DOKUMENTUAREN PROPIETATEAK

SORRERA DATA:	2019/10/04	**DOKUMENTUAREN SAILKAPENA**	Erabilera ofiziala - Barnekoa

SINADUREN KONTROLA

	DATA	SINADURA
EGILEA: Segurtasun arduraduna	2024/04/19	
ONARTZAILEA Segurtasun Batzordea	2024/07/16	

BERTSIOEN HISTORIKOA

BERTSIOA	DATA	EGILEA	ALDAKETAK
1.0	2019/10/04	Segurtasun arduraduna	Dokumentuaren hasierako bertsioa
1.1	2022/01/27	Segurtasun arduraduna	“Zibersegurtasuneko eta araudia betetzeko bulegoa” txertatzea Bileren maiztasuna aldatzea. Arau esparrua eguneratzea Bestelako aldaketak
1.2	2024/04/19	Segurtasun arduraduna	311/2022 Errege Dekretura, maiatzaren 3kora, SENa arautzen duenera, egokitzea.

Aurkibidea

1. ONESTEA ETA INDARREAN SARTZEA

DonostiaTIKeko zuzendaritzak 2019ko urriaren 9an onartutako testua.

“Informazioaren Segurtasunerako Politika” hau (aurrerantzean, Politika), indarrean sartuko da data horretan, eta hala jarraituko du Politika berri batek indargabetu arte.

Politika hau Donostiako Udalaren Informazioaren Segurtasunerako Politikan txertatzen da, DonostiaTIK Udalaren mendeko tokiko erakunde autonomo bat delako; hortaz, haren erregulazioa politika horretan jasotako edukira egokitzen da, organismoaren berezitasunei dagozkien berezko egokitzapen propioak eginda.

2. SARRERA

Administrazio Elektronikoaren garapena dela eta, informazio eta komunikazioen teknologien sistemek informazio kantitate handiak tratatu behar dute. Informazio hori, ordea, sistema horiek kaltetu ditzaketen mehatxu eta urrakortasun mota askoren menpe dago. Administrazio Elektronikoaren esparruan Segurtasun Eskema Nazionala (SEN) arautzen duen 311/2022 Errege Dekretuaren, maiatzaren 3koaren, helburua da informazio sistemak konfiantzazkoak izatea, dagokien funtzio zehazten arabera beren zerbitzuak etenaldirik gabe edo kontrolaz kanpoko aldaketarik gabe eskaintzea eta gordetzea, eta informazioa baimendu gabeko pertsonengana ez iristea.

SENa betetzeko xedean, herritarren eskura jarritako izapide elektronikoak bideratu behar dituzten informazio sistemak kaltetu ditzaketen arriskuen berri duenez, eta

kontuan izanik herritarrek Udalaren eskura jartzen dutela beren aktiborik baliotsuena, “beren informazioa”, DonostiaTIK ongi asko jabetzen da informazio sistemak behar bezala kudeatu behar direla eta hartu beharreko neurriak hartu behar direla tratatutako informazioari edo eskainitako zerbitzuen eskuragarritasunari, osotasunari edo konfidentzialtasunari nahi gabe edo nahita egin dakizkiekeen kalteen aurrean.

Horrenbestez, Segurtasun Eskema Nazionalaren (SEN) baitara biltzen diren DonostiaTIKeko departamentu eta/edo arlo guztiek kontuan izan behar dute IKTen segurtasuna sistemaren bizi zikloaren etapa bakoitzaren zati integrala dela, sistema sortzen denetik zerbitzutik ateratzen den arte, tartean igarota garapen edo eskuratze erabakiak eta ustiapen jarduerak. Segurtasun baldintzak eta finantzaketa beharrak zehatz identifikatu eta jaso behar dira plangintzan, eskaintzen eskaeran eta IKT proiektuen alorreko lizitazioko baldintza agirietan.

Beraz, DonostiaTIKentzat, Informazioaren Segurtasunaren helburua da informazioaren kalitatea eta zerbitzuen eskaintza etengabea bermatzea, eta, horretarako, eguneroko jarduera gainbegiratuko du edozein gorabehera hautemateko, eta prestasun osoz jardungo du gorabehera horiei aurre egin eta ahalik eta lasterren berregokitzeko, SENaren 8. artikuluan ezarritakoarekin bat etorrita.

3. DONOSTIATIKEN MISIOA

DonostiaTIKen misioa da kalitatezko zerbitzu teknologikoak ematea: informatikoak, telekomunikazioetakoak eta bestelakoak. Horretarako, konponbide integralak eta homogeneoak eskainiko dizkie bai udal antolakuntzari, herritarrei zerbitzu hobea eman diezaien, bai donostiar guztiei.

Helburu horiek erdiesteko, DonostiaTIKek bere gain hartzen du honako zerbitzu eta jarduera hauek kudeatzea eta egitea Donostiako Udalari eta haren mendeko beste organismo eta sozietate publiko batzuei:

- Prozedura informatikoa aplikatzea.
- Ahots komunikazioen eta datuek kudeaketa integrala.
- Datu Prozesuaren Zentroa sortzea eta ustiatzea, independentzia, datuen zaintza eta kualifikazioa behar bezala bermatuta.
- Telekomunikazio zerbitzuak eta aplikazio informatiko osoak, programak, ekipamenduak, aholkulariak eta DPZaren gaitasuna osatzeko edo eraginkortasuna hobetzeko behar den edozein elementu material eta giza bitarteko kontratatzea.
- Telekomunikazioko zerbitzuak eta zerbitzu informatikoak ezartzea.
- Lankidetza hitzarmenak edo zerbitzuak ematekoak egitea.
- Udal jarduerari aplikatutako telekomunikazioen eta informatikaren askotariko alderdien inguruko ikerketa, aholkularitza eta prestakuntza.

