia garatzea

4.1. Fitxen azalpena

Segurtasun-neurrien garapena fitxen bidez egingo da. Behar den segurtasuna lortze aldera, segurtasun-neurri proportzionatuak aplikatzerakoan, hiru alderdi hartuko dira kontuan: babestu beharreko informazio-sistemaren kategoria, babestu beharreko sistema osatzen duten aktiboak eta babestu beharreko sistemak eskatzen duen segurtasun-dimentsioa. Horregatik guztiagatik, fitxa bakoitzak honako eremuak ditu:

- **Neurria**: neurriaren izena.
- **Kodea**: erreferentzia unibokoa.
- **Helburua**: neurria eta segurtasun-politikaren atal bat lotzen ditu.
- **Irismena**: neurria ezartzea noraino den beharrezkoa adierazten du;
    - "baxua" gisa sailkatutako fitxek (kolore berdea) segurtasun-neurria informazio-sistema guztiei aplikatu behar zaiela adierazten dute.
    - "ertaina" gisa sailkatutako fitxek (kolore horia) segurtasun-neurria sailkapen ertaina duten informazio-sistemei aplikatu behar zaiela adierazten dute.
    - "altua" gisa sailkatutako fitxek (kolore gorria) segurtasun-neurria sailkapen ertaina duten informazio-sistemei aplikatu behar zaiela adierazten dute.
- **Bermeak**: segurtasun-neurriak bermatzen dituen segurtasun-bermeak adierazten ditu.
- **Hartzaileak**: segurtasun-neurria kontuan hartu beharko luketen rol funtzionalak.
- **Garapena**:
    - Neurriaren testuak, bestetik, honako zatiak ditu:
        - "Xede" bat: segurtasun-neurriaren helburua zehazten du.
        - "Azalpen" bat: segurtasun-neurria bera garatzen du.
        - Segurtasuneko "jardunbide" bat, neurriak hala eskatzen badu. Jardunbideen multzoa segurtasun-prozeduren barne egongo dira. (Ikus M-2-2 segurtasun-neurria)

4.2. Fitxen aurkibidea

Kodea	Azalpena
M-1	Segurtasun-politika
M-1-1	Segurtasun-politika
M-2	Informazioaren segurtasuna. Antolakuntzako alderdiak
M-2-1	Kontratazioa eta zerbitzu-mailari buruzko akordioak
M-2-2	Segurtasun-prozedurak
M-3	Aktiboen kudeaketa
M-3-1	Aktiboak erabiltzea eta haien gaineko erantzukizuna

M-3-2	Informazioa tratatzea
M-4	Giza baliabideak eta segurtasuna
M-4-1	Lanpostuaren ezaugarriak
M-4-2	Zuzentzeko, prestakuntza emateko eta kontzientziatzeko erantzukizunak
M-5	Segurtasun fisikoa eta ingurumenekoa
M-5-1	Inguru seguruak – sarbide-kontrola
M-5-2	Inguru seguruak – ingurumen-segurtasuna
M-5-3	Segurtasuna ekipoetan
M-6	Komunikazioak eta eragiketak kudeatzea
M-6-1	Funtzioak banatzea
M-6-2	Aldaketak planifikatzea
M-6-3	Kode kaltegarriaren aurkako babesa
M-6-4	Segurtasuna sare-zerbitzuetan
M-6-5	Euskarriak nola erabili
M-6-6	Babes-kopiak
M-6-7	Komunikazio-kanalak
M-6-8	Web-zerbitzuen eta -aplikazioen babesa
M-6-9	Sistema planifikatzea
M-6-10	Ikuskapena
M-6-11	Garraioa
M-7	Sarbide-kontrola
M-7-1	Baimena emateko prozesua / Erabiltzailearen sarbidea
M-7-2	Sarbide-kontrola
M-7-3	Sarerako sarbidea
M-7-4	Erabiltzailearen erantzukizunak
M-8	Informazio-sistemak eskuratzea, garatzea eta eguneratuta edukitzea
M-8-1	Segurtasun-eskakizunak
M-8-2	Kriptografia
M-8-3	Onartzea eta abian jartzea
M-9	Informazioaren segurtasunari buruzko intzidentziak kudeatzea
M-9-1	Intzidentziak kudeatzea
M-10	Zerbitzuaren jarraitutasuna kudeatzea
M-10-1	Ordezko baliabideak
M-10-2	Zerbitzuaren jarraitutasuna
M-10-3	Zerbitzuaren jarraitutasun-planak, informazioaren segurtasuna barne hartzen dutenak
M-10-4	Aldizkako probak
M-11	Betetzea

M-11-1	Legea betetzea
M-11-2	Zehaztapen teknikoak betetzea
M-12	Segurtasunaren kudeaketa
M-12-1	Arriskuen azterketa
M-12-2	Etengabeko hobekuntza

Neurria	Kodea	Helburua	Irismena
Segurtasun-politika	M-1-1	Segurtasun-politika	Baxua
Bermeak	**Norentzat**		
Segurtasun-berme guztiak	Erabiltzaile guztiak		

Garapena

Helburua

EAEko Administrazio Orokorrak eta bere Erakunde Autonomoek dokumentu honetarako azaldutako eremuko segurtasunari buruz duten jarrera jasotzea.

Segurtasun-politikak konpromiso-maila altua eskatzen du Administrazioaren aldetik, prestakuntza handia akatsak eta ahultasunak antzemateko, eta jarraitutasuna politika hori berritzeko eta eguneratzeko, erakunde modernoak eta informazio-sistemak etengabe aldatzen ari baitira.

Azalpena

Beraz, ITAren barruko informazioaren segurtasunaren kudeaketari buruzko argibideak eman behar dira. Hau da:

- Dokumentu honek, Segurtasun-eskuliburuak, arlo horretako Eusko Jaurlaritzaren (EAEko Administrazio Orokorra eta bere Erakunde Autonomoak) konpromisoa adierazten du, eta informazioaren segurtasunaz nola jokatu behar den ezartzen du.
- Segurtasun-politika aldiro-aldiro eta denbora-tarte jakin batzuetan berraztertu behar da, edo segurtasunari eragiten dioten aldaketa nabarmenak gertatzen direnean, politikaren egokitasuna eta eraginkortasuna ziurtatzeko asmoz.
- Segurtasun-politika dokumentu batean jaso behar da, eta hura onartu eta jakinarazi behar da.

Jarduerak

- Segurtasun-politika egitea eta eguneratzea.

Neurria	Kodea	Helburua	Irismena
Kontratazioa eta zerbitzu-mailari buruzko akordioak	M-2-1	Informazioaren segurtasuna. Antolakuntzako alderdiak	Ertaina
Bermeak	**Norentzat**		
Benetakotasuna , osotasuna, erabilgarritasuna, konfidentzialtasuna, trazabilitatea eta babesa	Funtzionarioak		

Garapena

Helburua

ITAren gainean jardueraren bat eskatzen duten hirugarrenekiko akordioetan, behar diren segurtasun-alderdi guztiak barne hartzea.

Azalpena

- Lehentasunezkoa da, kanpokoek erabilgarri dituzten lekuetan, ITAren segurtasuna ziurtatzea. Horregatik, garrantzitsua da segurtasuna kudeatzea kanpokoekin arlo horretako kontratuak egiten diren momentutik bertatik. Hau da:
  - Kanpokoei sarbidea eman aurretik, erabili behar diren ITAren aktiboen segurtasun-arrisku handienak zein diren identifikatu behar dira, kasuan kasuko neurri zehatzak ezartze aldera. Hartutako neurri horiek kanpokoarekin egindako kontratuan azaldu eta formalizatuta geratuko dira.
  - Aktiboen arrisku-azterketa egin behar da.
  - Kanpokoekin egindako akordioek edo kontratuek, ITAren aktiboetara sartzea badakarte, edo ITAri produktuak/zerbitzuak/besterik gaineratzen badizkiote, Segurtasun-eskuliburuak ezartzen dituen segurtasun-eskakizun guztiak bete behar dituzte.
  - Gainera, Zerbitzu Mailako Akordioak garatuko dira (aurrerantzean, ANS edo SLA euren ingelesezko sigletan), adostutako zerbitzu-kalitatearen maila finkatzeko eta formalizatzeko.

Jarduerak

- ANS kanpokoekin kudeatzea

Neurria	Kodea	Helburua	Irismena
Segurtasun-prozedurak	M-2-2	Informazioaren segurtasuna. Antolakuntzako alderdiak	Baxua

Bermeak	Norentzat
Benetakotasuna, osotasuna, erabilgarritasuna, konfidentzialtasuna, trazabilitatea eta babesa	Erabiltzaile guztiak

Garapena

Helburua

Informazioaren segurtasunari buruzko erantzukizun guztiak argi eta garbi zehaztea.

Azalpena

- Azaldutako segurtasun-arloari buruzko erantzukizun guztiak argi eta garbi zehaztuta egon behar dira.
  - Azaldutako segurtasun-arloari buruzko erantzukizunen esleipena zehaztutako segurtasun-politikaren arabera egin behar da.
  - Aktiboak babesteko erantzukizunak eta segurtasun-prozedurak aurrera eramateko erantzukizunak argi zehaztu behar dira.
  - Beharrekotzat jotzen denean, erantzukizun hori osatu egin behar da. Horretarako, arlo jakin batzuetan, eta informazioa prozesatzeko baliabide jakin batzuei dagokienez, lan egiteko ildo zehatzagoak ezarri behar dira.
  - Eusko Jaurlaritzak argi zehaztu behar ditu EAEko Administrazio Orokorrak eta bere Erakunde autonomoek aktiboak babesteko hartu behar dituzten erantzukizunak, Segurtasun-eskuliburu honetako neurrietan oinarrituta.
- ITAri dagokionez, Segurtasuneko Arduradun Nagusi bat proposatu behar da; berak hartu beharko du bere gain segurtasuna garatzeko eta ezartzeko ataza orokorra, eta bereziki, segurtasun-neurriak identifikatu beharko ditu. Segurtasuna garatzeko eta ezartzeko ataza orokorraren barruan honako arloak nabarmendu daitezke, eta arduradun funtzional bati esleitu beharko zaizkio beti:
  - Segurtasun-politika egitea eta eguneratzea.
  - ANS kudeatzea.
  - Erantzukizunak zehaztea eta funtzioak banatzea.
  - Aktiboaren bizitza-zikloa kudeatzea.
  - Informazioa sailkatzea.
  - Segurtasunaren arloko prestakuntza kudeatzea.
  - Informatika-ekipoak seguruak bihurtzeko kudeaketa.
  - Euskarriak kudeatzea.
  - Intzidentziak kudeatzea
  - Auditoretza-erregistroen kudeaketa.
  - Nortasunak eta sarbideak kudeatzea
  - Segurtasunaren kudeaketa garapeneko bizitza-zikloan.
  - Ziurtagirien bizitza-zikloa

- o Zerbitzuaren jarraitutasuna kudeatzea.
- o Segurtasun-auditoretzak kudeatzea.
- o Segurtasuna Kudeatzeko Sistema administratzea.

- Arlo horietan egindako lanak prozesuetan oinarritutako lan-esparru batean egingo dira. Lan egiteko modu horrekin, errazago izango da funtzioak era eraginkorrean banatzea, *M-6-1* neurriaren arabera.
- Funtzioak banatu ahal diren segurtasun-esparru guztietan ezarri beharko da, inork ez dezan modurik izan, baimenik gabe edo beste inork antzeman gabe, aktiboak eskuratzeko, aldatzeko edo erabiltzeko. Gertakari baten hasiera eta gertakari hori baimentzea banandu beharko lirateke, eta kontuan hartu beharko litzateke talka egiteko aukera kontrolak diseinatzerakoan.

Neurria	Kodea	Helburua	Irismena
Aktiboak erabiltzea eta haien gaineko erantzukizuna	M-3-1	Aktiboen kudeaketa	Baxua

Bermeak	Norentzat
Benetakotasuna, osotasuna, erabilgarritasuna, konfidentzialtasuna eta babesa	Erabiltzaile guztiak

Garapena

Helburua

ITAren aktiboek behar duten babesa lortzea eta horri eustea. Horretarako, inbentarioa egingo da, eta aktiboak behar bezala erabiltzeko arauak eta erantzukizunak zehaztuko dira.

Azalpena

- ITAren aktibo guztien inbentario osoa eta eguneratua egin behar da.
  - o Inbentario hori egiteko, aktiboak (ikus aktiboaren definizioa, ISOren arabera) formalki definitutako kategorietan banatu behar dira.
  - o Aktibo bakoitzak erregistro horretan beharrezko informazioa izan behar du jasota, aktibo hori identifikatu, deskribatu, sailkatu eta kokatu ahal izateko. Halaber, aktiboen jabeak zehartu beharko dira, eta zeintzuk diren horiek hartutako erantzukizunak.
  - o ITAren aktiboak sailkatu, etiketatu eta mantentzeko prozedurak garatu eta ezarri beharko dira.
  - o Aldiro-aldiro, urtean behien gutxienez, inbentarioaren osotasunaren eta benetakotasunaren jarraipen-prozedura definitu eta egikaritu beharko da, haren gainean egindako aldaketen erregistroa identifikatzeko eta eguneratzeko, inbentarioaren osotasuna bermatuko bada.
- Inbentarioa berorren ardura duten guztien eskura dagoela bermatu behar da, eta arduradunak inbentarioko datuak eguneratuta edukitzera behartuta daude.

Jarduerak

- Aktiboaren bizitza-zikloa

Neurria	Kodea	Helburua	Irismena
Informazioa tratatzea	M-3-2	Aktiboen kudeaketa	Baxua
Bermeak	**Norentzat**		
osotasuna, erabilgarritasuna, konfidentzialtasuna, eta babesa	Erabiltzaile guztiak		

Garapena

Helburua

Informazioak babes-maila egokia duela bermatzea. Horretarako, sailkatzeko ildoak ezarriko dira, baita informazioa etiketatzeko eta manipulatzeko mekanismoak ere.

Azalpena

- ITAn tratatutako informazio guztia sailkatuta egon behar da, eta horretarako honakoak hartu behar dira kontuan: konfidentzialtasuna, informazioak daukan garrantzia, eta informazioaren arriskuaren kudeaketa.
- Informazioaren sailkapenaren arabera, betekizun batzuk bete behar dira, modu seguruan erabiltzen dela ziurtatzeko.
- Datu pertsonalek, edozein dela ere sailkatuta dauden kategoria, datu pertsonalak babesteari buruzko indarrean dagoen legerian jasotako xedapenak bete beharko dituzte.

