Informazioaren Segurtasun Politika

Aurkibidea

1. HELBURUAK

Euskal Herriko Lan Harremanen Kontseiluak (aurrerantzean, LHK) informazioaren segurtasuna kudeatzeko esparru bat ezarri du Segurtasunerako Eskema Nazionala (aurrerantzean, SEN) administrazio elektronikoaren eremuan arautzen duen urtarrilaren 8ko 3/2010 Errege Dekretuak ezarritakoaren arabera, eta, horrela aktibo estrategiko gisa onartu ditu informazioa eta informazioaren euskarri diren sistemak.

Aipatutako esparruak, halaber, bere barnean hartzen du datu pertsonalen babesa, eta 2016ko apirilaren 27ko Europako Parlamentuaren eta Kontseiluaren 2016/679 Erregelamenduaren (EB) (aurrerantzean, DBEO) xedapenak hartzen ditu kontuan, baita arlo horren inguruko legeria nazionalean biltzen dena ere.

Erreferentziazko esparru hori ezartzearen funtsezko helburuetako bat oinarri batzuk ezartzea da eta oinarri horien gainean, langile publikoek eta herritarrek zerbitzuetarako sarbidea eduki ahal izango dute kudeaketa ingurune seguru batean, langile publikoen eta herritarren premiei aurrea hartu eta haien eskubideak gordeko ditugularik.

Honako hauek dira informazioaren segurtasunaren eta datuak babestearen alorreko helburu orokorrak:

- Erakundearen helburuak eta zeregina bete daitezen erraztea, informazio sistemak eta komunikazioak modu seguruan erabiliz.
- Tratatutako informazioaren eta tratamendu zerbitzuen eta prozesuen euskarri diren sistemen, gailuen eta elementuen babesa, arriskuarekiko proportzionala izango dena, lortzea informazioaren segurtasun dimentsioak, hau da, informazioaren benetakotasuna, konfidentzialtasuna, integritatea, eskuragarritasuna, trazabilitatea eta kontserbazioa gordez.
- Aplikatu beharreko legezko baldintzak betetzeko behar diren segurtasun neurriak edukitzea, bereziki datu pertsonalak babestearen eremuan eta zerbitzuak baliabide elektronikoen bitartez emateko eremuan.

LHKren Informazioaren Segurtasun Politika (aurrerantzean, Informazioaren Segurtasun Politika) LHK-k bere helburuak lortzeko oinarritzat erabiltzen duen tresna da. Informazioaren Segurtasun Politikak erantzukizunak identifikatzen ditu eta printzipioak eta jarraibideak ezartzen ditu Informazioaren eta Komunikazioen Teknologien (IKT) bitartez kudeatzen diren informazio zerbitzuak eta aktiboak egoki eta sendo babesteko.

2. IRISMENA

Politika hori LHKn lan egiten duten pertsona guztiei aplikatuko zaie eta nahitaez beteko dute, LHK-ko baliabideak eta SENak eta DBEOak eraginpean hartzen dituzten prozesuak ere betebehar horren barnean sartzen dira, kontuan izan gabe baliabide eta prozesu horiek erakundearen barnekoak diren edo hirugarrenekin egindako kontratuen edo akordioen bitartez erakundeari lotutako kanpokoak diren.

3. ERAKUNDEAREN ZEREGINA

Lan Harremanen Kontseilua Euskal Autonomia Erkidegoko erakunde publiko bat da, eta sindikatu eta enpresaburuen konfederazioen arteko elkarrizketa eta topaketarako organo gisa zein Eusko Jaurlaritzaren eta Eusko Legebiltzarraren gai soziolaboraletarako kontsulta organo gisa eratuta dago. Nortasun juridiko propioa du, eta independentzia osoz jarduten du bere funtzioak betetzean.

LHK-k bere eskumenak betetzeko modu eraginkorrean eta efizientean babestu behar diren informazio sistemak erabiltzen ditu.

4. ARAU ESPARRUA

LHK-k Informazioaren Segurtasun Politika horren eremuan betetzen dituen jardueren arau esparrua honako arau hauek osatzen dute, gainerakoak baztertu gabe:

- 59/2003 Legea, abenduaren 19koa, Sinadura Elektronikoari buruzkoa.
- 25/2007 Legea, urriaren 18koa, Komunikazio Elektronikoei eta Komunikazioen Sare Publikoei buruzko Datuak Kontserbatzeari buruzkoa.
- 37/2007 Legea, azaroaren 16koa, Sektore Publikoko Informazioa Berrerabiltzeari buruzkoa.
- 56/2007 Legea, abenduaren 28koa, Informazioaren Gizarteari Bultzada emateko Neurriei buruzkoa.
- 3/2010 Errege Dekretua, urtarrilaren 8koa, Segurtasunerako Eskema Nazionala Administrazio Elektronikoaren eremuan arautzen duena.
- 4/2010 Errege Dekretua, urtarrilaren 8koa, Elkarreragingarritasunerako Eskema Nazionala Administrazio Elektronikoaren eremuan arautzen duena.
- 9/2014 Lege Orokorra, maiatzaren 9koa, Telekomunikazioei buruzkoa.
- 39/2015 Legea, urriaren 1ekoa, Herri Administrazioen Administrazio Prozedura Erkideari buruzkoa.
- 40/2015 Legea, urriaren 1ekoa, Sektore Publikoaren Araubide Juridikoari buruzkoa.
- 2016ko apirilaren 27ko Europako Parlamentuaren eta Kontseiluaren 2016/679 Erregelamendua (EB), Datu Pertsonalen Tratamenduari dagokionez Pertsona Fisikoen Babesari eta datu horien Zirkulazio Askeari buruzkoa (aurrerantzean, Datuak Babesteko Erregelamendu Orokorra edo DBEO).
- 3/2018 Lege Organikoa, abenduaren 5ekoa, Datu Pertsonalak Babesteari eta eskubide digitalak bermatzeari buruzkoa (aurrerantzean, DBEDBLO).