- Aurrekoekin lotutako edozein zerbitzu edo jarduera.

4. IRISMENA

Politika hau DonostiaTIKek kudeatutako udal informazio sistemei aplikatuko zaie; izan ere, DonostiaTIKek zerbitzuak ematen eta jarduerak egiten ditu Donostiako Udalarentzat, haren erakunde autonomoentzat eta sozietateentzat, organismoaren sorreran zehaztutako helburuak betetzeko, bere estatutuen 7. artikuluan jasota dagoenez. Haren eginkizunak, berriz, 2. “DONOSTIATIKEN MISIOA” atalean zerrendatzen dira.

SENaren irismenaren barruan dauden DonostiaTIKeko kide guztiek nahitaez ezagutu eta bete behar dituzte “Informazioaren Segurtasunerako Politika” hau eta segurtasunaren alorreko araudia, eta Informazioaren Segurtasun Batzordearena izango da informazioa dagokien langileei helarazteko beharrezkoak diren bitartekoak jartzeko ardura.

5. ARAU ESPARRUA

DonostiaTIKen jarduerak eta, bereziki, zerbitzu elektronikoak garatzeko arau esparrua honako arau hauek osatzen dute:

- 311/2022 Errege Dekretua, maiatzaren 3koa, administrazio elektronikoaren alorrean Segurtasun Eskema Nazionala arautzen duena.
- 4/2010 Errege Dekretua, urtarrilaren 8koa, Administrazio Elektronikoaren esparruan Elkarreragingarritasun Eskema Nazionala arautzen duena.
- Ebazpena, 2016ko urriaren 13koa, Administrazio Publikoen Estatu Idazkaritzarena, Segurtasun Eskema Nazionalaren araberako Segurtasun Jarraibide Teknikoa onesten duena.
- Ebazpena, 2016ko urriaren 7koa, Administrazio Publikoen Estatu Idazkaritzarena, Segurtasunaren Egoeraren Txostenari dagokion Segurtasun Jarraibide Teknikoa onesten duena.
- Ebazpena, 2018ko martxoaren 27koa, Administrazio Publikoen Estatu Idazkaritzarena, Informazio Sistemen Segurtasun Auditoretzari dagokion Segurtasun Jarraibide Teknikoa onesten duena.
- Ebazpena, 2018ko apirilaren 13koa, Administrazio Publikoen Estatu Idazkaritzarena, Segurtasun Gorabeheren Jakinarazpenari dagokion Segurtasun Jarraibide Teknikoa onesten duena.
- 3/2018 Lege Organikoa, abenduaren 5ekoa, datu pertsonalak babesteari eta eskubide digitalak bermatzeari buruzkoa.

- 15/1999 Lege Organikoa, abenduaren 13koa, Datu Pertsonalak Babesteari buruzkoa, 23. eta 24. artikuluak.
- 2016/679 Erregelamendua (EB), Europako Parlamentu eta Kontseiluarena, 2016ko apirilaren 27koa, pertsona fisikoak babesteari buruzkoa, datu pertsonalen tratamenduari eta datuon zirkulazio libreari dagokionez; horren bidez indargabetu egiten da 95/46/EE Zuzentaraua (Datuak Babesteko Erregelamendu Orokorra).
- 7/1985 Legea, apirilaren 2koa, Toki Araubidearen Oinarriak arautzen dituena, apirilaren 21eko 11/1999 Legeak aldatua.
- 1308/1992 Errege Dekretua, urriaren 23koa, Armadaren Errege Institutua eta Behatokia Espainiako Metrologia Zentroari lotutako denboraren patroi nazionala eta laborategia gordetzeko laborategi izendatzen dituena.
- 34/2002 Legea, uztailaren 11koa, informazio gizartearen eta merkataritza elektronikoaren zerbitzuei buruzkoa.
- 57/2003 Legea, abenduaren 16koa, tokiko gobernua eraberritzeko neurriei buruzkoa.
- 1553/2005 Errege Dekretua, abenduaren 23koa, nortasun agiri nazionala eta horren sinadura elektronikoko ziurtagiriak nola eman arautzen duena.
- 37/2007 Legea, azaroaren 16koa, sektore publikoaren informazioa berrerabiltzeari buruzkoa.
- 25/2007 Legea, urriaren 18koa, komunikazio elektronikoei eta komunikazio sare publikoei buruzko datuak kontserbatzeari buruzkoa.
- 56/2007 Legea, abenduaren 28koa, informazioaren gizartea bultzatzeko neurriei buruzkoa.
- 56/2007 Legea, abenduaren 28koa, informazioaren gizartea bultzatzeko neurriei buruzkoa.
- 1494/2007 Errege Dekretua, azaroaren 12koa, desgaitasuna duten pertsonek informazioaren gizartearekin eta gizarte komunikabideekin lotutako teknologiak, produktuak eta zerbitzuak eskuratzeko oinarrizko baldintzei buruzko erregelamendua onesten duena.
- 1495/2011 Errege Dekretua, urriaren 24koa, sektore publikoko informazioa berrerabiltzeari buruzko azaroaren 16ko 37/2007 Legea garatzen duena Estatuko sektore publikoaren eremurako.
- 19/2013 Legea, abenduaren 9koa, gardentasunari, informazio publikoa eskuratzeko bideari eta gobernu onari buruzkoa.
- 9/2014 Legea, maiatzaren 9koa, Telekomunikazioei buruzkoa.