Jarduerak

- Informazioa sailkatzea

Neurria	Kodea	Helburua	Irismena
Lanpostuaren ezaugarriak	M-4-1	Giza baliabideak eta segurtasuna	Ertaina
Bermeak	**Norentzat**		
Konfidentzialtasuna	Erabiltzaile guztiak		

Garapena

Helburua

Enplegatuen eta kanpokoen funtzioak eta erantzukizunak formalizatzea, dokumentu honetan azaldutako politikaren arabera. Horrela, helburua da eragindako pertsona orok jakin dezala zein diren bere erantzukizunak, eta erantzukizun horiek lanpostua definitu aurretik zehaztea, eta kontratu baten bitartez agerian gera daitezela.

Azalpena

- Enplegatuek eta kanpokoek esleituta dauzkaten funtzioetarako soilik erabili ahalko dituzte ITAren aktiboak. Funtzio horiek aktiboak erabiltzeko edo haietara jotzeko eskatzen diren profiletan eta sarbideetan behar bezala islatuta egotea bermatu beharko da. Datu pertsonalak, eta indarrean dagoen legedi edo araudiaren mendeko beste edozein datu, tratatzeari buruzko legedia zehatz-mehatz aplikatzen dutenean, enplegatuek eta kanpokoek orduantxe beteko dituzte behar bezala ITAren inguruko neurriak.
- Informazioaren segurtasunari buruzko erantzukizunak langile bakoitzaren lan-baldintzetan agertuko dira, eta egiaztatu beharko da betetzen diren ala ez.
- Kanpokoek lan-baldintza horiek hasieratik sinatu beharko dituzte, eta horrela eskura izan dezaketen informazioa ez zabaltzeko konpromisoa, ezta lan-harremana eten ondoren ere, hartuko dute.
- Onartutako lan-baldintzak bete ezean, dagozkion akzio administratibo eta penalak hasi ahalko dira.

Jarduerak

- Erantzukizunak zehaztea eta funtzioak banatzea

Neurria	Kodea	Helburua	Irismena
Zuzentzeko, prestakuntza emateko eta kontzientziatzeko erantzukizunak	M-4-2	Giza baliabideak eta segurtasuna	Baxua

Bermeak	Norentzat
Konfidentzialtasuna	Erabiltzaile guztiak

Garapena

Helburua

Langileak eta kanpokoak ITAren segurtasunari eragiten dioten mehatxu eta arazoez, baita euren erantzukizun eta betebeharrez ere, jabetzen direla bermatzea. Horretarako, funtsezkoa da langileak eta kanpokoak arlo horretako politika betetzeko prestatuta egotea, eta horrela, gizakiak egindako hutsegitetatik etor daitezkeen arazoak gutxitzea.

Azalpena

- EAEko Administrazio Orokorraren eta bere Erakunde Autonomoen zuzendaritzak segurtasun-arloko gaiak aintzat hartu behar ditu. Horregatik, segurtasun, auditoretza, reporting eta kontroleko neurriak ezartzeko behar diren mekanismoak baliatu beharko ditu.
- Zuzendaritzak segurtasun-neurriak jakinarazi eta ezagutarazi behar ditu, hori baita funtsezko urratsa gai horietan kontzientziazioa lortzeko, eta segurtasun-jarduerak garatzen edo egikaritzen dituztenentzat behar diren prestakuntza-baliabideak jarri behar ditu.
- Langile guztiek eta kanpoko guztiek informazioaren segurtasunari buruzko prestakuntza egokia eskatu eta jaso beharko dute, Segurtasun-eskuliburu honetan zehaztutako arauak, estandarrak eta bestelako ildoak betetzeko xedez.
- Prestakuntza horrek bere barne hartuko ditu segurtasun-betekizunak, legezko erantzukizunak, kontrol-helburuak, baita jardunbide egokiak ITAren aktiboak erabiltzean ere. Langileek, euren prestakuntza-planetan, behar duten prestakuntza izango dute. Kanpokoentzat, enpresak berak irakatsi beharko dizkie beharrezko alderdi horiek bere langileei.

Jarduerak:

- Segurtasun-arloko prestakuntza planifikatzea

Neurria	Kodea	Helburua	Irismena
Inguru seguruak – sarbide-kontrola	M-5-1	Segurtasun fisikoa eta ingurumenekoa	Baxua

Bermeak	Norentzat
Osotasuna, konfidentzialtasuna eta erabilgarritasuna	Erabiltzaile guztiak

Garapena

Helburua

Instalazioetan baimenik gabe fisikoki sartzea, eta beraz, erakundearen informazioan sartzea, galaraztea.

Inguru Seguruak esaten zaie ITA kokatzeko erabiltzen diren gelei. Horretaz gain, e-Administrazioaren leku fisiko eta publikoak ere sartzen dira horren barruan. Aktiboak izaera ezberdinetakoak direnez, ITAren kokapena oso sakabanatuta dago (hainbat leku, hainbat kasuistika) eta batzuetan ITAren aktibo batzuek eta beste jatorri bateko aktibo batzuek kokapen bera izango dute. Eta horregatik, ITAren arloan ezin dira neurri espezifikoak definitu; aitzitik, izaera orokorreko neurri asko hartu beharko dira.

Azalpena

Neurri orokorrak (ITAri aplikatzen zaizkionak, nahiz eta ez diren beren-beregi berarentzat definitu).

Zerbitzariak kokatzeko gelei buruz:

- Ahal dela, eginkizun bakarreko gelak izango dira. Gelak beste erabilera batzuetarako ere erabiltzen badira, gela horietara langileak ez dira maiz sartu behar izango.
- Barruan langilerik ez badago, gelak itxita egongo dira.
- Honako hauek sartu ahalko dira bakarrik: barruan kokatuta dauden aktiboen (ekipamenduen) arduradunak, horien administrazioaren edo mantentze-lanetako arduraduna, zaintza-zerbitzuak eta horiek, berariaz, baimena eman dieten pertsonak.

Eraikinei (instalazioei) eta bertarako sarbideari buruz:

Instalazio guztiek (Administraziotik kanpoko instalazioek barne) ondokoa ahalbidetzen duten segurtasun fisikoko mekanismoak eduki behar dituzte:

- Baimenik ez duten pertsonei informazioa prozesatzen edo gordetzen den inguru seguruetara sartzea eragoztea.
- Baliabide informatikoen babesa ziurtatzea. Ikus M-5-2.

Beraz, segurtasun fisikoko perimetroa zehartu beharko da, eta horren barruan ITA kokatu. Segurtasun-perimetroak segurtasuneko oztopo fisikoak zein sarrera kontrolatzeko mekanismo egokiak izan behar ditu.

Oztopo fisikoei buruz:

- Informazioa tratatzeko baliabideak dituzten eraikinen perimetroak sendotasun fisiko nahikoa izan beharko du baimenik gabeko sarrerak galarazteko, eta horretarako kanpoaldeko hormak izango ditu eta ateetako eta leihoetako babesak.
- Neurri horiek osatu ahalko dira kontrol-mekanismoak, alarmak, burdin hesiak eta eraikinean sartzeko lekuetan, leihoak barne, sarrailak jarrita. Mekanismo horiek eraikin horien segurtasun-perimetroaren sendotasuna areagotuko dute, informazioaren segurtasunaren eskakizunen arabera.

Sarrera kontrolatzeko mekanismoei buruz:

- Behar bezala kontrolatu beharko dira eraikinetako zamalanetako eremuak.

- Ondoko lekuetako segurtasuna bermatzeko berariazko betekizunak zehaztuko dira. Hauek dira lekuak: administrazio-bulegoak, jendaurrekoak izan ala ez, zerbitzari-gelak eta ustiapen-zentroak, artxibo-eremuak, ekipamendu elektrikoko edo komunikazioko gelak, eta beste edozein eremu, bertan dagoen aktiboa dela-eta, segurutzat jo behar baldin bada. Beraz, sarbide-kontrola aktiboen sailkapenarekin eta bertan egiten den tratamenduaren funtzioarekin bat etorri beharko da.
- Sarbide-kontrola dagoen lekuetan, sartzeko eta bertan egoteko ematen diren baimenak lan-jardunak dakartzan beharren arabera ezarriko dira.
- Eremuka antolatuta, leku horietara sartzeko baimena duten pertsonen zerrenda eguneratuta eduki beharko da beti. Eremu horietarako aldi baterako sarbideak, ohiko ordutegitik kanpoko sarbideak barne, beren-beregi baimendu beharko dira.
- Sarbideak (sarrerak eta irteerak) dagokion sarbide-kontroleko mekanismoaren bidez erregistratuko dira.
- Pertsona guztiek, instalazioetan dauden bitartean, identifikadore bat eraman beharko dute beti, ondo ikusteko moduan.
- Garbiketa eta mantentze-lanetako langileak eta baimena duten gainerako langileak, sarbidearen ondorioetarako, berdin tratatuko dira.
- Informazio- eta komunikazio-sistemez gain (zerbitzariak), erakundearen eraikinetan edo kanpokoenetan dauden biltegiratzeko euskarriek, inork ez lapurtzeko edo kalte fisikorik ez izateko, babesturik egon behar dute, eta horretarako sarbide fisikoaren kontroleko mekanismoak erabiliko dira, euskarri horietara bakarrik baimendutako langileek jo dezaketela bermatzeko.
- Debekatuta dago sarrera kontrolatzeko mekanismoak manipulatzea, behar bezala ibil ez daitezen, adibidez ateak behar bezala ixtea oztopatuz.
- Inguru seguruak dauzkan aktiboen arabera, berariazko sarbide-kontrolak jarriko dira, saihestu nahi den arriskuaren araberakoak.
- Administrazioaren informazio- eta komunikazio-sistemak osatzen dituzten ekipoak ez dira euren instalazioetatik kanpo atera behar aktiboaren arduradunaren aldez aurreko baimenik gabe.
- Informazio- eta komunikazio-sistemetako elementuren bat esleituta dagoen instalazioetatik kanpo aldi baterako atera behar denean, irteera erregistratu beharko da. Elementu hori bere kokapenera itzultzen denean, itxi egingo da irten zenean zabaldu zen erregistroa.
- Halaber, Administrazioaren instalazioetan ekipoak sartzen direnean, erregistratu beharko dira ekipoak kontrolatu ahal izateko.
- Dagoen ekipamenduaren aldizkako kontrolak edo inbentariokoak egin behar dira, lapurretarik egon den antzemateko, egon bada eragindako kalteak konpontzeko, eta egon litezkeen erantzukizunak eskatzeko.

Bulegoko armairu eta bestelako edukiontziak:

- Bulegoetako armairuak badira, bertan dagoen ekipamendurako egokiak izan beharko dute, giltzaz itxita egongo dira, eta ez dira kokatu behar jendea pasatzen den lekuetan, edo administrazioko jendaurreko bulegoetan.

Jarduerak

- Fisikoki sartzeko baimena.

Neurria	Kodea	Helburua	Irismena
Inguru seguruak – ingurumen-segurtasuna	M-5-2	Segurtasun fisikoa eta ingurumenekoa	Baxua
Bermeak	**Norentzat**		
Erabilgarritasuna eta osotasuna	Erabiltzaile guztiak		

Garapena

Helburua

ITAren kalte fisikoak saihestea.

Azalpena

Neurri orokorrak (ITAri aplikatzen zaizkionak, nahiz eta ez diren beren-beregi ITArentzat definitu).

Zerbitzariak kokatzeko gelei buruz:

- Gelek hainbat sistema eduki beharko dituzte, ITAren azpiegitura lan egiteko baldintza onenetan edukitzeko. Gainera, neurri horiek ITA fisikoki arriskuan jar lezaketen gertaera fisikoak antzemateko balio behar dute:
  - Kea antzemateko sistemak.
  - Sua itzaltzeko sistema automatikoak.
  - Gelako tenperatura eta hezetasuna kontrolatzeko sistema automatikoak.
  - Sabai izuna eta zoru izun teknikoa.
  - Etenik gabeko argindar-sistemak.

Bulegoko armairu eta bestelako edukiontziak:

- Bulegoetako armairuak badira, bertan dagoen ekipamendurako egokiak izan beharko dute, eta ezaugarri beraziak eduki beharko dituzte hautsetik, sutatik eta hezetasunetik babesteko.

Neurria	Kodea	Helburua	Irismena
Segurtasuna ekipoetan	M-5-3	Segurtasun fisikoa eta ingurumenekoa	Baxua

Bermeak	Norentzat
Osotasuna, erabilgarritasuna eta konfidentzialtasuna	Sistema-administratzaileak

Garapena

Helburua

Ekipo pertsonalak galtzea, kaltetuak izatea, lapurtzea edo arriskuan jartzea saihestea, eta EAEko Administrazio Orokorraren eta bere Erakunde Autonomoen e-Administrazioaren inguruko jarduerak etetea saihestea.

Neurri hau Inguru Seguruetatik kanpo egon daitezkeen ekipo pertsonalei begira dago jarrita, M-5-1ean azalduta dagoen bezala.

Azalpena

- ITAren aktiboak kokatu edo babestu behar dira, ingurumeneko mehatxu eta arriskuak, eta baimenik gabeko sarbideak, saihesteko. Beharrezkoa ez bada, jendea gutxitan sartzen den lekuetan kokatu behar dira.
- Ekipoak behar bezala mantendu behar dira, erabilgarritasuna eta osotasuna bermatzeko.
- EAEko Administrazio Orokorraren eta bere Erakunde Autonomoen lokaletatik edo inguru seguruetatik kanpo dauden ekipoei segurtasuna aplikatu behar zaie, kontuan hartuta lokal horietatik kanpo lan egiteak dauzkan arriskuak. Jabea nor den aparte utzita, informazioa prozesatzeko edozein ekipo EAEko Administrazio Orokorraren eta bere Erakunde Autonomoen lokaletatik kanpo erabiltzeko baimena behar da.
- Informazioa prozesatzeko eta biltegiratzeko ekipoak honako hauek dira: edozein eratako ordenagailu pertsonal, agenda, eskuko telefono, txartel adimendu edo lan egiteko Administrazioarenak berarenak ez diren beste lokaletatik erabiltzen den edozein modu.
- Segurtasun arriskuak, hala nola kalteak, lapurretak edo galtzeak, asko alda daitezke lokalen arabera (adibidez, Inguru Seguruak edo aireportuak), eta hori kontuan hartu beharko da kontrol-mota egokienak zehazteko.