5. SEGURTASUNAREN ANTOLAMENDUA

LHK-ko segurtasunaren antolamendua gai horren inguruko jarduerak eta erantzukizunak identifikatuz eta definituz ezartzen da, baita jarduera eta erantzukizun horien euskarri den azpiegitura ezarriz ere.

Oro har, LHKren informazio sistemen erabiltzaile guztiak dira informazio aktiboen segurtasunaren erantzule, aktibo horiek behar bezala erabiliz, betiere dagozkien eskuduntza profesionalen eta akademikoen arabera.

Jarraian, Organoen eginkizunak eta erantzukizunak ez ezik, gobernu maila desberdinetan (betearazlea eta ekintza arlokoa) ezarritako rolak ere deskribatuko ditugu.

5.1. Organoak

5.1.1. Presidentetza

Informazioaren segurtasunaren alorrean, LHK-k, LHKren Presidentetzaren bitartez edo hark eskuordetuko duen pertsonaren bitartez, honako betebehar hauek ditu:

- Segurtasunerako Eskema Nazionalean ezarritako xedapenak betearaztea informazio sistema SENaren aplikazio eremuaren barnean dagoenean, eta, hala badagokio, jarraibideak ematea. Aintzat hartzekoak dira, halaber, datu pertsonalen babesaren arloan aplikatzen den legediari lotutako xedapenak (DBEO edo Datuak Babesteko Erregelamendu Orokorra, DBEB edo Datu Pertsonalak Babesteari eta Eskubide Digitalak Bermatzeari buruzko Lege Organikoa, eta egon litezkeen beste batzuk).

- LHKren Informazioaren Segurtasun Politika eta politika hori osatuko duen beste edozein politika sektorial –Informazioaren Segurtasun Batzordeak proposa dezakeena eta Segurtasunerako eta Elkarreragingarritasunerako Eskema Nazionalak, eta datu pertsonalen babesari lotutako legedia, betetzea ahalbidetzen duena– onartzea, baita politika horien aldaketa edo eguneratze guztiak ere.
- Informazioaren Segurtasun Batzordea eratzea eta Batzorde horretako kideak izendatzea.
- Informazioaren Segurtasunaren erantzulea eta Datuak babesteko ordezkaria izendatzea, Informazioaren Segurtasun Batzordeak proposatu ostean.
- Informazioaren Segurtasun Batzordeak proposatutako antolamendu garapena onartzea.
- Informazioaren segurtasunaren alorrean, berariazko neurriak hartzea Informazioaren Segurtasun Batzordeak proposatu ostean.

5.1.2. Informazioaren Segurtasun Batzordea

Informazioaren Segurtasun Batzordearen helburua informazio zerbitzuen eta aktiboen segurtasuna LHKn zaintzea da, gai horren eraginpean dauden organoen jardun guztiak behar bezala koordinatzea eta txertatzea bermatuz eta erraztuz.

Deskribatutako helburua betetzeko, Informazioaren Segurtasun Batzordeak honako eginkizun hauen erantzule da:

- Informazioaren Segurtasun Politika aldatzeko eta eguneratzeko proposamenak egitea, proposamenen egokitasuna gutxienez urtean behin ebaluatuz eta Kontseiluaren Presidentetzari proposatuz, Informazioaren Segurtasun Batzordearen presidentearen bitartez, proposamen horiek onartzea eta dagokionean berrikustea.
- Informazioaren segurtasun politika osatzen duten politika sektorialak egitea eta proposatzea, baita politika horien gaineko aldaketak ere, segurtasunerako eta elkarreragingarritasunerako eskema nazionalak betetzeko.
- Segurtasunerako eta elkarreragingarritasunerako eskema nazionalak Erakundearen eremuan betetzea ahalbidetzen duen antolamendu garapena egitea eta proposatzea.
- Informazioaren Segurtasunaren erantzulearen eta datuak babesteko ordezkariaren izendapenak proposatzea.
- Informazioaren Segurtasun Politika bete eta hedatzen ote den zaintzea, informazioaren segurtasunaren alorrean kontzientziatzeko eta prestatzeko jarduerak sustatuz LHK-ko langileentzat.
- Informazioaren segurtasunari eta datu pertsonalak babesteari buruz aplikatu behar den legezko araudi erregulatzailea eta sektoriala betetzen ote den zaintzea.
- Informazioaren Segurtasun Politika garatzeko beharrezkoak diren ebazpenak Presidentetzan aurkeztea, Informazioaren Segurtasun Batzordearen presidentearen bitartez, Presidentetzak onar ditzan.
- Batzordeak onartutako akordioak Erakunde osora hedatzea.
- Informazioaren Segurtasun Politika interpretatzean eta aplikatzean eta hainbat erantzuleren artean garatzean sor litezkeen gatazkak konpontzea, gatazka horiek Kontseiluaren Presidentetzan aurkeztuz, behar izanez gero.
- LHKren komunikazioa Zentro Kriptologiko Nazionalarekin eta datuak babesteko Kontrol Agintaritzarekin koordinatzeko jarraibideak Presidentetzari proposatzea Informazioaren Segurtasun Batzordearen presidentearen bitartez, Presidentetzak onar ditzan.
- Erakundearen informazio segurtasunaren egoerari eta Informazioaren eta Komunikazioaren Teknologien(IKT) inguruan sor litezkeen gorabeherei buruzko txosten erregularrak eskatzea; txosten horietako ondorioak, Informazioaren Segurtasun Batzordearen presidentearen bitartez,

Presidentetzara helaraztea, baita Segurtasunaren erantzuleari eta informazioaren segurtasunaren kudeaketa egiten laguntzeko sor litezkeen lantaldeei ere.