- 39/2015 Legea, urriaren 1ekoa, Administrazio Publikoen Administrazio Prozedura Erkidearena.
- 5/2015 Legegintzako Errege Dekretua, urriaren 30ekoa, Enplegatu Publikoaren Oinarrizko Estatutuaren Legearen Testu Bategina onesten duena.
- 9/2017 Legea, azaroaren 8koa, Sektore Publikoko Kontratuena, Europako Parlamentuaren eta Kontseiluaren 2014ko otsailaren 26ko 2014/23/EB eta 2014/24/EB zuzentarauen transposizioa egiten duena Espainiako ordenamendu juridikora.
- 12/2018 Errege Lege Dekretua, irailaren 7koa, Sareen eta Informazio Sistemen Segurtasunari buruzkoa.
- 1112/2018 Errege Dekretua, irailaren 7koa, sektore publikoko gailu mugikorren webguneen eta aplikazioen irisgarritasunari buruzkoa.
- 14/2019 Errege Lege Dekretua, urriaren 31koa, segurtasun publikoko arrazoiengatik presako neurriak hartzen dituena administrazio digitalaren, sektore publikoko kontratazioaren eta telekomunikazioen arloan.
- 6/2020 Legea, azaroaren 11koa, arlo horretan konfiantzazko zerbitzu elektronikoen zenbait alderdi arautzen dituena.
- 24/2021 Errege Lege Dekretua: 9/2017 Legea eta 3/2020 Errege Lege Dekretua aldatzea.
- 203/2021 Errege Dekretua, martxoaren 30ekoa, Sektore Publikoaren bitarteko Elektronikoen bidezko Jarduera eta Funtzionamenduari buruzko Erregelamendua onesten duena.
- 10/2021 Legea, uztailaren 9koa, urrutiko lanari buruzkoa.
- 2/2016 Legea, apirilaren 7koa, Euskadiko Toki Erakundeei buruzkoa.
- 4/2019 Foru Araua, martxoaren 11koa, Gobernu Onari buruzkoa foru gobernantza publikoaren esparruan.
- Donostiako Udal Gobernu Batzarraren 2016ko maiatzaren 17ko ebazpena, Informazioaren Segurtasunerako Politika onartu zuena eta hurrengo aldaketak.
- 163/2018 EBAZPENA, abenduaren 12koa, Jaurlaritzaren Idazkaritzako eta Legebiltzarrarekiko Harremanetarako zuzendariarena, zeinaren bidez xedatzen baita argitara ematea Gipuzkoako Foru Aldundiarekin sinatutako lankidetza hitzarmena, administrazio elektronikoko oinarrizko irtenbideak elkarri ematekoa.
- Administrazio elektronikoko oinarrizko irtenbideak elkarri emateko Euskal Autonomia Erkidegoko Administrazio Orokorrak Estatuko Administrazio Orokorrarekin 2017ko martxoaren 24an eta Gipuzkoako Foru Aldundiarekin 2018ko abenduaren 5ean sinatutako lankidetza hitzarmenei atxikitzeko protokoloa.

- Eta aplikagarriak diren gainerako arauak, hala nola Ondare Historikoaren Legea, Jabetza Intelektuala Babesteari buruzkoa, etab.

Horrez gain, arau esparruaren barruan sartzen dira aurrekoetatik eratorri eta egoitza elektronikoetan argitaratu diren eta administrazio elektronikoari aplika dakizkiokeen gainerako arau guztiak, politika honen aplikazio eremuaren barrukoak.

Arau esparrua mantentzea Informazioaren Segurtasunerako Batzordearen ardura izango da, bat etorriko da Donostiako Udalaren Informazioaren Segurtasunerako Politikaren aldaketekin, eta dokumentu honen eranskin batean mantenduko da, segurtasun politika eguneratzen den arte. Arlo horretan eskumena duen organoak argitaratutako eta nahitaez bete beharreko segurtasun jarraibide teknikoak barne, Administrazio Elektronikoaren Batzorde Sektorialak proposatuta eta Zentro Kriptologiko Nazionalaren (CCN) ekimenez, Segurtasun Eskema Nazionalean ezarritako moduan.

Halaber, Batzordearen ardura izango da Segurtasun Eskema Nazionalean ezarritakoa hobeto betetzeko aplikagarriak izango diren CCNren segurtasun gidak identifikatzea.

6. ARTIKULUAK BETETZEA

Administrazio elektronikoaren arloan Segurtasun Eskema Nazionala arautzen duen errege dekretuaren, oinarrizko printzipioak eta gutxieneko baldintzak jasotzen dituenaren, artikuluak betetzeko, DonostiaTIKek hainbat segurtasun neurri ezarri ditu. Neurri horiek babestu beharreko informazioaren eta zerbitzuen izaerarekiko proportzionalak dira, eta haiek ezartzean, kontuan hartu da eraginpeko sistemen kategoria.

Segurtasuna prozesu integral gisa eta gutxieneko pribilegioa

Segurtasuna prozesu integral gisa ulertuko da, eta prozesu hori sistemari lotutako elementu tekniko, giza elementu eta elementu material guztiek osatuko dute, baita antolakuntzako elementuek ere. Segurtasun Eskema Nazionala DonostiaTIKi aplikatzean, printzipio hori aplikatuko da, edozein jarduketa zehatz edo egoeraren ondoriozko tratamendu kanpo uzten duena.

Ahalik eta arreta handiena jarriko zaio prozesuan esku hartzen duten pertsonak eta haien hierarkiako arduradunak kontzientziatzeari, ezjakintasuna, antolaketa eta koordinazio falta edo jarraibide desegokiak segurtasunerako arrisku iturri izan ez daitezen.