Neurria	Kodea	Helburua	Irismena
Funtzioak banatzea	M-6-1	Komunikazioak eta eragiketak kudeatzea	Ertaina
Bermeak	**Norentzat**		
Osotasuna eta konfidentzialtasuna	Garatzaileak, Sistema-administratzaileak		

Garatua:

Helburua

Zerbitzurako edo arriskuaren kudeaketarako kritikoak diren atazak ez zaizkiola puntu bakar bati egokituko ziurtatzea, horrela informaziora jotzeko eta hura behar ez den bezala manipulatzeko aukerak gutxitzeko.

Funtzioak banatzea erantzukizunak esleitzeko metodo bat da, aukera ematen duena EAEko Administrazio Orokorraren eta bere Erakunde Autonomoen organo eskudun bakoitzaren informazioa behar ez den bezala, nahita edo nahi gabe, erabiltzeko arriskua gutxitzeko. Horretarako, kontu handiko eragiketa batzuen kudeaketa edo gauzatzea banatu egiten dira. Banaketa horren bidez, zerbitzurako edo arriskuaren kudeaketarako kritikoak diren atazak ez zaizkiola puntu bakar bati egokituko ziurtatzen da, horrela informaziora jotzeko eta hura behar ez den bezala manipulatzeko aukerak gutxituta.

Azalpena

- ITAren erabiltzaileei dagokienez, segurtasun-bermeentzako arriskua dagoen transakzioetarako baimenen esleipena eta banaketa egingo da.
- ITAren administratzaileei dagokienez, segurtasun-bermeentzako arriskua dagoen eragiketetarako baimenen esleipena eta banaketa egingo da.
- Aipatu behar da ataza hauek banatuta egon behar dutela: transakzioak eta eragiketak egitea eta onartzea, baimenak eskatzea eta esleitzea, kontrolak ezartzea eta jarraipena egitea.
- Arlo edo sail bakoitzeko eragiketen esleipena arlo edo sail horietako zuzendaritzek ezarritako banaketa-irizpideen arabera egingo da.
- Baldin eta, justifikatutako arrazoiengatik, ataza edo erantzukizun baten funtzioen banaketa egokia ezin bada egin, horien jarraipena eta ikuskapena arreta handiz egingo da, ondo egiten ote diren egiaztatzeko eta, behar ez bezalako erabilerak, halakorik egon bada, antzemateko.
- Organo eskudun bakoitzaren zuzendaritzaren ardura da esleitutako funtzio eta erantzukizunen jarraipena egitea aldian-aldian, funtzioen banaketa egokia egiten dela ziurtatzeko asmoz.
- Funtzioen banaketa hori hurrengo arlo hauetan egin behar da:
  - Funtzioetan
  - Garapenean
  - Sistemetan

Neurria	Kodea	Helburua	Irismena
Aldaketak planifikatzea	M-6-2	Komunikazioak eta eragiketak kudeatzea	Ertaina
Bermeak	**Norentzat**		
Osotasuna eta konfidentzialtasuna	Garatzaileak, Sistema-administratzaileak		

Garatua:

Helburua

Sisteman egindako aldaketak etengabe kontrolatzea, ITAri proposatutako aldaketa guztiak azter daitezen sisteman txertatzea komeni den ikusteko. Aldaketak planifikatu egin behar dira beti, eragindako zerbitzuak eskaintzeko orduan izan dezaketen eragina gutxitze aldera.

Azalpena

ITAren aplikazioetan eta osagaietan aldaketak egitea

- ITAren inguruan hasten diren informatika-garapeneko proiektuak, garapen-ziklo osoan zehar, informazioaren segurtasuneko berariazko betekizunak aintzat hartuta eraman behar dira aurrera.
- Garapen horretan honako printzipio hauek hartuko dira kontuan:
  - o Informazioaren segurtasunaren betekizunak aztertzeko eta zehazteko fasean, segurtasun-domeinuaren betekizunak kontuan hartuko dira.
  - o Neurrira egindako aplikazioak garatu bitartean, segurtasunez programatzeko oro har onartuta dauden gomendioak eta jokabide zuzenak hartu behar dira kontuan (datuak baliozkotzea, kodearen dokumentazioa, isilpeko informazioa biltegiratzea eta transmititzea, erroreak kontrolatzea, erregistroak eta auditoretzako pistak sortzea , baimena duten erabiltzaileak edo anonimoak sartzea, informazioaren segurtasuneko berariazko mekanismoak erabiltzea, eta aintzat har daitezkeen beste batzuk).
  - o Garapena eta probak probetako fitxategiak eta datu-baseak erabilita egingo dira, sistemaren probako datuak babesteari buruzko jokabide zuzenek ezartzen duten bezala.
  - o Informazioaren segurtasunari buruzko aldaketa-kontrolaren betekizunak ezarri beharko dira; helburua da aldaketa-prozesuan zehar informazioa edo haren erabilgarritasuna ez galtzea.
  - o Software bat ekoizpenean jarri aurretik, aztertu egin beharko da, EAEko Administrazio Orokorraren eta bere Erakunde Autonomoen segurtasuna arriskuan jar dezakeen kode gaiztoa antzemateko.
- Informazio- eta komunikazio-sistemak hondatzeko arriskua gutxitzeko, aldaketak egiteko kontrolak ezarri beharko dira. Aplikazioen kodea aldatzeak ondorio kaltegarriak izan ditzake ekoizpenaren arloan. Ondorio kaltegarri horiek ez gertatzeko, arauak ezarri behar dira, ekoizpenaren arloan ahalik eta etenik txikienak sortzeko. Arauak ondokoei buruzkoak izango dira:
  - o Programatzaileak sistemetan sartzeari buruzkoak
  - o Baimen-mailei buruzkoak.
  - o Hobetu daitezkeen aplikazioak antzemateari buruzkoak.
  - o Bertsioen kontrolaren jarraipenari buruzkoak.
  - o Softwarea eguneratzeko irizpideei buruzkoak.
- Hobekuntzak ekoizpenean ezarri aurretik, softwarearen eraginkortasuna proba-ingurunean egiaztatu behar da, eta ziurtatu betekizun guztiak betetzen dituela honako arloetan: softwarearen kalitatea, aplikatu beharreko araubideak zehaztutako informazio-segurtasuna, eta abar. Arreta berezia jarri behar da proba datuak ez daitezen ekoizpenera pasa.
- Operazio horren ondoren, Sistemen dokumentazioa eguneratu behar da, eta aurreko bertsioen

historikoa artxibatu eta mantendu behar da.

ITAren oinarrizko softwarearen aldaketak

- Oinarrizko softwarea aplikazioak funtzionatzeko beharrezkoak diren programen eta utilitateen multzoari esaten zaio.
- Egiten diren aldaketek oinarrizko softwareari eragiten diotenean, eta bereziki, sistema eragileari, aldaketak aztertu, berraztertu eta probatu beharko dira, informazioaren segurtasunean ez dutela eraginik ziurtatzeko.
- Oinarrizko softwarean egin beharreko aldaketa-prozesua behar adinako aurrerapenaz jakinarazi beharko da, sistemak, eta inoiz aplikazioak, aldez aurretik gertatu ahal izateko.
- Horrez gain, sistemetan edozein aldaketa egiten denean, jarduera-jarraitutasun planak berraztertu beharko dira, agian eragina izan dutelako.

Neurria	Kodea	Helburua	Irismena
Kode kaltegarriaren aurkako babesa	M-6-3	Komunikazioak eta eragiketak kudeatzea	Baxua

Bermeak	Norentzat
Osotasuna, erabilgarritasuna eta konfidentzialtasuna	Sistema-administratzaileak

Garapena

Helburua

Softwarearen eta informazioaren osotasuna mota logikoko mehatxu jakinetatik (malwarea, orokorrean) babestea.

Azalpena

- ITAren osagai guztiek konfigurazio segurua izan beharko dute (sekurizazioa) edozein motatako sareetara konektatu aurretik.
- Sekurizazioa bereziki murriztailea izan beharko da suebakietan, ingurunearen segurtasuna bermatzeko ekipoetan, eta Interneterako edo beste sare publikoetarako sarbidea duten sare segmentuetan kokatutako sistemetan.
- Konfigurazio segurua dagokien arduradunek ezarriko dute.
- Sekurizazio-neurriak, edo konfigurazio seguruko parametroak, behin zehaztuta, aztertuta eta probatuta, ekipoak instalatzeko planean sartu beharko dira.
- Konfigurazio seguruko parametroak aktiboaren beraren sailkapenaren araberakoak izango dira.
    - Kontuan hartu beharko da zein informazio mota den, eta zein erabiltzaile-talde sartzen diren. Sistemara sartzen diren erabiltzaileak eta erabiltzaile-taldeak, baita sistemak biltegiratuta duen edo tratatzen duen informazioa ere, kontuan hartuko dira sisteman sartzeko baimenak esleitzerakoan. Esleipena baimen txikienaren printzipioaren arabera egin behar da; erabiltzaileek operatzeko nahitaezkoak dituzten baimenak emango dira bakarrik.
    - Ematen dituzten sare-zerbitzuen araberakoak. Sistemak eskaini behar dituen sare-zerbitzuak identifikatu beharko dira, eta gainerakoak deshabilitatu. Berez, behar ez den eta baimenik ez duen zerbitzu oro deshabilitatu behar da, eta gero bakarrik espresuki eskatzen direnak habilitatuko dira. Ildo horretan, urrunetik konektatzen diren erabiltzaileek erabil dezaketen komunikazio-zerbitzuak ezabatzeko arreta handiz jokatu behar da.
- Sekurizazio-prozesuaren barruan, sisteman inor bidegabe sartzen den antzemateko softwarea instalatu eta konfiguratu beharko da, eta dagozkion erregistroak jarri beharko dira.
- Urrutiko diagnostiko-ataketarako sarbideak era seguruan kontrolatu behar dira, baimenik gabeko sarrerak saihesteko. Segurtasun-mekanismo egokiarekin babestu behar dira, bakarrik sartu ahal izateko hardwarearen eta softwarearen mantentze-lanen ardura duten pertsonek eskatuta.
- Segurtasun-konfigurazioa definitzeko, horren ardura dute talde teknikoek banaketa-zerrenda irekietan argitaratutako ahulguneen, edo fabrikatzaileen buletinetan argitaratutakoen jarraipena egingo dute. Nolanahi ere, argitaratutako ahulgunearen eragina, eta segurtasun-konfigurazioa aldatzeak izan dezakeen eragina, aztertuko dira. Fabrikatzaileek argitaratutako segurtasun-eguneratzeekin arreta handiz jokatu behar da, “0-day” edo “0-eguna” motako erasoak saihesteko.
- Sistemen konfigurazio seguruei buruzko dokumentazio eguneratua eduki behar da. Dokumentazio hori isilpekoa izango da.

Jarduerak

- Sekurizazio-prozesua eta adabakiak eta ahulguneak kudeatzea.

Neurria	Kodea	Helburua	Irismena
Segurtasuna sare-zerbitzuetan	M-6-4	Komunikazioak eta eragiketak kudeatzea	Baxua [++]
Bermeak	**Norentzat**		
Osotasuna, erabilgarritasuna eta konfidentzialtasuna	Sistema-administratzaileak		

Garapena

Helburua

Sareetako informazioaren babesa ziurtatzea.

Azalpena

- Sare-kontratu orotan, segurtasun-ezaugarriak, zerbitzu-mailak eta sare-zerbitzu guztien betekizunak identifikatu eta sartu behar dira, hornidura barnekoa edo kanpokoa den alde batera utzita.
- Sareko zerbitzuen hornitzaileak kontratatutako zerbitzuak modu seguruan erabiltzeko daukan ahalmena zehaztu eta monitorizatu behar da aldiro-aldiro, eta auditoretza egiteko eskubidea hitzartu behar da.Zerbitzu jakin batzuetarako segurtasun-hitzarmen egokiak identifikatu behar dira, kontuan hartuta segurtasun-ezaugarriak, zerbitzu-mailak eta kudeaketa-eskakizunak. EAEko Administrazio Orokorrak eta bere Erakunde Autonomoek sareko zerbitzuen hornitzaileek neurri horiek ezartzen dituztela ziurtatu behar dute.
- Sareko zerbitzuek honako hauek hartzen dituzte barne: konexioen hornikuntza, sare-zerbitzu pribatuak, balio erantsiko sareak (Value Added Network) eta sare-segurtasuneko soluzioak, hala nola firewall-ak eta bidegabeko sarrerak (intrusioak) antzemateko sistemak.
- Autentifikatzeko, kodifikatzeko eta sarera konektatzeko kontrolak ezarri behar dira. Ezarri beharreko kontrolen sendotasuna aurretik egin beharreko arrisku-azterketan oinarrituko da.

Jarduerak

- Zerbitzu-mailako hitzarmenak kudeatzea

Neurria	Kodea	Helburua	Irismena
Euskarriak nola erabili	M-6-5	Komunikazioak eta eragiketak kudeatzea	Baxua [+]
Bermeak	**Norentzat**		
Osotasuna eta konfidentzialtasuna	Erabiltzaile guztiak		

Garapena

Helburua

Erakundearen aktiboak, zaintzen edo garraiatzen diren bitartean, baimenik gabe ezagutzera ematea, aldatzea edo suntsitzea saihestea (kasu honetan euskarri elektronikoak edo ez elektronikoak izan daitezke —paper-euskarria—), eta aktiboak modu seguruan ezabatzeko eta suntsitzeko politika bat ezartzea.

Azalpena

- Euskarri hauek, garraiatzen diren bitartean, baimenik gabeko sarreren, erabilera desegokiaren eta galbideratzearen aurka babestu beharko dira. Adibidez, ingurumen aldetik (hezetasuna, beroa…) eta giza faktoreen aldetik (giltzaz itxitako edukiontziak, eskura entregatzea…) paketatze seguru bat erabiliz, hainbat entregatan eta ibilbide desberdinetatik egin daiteke bidalketa bat.
- Euskarri elektronikoetan dagoen informazioak teknika kriptografikoak erabili beharko ditu, M-8-2 neurriak ezartzen duen bezala.
- Isilpeko informazioa daukaten euskarriak, beren zeregina bukatu ondoren, fisikoki suntsitu, ezabatu edo gain-idatzi behar dira jatorrizko informazioa berreskuratzea ezinezko egiten duten teknikak erabiliz.

Neurria	Kodea	Helburua	Irismena
Segurtasun-kopiak	M-6-6	Komunikazioak eta eragiketak kudeatzea	Ertaina
Bermeak	**Norentzat**		
osotasuna, erabilgarritasuna, konfidentzialtasuna, eta babesa	Sistema-administratzaileak		

Garapena

Helburua

Informazioaren eta hura tratatzeko baliabideen osotasuna eta erabilgarritasuna mantentzea, babes-kopien sistema sendoa erabilita.