- Inbertsio horizontal arrazionalak eta neurrizkoak sustatzea informazioaren segurtasunaren inguruko premiei erantzuteko baliabideak eskuragarri izango direla bermatzeko.
- Erabiltzen diren informazio mota desberdinak eta emandako zerbitzuak balioesteko irizpideak definitzea informazio sistema desberdinen arrisku azterketak bateratzeko.
- Informazioaren Segurtasun Batzordearen presidentearen bitartez, Presidentetzari LHKren informazioaren, zerbitzuen eta informazio sistemen Aplikagarritasun Aitorpena –SENaren erregulazioan ezarrita dagoena– proposatzea, Presidentetzak onar dezan.

5.2. Rolak

5.2.1. Informazioaren Segurtasun Batzordearen presidentea

Informazioaren Segurtasun Batzordearen Presidentetza LHK-ko Informazioaren Segurtasunaren erantzule izendatutako pertsonari egokituko zaio.

Presidenteak honako eginkizun hauek ditu:

- Informazioaren Segurtasun Batzordearen ordezkari izatea.
- Bilkuren deialdiak erabakitzea eta gai zerrenda ezartzea.
- Bilkuren buru izatea eta sor litezkeen eztabaidak moderatzea.
- Erabakiak hartzeko garaian sortzen diren berdinketak erabakitzea, baldin eta berdinketak baleude, bere kalitateko botoa erabiliz.
- Legeak betetzen direla ziurtatzea.
- Informazioaren Segurtasun Batzordearen aktak eta proposamenak ikus-onestea, baita Batzorde horrek hartutako erabakien ziurtagiriak ere.
- Informazioaren Segurtasun Batzordearen akordioak eta ebazpenak Presidentetzara igortzea, Presidentetzak onartzeko bidezkoa denean.
- Batzordekideak eta organoaren Idazkaritzako titularrak izendatzea.
- Batzordekide izateagatik dagozkion eginkizun guztiak betetzea.

5.2.2. Informazioaren Segurtasun Batzordeko kideak

Honako rol hauek esleituta dituzten pertsonak izango dira Informazioaren Segurtasun Batzordeko kideak:

- Sistemen erantzulea.
- Datuak babesteko ordezkaria.

Batzordekideek honako eginkizun hauek izango dituzte:

- Bileretara bertaratzea, eztabaidetan parte hartzea eta galde-eskeak egitea.
- Beren boto eskubideaz baliatzea, botoaren zentzuaz gain botoa justifikatzen duten arrazoiak adieraztea.
- Batzordeak edo Batzordearen Presidentetzak esanbidez agintzen dizkion eginkizunak betetzea.
- Informazioaren Segurtasun Politika eta haren garapena batzordekideak ordezkari diren eremuan hedatu eta aplikatzen ote diren zaintzea.
- Ahalik eta informazio zehatzena lortzea esleitutako eginkizunak betetzeko.
- Batzordekide izateagatik dagozkion eginkizun guztiak betetzea.

5.2.3. Informazioaren Segurtasun Batzordearen Idazkaritza

Informazioaren Segurtasun Batzordearen Idazkaritza Batzordearen Presidentetzak izendatuko du LHKri atxikitako funtzionarioen artetik, eta ez da batzordekide izango.

Idazkariak honako eginkizun hauek ditu:

- Bileratara bertaratzea; hitza izango du, baina botorik ez.
- Bilkuren deialdiak kudeatzea Batzordearen Presidentetzak agintzen duenean.
- Bilkurak egiteko aretoa prestatzea.
- Bilkuren aktak idaztea, eta bere sinadurarekin eta Batzordearen Presidentetzaren oniritziarekin baimentzea.
- Batzordearen Presidentetzaren oniritziarekin onartutako akordioen, irizpenen eta kontsulten ziurtagiriak egitea.
- Organoko kide bakoitzaren komunikazioak, eta, horrenbestez, jakinarazpenak, datu eskaerak, zuzenketak, edo berak ezagutu behar dituen bestelako idazki mota guztiak jasotzea.
- Batzordekide izateagatik dagozkion eginkizun guztiak betetzea.

5.2.4. Informazioaren Segurtasun Batzordeko bestelako bertaratuak

Beren eginkizuna, ezagutza edo espezializazioa dela medio, Informazioaren Segurtasun Batzordearen bilkuraren batera deitu diren pertsonak bertaratu ahal izango dira; hitza izango dute, baina botorik ez.

5.2.5. Informazioaren Segurtasunaren erantzulea

Informazioaren Segurtasunaren erantzuleak informazioaren segurtasunaren eta zerbitzuen baldintzak betetzeko erabakiak zehaztu behar ditu.

Lan Harremanen Kontseiluaren idazkari nagusia izendatuko da Informazioaren Segurtasunaren erantzule.