Informazio sistemak diseinatzean, funtzioak ondo betetzeko behar diren gutxieneko pribilegioak bakarrik emango dira, eta, horretarako, honako alderdi hauek txertatu behar dira:

a) Sistemak erakundeak bere eskumeneko edo kontratuetako helburuak lor ditzan beharrezkoa den gutxieneko funtzionaltasuna emango du.

b) Jardueraren eragiketa, administrazio eta erregistro funtzioak gutxienekoak izango dira, eta ziurtatuko da baimendutako pertsonek bakarrik, baimendutako ekipo edo lekuetatik bakarrik, eskuratu daitezkeela. Hala behar bada, ordutegi murrizketak eta sarbide gune ahaldunduak ezarriko dira.

c) Ustiapen sistemako funtzioak ezabatu edo desaktibatuko dira, baldin eta interesekoak edo beharrezkoak edo lortu nahi den helbururako egokiak ez badira. Sistemaren erabilera arruntak erraza eta segurua izan behar du; hala, erabilera ez seguru bat egiteko, erabiltzaileak ekintza kontziente bat egin beharko du.

d) Segurtasuna ezartzeko gidak aplikatuko dira, teknologia ezberdinetarako, sistemaren kategorizaziora egokituak, beharrezkoak edo egokiak ez diren funtzioak kentzeko edo desaktibatzeko.

Etengabeko zaintza, aldizkako berrebaluazioa eta osotasuna, sistema eguneratzea eta segurtasun prozesua etengabe hobetzea.

DonostiaTIKen etengabeko zaintzak aukera emango du jarduera edo jokabide anomaloak detektatzeko eta behar bezala erantzuteko.

Aktiboen segurtasun egoeraren etengabeko ebaluazioak aukera emango du haien bilakaera neurtzeko, zaurgarritasunak detektatuko eta ezarpen gabeziak identifikatuko baitira.

Segurtasun neurriak aldizka berrebaluatuko eta eguneratuko dira, eta haien eraginkortasuna arriskuen eta babes sistemen bilakaerari egokituko zaio; hortaz, baliteke segurtasuna birplanteatu behar izatea, beharrezkoa bada.

Sistemaren aktiboetan elementuak, hala fisikoak nola logikoak, sartu edo aldatu baino lehen, beharrezkoa da horien baimen formal bat edukitzea.

Ebaluazio eta monitorizazio etengabeak aukera emango dute sistemen segurtasun egoera egokitzeko, ezarpen gabezien, identifikatutako zaurgarritasunen eta eragiten dieten eguneratzeen arabera, baita haiei eragiten dien edozein intzidentzia garaiz detektatzeko ere.

Ezarritako segurtasun prozesu integrala etengabe eguneratu eta hobeto beharko da. Horretarako, jardun nazionalean eta nazioartekoan aintzatetsitako irizpideak eta metodoak aplikatuko dira, informazio teknologien segurtasuna kudeatzearen ingurukoak.

Langileen kudeaketa eta profesionaltasuna

DonostiaTIKeko kide guztiek, zeinak SENen eremuaren barruan baitaude, segurtasun arloan dituzten betebeharren, obligazioen eta arduren prestakuntza eta informazioa jasoko dute Haien jarduna gainbegiratu egingo da, ezarritako prozedurei jarraitzen dietela egiaztatzeko.

Sistemaren erabilera seguruaren esanahia eta irismena zehaztu eta islatu egingo da dagokion zuzendaritzak edo organo gorenak onetsitako segurtasun arauetan. Halaber, langileek beren lanpostuan jarduteko behar duten gutxieneko prestakuntza eta esperientzia zehaztuko dira.

Segurtasun sistemetako segurtasuna langile kualifikatu, dedikatu eta ikasiek artatuko, berrikusiko eta auditatuko dute, bizi zikloko fase guztietan: plangintza, diseinua, eskuratzea, eraikuntza, ezartzea, ustiatzea, mantentzea, intzidentziak kudeatzea eta desegitea.

Era objektiboan eta diskriminaziorik gabe, eskatuko da zerbitzuak ematen dizkiguten erakundeek profesional kualifikatuak izatea, emandako zerbitzuen kudeaketa eta heldutasun maila egokia dutenak.

Arriskuetan oinarritutako segurtasunaren kudeaketa eta arriskuen analisia eta kudeaketa

Arriskuen analisia eta kudeaketa segurtasun prozesuaren funtsezko zati bat izango da, eta jarduera jarraitua izango da, etengabe eguneratua.

Arriskuen kudeaketak aukera emango du ingurune kontrolatu bat mantentzeko, eta, beraz, arriskuak maila onargarrietara murrizteko. Maila horietara murrizteko, segurtasun neurriak era egokian, orekatuan eta tratatutako informazioaren, eman beharreko zerbitzuen eta dituzten arriskuen nolakotasunaren neurrikoan ezarriko dira.

Kudeaketa hori egiteko, sistemak dituen arriskuak aztertuko eta tratatuko dira. II. eranskinean xedatutakoa hargatik eragotzi gabe, nazioartean aintzatetsitako metodologiaren bat erabiliko da. Arriskuak apaltzeko edo ezabatzeko hartutako neurriek justifikatuta egon beharko dute, eta, nolanahi ere, arriskuen neurrikoak izango dira.

Segurtasun gorabeherak, prebentzioa, detekzioa, erreakzioa eta suspertzea

DonostiaTIKek segurtasun gorabeherak kudeatzeko prozedura bat du, detekzio mekanismoak, sailkapen irizpideak eta analisi eta ebazpen prozedurak ere bai, baita interesdunei komunikatzeko bideak ere.

Sistemaren segurtasunak prebentzio, detekzio eta erantzunerako ekintzak aurreikusiko ditu, zaurgarritasunak txikitzeko eta dituen mehatxuak ez materializatzea lortzeko edo, gertatzen bada, erabiltzen duen informazioari edo ematen dituen zerbitzuei larri ez eragiteko.

Prebentzio neurriek disuasiorako edo arrisku azalera txikitzeko osagaiak izan ahalko dituzte, eta mehatxuak materializatzeko aukera kendu edo murriztu behar dute.

Detekzio neurrien xedea izango da zibergaizkile bat dagoen jakitea.