Kontuan hartu behar da informazioa "*egituratuta*" egon daitekeela (informazioa sistema zentralizatu betean badago, eta informazioa datu-base batean logikoki antolatuta badago, eta bertara jo ahal bada ITAren bidez) edo "*egituratu gabe*" egon daitekeela (informazioa ez badago sistema zentralizatu batean, baizik eta fitxategi ofimatikoetan sakabanatuta, antolaketa bakar eta argirik gabe; informazio mota hori ITAk berak sor dezake, edo herritarrekiko kudeaketa-prozesuetan ITAk bere gain hartzen dituen prozesuek behar duten zati bat izan daiteke.

Azalpena

- Sistemak kudeatzen eta haietan eragiketak egiten dituzten langileek ITAren informazio-sistemetan dagoen eta babes-plan bat aurreikusita daukan informazio guztiaren babes-kopiak egin behar dituzte, aldiro-aldiro. Kopia horietan babestu beharko dira honako hauek: datuak, sistemen konfigurazio-datuak, softwarea, gertakarien erregistroak eta auditoretzako pistak, eta hori guztia gero errekuperatu ahal izateko behar den dokumentazioa.
- Langileen lan-estazioetan bertan gordetako datuen babes-kopiarik ez da egin beharko.
- Babes-kopiak egiteko maiztasunak hainbat gauzarekin zuzenki proportzionala izan behar du. Hona hemen gauza horiek: biltegiratutako informazioa zenbateraino den garrantzitsua edo arretaz erabiltzekoa, zenbatean behin aldatzen edo eguneratzen den, zein arrisku dagoen sistemak huts egiteko edo hondatzeko. Maiztasuna babes-planean azalduko da, eta arlo horretan DBLO garatzen duen araudiak ezarritakoa bete beharko da.
- Babes-kopiak huts egitea, edo hura ez egitea, segurtasuneko intzidentziatzat joko da, eta horrela jakinarazi beharko da.

Neurri honetan identifikatutako jarduerak:

- Babes-kopien kudeaketa

Neurria	Kodea	Helburua	Irismena
Komunikazio-kanalak	M-6-7	Komunikazioak eta eragiketak kudeatzea	Baxua

Bermeak	Norentzat
Konfidentzialtasuna eta osotasuna	Erabiltzaile guztiak

Garapena

Helburua

Administrazio Elektronikoaren Legean onartuta dauden baina ITAk ezartzen dituen segurtasun mekanismoetan ez dauden komunikazio-bide telematikoetan segurtasun-neurriak ezartzea.

Azalpena

- ITAk bere jakinarazpen-sistema du, baliabide telematiko klasikoak (posta elektronikoa, faxa, telefonoa) baino sendoagoa eta seguruagoa. Horregatik, beste komunikazio-bide horiek baliabide alternatibotzat joko dira; horiekin administrazioko izapideak hasi ahalko dira, betiere izapidea hasi nahi duen herritarra zalantzarik gabe identifikatzeko segurtasun-neurririk baldin badago. Gainontzeko jakinarazpen telematikoak edo beste eskakizun batzuk ITAren bidez egingo dira
- ITAren esparruaren barruan, administrazioko izapideak hasteko telefonoa erabiliko da, baldin eta herritarra argi eta garbi identifikatzea ahalbidetzen duen kontrol-protokoloa ezartzen bada.
- ITAren esparruaren barruan, posta elektronikoa funtzionarioen arteko barne-komunikaziorako erabiliko da, eta herritarrekin modu informalean komunikatzeko baliabide alternatibo gisa.
- Arreta berezia jarriko da posta elektronikoa komunikazio-bide gisa ez erabiltzeko, Administrazioarentzat kritikoa izan daitekeen informazioa bidaltzeko edo jasotzeko.

Neurria	Kodea	Helburua	Irismena
Web-zerbitzuetako eta -aplikazioetako edukien babesa	M-6-8	Komunikazioak eta eragiketak kudeatzea	Baxua
Bermeak	**Norentzat**		
Erabilgarritasuna, konfidentzialtasuna eta osotasuna	Sistema-administratzaileak		

Garapena:

Helburua

Jendearentzat eskuragarri dagoen informazioa babestea, baimenik gabe inork alda ez dezan.

Azalpena

- Edukien osotasuna babesteko asmoz, ITAren sarbide-sistema publikoek mekanismo batzuk instalatuta eta aktibatuta eduki behar dituzte, edukiak baimenik gabe aldatu diren automatikoki antzeman ahal izateko.
- Edukiak baimenik gabe aldatu direla antzemanez gero, sistema horiek sarbide-sistema publikoen operatiboaz arduratzen diren langileentzat alertak sortu behar dituzte, berehala jatorrizko edukiak, eskuz edo automatikoki, berriro jarri ahal izateko.
- Halakoetan, ahalik eta azkarren, intzidentzia egon dela jakinarazi beharko da, intzidentzia hori aztertu ahal izateko.

Neurria	Kodea	Helburua	Irismena
Sistema planifikatzea	M-6-9	Komunikazioak eta eragiketak kudeatzea	Ertaina [+]

Bermeak	Norentzat
Osotasuna, erabilgarritasuna eta konfidentzialtasuna	Garatzaileak, Sistema-administratzaileak

Garapena

Helburua

Sistemetan hutsegiteak gertatzeko arriskua gutxitzea. Hori lortzeko bi ekimen finkatzen dira: sistemaren gaitasunen kudeaketa, eta irizpide formalak ezartzea aldaketak edo informazio-sistema berriak onartzeko.

Azalpena

- Baliabideen erabilera monitorizatu, doitu egin behar da, eta etorkizuneko gaitasun-eskakizunen proiekzioak egin behar dira, ITAk nahi dugun moduan funtzionatu dezan.
- Jarduera berri bakoitzaren eta prozesuan dagoen jarduera bakoitzaren gaitasun-eskakizunak identifikatu behar dira, sistema nola monitorizatu eta doitu planifikatu behar da, haien erabilgarritasuna era eraginkortasuna bermatzeko eta hobetzeko. Arreta eskaini behar zaie hornitzeko orduan itxaronaldi luzeak dituzten baliabideei.
- Informazio-sistema berriak, eguneratzeak edo bertsio berriak onartzeko irizpidea ere ezarri beharra dago, eta garatu bitartean eta onartu aurretik, sistemaren proba egokiak egin behar dira.
- Aktiboen arduradunek sistema berrien eskakizunak eta haiek onartzeko irizpideak ondo definituta, onartuta, dokumentatuta eta probatuta daudela ziurtatu behar dute.
- Informazio-sistema berriek, eguneratzeek edo bertsio berriek onarpen formala lortu ondoren migratu behar dute ekoizpenera.
- Prozesu berri bat onartzeak berekin ekar dezake ziurtatzeko eta egiaztatzeko prozesu formal bat, segurtasun-eskakizunak behar bezala kontuan hartu direla egiaztatzeko.

Neurria	Kodea	Helburua	Irismena
Ikuskapena	M-6-10	Komunikazioak eta eragiketak kudeatzea	Ertaina [+]
Bermeak	**Norentzat**		
Osotasuna eta konfidentzialtasuna	Erabiltzaile guztiak		

Garapena

Helburua

Susmagarriak edo ustekabekoak diren jokabideak antzematea eta horiei aurre egitea. Jardueren erregistro-sistemak (log-ak) ezarriko dira, ITAren eta erabiltzaileen jarduerek sortutako datuak jasotzeko. Erregistro-sistema horiek aktibatuta egon behar dute sistemak, sareak, aplikazioak eta erabiltzaileen identifikadoreak operatibo daudenean.

Azalpena

- Aktibo bakoitzarentzat, aktibo-motaren arabera, erregistratzeko eta aurkitzeko mekanismo egokiak zehaztuko dira. Mekanismo horiek gai izan behar dute sortutako erregistroaren zehaztasun-maila aukeratzeko.
- Aplikazioek jarduera-erregistroak sortu beharko dituzte, aukera ematen dutenak eragiketen eta gertakarien jarraipena erraz egiteko. Erregistroak erraz ikusteko moduan, garden, biltegiratu behar dira.
- Gertakariak erregistratzeko mekanismoek alerta bat sortuko dute, arrazoia edozein dela ere, erregistrorik sortu ezin badute.
- Gertakarien erregistroek sistema, sare, aplikazio eta erabiltzaileei buruz ematen duten informazioa dela-eta, erregistro horietara bakarrik jo ahalko dute haiek aztertzeko baimena duten pertsonek.
- Erregistroak babestuta egongo dira baimenik gabe inork ez aldatzeko edo ezabatzeko. Erregistroak komunikazio-sareen bidez bidaltzen badira, urrutitik irakurri ahal izateko edo biltegi zentraletara bidaltzeko, babestu beharko dira, baimenik gabe ez daitezen aldatu edo inork ez ditzan eskuratu.
- Erregistroak aldez aurretik erabakitako denboraldian gordeko dira, eta gutxienez momentu bakoitzean indarrean dagoen legediak ezarritakoan.
- Gertakarien erregistroak auditoretza-pista gisa erabiliko dira, berrikusteko eta kontrolatzeko funtzioarekin. Horren ondorioz, eta sistemek sortutako erregistroen artean korrelazio egokia egon dadin, sistema guztien erlojuak sinkronizatuta egon behar dira.
- EAEko Administrazio Orokorraren eta bere Erakunde Autonomoen jarduera jasotzen duten informazioko erregistroak (zerga arloko datuak, datu administratiboak, kontabilitateko datuak, edo legearen ikuspuntutik nahitaezkoa den bestelako edozein informazio garrantzitsu) biltegiratuta eta babestuta egon behar dira, ez daitezen gal, suntsi, aldaraz edo faltsutu, eta horrela indarrean dagoen legedia bete dadin.

Jarduerak

- Log-ak kudeatzea

Neurria	Kodea	Helburua	Irismena
Aktibo fisikoen gaineko eragiketak inguru seguruetatik kanpo	M-6-11	Komunikazioak eta eragiketak kudeatzea	Baxua
Bermeak	**Norentzat**		
Osotasuna eta konfidentzialtasuna	Erabiltzaile guztiak		

Garapena:

Helburua

Erakundearen inguru seguruetatik kanpo garraiatzean, informazioa daukaten ITAren aktiboak bidegabe erabiltzea, hondatzea edo baimenik gabe haietara jotzea saihestea. Neurri hau ez dagokie ekipo pertsonalei (ikus M-5-3 neurria).

Azalpena

- Lan egiteko ohiko lekutik ateratako ITAren ekipoak eta datu-euskarriak ez dira utzi behar jaramon egin gabe leku publikoetan.
- Lan egiteko lekutik ateratako ekipoak aseguru egokiarekin babestuko dira, eta garraioan fabrikatzaileak ekipoak babesteko emandako jarraibideak kontuan hartuko dira.
- Saihestuko da, ahal den neurrian, ekipoak kontu handiko informazioa edukitzea. Ahal dela, informazio hori modu seguruan ezabatu beharko litzateke inguru seguruetatik irten aurretik.

Neurria	Kodea	Helburua	Irismena
Baimena emateko prozesua / Erabiltzaileen sarbidea	M-7-1	Sarbide-kontrola	Baxua

Bermeak	Norentzat
Benetakotasuna eta konfidentzialtasuna	Erabiltzaile guztiak

Garapena

Helburua

Objektu batek (pertsona batek, programa batek edo gailu batek) ITAra sartzeko baimenik duen (autentifikazioa) eta zein baimen-mailarekin sar daitekeen (autorizazioa) erabakitzeko kontrolak ezarriko dituen baimentze-prozesua formalizatzea.

Azalpena

- Informaziorako sarbidea eta informazioa prozesatzeko baliabideak kontrolatu behar dira, segurtasun-eskakizunak oinarri hartuta.
- Sarbide-kontroleko politika ezarri, dokumentatu eta berrikusi behar da, sarbiderako segurtasun-eskakizunak oinarri hartuta. Sarbide-kontroleko arauak eta erabiltzaile edo erabiltzaile-talde bakoitzarentzako eskubideak argi ezarri beharko lirateke. Sarbide-kontrolek fisikoak zein logikoak izan behar dute, eta elkarri lotuta joan behar dute.
- Langileei eta kanpokoei argi azaldu behar zaie zein diren sarbide-kontrolek bete behar dituzten eskakizunak. Sarbide-kontroleko arauak prozedura formalek eta argi zehaztutako erantzukizunek babestu behar dituzte.
- Prozedura formal egokiak ezarri behar dira, ITAren arloan, informazio-sistemetarako eta -zerbitzuetarako sarbide-eskubideen esleipena kontrolatzeko. Beraz, erabiltzailea erregistratzeko eta des-registratzeko prozedura formalizatua egon behar da, informazio-sistemetarako eta -zerbitzuetarako sarbide-eskubidea emateko eta kentzeko, baita baimenen esleipena eta erabilera kontrolatzeko ere.
- Prozedurek erabiltzailearen sarbide-zikloko fase guztiak hartu behar dituzte bere baitan, erabiltzaileen hasierako erregistroarekin hasi eta erregistroak ezabatu arte. Egoki denean, arreta berezia eskatzen du sarbide-eskubide pribilegiatuak nori eman erabakitzeak, horrek ematen baitie erabiltzaileei sistemaren kontrolak gainditzeko aukera.
- Erabiltzaileen kudeaketa errazteko, sarbide-profilak egiteko aukera aztertu behar da. Profilek erabiltzaileentzat ohikoak diren sarbide-eskubide batzuk bere baitan hartzen dituzten eskakizunetan oinarrituta egon behar dute.
- Aztertu behar da langile-kontratuetan eta zerbitzu-kontratuetan klausula batzuk sartzea, zerbitzuko langileak edo agenteak baimenik gabe sartzen saiatuz gero, zehapenak zehaztuko dituztenak.
- Erabiltzaileen sarbidea, eta informazioaz eta aplikazioaren sistemaren funtzioez arduratzen diren laguntza teknikoko langileena, murriztu behar dira, zehaztutako sarbide-politikarekin bat etorriz.
- Langilearentzat funtzio publikoan (oinarrizko profila) oinarritutako baimen-prozedura planteatzen da. Behar dituen gainerako aplikazioetan sartzeko, sarbide diskrezionala erabiliko da.
- Kanpokoentzat, aplikazioetan eta sistemetan sartzeko, sarbide diskrezionala erabiliko da.