Honako hauek dira Informazioaren Segurtasunaren erantzulearen eginkizunak:

- Informazioaren eta dagozkien erantzuleek ezarritako zerbitzuen segurtasun baldintzak betetzeko beharrezkoak diren erabakiak zehaztea.
- Erabiltzen den informazioaren eta informazio sistemek emandako zerbitzu elektronikoen segurtasuna sustatzea.
- Informazio sistemen segurtasunarekin lotutako dokumentazio oro aztertzea eta Informazioaren Segurtasun Batzordean aurkeztea Batzorde horrek onar dezan.
- Informazio sistemen segurtasun egoeraren jarraipena eta kontrola egitea, segurtasun neurriak egokiak direla egiaztatuz arriskuen azterketa eginez.
- Proposatutako segurtasun neurriak ezartzea ahalbidetuko duen segurtasunaren plan zuzentzailea osatuko duten proiektu eta jardun guztiak ezartzea eta informazio sistemaren erantzuleari aurkeztea.
- Segurtasun gorabeheren ikerketa egiten laguntzea eta ikerketa hori gainbegiratzea gorabeheren berri ematen denetik gorabeherak konpondu arte.
- Aldizkako segurtasun txostenak egitea Informazioaren Segurtasun Batzorderako. Txosten horietan denboraldi bakoitzeko gorabehera garrantzitsuenak bilduko dira.
- Aldizkako auditoriak egitea edo sustatzea segurtasun neurriak behar bezala aplikatzen direla eta informazioaren segurtasunaren alorreko antolamenduari dagokionez indarrean dauden arauak eta prozedurak betetzen direla bermatzeko. Auditoria horietatik ateratzen den txostena informazio sistemen erantzuleei eta zerbitzua ematen duen erantzuleari bidaliko zaie aurkitutako akatsak konpontzeko.

- Arriskuen azterketa egiteko metodologia eta tresnak zehaztea eta ezartzea.
- Beharrezkoa denean, SENari buruzko Informazio sistemen aplikagarritasunari buruzko aitorpenak idaztea.
- Zerbitzuen eta sistemen erantzuleekin batera, segurtasun prozedura eraginkorrez gain, jarraitutasun planak eta gorabeherei erantzuteko planak egitea.

5.2.6. Zerbitzuaren eta Informazioaren erantzulea

Zerbitzuaren eta Informazioaren erantzulea zerbitzuaren titularra da, eta behar adinako eskumena du dagokion zerbitzua emateari eta zerbitzuaren helburuari buruz erabakitzeko, baita tratatutako informazioaren helburuari, edukiari eta erabilerari buruz erabakitzeko ere. Era berean, segurtasun baldintzak zehaztu behar ditu, betiere Segurtasunerako Eskema Nazionala Administrazio Elektronikoaren eremuan arautzen duen urtarrilaren 8ko 3/2010 Errege Dekretuaren I. Eranskinean ezarritako esparruaren barnean.

Honako hauek dira Zerbitzuaren eta Informazioaren erantzulearen eginkizunak:

- Zerbitzuaren eta tratatutako informazioaren segurtasun mailak zehaztea eta eguneratuta edukitzea, informazioaren segurtasunari eragiten dieten gorabeheren inpaktuak balioetsiz, betiere SENaren 44. artikuluan ezarritakoaren arabera.
- Informazioaren Segurtasunaren erantzulearekin batera, derrigorrezko arrisku azterketak egitea, eta ezarri behar diren babesak hautatzea.
- Arriskuen azterketan kalkulatutako zerbitzuei buruzko hondar arriskuak onartzea.
- Informazioaren Segurtasunaren erantzulearekin batera, arriskuen jarraipena eta kontrola egitea.
- Informazioaren Segurtasunaren erantzulearen arabera, zerbitzu elektroniko bat emateari edo informazio jakin bat erabiltzeari uztea, baldin eta segurtasun akats larriak daudela jakinarazten bazaio.
- Informazioaren Segurtasunaren erantzulearekin batera, segurtasun prozedura eraginkorrez gain, jarraitutasun planak eta gorabeherei erantzuteko planak egitea.

5.2.7. Sistemen erantzulea

Sistemen erantzulea Informazioaren Segurtasun Batzordeak LHKri atxikitako funtzionarioen artetik izendatzen duen postu operatibo bat da, Erakundearen sistemak kudeatzeaz arduratzen dena. Zeregin hori SENean aipatzen den “Sistemaren erantzulearen” baliokidea da.

Honako hauek dira Sistemen erantzulearen eginkizunak:

- Informazio Sistemak garatzea, sistema horiekin lan egitea eta haiek mantentzea bizi ziklo osoan, haien zehaztasunen eta instalazioaren ziklo osoan, eta sistemak behar bezala ibiltzen direla egiaztatzea.
- Informazio Sistemen tipologia eta kudeaketa sistema definitzea; horretarako, sistema horien erabilera irizpideak eta sistema horietan eskuragarri dauden zerbitzuak ezarriko dira.
- Sistemen osagaien hornitzaileek sistemak garatzeko, instalatzeko eta probatzeko etapetan aplikatuko dituzten segurtasun neurriak erabakitzea, ziurtatuz segurtasun neurri espezifikoak behar bezala txertatzen direla segurtasun esparru orokorraren barnean.
- Sistemen erantzuleak erabaki dezake informazio jakin bat erabiltzeari edo zerbitzu jakin bat emateari uztea, baldin eta jakinarazten badiote ezarritako betekizunen asebetetze mailari eragin diezaioketen segurtasun akats larriak daudela. Erabaki hori eraginpean hartutako zerbitzuaren eta informazioaren erantzuleekin eta Segurtasunaren erantzulearekin adostu behar da, erabakia bete aurretik.

- Informazioaren Segurtasunaren erantzulearekin batera, segurtasun prozedura eraginkorrez gain, jarraitutasun planak eta gorabeherei erantzuteko planak egitea.

5.2.8. Sistemaren administratzailea

Sistemaren administratzailea Informazioaren Segurtasun Batzordeak LHKri atxikitako funtzionarioen artetik eta Informazioaren eta Komunikazioaren Teknologia zerbitzuak ematen dituen erakundetik kanpoko langileen artetik izendatutako postu operatibo bat da, sistemari eusteko eta sistema mantentzeko lanez arduratzen dena.