Erantzuteko neurriak behar diren unean kudeatuko dira, eta haien xedea izango da segurtasun gorabehera batek ukitutako informazioa eta zerbitzuak lehengoratzea.

Informazio sistemak formatu elektronikoko datuen eta informazioen kontserbazioa bermatuko du.

Halaber, sistemak zerbitzuak eskuragarri mantenduko ditu informazio digitalaren bizi ziklo guztian, ondare digitala mantentzeko oinarria diren ikusmoldeari eta prozedurei jarraituz.

Defentsa lerroak eta prebentzioa elkarri konektatutako beste sistema batzuetan

DonostiaTIKek geruza askotan oinarritutako babes estrategia bat ezarri du. Geruza horiek antolakuntza neurriek eta neurri fisikoek eta logikoek osatzen dituzte; horrela, horietakoren bat arriskuan badago, erreakzio egokia gara daiteke saihestu ahal izan ezin diren gorabeheren aurka, eta, hortaz, txikitu egiten da sistema osoa arriskuan jartzeko aukera eta hartan izango duen azken eragina.

Informazio sistemaren perimetroa babestuko da, bereziki entitatearen sistema sare publikoetara konektatzen denean, 9/2014 Legean, maiatzaren 9koan, Telekomunikazioei buruzkoan definitzen diren moduan; izan ere, segurtasun gorabeheren prebentzio, detekzio eta erantzun lanak indartuko dira orduan.

Nolanahi ere, sistema beste sistema batzuekin konektatzetik eratorritako arriskuak aztertuko dira, eta haien batze puntua kontrolatuko da. Sistemen arteko elkarrekiko konexioa egokia izan dadin, dagokion segurtasun jarraibide teknikoan xedatutakoari jarraituko zaio.

Funtzioak bereiztea eta segurtasun prozesua antolatzea eta ezartzea

DonostiaTIKek bere segurtasuna korporazioko kide guztiak konprometituz antolatu du, argi bereizitako erantzukizunak dituzten segurtasun rolak izendatuta, dokumentu honen “SEGURTASUNAREN ANTOLAKUNTZA” atalean jasota dagoenaren arabera.

Sarbideen baimena eta kontrola

DonostiaTIKek informazio sistemara sartzeko kontrol mekanismoak ezarri ditu, beharrezkoak diren eta behar bezala baimenduta dauden erabiltzaileetara, prozesuetara, gailuetara eta bestelako informazio sistemetara mugatuta, eta baimendutako funtzioetara soilik.

Instalazioen babesa

DonostiaTIKek sarbide fisikoa kontrolatzeko mekanismo bat ezarri du, baimenik gabeko sarbideak aurreikusita, baita informazioari eta baliabideei egindako kalteak ere; hala, segurtasun perimetroak, kontrol fisikoak eta arloetako babes orokorrak finkatu ditu.

Segurtasun produktuak eskuratzea eta segurtasun zerbitzuak kontratatzea

DonostiaTIKek, segurtasun produktuak eskuratzean edo zerbitzuak kontratatzean, sistemaren kategoriaren neurriko erabilera eta zehaztutako segurtasun maila kontuan hartuko ditu, baita eskuratzearen xedearekin lotutako segurtasun funtzionalitate ziurtatua edukitzea ere.

Segurtasun zerbitzuak kontratatzeko, profesionaltasunaren inguruan xedatutakoari jarraituko zaio.

Biltegiratuta eta iragaitzazko informazioaren babesa eta jardueraren jarraikortasuna

DonostiaTIKek arreta berezia jarriko dio informazio biltegiratuari edo iragaitzazkoari, ekipamenduetan edo gailu eramangarri edo mugikorren, gailu periferikoen, informazio euskarrien eta sare irekietako komunikazioen bidezkoari, zeinak bereziki aztertu beharko baitira babes egokia lortzeko.

Epe luzean errege dekretu honen aplikazio eremuan sartutako informazio sistemek sortutako dokumentu elektrikoak berreskuratzeko eta kontserbatzeko prozedurak aplikatuko dira, beharrezkoa denean.

Errege dekretu horrek aipatutako informazio elektronikoaren zuzeneko kausa edo ondorioa den eta euskarri ez elektronikoan dagoen informazio hori haren segurtasun maila berarekin babestu beharko da. Horretarako, euskarriaren nolakotasunaren araberako neurriak aplikatuko dira, aplikagarriak diren arauei jarraituz.

Sistemek segurtasun kopiak izango dituzte eta ohiko bitartekoak galduz gero eragiketekin jarraitzeko behar diren mekanismoak ezarriko dira.

Jarduera erregistroak eta kode kaltegarria detektatzea

DonostiaTIKek, errege dekretuaren xedea betetzeko asmoz, eta ukitutakoen ohorerako, norberaren eta familiaren intimitaterako eta norberaren irudirako eskubidea guztiz bermatze aldera, datu pertsonalak babesteari buruzko araudiari, funtzio publikoaren edo lanaren ingurukoari eta aplikagarriak diren gainerako xedapenei jarraituz, erregistratu egingo ditu erabiltzaileen jarduerak, eta jarduera desegokiak edo baimendu gabeak monitorizatzeko, aztertzeko, ikertzeko eta dokumentatzeko behar-beharrezkoa den informazioa bilduko du, une oro identifikatu ahal izateko nor ari den jardunean.