Jarduerak

- Nortasunak eta sarbideak kudeatzea

Neurria	Kodea	Helburua	Irismena
Sarbide-kontrola	M-7-2	Sarbide-kontrola	Baxua
Bermeak	**Norentzat**		
Benetakotasuna eta konfidentzialtasuna	Erabiltzaile guztiak		

Garapena

Helburua

ITAn, objektuak (pertsonak, programak, gailuak) autentifikatzerakoan eta baimenak ematerakoan inplementatu behar diren kontrol zehatzak ezartzea.

Azalpena

- **Erabiltzaileak identifikatu eta autentifikazioa**
  - EAEko Administrazio Orokorraren eta bere Erakunde Autonomoen ITAn sartzeko behar bezala baimendutako erabiltzaile-identifikadorea erabili beharko da.
  - Erabiltzaile-identifikadorea pertsona fisiko bati esleituko zaio, eta norberarena eta besterenezina izango da.
  - Erabiltzaile-identifikadoreari lotuta, sisteman datu batzuk gordeko dira, gutxienez aukera emango dutenak identifikadorea erabiltzailearekin modu unibokoan lotzeko, eta horrela erabiltzaile bakoitzari egotzi ahalko zaizkio bere erabiltzaile-identifikadorearekin egindako jarduerak.
  - Informazio- eta komunikazio-sistemetan sartzeko identifikadoreak eta pasahitzak erabiltzeak, baita horiekin lotutako egiaztatze-prozedurek ere, langileen nortasuna ziurtatu behar dute, eta aukera eman sarbide-baimen pertsonalizatuak esleitzeko.
- **Aldi-baterako erabiltzaileak**
  - EAEko Administrazio Orokorreko eta bere Erakunde Autonomoetako langile finkoak ez diren erabiltzaileek aldi-baterako identifikadoreak jaso behar dituzte, eta horiek langile berrientzat erabiltzen diren onartze-prozedura berberak jarraitu behar dituzte. Erabiltzaile horien sarbide-eskubideak bakarrik beharrezkoa den denborarako eman behar dira.
- **Erabiltzaile generikoak**
  - Ez dago baimenik erabiltzaile generikoak sortzeko edo erabiltzeko.
  - Erabiltzaile guztiek izan behar dute esleituta ondo identifikatutako erantzule uniboko bat.
  - Halaber, laneko funtzioek justifikatutako egoeretan izan ezik, pertsona fisiko bakoitza erabiltzaile-identifikadore bakarrarekin egongo da lotuta. Salbuespen gisa, pertsona batek erabiltzaile-identifikadore bat baino gehiago izan ahalko du, baldin eta identifikadore bakoitzari esleitutako pribilegioak desberdinak badira eta teknikoki posible ez bada guztiak jasotzea erabiltzaile-identifikadore bakarrean, edo gomendagarria ez bada, segurtasuneko arrazoiengatik, pribilegio guztiak identifikadore bakarrean edukitzea.
  - Erabiltzaileek identifikazio bakarra izango dute sistema guztietarako, eta identifikadore pertsonalari esker, jakin ahalko da zeintzuk diren erabiltzaile bakoitzak hainbat sistematan egindako eragiketak.
- **Sarbide-identifikadoreak blokeatzea**
  - Baimenik gabeko sarrerarik ez egoteko, erabiltzaileak identifikatzeko eta autentifikatzeko prozedurak, erabiltzaile-identifikadorea eta pasahitza sartuta, kontrolak izan beharko ditu erabiltzailea automatikoki blokeatzeko eta aldi baterako ezgaitzeko, honako kasu hauetan:
    - Saiakuntzen gehienezko kopurua gainditzeagatik. Erabiltzaile-identifikadorea edo sartzeko pasahitza oker sartzen bada, behin eta berriz, aurretik erabakitako aldietan baino gehiagotan.

- Erabiltzaileak sistema ez erabiltzeagatik. Erabiltzailea ez bada sartzen sisteman aurretik ezarritako egun naturaleko epe jakin batean.

- Halako egoeretan, edo erabiltzaile-identifikadorearen blokeoa eragiten duen beste edozeinetan, erabiltzaileak, ezarritako prozeduren bitartez, bere erabiltzaile-profila birgaitzeko eta dagokion identifikadorea desblokeatzeko eskatu beharko du.

- Administratzaile diren erabiltzaileen kontuak ez dira blokeatuko, erabiltzaile horiei zerbitzua ukatzeko erasorik gerta ez dadin. Horren ordez, teknikoki posible den heinean, hutsune hori konpentsatzeko kontrol egokiak jarri beharko dira, administratzaile profila esleituta daukaten erabiltzaile pasahitzak erabilita, saioa hasteko huts egindako saiakuntzak monitorizatzeko.

Neurria	Kodea	Helburua	Irismena
Sarerako sarbidea	M-7-3	Sarbide-kontrola	Baxua
Bermeak	**Norentzat**		
Benetakotasuna, konfidentzialtasuna eta trazabilitatea	Erabiltzaile guztiak		

Garapena

Helburua

Sare-zerbitzuetara baimenik gabe sartzea, barrutik zein kanpotik, saihestea.

EAEko Administrazio Orokorraren eta bere Erakunde Autonomoen sare korporatiborako sarrerak kanpotik egiten direnean arrisku-maila handia dago (sare korporatiboa zabaltzea ezagutzen ez diren eta kontrolatzen ez diren kanpoko sare eta sistemei; sare horiek agian beste konexio batzuk dauzkate, etab.).

Neurri honen arabera, urruneko sarbide-zerbitzuak baimenduta egoteko honako premietarako izan behar dira: jarduerarako, mantentze-lanetarako eta laguntza teknikorako.

Azalpena

- Mekanismoak ezarri beharko dira, ondokoak behar bezala tratatzeko: bidalitako informazioa, erabilitako sistemak eta baliabideak, sarrerak egin dituzten pertsonen nortasuna, eta sisteman sartzeak, oro har, dauzkan ondorioak.
- Urruneko sarbide-zerbitzuek autentifikazio-mekanismoak izan beharko dituzte, gutxienez, erabiltzailea/pasahitza parean (beti kanal zifratu batez bidez) edo gako publikoko kriptografian oinarrituta. Aldi berean, informazioa zenbateraino den kontu handikoa, komunikazioa zifratuta egon behar da. Nahitaez, pasahitza inork ez ulertzeko moduan transmititu beharko da.
- Urruneko sarbide-pribilegioak dituzten erabiltzaileek, euren ekipoa EAEko Administrazio Orokorraren eta bere Erakunde Autonomoen sare korporatibora urrutitik konektatuta dagoenean, aldi berean beste inongo sarera ez dagoela konektatuta ziurtatu beharko dute.
- Urruneko sarbide-pribilegioak dituzten langileen ardura da ziurtatzea urruneko sarbidea ez dutela baimenik gabeko edo Administraziotik kanpoko langileek erabiltzen. Barne-sarera urrutitik sartzeko aukera duten langileek une oro gogoratu beharko dute euren ekipoaren eta Administrazioaren arteko urruneko konexioak sare korporatiboaren luzapenak baino ez direla, eta isilpeko informaziora jotzeko bidea ireki dezaketela. Langileek EAEko Administrazio Orokorraren eta bere Erakunde Autonomoen aktiboak babesteko ahal diren eta arrazoizkoak diren neurri guztiak hartu behar dituzte.
- Horregatik, debekatuta dago Interneten bidez erabiltzaile-identifikadoreak, pasahitzak edo kredentzialak, sarearen barne-konfigurazioak edo helbideak bidaltzea. Beharrezkoa izanez gero, informazio hori zifratuta bidaliko da.
- EAEko Administrazio Orokorraren eta bere Erakunde Autonomoen sareen arteko konexioek bakarrik nahitaezkoa eta baimenduta dagoen informazio trukaketa onartu behar dute. Horretarako, iragazketa-elementuak erabili behar dira (adibidez, suebakiak) sare bakoitzaren perimetroa zehazteko, ezarritako elkarreragingarritasun-arauekin bat etorriz.
- Perimetroen bidez sareak banatzeko irizpidearen helburua da sarea segmentatzea, sareak fisikoki independenteak izatea, eta informazioaren segurtasunaren ikuspuntutik antzeko eskakizun edo ezaugarriak dituzten osagaiak batera jartzea.
- Segurtasun-perimetro desberdinetan kokatutako sareen arteko trafiko-fluxuak haien artean onartuta dauden eta ez dauden trafiko-motetan oinarrituko dira.
- IP helbideratzearen barne-eskemak ezkutatzeko, eta helbideratze-planetako gatazketatik datozen arazoak konpondu ahal izateko, helbideak itzultzeko mekanismoak erabiltzeko modua egon behar da. (adibidez, NAT).

Neurria	Kodea	Helburua	Irismena
Erabiltzailearen erantzukizunak	M-7-4	Sarbide-kontrola	Baxua
Bermeak	**Norentzat**		
Benetakotasuna eta konfidentzialtasuna	Funtzionarioak		

Garapena

Helburua

Baimenik gabeko erabiltzaileak sartzea saihestea, eta beraz, zabaldu ezin daitekeen edo legeak bereziki babesten duen informazioa lapurtzea edo arriskuan jartzea eragoztea.

Erabiltzaileek sarbide-kontrola eraginkorra izan dadin duten erantzukizunaz jabetuta eta arduratuta egon behar dute. Bereziki, pasahitzak erabiltzeari dagokionez.

Azalpena

- EAEko Administrazio Orokorraren eta bere Erakunde Autonomoen langile guztiek idazmahaia eta pantaila garbitzeko arau batzuk jarraituko dituzte, biltegiratzeko gailuak, dokumentazioa eta informazioa babestuta gera daitezen langileak lanpostutik alde egiten duenean.
- Arau horiek Administrazioko langile guztiek ezagutuko dituzte, eta informazioaren segurtasuneko prestakuntzaren barruan sartuko dira, gai horretaz kontzientziatzeko.
- Arau horietan honako jarraibideak zehaztuko dira:
  - Dokumentuak, txostenak eta baliabide informatikoak, hala nola zintak edo diskoak, giltzapean gorde beharko dira, bereziki lan orduz kanpo. Kontu handikoa edo kritikoa den informazioa, behar ez denean, leku seguru batean gorde behar da, giltzapean, bereziki bulegoa hutsik dagoenean.
  - Lan-estazioek, terminalek, eta inprimagailuek autentifikatzeko-sistema, giltza edo sarbide-kontroleko eta blokeo automatikoko mekanismoren bat izan beharko dute, horiek zaintzen inor ez badago.
  - Postontziak ezin dira jaramon egin gabe utzi, babestuta ez badaude.
  - Isilpeko informazioa erabiltzen den inguruneetan, euskarri fisikoa papera bada, inprimagailuak lan orduz kanpo baimenik gabe erabiltzetik babestu beharko dira.
  - Sailkatuta dagoen edo kontu handikoa den informazioa inprimatzen bada, berehala jaso beharko da inprimagailuetatik.

Neurria	Kodea	Helburua	Irismena
Segurtasun-eskakizunak	M-8-1	Informazio-sistemak eskuratzea, garatzea eta eguneratuta edukitzea	Baxua
Bermeak	**Norentzat**		
Osotasuna eta konfidentzialtasuna	Garatzaileak, Sistema-administratzaileak		

Garapena

Helburua

Segurtasuneko betekizunak/neurriak ITAn integratuta daudela ziurtatzea.

Azalpena

- Informazio-sistema berrietarako edo lehendik dauden sistemak aldatzeko zerbitzu-baldintzak ezartzerakoan, segurtasunaren arloko baldintzak zehaztu behar dira.
- Informazio-sistema berrietarako edo ITAn lehendik dauden sistemak hobetzeko merkataritza-baldintzen enuntziatuek segurtasun-kontrolen baldintzak zehaztu behar dituzte.
- Baldintza eta kontrol horiek eragindako informazio-aktiboen balio komertziala islatu behar dute, baita segurtasun-hutsegite batek edo segurtasun-ezak ekar lezaketen kalte komertziala ere.
- Baldintza horiek informazio-sistemen proiektuen hasierako faseetan sartu behar dira. Diseinu-fase horretan sartutako kontrolak askoz ere merkeagoak dira ezartzen eta mantentzen, sistema ezarri bitartean edo ezarri ondoren sartutako haiek baino.
- Egoki iritziz gero, gerentziak modu independentean balioztatutako eta ziurtatutako produktuak erabiltzea erabaki dezake. Informazioko teknologietako segurtasun-produktuak balioztatzeko irizpideei buruzko informazio gehiago hemen aurki daiteke: ISO/IEC 15408.

Jarduerak

- Segurtasuneko baldintzak aztertzea

Neurria	Kodea	Helburua	Irismena
Kriptografia	M-8-2	Informazio-sistemak eskuratzea, garatzea eta eguneratuta edukitzea	Ertaina
Bermeak	**Norentzat**		
Benetakotasuna, osotasuna eta konfidentzialtasuna	Garatzaileak, Sistema-administratzaileak		

Garapena

Helburua

Teknika kriptografikoak erabilita, konfidentzialtasunaren, benetakotasunaren eta osotasunaren ikuspuntutik informazioa babestea. Halere, garrantzi berezia du sistema kriptografiko bakoitzak gakoak kudeatzeko zer sistema erabiltzen duen.

Azalpena

Gako kriptografikoak kudeatu behar dituzten informazio-sistemek horiek kudeatzeko softwarea eta informazioa zifratzekoa izan beharko dute. Aukera hauek izango dituzte:

- **Gakoak sortzea.**
- **Gakoak banatzea kanal segurua erabilita.**
- **Gakoak aktibatzea.**
- **Gakoak gordetzea eta haiek lortzea**. Gakoak fisikoki oso ondo babestuta egon behar dute, eta haiek lortzeko oso baimen zorrotzak eskatuko dira, konfidentzialtasuna zaintzeko asmoz.
- **Gakoak aldatzea eta eguneratzea**. Aldatuz gero, gako berria berriro banatzeko prozedura aplikatu beharko da, eta hala badagokio, aurrekoa erabiltzeari utzi eta/edo ezabatu beharko da.
- **Gakoak arriskupean egotea**. Gakoak arriskuan daudela jakinarazteko prozedurak eta erantzukizunak ezarri behar dira, baita gakoen konfidentzialtasuna arriskuan jartzen duten egoeretan hartu beharreko neurriak ere.
- **Gakoak berreskuratzea**. Prozedurak, erantzukizunak eta mekanismoak ezarri behar dira, gako kriptografikoak galduz gero, horiek berreskuratu ahal izateko. Zehaztu beharko da zer baldintza behar diren gakoak berrekuratzeko, gako horiekin zifratutako informazioa berreskuratu ahal dela bermatzeko.
- **Gakoak artxibatzea** (gakoen fideikomisoa). Konfidentzialtasun-eskakizunak handiak badira, gakoak kokapen desberdinetan edo profil desberdinei banatzeko teknikak erabili beharko dira, gakoak segurtasun handiz zaintzen direla bermatzeko.
- **Gakoak suntsitzea**. Gakoak suntsitzeko prozedurak eta erantzukizunak ezarri beharko dira, eta ziurtatu beharko da ez dagoela gako horiek erabilita zifratutako daturik.
- **Gakoen kudeaketarekin lotutako eragiketak erregistratzea**. Egindako jardueren erregistroa gorde beharko da, eta gutxienez, honakoak jasoko dira:
    - Gako simetrikoen hartzaileak.
    - Nork egin duen jarduera bakoitza.
    - Noiz egin den jarduera bakoitza.
- Erabili beharreko algoritmoak aukeratzean, kontuan hartuko da zifratzeko mekanismokoak erabiltzeari buruzko indarrean dagoen legeria. Zifratzeko algoritmoak aukeratzean kontuan hartu beharreko beste alderdi batzuk algoritmoaren sendotasuna eta eraginkortasuna dira, baita zifratze-mota ere, simetrikoa ala asimetrikoa.