Honako hauek dira Sistemaren administratzailearen eginkizunak:

- Informazio Sistemari aplikatzekoak diren segurtasun neurriak ezartzea eta kontrolatzea, neurri horiek betetzen direla ziurtatuz.
- Informazio Sistemaren segurtasun mekanismoen eta zerbitzuen oinarri diren hardwarea eta softwarea kudeatzea, haien konfigurazioa eta eguneratzea kontrolatuz, segurtasun maila egokia izateko.
- Onartutako segurtasun prozedura eraginkorrak aplikatzea, baita prozedura horiek aplikatzen direla bermatzea ere.
- Hardwarearen eta softwarearen instalazioak eta beren aldaketak eta hobekuntzak gainbegiratzea segurtasuna ez dagoela arriskuan eta unean-unean berariazko baimenetara egokitzen direla bermatzeko.
- Segurtasun ekitaldiak kudeatzeko tresnek eta sisteman inplementatutako auditoria teknikoko mekanismoek emandako sistemaren segurtasun egoera monitorizatzea.
- Segurtasunarekin lotutako edozein anomaliaren, konpromisoren edo ahuleziaren berri ematea Informazioaren Segurtasunaren erantzuleari eta Sistemen erantzuleari.
- Segurtasun gorabeherak ikertzen eta konpontzen laguntzea, gorabeherak detektatzen direnetik konpontzen diren arte.

5.2.9. Tratamenduaren erantzulea

DBEOren xedapenen arabera, Tratamenduaren erantzulea, berak bakarrik edo beste batzuekin batera, tratamenduaren helburuak eta baliabideak ezartzen dituen pertsona fisikoa edo juridikoa, agintaritza publikoa, zerbitzua edo bestelako erakundea da.

Zeregin hori, Lan Harremanen Kontseiluari dagokiona, Zerbitzuaren eta Informazioaren erantzuleak beteko du, edo, hura egon ezean, Kontseiluaren Presidentetzak.

Honako hauek dira Tratamenduaren erantzulearen eginkizunak eta betebeharrak:

- Neurri tekniko eta antolamenduzko neurri egokiak aplikatzea tratamendua Erregelamenduarekin bat datorrela egiaztatzeko eta hori frogatu ahal izateko.
- Interesdunei jakinarazteko betebeharra betetzea, interesdunen onespena jasotzea beharrezkoa denean eta interesdunen eskubideak eta askatasunak zaintzea.
- Tratamendu jardueren erregistro bat egitea (DBEOren 30. artikulua). Erregistro hori idazki bidez jasoko da, baita formatu elektronikoan ere.
- Neurri tekniko eta antolamendu neurri egokiak aplikatzeko behar adinako bermeak eskaintzen dituzten erantzuleak soilik hautatzea.
- Kontratu edo egintza juridiko bat sinatzea erantzulearekin (DBEOren 28. artikulua). Kontratu hori idazki bidez jasoko da, baita formatu elektronikoan ere. Kontratu horrek tratamenduaren

xedea, iraupena, izaera eta helburua ezarriko ditu, baita interesdunen datu pertsonalen eta kategorien eredua, eta erantzulearen betebeharrak eta eskubideak ere.

- 55. artikuluaren arabera, segurtasun urratzeen berri ematea kontroleko agintaritza eskudunari atzerapen bidegaberik gabe, eta, ahal izanez gero, urratzearen berri izan ondorengo 72 orduetan beranduenez, betiere nekez gerta badaiteke segurtasun urratze hori arrisku bat izatea pertsona fisikoen eskubideetarako eta askatasunetarako.
- Datuak Babesteko ordezkari bat izendatzea DBEOren 37. artikuluan eta DBEDBLOren 34. artikuluan aurreikusitako kasuetan.

5.2.10. Datuak babesteko ordezkaria

DBEOren xedapenen arabera, Datuak babesteko ordezkaria datuak babesteari buruzko araudia betetzen dela bermatzeaz arduratuko da. Zeregin hori Informazioaren Segurtasun Batzordeak izendatzen du LHKri atxikitako funtzionarioen artetik eta aholkularitza espezializatuko zerbitzuak egiten dituen erakundetik kanpoko langileen artetik, eta hainbat pertsona fisikok edo juridikok partekatu ahal izango dute.

Honako hauek dira Datuak babesteko ordezkariaren eginkizunak:

- Informazioa ematea eta aholkatzea tratamenduaren erantzuleari edo arduradunari eta Erregelamendu honen eta Europar Batasuneko edo Estatu kideetako datu babesei buruzko bestelako xedapenen arabera dagozkien betebeharren tratamenduaz arduratzen diren langileei.
- Gainbegiratzea Erregelamendu honetan ezarritakoa, Europar Batasuneko edo Estatu kideetako datuak babesteari buruzko bestelako xedapenak eta datu pertsonalak babestearen arloan tratamenduaz arduratzen den erantzulearen edo arduradunaren politikak, tratamendu eragiketetan parte hartzen duten langileen erantzukizunak esleitzea, haien kontzientziazioa eta prestakuntza barne, eta dagozkion auditoriak betetzen ote diren.
- Datuak babesteari buruzko inpaktu ebaluazioaren gainean eskatzen zaion aholkularitza ematea eta DBEOren 35. artikulua aplikatzen ote den gainbegiratzea.
- Kontroleko agintaritzarekin lankidetzan aritzea.

Kontroleko agintaritzaren kontaktu puntua izatea tratamenduari buruzko gaietarako, 36. artikuluan aipatzen den aurretiko kontsultarako ere bai, eta beste edozein gairi buruzko kontsultak egitea, hala badagokio.

5.2.11. Tratamenduaren arduraduna

DBEOren xedapenen arabera, Tratamenduaren arduraduna, berak bakarrik edo beste batzuekin batera, tratamenduaren erantzulearen bitartez datu pertsonalak tratatzen dituen pertsona fisikoa edo juridikoa, agintaritza publikoa, zerbitzua edo bestelako erakundea da.