Informazio sistemen segurtasunari eusteko, eta administrazio publikoen jarduketaren printzipioak zorrotz betetzen direla bermatzeko, eta, Datuak Babesteko Erregelamendu Orokorrean xedatutakoari jarraituz, bertan jasotako helburua mugatzeko, datuak minimizatzeko eta kontserbazio epea mugatzeko printzipioak errespetatuz, entitateak sartze edo irteten diren komunikazioak aztertu ahalko ditu, behar-beharrezkoa eta neurrikoa denean eta soilik informazioaren segurtasunerako helburuarekin, posible izan dadin sareetara eta informazio sistemetara baimendu gabeko sarbidea galaraztea, zerbitzua ukatzeko erasoak geldiaraztea, kode kaltegarria asmo txarrez zabal dadin saihestea eta aipatutako sareen eta informazio sistemen kontrako bestelako kalteak egitea.

Erantzukizunak zuzentzeko edo, hala badagokio, eskatzeko, informazio sistemara sartzen den erabiltzaile bakoitzak identifikazio bakarra izango du, une oro jakin dadin nork jasotzen dituen sarbide eskubideak, nolakoak diren eta nork egin duen jarduera jakin bat.

Azpiegitura eta zerbitzu komunak

DonostiaTIKek aintzat hartuko du administrazio publikoen azpiegiturak eta zerbitzu komunak erabiltzeak, partekatuak edo transbertsalak barne, erraztu egingo duela errege dekretuan xedatutakoa betetzea.

Betetze profil espezifikoak eta ezarpen seguruak aplikatzeko entitateak egiaztatzea

DonostiaTIKek kontuan hartuko du aplikagarriak zaizkion betetze profil espezifikoak aplikatzea.

7. SEGURTASUNAREN ANTOLAKETA

DonostiaTIKen, jarraian adierazitako moduan dago egituratuta Informazioaren Segurtasuna.

7.1 Informazioaren segurtasunerako rolak

DonostiaTIKek rol hauek ezarri ditu segurtasuna antolatzeko:

- Informazioaren arduraduna eta Zerbitzuen arduraduna: Informazioaren Segurtasun Batzordeak hartuko ditu bere gain erantzukizun horiek.
- Informazioaren Segurtasunerako arduraduna: DonostiaTIKeko Zerbitzu burua.
- Sistemaren arduraduna: DonostiaTIKeko Produkzio burua.
- POC (kontakutrako puntua eod pertsona): DonostiaTIKeko Zerbitzu burua

7.2 Informazioaren Segurtasun Batzordea

DonostiaTIKek Informazioaren Segurtasunerako Batzordea eratu du, Donostiako Udaleko Informazioaren Segurtasunerako Batzordearekin koordinazio eta lankidetza organo erabakitzaile gisa, honako osaera honekin:

- Presidentea: DonostiaTIKeko zuzendari kudeatzailea.
- Idazkaria: Datuak babesteko ordezkariaren solaskidea.

Kideak:

- Informazioaren Segurtasunerako arduraduna: DonostiaTIKeko Zerbitzu burua.
- Sistemaren arduraduna: DonostiaTIKeko Produkzio burua.
- Datuen Babeserako ordezkariaren solaskidea: DonostiaTIKeko idazkari teknikoa.

Datuen Babeserako ordezkariaren solaskideak Informazioaren Segurtasun Batzordearen bileretan parte hartuko du, hitzarekin baina botorik gabe, baldin eta datu

pertsonalen tratamenduarekin erlazionatutako gaiak landu behar badira bertan, edo bertan parte hartzeko eskatzen zaion bakoitzean. Nolanahi ere, gai baten inguruan bozketa egin behar bada, Datuen Babeserako ordezkariaren iritzia jasota gelditukо da aktan.

Halaber, hautaz, batzordearen lanetan lantalde espezializatuak ezarri ahalko dira, barnekoak, kanpokoak zein mistoak.

Informazioaren Segurtasun Batzordearen ohiko bilerak sei hilean behin egingo dira.

Ezohiko bilerak ere egin ahalko dira, beharra dagoen bakoitzean.

7.3 Zibersegurtasuneko eta Araudia Betetzeko Bulegoa

DonostiaTIKek Zibersegurtasuneko eta Arauak Betetzeko Bulegoa eratu du, eta aholkularitza eta lan batzorde bat sortu du, segurtasun rolen funtzioak eta erantzukizunak betetzen laguntzeko. Honako hauek osatuko dute:

- Informazioaren Segurtasunerako arduraduna
- Sistemaren arduraduna
- Zibersegurtasuneko Sistemen bi teknikari
- Proiektu Informatikoen Kudeaketako eta Garapeneko, Segurtasuneko eta Kalitateko teknikari bat

Halaber, aukeran, bulegoaren lanetan lantalde espezializatuak ezarri ahalko dira, barnekoak, kanpokoak zein mistoak.

Bulego hau gutxienez sei hilean behin bilduko da. Hartutako erabakiak aktetan jasoko dira, eta akta horiek Informazioaren Segurtasunerako Batzordeko buruari helaraziko zaizkio, jakinaren gainean egon dadin.

7.4 Segurtasun Eskema Nazionalari atxikitako arduradunen eginkizunak

Jarraian adierazita eta finkatuta daude arduradun bakoitzaren eginkizunak eta erantzukizunak:

- **Informazio eta Zerbitzu arduraduna**. Haren funtzioak izango dira:
  - Segurtasun kategoriaren balorazioak egitea, informazioaren edo zerbitzuen segurtasunari eskuragarritasunean, autentikotasunean, osotasunean, konfidentzialtasunean edo trazabilitatean kalte eginez eragingo liokeen gorabehera batek izango lukeen inpaktuaren balorazioaren arabera.
  - Zerbitzuari eta informazioari aplikatzekoak diren segurtasun baldintzak ezartzea eta onestea, 311/2022 Errege Dekretuaren, maiatzaren 3koaren, I. eranskinean ezarritako esparruaren barruan. Proposamena egin diezaioke Segurtasun Eskema Nazionaleko (SEN) Segurtasun arduradunari eta Sistemaren arduradunaren iritzia entzungo du.