- Zifratzeko gakoen luzera bat etorriko da zifratu behar diren datuen konfidentzialtasuna bermatu nahi den denbora-tartearekin.
- Zifratzeko gakoak isilpeko informaziotzat joko dira eta, beraz, haien jabeak bakarrik izango du haietarako sarbidea. Zifratzeko gakoak haien sendotasuna bermatuko duten eran sortu behar dira. Gakoak sortzeko erabiltzen diren formulak, algoritmoak edo bestelako espezifikazioak dituzten programak edo artxiboak segurtasun-neurririk handienak erabilita kontrolatu behar dira.
- Zifratzeko gakoak ulertezinak izan behar dira, eta ez dira software-programen barruan sartu behar Ordenagailuek eta komunikazio-sistemek kontrolak izan behar dituzte ezarrita, biltegiratutako gakoak errekuperatzea galarazteko.
- Zifratutako informazioaren erabilgarritasuna bermatu behar denean, gakoak errekuperatzeko moduak dituzten zifratze-sistemak erabiliko dira.
- Aplikazioen eta informazioaren beharretara egokitutako zifratze-moduak hautatzeko, honako segurtasun-zehaztapenak ezarriko dira:
    - Zifratze-kontrolei buruzko legezko araubidea identifikatuko da.
    - Informazioaren konfidentzialtasuna zaintzeko erabiliko den zifratze-algoritmoa zehaztu beharko da kasu bakoitzerako, eta horretarako hainbat gauza aztertu beharko dira. Gutxienez, honako segurtasun-baldintzak zehaztuko dira:

Algoritmoa edo soluzioa nola erabili

- Zein mailatan zifratuko den informazioa:
    - Datuak igortzean. Aplikazioaren barruan zifratu daiteke edo igortzean bertan.
    - Biltegiratzean. Datu-basea edo fitxategi-sistema zifratu daitezke.
- Soluzioaren eskalagarritasuna, etorkizunean hedatzeko beharrizanak kontuan hartuta. Bereziki, gakoak trukatzeko sistema izan beharko da egokia, aintzat hartuta sekretu partekatuan oinarritutako soluzioek ez dutela modu egokian eskalatzen.
- Aukeratutako soluzioak onartzen dituen funtzionalitate osagarriak, hala nola:
    - Gakoak trukatzeko metodo desberdinak erabiltzeko aukera.
    - Beste sistema batzuekin trukatzeko, zenbat zifratze-algoritmo onartzen dituen.
- Soluzioak onartzen duen zifratze-metodoa:
    - Hardware bidez zifratzea
    - Software bidez zifratzea
- Etorkizunean soluzioa hedatzeko aukerak, eragiketa kriptografiko berriak sartuta.
- EAEko Administrazio Orokorraren eta bera Erakunde Autonomoen informazio-eta komunikazio-sistemetan, mezuaren edo transakzioaren onarpena bermatzea beharrezkoa denean, jatorriaren benetakotasunaren eta informazioaren osotasunaren bidez, sinadura elektronikoaren teknika erabiliko da.
- Sinaduraren teknika erabiltzeko, indarrean dagoen legeriak ezarritakoari jarraituta, aitorpena duen autoritate ziurtagiri-emaile batek emandako ziurtagiri digitalak erabili behar dira.

Neurria	Kodea	Helburua	Irismena
Onartzea eta abian jartzea	M-8-3	Informazio-sistemak eskuratzea, garatzea eta eguneratuta edukitzea	Baxua
Bermeak	**Norentzat**		
Osotasuna eta erabilgarritasuna	Garatzaileak, Sistema-administratzaileak		

Garapena

Helburua

ITAren ekoizpen-inguruneetan softwarea ezarri bitartean, softwarea hondatzeko arriskua gutxitzea. Prozesu hori guztiz kontrolatuta egon behar da. Neurri honek M-6-2 neurria osatzen du.

Azalpena

- Programa-liburutegiak eguneratu aurretik, dagozkion probak arrakastaz bukatu behar dira, eta amaierako erabiltzailearen baimena lortu behar da.
- Eguneratzeak horretan adituak diren teknikariek egingo dituzte, eta auditoretzako pista gisa geratuko dira erregistratuta.
- Aktiboaren arduradunaren idatzizko baimena beharko da.
- Bakarrik kode exekutagarria gordeko da.
- Kode exekutagarria ez da ekoizpen-ingurunera pasako harik eta probak egin arte, eta emaitza ontzat eman arte.
- Ekoizpen-ingurunean beharrezkoak ez diren ezaugarriak edo funtzionalitateak identifikatuko dira , eta softwarea instalatzerakoan desaktibatuko dira.
- Modulu exekutagarriak ez dira zuzenean eraman behar proba-inguruneko liburuetatik ekoizpen-ingurune liburutegietara, esleitutako arloak aurretik konpilatuta ez badaude.
- Aurreko bertsioak gorde egingo dira segurtasun-arrazoiengatik. Behar diren kopia guztiak egingo dira ekoizpen-ingurunera pasatu aurretik.
- Aplikazio bakoitzerako, erroreak kudeatzeko prozedurak egon behar dira, haien trazabilitatea lortu ahal izateko.
- Softwarearen aldaketak egin aurretik, haren mantentze-lanak egiteko kanpokoekin dauden kontratuak berrikusi beharko dira, horietako askok ez baitute uzten aldaketak bezeroak berak egiten euren baimenik gabe.
- Garapen- edo proba-inguruneetatik ekoizpen-ingurunera pasatzeko, aukerarik badago, softwarearen bertsioak kontrolatzen dituzten tresna automatikoak erabiliko dira, huts egiteak gertatuz gero, sistemak lehengoratu ahal izateko.
- Hondamendien aurreko neurri gisa, programa-liburutegien eguneratze guztien erregistroa eduki behar da, eta aurreko bertsioak denbora batez gorde behar dira.
- Arreta-neurri berberak eduki behar dira hirugarrenei erositako softwarearekin; kasu horretan, hornitzaileak emandako laguntza teknikoko jarraibideak hartu behar dira kontuan.

Neurria	Kodea	Helburua	Irismena
Intzidentziak kudeatzea	M-9-1	Informazioaren segurtasunari buruzko intzidentziak kudeatzea	Ertaina
Bermeak	**Norentzat**		
Osotasuna, erabilgarritasuna eta konfidentzialtasuna	Erabiltzaile guztiak		

Garapena

Helburua

ITArekin lotutako gertakariak eta informazioaren segurtasuneko ahulguneak behar bezala zuzendu ahal izateko moduan jakinaraziko direla ziurtatzea. Gertakari bat jakinarazteko eta eskalatzeko prozedura formalak ezarriko dira.

Azalpena

- EAEko Administrazio Orokorreko eta bere Erakunde Autonomoko langile guztiek eta zerikusirik duten kanpoko guztiek aktiboen segurtasunean eragina izan dezaketen gertakariak eta ahulguneak jakinarazteko prozeduren berri izan behar dute. Edozein gertakari eta informazioaren segurtasuneko edozein ahulgune ahalik eta azkarren, eta harremanetarako zehaztutako prozedurari jarraituz, jakinarazteko eskatu behar zaie.
- Intzidentziak jakinarazteko prozedura honakoak hartuko ditu barne:
    - Jakinarazpen-prozedura egokiak, informazioaren segurtasuneko gertakariak jakinarazten dituzten haiei, arazoa aztertu eta konpondu ondoren, emaitzak jakinarazten zaizkiela ziurtatzeko.
    - Informazioaren segurtasuneko gertakariak jakinarazteko formatuak, jakinarazpen-ekintza babesteko, eta jakinarazten duen pertsonari, informazioaren segurtasuneko gertakari bat gertatuz gero, beharrezkoak diren ekintza guztiak gogorarazten laguntzeko.
    - Segurtasun-gertakari bat egonez gero, behar bezala jokatzeko jarraibideak:
        - o Berehala idatzi xehetasunik garrantzitsuenak (adibidez, zer ez den bete edo zer arau urratu den, zerk ez duen funtzionatzen une horretan, pantailako mezuak, jokabide arraroak);
        - o Ez egin ezer norbere kontura; aitzitik, berehala jarri harremanetan zehaztutako puntuarekin;
        - o Segurtasuneko urraketak egin dituzten langileen edo kanpokoen kasuan, diziplinako prozedura formala erabiliko da.
- Intzidentzien kudeaketa eraginkorra bermatzeko, gertakariak eta informazioaren segurtasuneko ahulguneak, behin jakinarazita, modu egokian kudeatzeko, behar diren erantzukizunak eta prozedurak ezarriko dira.
- Informazioaren segurtasuneko intzidentzien aurrean erantzuteko, eta haiek monitorizatzeko, ebaluatzeko eta kudeatzeko, etengabeko hobekuntza-prozesua aplikatuko da. Ebidentziak behar izanez gero, legeak esandakoa beteta jasoko dira.
- Gertakariak eta informazioaren segurtasuneko ahulguneak jakinarazteaz gain, sistemak, alertak eta puntu ahulak monitorizatuko dira, informazioaren segurtasuneko intzidentziak antzemateko. Kontuan hartuko da:
    - Segurtasuneko intzidentzia mota desberdinei aurre egiteko, prozedura desberdinak egon behar dira.
    - Prozedurek honako hauek hartzen dituzte barne:

- Intzidentziaren arrazoiaren azterketa.
- Eustea (ahal den guztia egitea arazoa konpontzeko).
- Ekintza zuzentzailea ezartzea.
- Eragindakoei jakinaraztea.
- Ekintza hizketakide egokiei jakinaraztea.

- Auditoretzako pistak eta antzeko ebidentziak jasoko dira, besteak beste:
  - Arazoaren barne-azterketa egiteko.
  - Auzitegi-ebidentzia gisa erabiltzeko, halakoetan: kontratuaren edo errekerimendu arautzailearen ustezko urraketan, edo lege-ekintzaren kasuan, zibila zein kriminala izan.
  - Softwarearen edo eragindako zerbitzuaren hornitzaileekin kalte-ordainak negoziatzeko.
- Sistemen ohiko funtzionamendua berreskuratzeko ekintzak kontrolatuko dira. Honakoa ziurtatu behar da:
  - Bakarrik argi eta garbi identifikatuta eta baimenduta dauden langileek jo ahalko dute sistemetara eta datuetara.
  - Egindako larrialdietako ekintza guztiak xehetasunez dokumentatuko dira.
  - Larrialdietako ekintzak gerentziari jakinaraziko zaizkio, eta behar bezala berrikusi behar dira.
  - Sistemen osotasuna ahalik eta azkarren berrezarriko da.

- Informazioaren segurtasunari buruzko intzidentziak kudeatzeko helburuak zuzendaritzarekin adostuko dira, eta intzidentziak konpontzeko arduradunak eta horretan dabiltzanak informazioaren segurtasuneko intzidentziak kudeatzeko orduan erakundearen lehentasunez jabetuta daudela bermatuko da.

Jarduerak

- Segurtasuneko intzidentziak kudeatzea

Neurria	Kodea	Helburua	Irismena
Ordezko baliabideak	M-10-1	Zerbitzuaren jarraitutasuna kudeatzea	Handia
Bermeak	**Norentzat**		
Osotasuna , erabilgarritasuna eta babesa	Sistema-administratzaileak		

Garapena

Helburua

Lan-ingurune bakarra/komuna sortzea, zerbitzuaren jarraitutasunerako estrategiak ezarri ahal izateko.

Azalpena

- Kontuan hartuta informazioa dela EAEko Administrazio Orokorraren eta bere Erakunde autonomoen aktiborik garrantzitsuenetakoa, funtsezkoa da ITAren esparruan informazioa, zati bat edo guztia, galtzeko arriskua gutxitzea.
- Horretarako, zerbitzari zentraletan, sare-zerbitzarietan, komunikazio-zerbitzuetan dagoen informazioa, eta, oro har, ITAren operatiboarentzat garrantzitsua den edozein informazio, aldiro-aldiro egindako babes-kopietan egon behar da, ustekabean galduko balitz, berreskuratu ahal izateko.
- Biltegiratzeko baldintzek euskarriak ez direla hondatuko ingurumeneko arrazoiengatik bermatu behar dute. Hona hemen arrazoi horietako batzuk: muturreko tenperaturak, eremu magnetikoak, hezetasuna, sua, hautsa, eta abar. Euskarri horien egoeraren kontrola eraman behar da, zahartu direlako edo behin eta berriz erabili direlako, kalitatea galtzen delako, eta horrelakorik saihesteko.
- Halaber, euskarri horiek dauden lekura fisikoki sartu ahal izateko kontrol-mekanismoak jarri beharko dira.

Jarduerak

- Zerbitzuaren jarraitutasuna kudeatzea

Neurria	Kodea	Helburua	Irismena
Zerbitzuaren jarraitutasuna	M-10-2	Zerbitzuaren jarraitutasuna kudeatzea	Ertaina
Bermeak	**Norentzat**		
Osotasuna , erabilgarritasuna eta babesa	Sistema-administratzaileak.		

Garapena

Helburua

Jarduera-etenak izanez gero, erantzun ahal izatea, eta ITAk huts eginez gero, Administrazioaren aktiboak babestea. Zerbitzuaren jarraitutasuna kudeatzeko prozesu bat ezarri beharko da, erakundearen gaineko eragina gutxitzeko, eta aktiboak galduta ere, maila onargarri bateraino berreskuratu ahal izateko, horretarako kontrol prebentiboak eta berreskuratzeko kontrolak jarrita.