Honako hauek dira Tratamenduaren arduradunaren eginkizunak eta betebeharrak:

- Kontratu edo egintza juridiko bat sinatzea erantzulearekin (DBEOren 28. artikulua). Kontratu hori idazki bidez jasoko da, baita formatu elektronikoan ere. Kontratu horrek tratamenduaren xedea, iraupena, izaera eta helburua ezarriko ditu, baita interesdunen datu pertsonalen eta kategorien eredua, eta erantzulearen betebeharrak eta eskubideak ere.
- Kontratuan ezarritakoa betetzea, datu pertsonalak erantzulearekin adostutako helburuetarako soilik tratatuz; erantzuleak emandako agindu dokumentatuei jarraituz, eta erantzuleari lagunduz bere betebeharrak bete ditzan.

- Tratamendu jardueren erregistro bat egitea (DBEOren 30. artikulua). Erregistro hori idazki bidez jasoko da, baita formatu elektronikoan ere.
- Kontroleko agintaritzarekin lankidetzan aritzea (DBEOren 31. artikulua), agintaritza horrek eskatzen dion informazioa emanez eta agintaritzak bere eginkizunak gauzatuz agintzen diona betez.
- Egiten dituzten tratamenduei aplikatzekoak zaizkien segurtasun neurriak zehaztea (DBEOren 32. eta 33. artikuluak), arriskuarekiko egokia den segurtasun maila bermatzeko eta langileek kontratuaren mugak eta aplikatzekoa den legeria betetzen dituztela bermatzeko.
- Ezagutzen dituen segurtasun urratzeen berri ematea erantzuleari (DBEOren 33.2 artikulua) atzerapen bidegaberik gabe.
- Datuak Babesteko ordezkari bat izendatzea DBEOren 37. artikuluan eta DBEDBLOren 34. artikuluan aurreikusitako kasuetan.

5.3. Izendatzeko prozedura

LHKren Presidentetzari dagokio Informazioaren Segurtasun Batzordeko kideak izendatzea eta kargutik kentzea, politika honetan definitutako eskumenak betetzeko. Era berean, Presidentetzak izendatuko ditu Informazioaren Segurtasunaren erantzulea eta Datuak babesteko ordezkaria.

Zeregin horiek garrantzitsuak direnez, Informazioaren Segurtasun Batzordeko kideak, Informazioaren Segurtasunaren erantzulea eta Datuak berrikusteko ordezkariaren izendapenak 4 urtean behin berrikusiko dira edo Erakundean aldaketaren bat dagoenean edo lanposturen bat hutsik geratzen denean.

6. GIZA BALIABIDEEI BURUZKO SEGURTASUNA

LHK-k segurtasun neurriak ezarriko ditu langile guztientzat harremana izaten hasten denetik harremana amaitu arte. Neurri horiek LHKrekin zuzenean edo zeharka elkarlanean aritzen diren pertsona eta hirugarren erakunde guztiekin partekatuko dira.

Bereziki, prestakuntza eta kontzientziazio jarduerak gauzatuko dira langileak guztiz jabetzeko erakundearen jarduera guztiei eta erakundeko kide guztiei eragiten dien informazioaren segurtasunarekin duten erantzukizunaz, baita dauden arriskuekiko sentsibilitatea izateko ere.

Bi helburu daude: alde batetik, guztiz jabetzea informazioaren segurtasuna Erakundearen erabiltzaile guztien eta jardueren artean zabalduta eta banatuta dagoela, SENaren 5. artikuluan biltzen den Segurtasun Integralaren printzipioaren arabera; eta, bestetik, beharrezkoak diren baliabideak prestatzea prozesuan esku hartzen duten pertsona guztiek eta pertsona horien goragoko erantzuleek dauden arriskuekiko sentsibilitatea izan dezaten.

7. ARRISKUEN KUDEAKETA

Politika horri lotutako sistema guztiak arriskuak kudeatzeko prozesu baten mende jarri beharko dira, zer arriskuren eraginpean dauden ebaluatuz eta arrisku horiek arintzeko beharrezkoak diren kontraneurriekin tratatuz. Prozesuko azterketa honela errepikatuko da:

- Erregulartasunez, gutxienez urtean behin
- Erabilitako informazioa aldatzen denean
- Emandako zerbitzuak aldatzen direnean
- Segurtasunaren inguruko gorabehera larriren bat gertatzen denean
- Ahulezia larrien berri ematen denean

Arriskua aztertzeko eta kudeatzeko, MAGERIT metodologia (Informazio Sistemen Arriskuak Aztertzeko eta Kudeatzeko Metodologia) jarraituko da. Metodologia hori Administrazio Elektronikoaren Goi-mailako Kontseiluak egin du eta Administrazio Publikoetara bideratuta dago.

Arriskuen azterketak elkartzeko, Informazioaren Segurtasun Batzordeak erreferentziazko balioespen bat ezarriko du erabiltzen diren informazio mota desberdinetarako eta emandako zerbitzu desberdinetarako. Informazioaren Segurtasun Batzordeak dinamizatuko du baliabideen eskuragarritasuna sistemen segurtasun premiei erantzuteko, izaera horizontaleko inbertsioak sustatuz.

8. INFORMAZIOAREN SEGURTASUN POLITIKAREN GARAPENA

Informazioaren Segurtasun Politika hori LHKren alderdi espezifikoei aurre egingo dien Segurtasun Araudi baten bitartez garatuko da.

Segurtasun Araudia eskuragarri egongo da LHKren intranetean araudia ezagutu nahi duten Erakundeko kide guztientzat, bereziki LHKren informazio eta komunikazio sistemak erabiltzen, egikaritzen edo administratzen dituztenentzat.