- Zerbitzuan eta informazioan eragina duten hondar arriskuak onartzea.

- **Informazioaren Segurtasunerako arduraduna**. Erabakiak hartuko ditu, Informazioaren eta Zerbitzuen segurtasunerako baldintzak betetzeko. Honako hauek dira bere eginkizun nagusiak:
  - Sistemaren segurtasun kategoria erabakitzea.
  - Informazio sistemek emandako zerbitzu elektronikoak eta maneiatutako informazioa segurtasun maila egokian mantentzea eta hori egiaztatzea.
  - Prestakuntza eta kontzientziazioa bultzatzea informazioaren segurtasunari dagokionez.
  - Segurtasun politikak prestatzea eta erakundeak onesteko proposatzea, neurri tekniko eta antolakuntzako egoki eta proportzionatuekin, erabiltzen diren informazio sistemen eta sareen segurtasunean eragina izan dezaketen arriskuak kudeatzeko, eta antolakuntzan eta zerbitzuetan eragin dezaketen zibergorabeherak saihestu edo haien ondorioak minimizatzeko.
  - Antolakuntzarako prozedurak, araudiak eta segurtasun politikak garatzea, eraginkorrak direla gainbegiratzea, eta aldian behin segurtasuneko auditoretzak egitea.
  - Arriskuen analisia egin dadin bultzatzea.
  - Aplikagarritasun Adierazpena formalki onestea.
  - POC moduan (kontakurako puntua edo pertsona):
    - Ematen diren zerbitzuen segurtasun betekizunak betetzen direla eta zerbitzu horien eremuko informazioa bideratzea eta gainbegiratzea, eta gorabeherak kudeatzea.
  - Segurtasuneko gorabeherei dagokienez:
    - Erreferentziazko CSIRT taldearekin (bereziki Kriptologia Zentro Nazionalarekin eta Datuak Babesteko Espainiako Agentziarekin) koordinatzeko kontaktu gune espezializatua osatzea.
    - Erreferentziazko CSIRTaren bidez eta gehiegi atzeratu gabe, zerbitzua aztora dezaketen gorabeheran berri ematea eskumena duen agintariari.
    - Eskumena duen agintariaren jarraibideak eta gidak jasotzea, interpretatu eta aplikatzea, dela ohiko eragiketetarako, dela gabeziak konpontzeko.
    - Eskumena duen agintariarentzat edo erreferentziazko CSIRTarentzat informazioa bildu eta prestatzea, eta informazio hori ematea, horiek eskatuta edo bere ekimenez.

- **Sistemaren arduraduna**. Eginkizun hauek izango ditu:

- Informazio sistema garatu, jardunean eduki eta mantentzea, haren bizi ziklo osoan zehar.
- Beharrezkoak diren eragiketa prozedurak prestatzea.
- Informazio Sistemaren tipologia eta kudeaketa zehaztea, eta erabilera irizpideak eta eskainiko dituen zerbitzuak ezartzea.
- Berariazko segurtasun neurriak segurtasun esparru orokorrean behar bezala integratzen direla bermatzea.
- Informazio jakin bat tratatzeari edo zerbitzu jakin bat eskaintzeari uzteko proposatzea, segurtasuneko gabezia larrien ondorioz litekeena bada ezarritako baldintzak bete ezin izatea. Azken erabakia erakundeko zuzendaritzak hartuko du, baina dagozkion zerbitzuen eta informazioaren arduradunekin eta Informazioaren Segurtasunerako arduradunarekin hitzartu behar da.
- Sistemaren edo sistemen kategorizazioa ezarri eta formalki onestea, SENeko Zerbitzu arduradunaren eta Informazio arduradunaren balorazioan oinarrituta, SENaren Errege Dekretuko I. eranskinean ezarrita dagoen moduan.
- Sistemaren segurtasunaren administratzailearen eginkizunak betetzea:
  - Informazio sisteman aplika daitezkeen segurtasun neurriak inplementatu, kudeatu eta mantentzea.
  - Hala dagokionean, informazio sistemaren segurtasuneko mekanismoek eta zerbitzuek oinarri dituzten hardwarea eta softwarea kudeatu, konfiguratu eta eguneratzea.
  - Sistemaren erabiltzaileei emandako baimenak eta pribilegioak kudeatzea, eta sistemako jarduna baimendutakora egokitzen dela monitorizatzea.
  - Segurtasun Prozedura Operatiboak (POS) ezartzea.
  - Ezarritako segurtasun kontrolak behar bezala gauzatzen direla bermatzea.
  - Informazio sistema erabiltzeko onartutako prozedurak aplikatzen direla bermatzea.
  - Hardwarea eta softwarea instalatu, aldatu eta hobetzeko lanak gainbegiratzea, segurtasuna arriskuan jartzen ez dela eta uneoro dagozkion baimenak betetzen direla bermatzeko.
  - Sistemaren segurtasun egoera monitoritzatzea, sistemako segurtasun ekintzak kudeatzeko tresnen eta auditoretza teknikoa egiteko mekanismoen bidez.

- Informazioaren Segurtasunerako arduradunari segurtasunarekin erlazionatutako edozein anomalia, estutasun edo ahuleziaren berri ematea.
- Segurtasuneko gorabeherak ikertzen eta konpontzen laguntzea, detektatzen direnetik guztiz konpondu arte.