Azalpena

- Prozesu honek zerbitzu kritikoak identifikatu beharko lituzke, eta zerbitzuaren jarraitutasunarekin lotutako informazioaren segurtasuna kudeatzeko eskakizunak beste jarraitutasun-eskakizun batzuekin integratu beharko lituzke; azken eskakizun horiek honelako alderdiekin dute zerikusia: eragiketak, langileak, materialak, garraioa eta baliabideak. Prozesu honek funtsezko ondoko elementuak izango ditu:
    - e-Administrazioa dela-eta, ulertzea zein diren EAEko Administrazio Orokorrak eta bere Erakunde Autonomoek dauzkaten arriskuak, zein probabilitate dagoen arrisku horiek gertatzeko eta zenbat denboratan iraungo luketen. Zerbitzu kritikoak identifikatu beharko lirateke eta lehentasunak ezarri.
    - Zerbitzu bakoitzeko aktiboak identifikatzea.
    - ITAn segurtasun-intzidentzia bat gertatuz gero, zein izango litzatekeen zerbitzuan izango lukeen eragina ulertzea.
    - Aintzat hartuko da aseguruak erostea, zerbitzuaren jarraitutasun-prozesuaren zati bat bezala.
    - Aldian-aldian, eta zerbitzuan aldaketak egon badira, jarraitutasun-planak eguneratu eta probatu egingo dira , eta behar diren hobekuntza-neurriak aplikatuko dira.
    - Langileen segurtasuna eta informazioa prozesatzeko baliabideen babesa ziurtatuko dira.
    - Zerbitzuaren jarraitutasuna prozesuetan sartuko da, eta erantzukizun egokiak esleituko dira.
- Hondamendiek, segurtasuneko hutsegiteek, zerbitzua eta zerbitzuaren erabilgarritasuna galtzeak, horiek guztiek dituzten ondorioek nolako eragina duten egiten ari den jardueran aztertu behar da. Zerbitzuaren jarraitutasun-planak garatu eta ezarri beharko lirateke, funtsezko jarduerak berriz hastea ziurtatzeko.
- Zerbitzuaren jarraitutasunaren kudeaketak kontrolak izan beharko lituzke arriskuak identifikatzeko eta gutxitzeko. Arriskuak ebaluatzeko prozesu orokorraz arduratzeaz gain, gertakari kaltegarrien ondorioak murriztu beharko lituzke, eta eskaintzen den zerbitzurako beharrezkoa den informazioa erabilgarri egotea ziurtatu beharko luke.

Neurria	Kodea	Helburua	Irismena
Zerbitzuaren jarraitutasun-planak, informazioaren segurtasuna barne hartzen dutenak	M-10-3	Zerbitzuaren jarraitutasuna kudeatzea	Handia
Bermeak	**Norentzat**		
Osotasuna , erabilgarritasuna eta babesa	Sistema-administratzaileak		

Garapena

Helburua

ITAk zerbitzuak emateko gaitasuna honda dezaketen etenak edo hutsegiteak gertatuta ere, ITAren zerbitzua normaltasunera itzultzea ziurtatzea. Horretarako, Zerbitzua Berreskuratzeko Planak egingo dira, aldiro-aldiro eguneratu, eta probatu egingo dira.

Azalpena

- Zerbitzu-jarraitutasun Planak eduki beharko dira, zerbitzuari eragiten dion edozein arazo egonda ere, hura berreskuratu ahal izateko.
- Zerbitzu-jarraitutasun Planak dokumentatuta, probatuta eta eguneratuta egon behar dira. Guztiek ezagutu behar dituzte, eta hondamendia edo arazoa egonez gero, aplikatzeko errazak izango dira.
- Plan horiek, gutxienez, EAEko Administrazio Orokorraren eta bere Erakunde Autonomoen prozesuen jarraitutasunari probabilitate handienez eragin diezaioketen arriskuak hartu behar dituzte kontuan, eta balio behar dute arazoa gainditzeko aurreikusita dauden baliabideak erabilgarri egon daitezen, eta prozesu horien jarraitutasuna bermatzeko, horietako bakoitzerako ezarritako gehienezko denboran, gainera.

Neurria	Kodea	Helburua	Irismena
Aldizkako probak	M-10-4	Zerbitzuaren jarraitutasuna kudeatzea	Handia
Bermeak	**Norentzat**		
Osotasuna , erabilgarritasuna eta babesa	Sistema-administratzaileak		

Garapena

Helburua

Zerbitzu-jarraitutasun planak probatzea eraginkorrak izaten jarraitzen dutela egiaztatzeko, edo proben emaitzak egokiak izan ez badira, egokitzeko.

Azalpena

- Zerbitzu-jarraitutasun Plan bakoitzerako proba-plan bat egingo da, eta bertan azalduko da elementu bakoitza nola eta noiz probatuko den. Proba-plan horretan honako hauek sartuko dira: aktibatzeko hainbat egoeraren simulazioa, berreskuratzeko proba teknikoak, berreskuratzeko probak ordezko lekuetan, eta beste edozein saiakuntza.
- Zerbitzu-jarraitutasun Planak aldiro-aldiro berrikusiko dira, gertatutako balizko aldaketetara egokitzeko. Halaber, planean parte hartzen duen pertsona bakoitzaren erantzukizunak eguneratu egingo dira aldizkako berrikuspenetan.
- Gainera, eta ahal bezain azkarren, jardueraren jarraitutasun-planak eguneratu beharko dira, honelakorik gertatuz gero:
  - Planean erantzukizunak dituzten langileak aldatzen badira.
  - Jarduera-estrategiako aldaketak
  - Legeria-aldaketak.
  - Aldaketak baliabideetan.
  - Aldaketan lokalizazioetan.
  - Aldaketak kanpokoekin egindako kontratuetan.
- Zerbitzu-jarraitutasun Plan bakoitza, aldizka edo ahalik eta azkarren, berrikusteko erantzukizunak esleituko dira, eta antzemandako aldaketa guztiak, ordura arte plan horietan jasota egon ezean, berehala eguneratu beharko dira, dagokion azterketa egin ondoren.

Neurria	Kodea	Helburua	Irismena
Legea betetzea	M-11-1	Betetzea	Baxua
Bermeak	**Norentzat**		
Benetakotasuna, osotasuna, erabilgarritasuna, konfidentzialtasuna eta babesa	Erabiltzaile guztiak		

Garapena

Helburua

Erakundean lege-arloko segurtasunean egon litekeen zirrikiturik edo arazorik antzematea eta halakorik saihestea.

Azalpena

- EAEko Administrazio Orokorraren eta bere Erakunde Autonomoen erantzukizuna da ITAko informazioari eta komunikazioei aplikatu beharreko legeria une oro ezagutzea, eta legeri hori aplikatu beharreko eremua, eskatzen diren neurriak ezartzeko denboraldia, eta berrikusteko eta ikuskatzeko ezarrita dauden prozesuak dokumentatuta edukitzea.
- Zehazki, hurrengo puntuei buruzko araudia hartu behar da kontuan:
  - Datu pertsonalen tratamendua.
  - Informazioaren pribatutasuna.
  - Kanpokoekin egindako kontratuak.
  - Segurtasun pertsonala.
  - Jabetza intelektualeko eskubideak.
  - Segurtasun fisikoa eta ingurumenekoa.
  - Sistemen azpiegitura.
  - Legezko ekintzak arduragabekeriagatik edo kontratua ez betetzeagatik.
  - Probak jasotzea informatika-delituak daudenean.
  - Sistema-auditoretza
  - Informazioa monitorizatzea eta erabiltzaileen eskubideak.
  - Sinadura elektronikoa eta zifratze-algoritmoak erabiltzea.
  - Zerbitzu telematikoak Informazioaren Gizartean.
- Halaber, Informatikaren eta Telekomunikazioen Zuzendaritzaren ardura da **Segurtasun-eskuliburua** eguneratzea.
- EAEko Administrazio Orokorrean eta bere Erakunde Autonomoetan tratatzen den informazio pertsonala behar bezala babesteko xedez, Segurtasun-eskuliburu honetan jasotako arau guztiak hartuko dira kontuan.

Jarduerak

- Auditoretzak kudeatzea

Neurria	Kodea	Helburua	Irismena
Zehaztapen teknikoak betetzea	M-11-2	Betetzea	Handia
Bermeak	**Norentzat**		
Benetakotasuna, osotasuna, erabilgarritasuna, konfidentzialtasuna eta babesa	Erabiltzaile guztiak		

Garapena:

Helburua

Erakundean arlo teknikoaren segurtasunean egon litekeen zirrikiturik edo arazorik antzematea eta halakorik saihestea.

Azalpena

- ITAren segurtasuna aldian-aldian berrikusi behar da.
  - Berrikuspen horiek ITAri dagozkion segurtasun-neurrietan oinarrituta egin behar dira. Aplikatu beharreko ezarpen-estandarrak betez ikuskatu behar dira, eta dokumentatutako segurtasun-kontrolak erabilita.
  - ITAren aktiboen arduradunek, euren erantzukizun peko arloko informazioa segurtasun-neurri egokiekin eta segurtasuneko beste edozein eskakizunekin bat etorriz prozesatzen dela egiaztatu behar dute, aldiro,aldiro.
  - Berrikustearen ondoren, arauren bat betetzen ez dela konturatuz gero, arduradunek horren arrazoiak bilatu beharko dituzte, eta ekintza zuzentzailea ezarri.
  - Berrikuste eta ekintza horiek erregistratu behar dira.
  - Zehaztapen teknikoak betetzen direla aztertzea pertsona aditu bati dagokio (adibidez, sistemetako ingeniari bati) eta lan horretarako berariaz baimenduta egon behar da.

Neurria	Kodea	Helburua	Irismena
Arriskuen azterketa	M-12-1	Segurtasunaren kudeaketa	Ertaina
Bermeak	**Norentzat**		
Segurtasun-berme guztiak	Funtzionarioak		

Garapena

Helburua

Arriskuen azterketa lanabes gisa erabiltzera behartzea, beharrezkoa den segurtasun-eremuetan.

Azalpena

- Arriskuen ebaluazioak egiteko bi gauza hartu behar kontuan: batetik, arriskuak zenbaterainokoak diren kalkulatzeko ikuspegi sistematikoa (arriskuaren azterketa) eta, bestetik, arriskuen garrantzia zehazteko, aurreikusitako arriskuak arrisku-irizpide batekin konparatzeko prozesua (arriskuaren ebaluazioa).
- Arriskuen ebaluazioek arriskuak identifikatu eta kuantifikatu behar ditu eta lehentasunak ezarri, hori guztia arriskua onartzeko irizpidearekin eta Administrazioarentzat garrantzitsuak diren helburuekin alderatuta. Emaitzetan oinarrituta zehaztu beharko da zein den kudeaketa-ekintza egokia, eta zein diren lehentasunak ITAren segurtasun-arriskuen aurrean, eta arrisku horien aurka babesteko aukeratu diren segurtasun-neurriak ezartzeko orduan.
- Neurri hauetan arriskuaren azterketa egin behar da:
    - M-2-1
    - M-5-1
    - M-5-3
    - M-6-2
    - M-6-3
    - M-10-2
    - M-10-3

Neurria	Kodea	Helburua	Irismena
Etengabeko hobekuntza	M-12-2	Segurtasunaren kudeaketa	Ertaina
Bermeak	**Norentzat**		
Segurtasun-berme guztiak	Funtzionarioak		

Garapena

Helburua

Etengabeko hobekuntza-prozesua ezartzea, sistema formal bat edukitzearren erakundearen heldutasun-maila handitzeko, segurtasunaren ikuspuntutik begiratuta.

Azalpena

- ITAren arloan etengabeko hobekuntza bermatzeko prozedura ezarri behar da. Helburu hori lortzeko, eraginkortasunari, heldutasun-mailari edo segurtasun-sistemaren kalitate-mailari buruzko galderak erantzuteko beharrekoa den informazioa eduki behar da.
- Horretarako, ISO 27001 arauan jasota dauden metrikak edo adierazleak erabil daitezke. Arau horren eskakizunetako bat da segurtasun-neurrien eraginkortasuna neurtzea, segurtasun-betekizunak betetzen direla ziurtatzeko.
- ITA, segurtasunari dagokionez, zein egoeratan dagoen behin jakinda, momentu egokian erabaki zuhurrak hartu ahalko dira, eta modu proaktiboan (nahi ez diren egoerak gertatu aurretik) kudeatu ahalko da ITAren segurtasuna.

Jarduerak

- Segurtasuna Kudeatzeko Sistema administratzea.

5. Glosategia

Urruneko sarbidea: Barne-sarerako sarbidea, telefonia-sare kommutatuaren bidez edo beste sarbide-sare publiko baten bidez.

Aktiboa: Erakundearentzat balioa duen edozer. Zehatzago esanda, informazio-sistemaren baliabidea edo harekin lotutakoa, erakundeak ondo funtzionatzeko eta ezarritako helburuak lortzeko nahitaezkoa dena.

Zerbitzu-mailako akordioak (ZMA): ikus SLAren (Service Level Agreement) definizioa.

Mehatxua: Sistemari kalte egin ahal dion edozein gorabehera edo gertakari. Kalteak honelakoak izan daitezke: zerbitzua ukatzea edo suntsitzea, baimenik gabe datuak ezagutzera ematea edo datuak aldatzea.

Arriskuen azterketa: Erakunde batek aurre egin beharreko segurtasuneko mehatxuek izan dezaketen eragina, eta horiek gertatzeko dauden probabilitateak, aztertzea. Helburua da beharrezkoak diren segurtasun-kontrolak diseinatzea eta ezartzea, horiek ezartzeko lehentasunak zehaztea, eta dauden arriskuak gutxitzea.

Antibirusak: Birusen bila, memoriak, disko-unitateak, mezuak edo transmisioak aztertzen dituzten programa informatikoak. Antibirusak birus bat antzematen duenean, erabiltzaileari jakinarazten dio, eta berehala eta automatikoki kutsatuta dauden fitxategiak, direktorioak edo diskoak desinfektatzen hasten da.

“zero-day” / “0 day” / “0 eguna” erasoak: konponbiderik edo adabaki ezagunik ez duten sistemen edo aplikazioen ahulguneak baliatzen dituzten mehatxu informatikoak.

Segurtasunari buruzko auditoretza: Informazio-sistema bat kontrolatzen ari dela, eta nahi diren helburuetarako jarritako kontrolak egokiak direla, ziurtatzeko erabiltzen den prozedura. Jardueren azterketa bat ere egiten da, sistema informatikoan intrusiorik edo bidegabekeriarik egon den antzemateko.