9. LANGILEEN BETEBEHARRAK

LHK-ko langileek nahiz LHKrekin zuzeneko edo zeharkako lanbide loturaren bat duten pertsonek Informazioaren Segurtasun Politika hau eta berau garatzen duen araudia (Sistemak eta Informazioa Erabiltzeko Araudia sartzen da araudi horren barnean) bete beharko dute beren jardun eremuan. Informazioaren Segurtasun Batzordeari dagokio beharrezkoak diren baliabideak edukitzea informazioa eraginpekoei iristeko.

LHK-ko kide guztiak bertaratuko dira segurtasunaren arloko kontzientziazio bilkuretara Informazioaren Segurtasun Batzordeak erabakitzen duen eta prestakuntza eta kontzientziazio planean bilduta dagoen aldizkakotasunarekin.

IKT sistemen erabileran, operazioan edo administrazioan erantzukizuna duten pertsonek prestakuntza jasoko dute sistemak modu seguruan erabiltzeko, langile horiek beren lana egiteko prestakuntza hori behar duten heinean. Prestakuntza nahitaez egin beharko da edozein erantzukizun bere gain hartu aurretik, bai erantzukizun hori langileari lehenengo aldiz esleitu bazaio, bai langilea lanpostuz aldatu bada edo lanpostuan zuen erantzukizuna aldatu bazaio.

10. HIRUGARREN ALDERDIAK

LHK-k beste erakunde batzuei zerbitzuak ematen dizkienean edo beste erakunde batzuen informazioa erabiltzen duenean, Informazioaren Segurtasun Politika honen berri emango zaie, Informazioaren Segurtasun Batzordeak jakinaren gainean jartzeko eta haiekin koordinatzeko bideak ezarriko dira, eta segurtasun gorabeheren aurrean erreakzionatzeko jardun prozedurak ezarriko dira.

LHK-k hirugarrenen zerbitzuak erabiltzen dituenean, bere sistemetarako sarbidea errazten duenean edo hirugarrenei buruzko informazioa ematen duenean, Segurtasun Politika honen eta dagokion Segurtasun Araudiaren berri emango zaie. Hirugarren alderdi hori araudi horretan ezarritako betebeharren mende egongo da, eta bere prozedura operatiboak garatu ahal izango ditu araudi hori betetzeko.

Prozedura espezifikoak ezarriko dira jakinaren gainean jartzeko gorabeherei buruz eta gorabeherak konpontzeko, baita informazio konfidentziala trukatzeko ere, besteak beste.

Hirugarren alderdiek Segurtasun Politikaren eta dagokion Segurtasun Araudiaren berri eman beharko diete beren langileei, eta LHKri esanbidez adieraziko zaio ezagutzen dutela eta betetzeko konpromisoa hartzen

dutela, baita hura ez betetzearen ondorioz sortzen diren erantzukizunak beren gain hartuko dituztela ere. Ziurtatuko da hirugarrenen langileak behar bezala kontzientziatuta daudela segurtasunaren alorrean, Politika honetan ezarritako maila berean gutxienez.

Hirugarren alderdiren batek ezin badu Politikaren alderdiren bat bete aurreko paragrafoan eskatzen denaren arabera, Segurtasunaren erantzulearen txosten bat eskatuko da. Txosten horretan zehaztuko da zer arrisku dauden eta arrisku horiek nola tratatu behar diren. Txosten hori informazioaren eta eraginpeko zerbitzuen erantzuleek onartu beharko dute aurrera jarraitu aurretik.

11. INFORMAZIOAREN KONFIDENTZIALTASUNA

11.1. Informazio konfidentzialaren definizioa

LHK-k ofizialki edo indarreko legeria betez hedatu edo argitaratu ez duen informazio oro hartuko da informazio konfidentzialtzat.

Informazio konfidentziala hainbat modutara jasota egon daiteke, hala nola ahoz, ikusiz, idatziz, baliabide magnetikoetan edota beste edozein baliabide edo euskarritan grabatuta, ukitzeko moduan edo modu ukiezinean, “konfidentzial” gisa markatuta edo ez, eta LHK-ko langileek sortutako edo LHK-k nolabaiteko harremana duen hirugarren alderdiek emandako informazioa eduki dezake. Informazio konfidentzialaren barnean sartzen dira, halaber, datu pertsonalak.

Ezin izango da konfidentzialtzat hartu ohiko eta legezko informazio bideak erabiliz ezagutu daitekeen informazioa, ezta jende guztiak ezagutzen duen informazioa ere.

11.2. Konpromisoa

LHKren informazio konfidentzialean sartzen den pertsona orok –eta une honetatik aurrera enplegatu guztiek–, alde batera utzi gabe konpromisoa bere kontratuan ezarrita dagoen ala ez, konfidentzialtasun akordio bat sinatu beharko du. Akordio horretan esplizituki eta argi azalduko da informazio konfidentzialaren erabilera murriztailea izango dela nahitaez eta informazio hori isilpean gorde behar dela, informazio horretarako sarbidea eta hedapena mugatuz.

Betebehar hori LHK-ko langileei eskatuko zaie, kontuan izan gabe langile horiek beren kontratuetan konfidentzialtasun klausula sinatu duten edo ez. Betebehar horrek indarrean jarraituko du Erakundeari lotzen dion lan harremana iraungi ondoren ere.

11.3. Ezagutzera ez ematea

Informazio konfidentziala ezin da ezagutzera eman, salbu eta ezagutzera ematea ahalbidetzen duen aurretiko baimena badago. Baimen hori espresuki eta idazki bidez eman behar da, beharrezkoak diren baldintzetara soilik mugatuko da, eta, nolanahi ere, ahalik eta modu murriztailenean interpretatu beharko da.