Autentifikazioa: Sistema baten aurrean pertsona baten nortasuna eta benetakotasuna egiaztatzeko, edo informazio jakin baten osotasuna frogatzeko, erabiltzen den prozedura.

- Erabiltzaileak ezagutzen duen zerbait, adibidez, pasahitz bat.
- Erabiltzaileak daukan zerbait, adibidez, banda magnetikodun txartel bat, bertan dauzkana erabiltzailearen identifikazio/autentifikazio datuak.
- Ezaugarri fisikoren bat, hala nola, hatz-markak edo ahotsa.

Autentifikazio sendoa: Autentifikazio-mekanismoetatik aldi berean bi erabiltzen dituen autentifikazio-prozedura, prozeduraren segurtasuna indartzeko helburuarekin.

Benetakotasuna: Ezaugarri horren bidez informazio bat sortzen duen erabiltzailearen nortasuna bermatzen da, hau da, ziurtasun osoz ezagutzen da nork bidaltzen edo sortzen duen informazio jakin bat.

Autorizazioa: Sistemako entitate bati ematen zaion eskubidea edo baimena, sistemaren baliabide batera sartu ahal izateko.

Brithish Standard 7799 (BS7799): Informazioaren segurtasunari buruzko estandar britainiarra, bi zatitan banatua. Lehen zatia jardunbide egokien kodea da, eta informazio-sistemak babesteko jarraibideak ematen ditu. Bigarren zatiak informazioaren segurtasuna kudeatzeko sistemen zehaztapenak ezartzen ditu.

Bizitza-ziklo informatikoa: informazio-sistemek, sortzen direnetik ezabatzen diren arte, jarraitzen duten zikloa. Honako fase hauek ditu: bideragarritasuna aztertzeko fasea, betekizunak aztertzeko eta zehazteko fasea, diseinatzeko eta egiteko fasea, onartu eta ekoizpenera pasatzeko fasea, mantentzeko fasea eta ezabatzeko fasea.

Zifratzea: Testu bat modu ulertezinean eraldatzeko erabiltzen den prozesua. Bi motatakoa izan daiteke: lehenengoan, jatorrizko datuak ezin dira berreskuratu (bide bakarreko zifratzea), eta bigarrenean, bakarrik berreskuratu daitezke dezifratzeko alderantzizko prozesua erabilita (bide biko zifratzea).

Kode gaiztoa (malwarea): ondorengo elementu bati edo batzuei kalte egitea helburua duen edozein software, makro, activex, javascript …Hona hemen elementuak: ekipoak, sistema informatikoak, komunikazio-sareak eta erabiltzaileak -azken horiek ezer jakin gabe- (sistemak moteltzea, iruzurrezko erabilerak, informazio lapurtzea…); adibidez, birusak, harrak, troiarrak, joke-ak, (adarra jotzeko programak), hoax-ak (gezurrezkoak), bonba logikoak, spywarea, adwarea, keylogger-ak, etab.

Konfidentzialtasuna: Ezaugarri horren bidez galarazten da informazioa baimenik gabeko norbanakoen, erakundeen edo prozesuen esku jartzea, edo haiei komunikatzea edo haien artean zabaltzea.

Negozioaren jarraitutasuna (jarduera): eragiketa informatikoak eta jarduerakoak etenik gabe jarraitzen dutela bermatzen duten kontrolak, edo gertakari bat edo hondamendi bat gertatzen denean, zerbitzua etenda dagoen denbora ahalik eta gehien gutxitzen duten kontrolak.

Sarbide-kontrola: Sistema baten edo sare baten aktibo informatikoen gaineko eskubideak edo pribilegioak murrizteko prozesua.

Segurtasun-kontrola: Babes-mekanismo bat (teknikoa edo antolakuntzakoa), sistema, osagai edo prozesu baten gaineko segurtasun-arriskua gutxitzen laguntzen duena.

Babes-kopia: Informazioaren eta softwarearen kopia. Horiek galduz gero, berreskuratzeko aukera ematen du.

Kredentziala: entitate (pertsona, informazio-sistema edo aplikazio) baten identitatea zein den edo baimenik duen erakusteko, igorritako edo aurkeztutako datuak.

Kriptografia: Algoritmoak aztertzen dituen zientzia da. Datuen konfidentzialtasuna eta benetakotasuna ziurtatzeko erabiltzen da. Horretarako, jatorrizko datuak eraldatutako beste datu batzuekin ordezkatzen dira. Datuak jatorrizko formara bihurtzeko algoritmo kriptografikoa eta gako egokiak behar dira. Izen hori ematen zaio, baita ere, informazioa ezkutatzeko asmoz eta hura ez aldatzeko eta baimenik gabe inork ez erabiltzeko helburuarekin, datuak eraldatzeko printzipioak, moduak eta metodoak bere baitan hartzen dituen diziplinari.

Segurtasunari buruzko araudia: Erakunde baten segurtasunaren arloko jarraibideak eta betebeharrak ezartzen dituen dokumentuen multzoa. Honako hauek osatzen dute: segurtasun-politika, segurtasunari buruzko arauak, segurtasuneko estandarrak, segurtasuneko prozedurak eta segurtasun-gidak.

Datuak: Entitate baten irudikapen sinbolikoa (zenbakizkoa, alfabetikoa, algoritmikoa, etab.), atributua edo ezaugarria dira. Datuek, berez, ez dute balio semantikorik (zentzurik) baina behar bezala tratatuta (prozesatuta) kalkuluak egiteko edo erabakiak hartzeko erabil daitezke. ITAren barruan, datu terminoa ITAren konfiguraziori buruzko informazioaz hitz egiteko erabiltzen da.

Dezifratzea: Zifratuta dagoen testu bat abiapuntu hartuta, jatorrizko testua lortzen duen eragiketa

Datuak banantzea (ezkutatzea): Pertsonen benetako datuekin egindako prozesua, datuok proba- eta garapen-inguruneetan tratatzeko. Pertsonen eta beren datu pertsonalen arteko harremanak ezabatu egiten dira, eta fikziozko batzuk sortzen dira, identifikazioa galarazteko.

Erabilgarritasuna: Ezaugarri horren bitartez baimena duten erabiltzaileek sarbidea dute informaziora eta harekin lotutako aktiboetara behar denean, eta erabilera baimendua ukatzeko saiakuntzak galarazten ditu.

Segurtasun-domeinua: elementu-multzo bat, segurtasun-politika bat, segurtasun-autoritate bat, eta segurtasuneko jarduera multzo bat. Zehaztutako jardueretarako, elementuen multzoa segurtasun-politikaren mende dago, eta segurtasun-politika segurtasun-domeinurako dagoen segurtasuneko agintaritzak kudeatzen du.

EDI (Electronic Data Interchange): negozio-datuen trukea, negozioko partner-ren edo gobernu-erakundeen informazio-sistemen artean, formatu estandarretan.

Segurtasun-estandarra: Erakundean ezarritako jarraibide zehatzak dira, segurtasuneko arlo jakin batzuekin lotuta, hala nola, liburutegi kriptografikoak erabiltzea, lehendik ezarritako segurtasun-arkitekturak erabiltzea, etab.

Kanpora ateratzea (externalizazioa): Erakundearen prozesu bat beste erakunde baten esku uzten denean, normalean zerbitzu-mailako hitzarmen baten bidez.

Sinadura digitala: Algoritmo kriptografiko batek sortutako balioa, informazio-aktibo bati eranzten zaiona. Modu horretan, informazio horren hartzaileak haren osotasuna eta benetakotasuna egiaztatu ditzake.

Hardwarea: Sistema edo ekipo baten osagai fisikoak.

Identifikazioa: Sistema bati identifikadore bat aurkezteko egintza edo prozesua, sistemak entitatea ezagutu ahal dezan, beste batzuen artean.

Eragina: Segurtasun-mehatxu bat gauzatzen denean izaten den emaitza, gehienetan, negatiboa.

Atzera bota ezina (onartu behar izatea): Transakzio bateko edo igorpen bateko informazioaren ezaugarria. Bermea ematen dio igorleari hartzaileak ez duela jasotakoa atzera botako, eta alderantziz.

Argibideak: Antolatuta dauden, esanahi bat duten eta ITAk tratatzen dituen datuen multzoa. Informazioa aktibotzat jotzen da (ikus aktiboaren definizioa).

Osotasuna: Ezaugarri horren bitartez bermatzen da informazioa prozesatu, garraiatu edo biltegiratu den bitartean, ez dela baimenik gabe aldatu edo eraldatu, eta aldaketarik egon bada, oso erraza da antzematea.

ISO/IEC 27002:2005: Informazioaren segurtasunean jardunbide egokiak barne hartzen dituzten kontrolen multzoa. BS7799ren lehen zatiaren estandarizazioaren emaitza da.

Sinadura Elektronikoaren Legea: Erakundeen arteko harremanetan erabiltzeko, sinadura digitaleko mekanismoen balio-esparrua zehazten duen legea.

Informazioaren Gizartearen Zerbitzuen Legea (IGZL): Interneten bidez ematen diren zerbitzuak direla-eta, kontrolak ezartzea helburu duen legea. Zerbitzu horiek ematen dituzten pertsona fisikoen trazabilitatea bermatzeko neurriak ezartzen ditu.

Datu Pertsonalak Babesteko Legea (DPBL): datu pertsonalen tratamendua, askatasun publikoak eta pertsona fisikoen oinarrizko eskubideak bermatzea eta babestea helburu duen legea.

Monitorizazioa: erabiltzaileen, sistemen edo erakundearen sareen jarduerak eskuratzeko eta denbora errealean aztertzeko prozesua, pertsonek zein tresna automatizatuek egina.

Nahitaez onartu beharra: ikus atzera bota ezina.

Segurtasunari buruzko araudia: Segurtasun-politikako jarraibideetatik eratorritako arau orokorrek osatzen dute. Segurtasunari buruzko araudiek funtzioak eta erantzukizunak esleitzen dizkiete erakundearen barruko profil batzuei, eta informazioaren segurtasunari buruzko betebeharrak eta debekuak ezartzen dituzte.

Jarduera-jarraitutasun planak: gertakari bat edo hondamendi bat gertatzen denean, eragiketa informatikoek eta erakundeak behar bezala funtzionatzen jarrai dezaten, erantzukizunak eta jarraitu beharreko prozesuak zehazten dituen plana.

Segurtasun-politika: Erakunde baten informazioaren segurtasunaren oinarrizko jarraibide iraunkorrek osatzen dute. Jarraibide horiek araudiaren barruan hurrengo mailetako jardute-esparrua zehazten dute. Normalean, dokumentu labur eta zehatza izaten da, eta segurtasuneko gainerako araudia egiteko erreferentziatzat hartzen da.

Segurtasun-prozedura: Informazioaren segurtasunarekin lotutako atazak aurrera eramateko jarraibide zehatzak ematen ditu. Prozedurek jardute-esparru murriztua dute, eta beti dute izaera operatiboa. Prozedurek segurtasuneko estandarrak osatzen dituzte, eta horiek betetzeko eman beharreko urratsak zehazten dituzte.

Erregistroa: Erabiltzaileen, sistemen edo sareen jarduera biltegi batean gordetzeko prozesua, ondoren pertsonek edo trena automatizatuek aztertu ahal izateko.

Segurtasun Neurrien Erregelamendua: antolakuntzako neurrien eta neurri teknikoen multzoa. Datu Pertsonalen Babesari buruzko Lege Organikoa betetzeko ezartzen da.

Informazioaren babes-kopiak egitea: Informazioaren eta erakundearen informazio-sistemen softwarearen babes-kopiak aldiro-aldiro egiteko prozesua.

Segurtasun-arduraduna. Erakundean, informazioaren segurtasuna kudeatzen eta mantentzen duen pertsona.

Lehengoratzea: Jatorrizko informazio-sistemetan informazioa edo softwarea galdu delako, babes-kopietan gordetako informazioa eta softwarea berreskuratzeko prozesua.

Segurtasun-arriskua: egoera bat, zeinetan segurtasuneko ahulgunea eta hura aprobetxatzeko nahia eta gaitasuna duen balizko aurkaria batera ematen diren.

Atazak banatzea: Ataza batzuk egitea edo erantzukizun-esparru batzuen kudeaketa banatzeko metodoa. Helburua da informazioa edo zerbitzuak baimenik gabe aldatzeko edo gaizki erabiltzeko aukerak gutxitzea.

Jarraipena: Erakundean ezarritako kontrol-mekanismoen eraginkortasuna aldian-aldian egiaztatzeko prozesua.

Informazioaren sistemen eta teknologien segurtasuna: Prozesu eta neurrien multzoa, batetik, informazioa edozein peril, kalte edo arriskutik babesteko, haren konfidentzialtasuna, osotasuna, erabilgarritasuna, benetakotasuna eta onarpena zaintzeko, eta bestetik, informazioa bera transmititzen, biltegiratzen eta prozesatzen duten elementuak babesteko (hardwarea, softwarea, sareak, datuak eta langileak babesteko) funtzionamendu okerrik gerta ez dadin.

***Service Level Agreement*.** SLA (Service Level Agreement) edo ZMH (Zerbitzu-mailako Hitzarmena) zerbitzu-hornitzaile baten eta bere bezeroaren arteko kontratu idatzi bat da, zerbitzuren kalitate-maila finkatzeko. Oro har, bi alderdien, hornitzailearen eta bezeroaren, arteko harremana zehazten du. SLA batek bezeroaren beharrak identifikatu eta zehazten ditu, eta aldi berean, zerbitzu-itxaropenak kontrolatzen ditu, hornitzailearen gaitasuna kontuan hartuta. Helburua da ulermen-esparru bat eskaintzea, gatazka-arloak gutxitzea, eta, eztabaidaren aurrean, elkarrizketa sustatzea.

Softwarea: programa informatikoak (hardwarean biltegiratuta eta berak egikarituta) eta programei lotutako datuak (horiek ere hardwarean daude biltegiratuta).

Izapidetze telematikoa: prozedurak izapidetzeko teknologia berrienak erabiltzea. Bidea ematen du orain arte funtzionarioek edo agintari eskudunak egiten zutena automatikoki egiteko. Administrazioak baliabide telematikoen bidez izapidetutako prozeduren izapidetze-egoera jakiteko modua eskainiko die herritarrei.

Telelana: Urruneko lekutik egindako lana (normalean, etxetik) eta modem-a edo bestelako konexio-mekanismo bat duen ordenagailu baten bidez bulegora konektatuta.

Segurtasuneko ahulguneak: Informazio-sistema baten, segurtasun-prozeduren, barruko kontrolen eta abarren ahultasuna, segurtasun-arazo bat eragiteko erabil litekeena.