Debeku horren barnean sartzen da LHKren informazio konfidentziala sare sozial pertsonalen bitartez edo LHK-ko enplegatuek edo langile laguntzaileek komunikatzeko erabiltzen dituzten antzeko moduen bitartez ezagutzera ematea.

11.4. Erabilera

Informazio konfidentzialaren erabilera lan jarduera edo lanbide jarduera garatzeko behar-beharrezkoa denera murriztu beharko da, aplikatzekoak diren legeak eta araudiak, sinatutako konfidentzialtasun

kontratuak eta barne politikak eta barne kodeak, bereziki konfidentzialtasun politika hau, errespetatu behar ditu.

Debekatuta dago informazio konfidentziala edozein modutan artxibatzea, biltzea, erabiltzea edo tratatzea, hori justifikatzen duten lan edo lanbide arrazoiak badaude izan ezik. Hala ere, beharrezkoak diren neurriak ezarriko dira informazioaren konfidentzialtasuna bermatzeko.

11.5. Itzultzea edo suntsitzea

LHKren informazio konfidentziala duten pertsonek, edozein euskarri motatan (dokumentazioa edo fitxategia), ulertu beharko dute informazio hori aldi baterako soilik edukiko dutela, eta horrek ez diela inolako eskubiderik ematen informazio horren jabe egiteko edo informazio hori kopiatzeko.

Era berean, material horiek Erakundeari itzuli beharko zaizkio material horiek aldi batean erabiltzea eragin duten zereginak amaitu bezain laster, eta, nolanahi ere, kontratu harremana amaitzen denean. Material horiek beharrezkoak ez badira eta material horiek suntsitzeko baimena izanez gero, material horiek suntsitu egin beharko dira, araudiaren xedapenen arabera, zereginak amaitu ondoren.

12. DATU PERTSONALEN BABESA

LHK-k, bere eginkizunak betez, datu pertsonalak erabili behar ditu. Horregatik, interesdunen eskubideak eta askatasunak bermatuko dira, baita informazioaren, komunikazioen eta tratamenduen euskarri diren informazio sistemen segurtasuna ere indarreko legerian aurreikusitako neurrien arabera.

Beharrezkoak diren bermeak lortzeko, honako bidezko ekintza hauek guztiak egingo dira:

- Tratamenduei buruzko arrisku azterketak egitea, baita pribatutasunean duen eraginaren ebaluazioak ere tratamenduen ondorioz eraginpean hartutakoen eskubideak eta askatasunak arrisku handian jar badaitezke.
- Neurri teknikoak eta antolamendu teknikak diseinatzea eta ezartzea datu pertsonalen tratamenduei buruzko arriskuak arintzeko automatikoki eta diseinutik abiatuta.
- Berriro diseinatzea arindu eta onartu ezin diren arriskuak arintzeko prozesuak.
- Behar den dokumentazio oro egitea prozesuei eusteko eta eraginpean hartutakoen eskubideak eta askatasunak bermatzeko, indarreko araudiak ezarritako printzipioak betez.
- Betebeharrak helaraztea datu pertsonaletarako sarbidea duten langile guztiei.
- Tratamenduaz arduratzen diren pertsonekiko harremanak kudeatzea ezarritako irizpide batzuen arabera, betebeharrak eta segurtasun baldintzak formalizatzen dituzten kontratuen bitartez arautzea barne.
- Tratamendu jardueren erregistro bat mantentzea.
- Aplikatzekoak diren legeen xedapenen arabera, eskatutako epeen barnean honako honen berri ematea datuak babesteko eskumena duen agintaritzari:
  - Egindako tratamenduak.
  - Egindako inpaktu ebaluazioen emaitzak.
  - Europar Batasunetik (EB) kanpo egingo diren nazioarteko transferentziak.
  - Datuak babesteko ordezkaria (DBO) izendatzea eta harekin harremanetan jartzeko datuak.
  - Interesdunen eskubideen eta askatasunen aurka arriskua izatea ekarriko duten segurtasun urratzeak, urratze horiek detektatu ondorengo 72 orduetan.
  - Lege batek edo datuak babesteko eskumena duen agintaritzak aginduta eskatzen den edozein informazio.
- Tratamenduen eraginpean daudenei tratamenduei buruzko geruzen araberako informazioa ematea, labur, gardentasunez, ulertzeko moduan eta erraz eskuratzeko moduan.

- Eraginpekoen baimena espresuki eta argi jasotzea, eta tratamenduekin hasi aurretik eta/edo lagapenak ezarri aurretik.
- Eraginpekoen eskubideen eta askatasunen aurka arrisku handi bat eragiten duten Segurtasun urratzeak jakinaraztea eraginpekoei urratze horiek detektatu ondorengo 72 orduetan.

13. BERRIKUSTEKO PROZEDURA

Informazioaren Segurtasun Batzordearen egitekoa izango da Informazioaren Segurtasun Politika hori urtero berrikustea eta Politika hori berrikusteko edo mantentzeko proposamena egitea.

Bidezkoa bada aldaketa eta/edo eguneratze bat egitea eta proposatzea, Politika Alkatetzara igorriko du Informazioaren Segurtasun Batzordeak, eta Politika hori onartu ostean, Informazioaren Segurtasun Batzordeak banatuko du eraginpeko alderdi guztiek horren berri izan dezaten.

14. ONARTZEA ETA INDARREAN JARTZEA

2019ko maiatzaren 6an presidenteak onartutako testua.

Informazioaren Segurtasun Politika hau eraginkorra izango da data horretatik aurrera eta Politika berri batek ordezkatzen duen arte.

15. ALDAKETEN HISTORIA

ALDAKETEN HISTORIA		
Bertsioa	Data	Aldaketaren deskribapena
001	2019/04/08	Dokumentuaren lehen bertsioa