7.5 Informazioaren Segurtasun Batzordearen eginkizunak

Informazioaren Segurtasun Batzordearen eginkizunak hauek izango dira:

- Informazioaren Segurtasunaren alorrean,administrazioak eta arlo desberdinek agertzen dituzten kezkei erantzutea, eta, erregulartasunez, zuzendaritzari Informazioaren Segurtasunaren egoeraren berri ematea.
- Arduradun desberdinen artean eta/edo segurtasuneko rol desberdinen artean erantzukizunekin erlazionatuta egon litezkeen gatazkak konpontzea, eta erabakiak hartzeko nahikoa aginterik ez duen kasuetan, goragoko maila batera eramatea.
- Informazio arduradunaren eta Zerbitzu arduradunaren eginkizunak bere gain hartzea.
- Donostiako Udaleko Informazioaren Segurtasun Batzordearekin koordinatzea DonostiaTIKen estatutuetan zehaztutako helburuak lortzeko eta politika hori eguneratzeko eta mantentzeko, bai eta politika aplikatzeko irizpide komunak emateko ere, udal informazioaren segurtasunean eragin badezakete.
- Informazioaren Segurtasunaren kudeaketa sistemaren etengabeko hobekuntza sustatzea. Horretarako:
    - Informazioaren Segurtasunaren alorreko arlo desberdinen ahaleginak koordinatuko ditu, ahalegin horiek sendoak izan daitezen, gai honen inguruan erabakitako estrategiarekin bat etor daitezen eta bikoizketak saihestu daitezen.
    - Informazioaren Segurtasuna hobetzeko planak proposatuko ditu, dagokion aurrekontu hornikuntzarekin, eta, baliabideak mugatuak direnean, segurtasunaren alorreko jarduerei lehentasuna emango die.
    - Proiektu guztietan, hasieran zehazten direnetik abian jartzen diren arte, Informazioaren Segurtasuna aintzat hartzea zainduko du (Privacy by Design). Bereziki zainduko du bikoizketak murriztuko dituzten eta IKT sistema guztien funtzionamendu homogeneoa sustatuko duten zerbitzu horizontalak sortzen eta erabiltzen direla.
    - Udalak bere egiten dituen hondar arrisku nagusien gaineko jarraipena egingo du, eta haiei aurre egiteko balizko jarduerak gomendatuko ditu.

- Segurtasunaren alorreko gorabeheren kudeaketaren gaineko jarraipena egingo du, eta haiei aurre egiteko jarduera posibleak gomendatuko ditu.
- Informazioaren Segurtasun Politika prestatuko eta berrikusiko du, onesteko.
- Informazioaren Segurtasun araudia prestatuko du, onesteko.
- Informazioaren segurtasuneko prozedurak eta gainerako dokumentazioa egiaztatzea, onesteko.
- Informazioaren Segurtasun Politikako “Arau Esparrua” eguneratuta mantenduko du.
- Sisteman aplika daitezkeen segurtasuneko CCN gidak identifikatuko ditu.
- Langileak trebatzeko eta sentsibilizatzeko prestakuntza programak landuko ditu Informazioaren Segurtasunaren arloan (bereziki datu pertsonalen babesari dagokionez).
- Administratzaileen, eragileen eta erabiltzaileen prestakuntza eta kalifikazio betekizunak egitea eta onestea, informazioaren segurtasunaren ikuspuntutik.
- Aldizkako SEN auditoretzak eta datuen babeseko araudia egitea sustatzea, administrazioak informazioaren segurtasunaren arloan dituen obligazioak betetzen dituela egiaztatu ahal izateko.
- Informazioaren segurtasuna egoeraren berri emango dio Zuzendaritzari.
- Berritzea

7.6 Izendatzeko prozedurak

DonostiaTIKeko Zuzendaritzak batzordea eratuko du eta erantzukizunak eta segurtasun rolak izendatuko ditu. Izendapen guztiak 4 urtean behin edo postuak hutsik gelditzen diren guztietan berrikusiko dira. Izendapen guztiak 4 urtean behin berrikusiko dira, edo lanpostuak hutsik geratzen direnean.

8. DOKUMENTAZIOAREN EGITURA

DonostiaTIKek prozedura dokumentatu bat du, zeinean ezartzen baita Donostiako Udalean eta DonostiaTIKen SENa betetzeko kudeaketa sistemaren (SENKS) dokumentuak egiteko, berrikusteko, onesteko, eguneratzeko, banatzeko, kontrolatzeko eta artxibatzeko metodoa.

9. DATU PERTSONALAK

DonostiaTIKek egokiak, bidezkoak eta ez gehiegizkoak direnean soilik bilduko ditu datu pertsonalak, betiere erlazioa badute datu horiek eskuratzeko helburuekin eta eremuarekin. Era berean, Datuak Babesteko indarreko araudia betetzeko beharrezkoak diren neurri teknikoak eta antolakuntzakoak hartuko ditu.

10. INFORMAZIOAREN SEGURTASUNERAKO POLITIKAREN GARAPENA

Informazioaren Segurtasun Batzordeak onetsi du kudeaketa sistema bat garatzea eta segurtasun estandarren arabera ezarri, inplementatu, mantendu eta hobetzea. Sistema hori egokitu egingo da DonostiaTIKen eta Donostiako Udalean aplikagarriak diren Segurtasun Eskema Nazionaleko segurtasun kontrolak kudeatzeko balio izan dezan. Sistema dokumentatuta egongo da eta kontrolen eta Batzordeak ezarritako helburuak betetzearen ebidentziak eskainiko ditu. Dokumentuak kudeatzeko prozedura bat egongo da, "Dokumentazioa kudeatzeko prozedura. 00-PR" izenekoa, eta sistemaren segurtasun dokumentazioa egituratzeko, kudeatzeko eta eskuratzeko jarraibideak ezarriko ditu.

Informazioaren Segurtasun Batzordeari dagokio Politika hau urtero berrikustea eta, beharrezkoa balitz, hura hobetzeko proposamenak egitea, DonostiaTIKen Zuzendaritzak onesteko.

11. HIRUGARRENAK

DonostiaTIKek beste erakunde batzuei zerbitzuak ematen dizkienean edo beste erakunde batzuen informazioa erabiltzen duenean, erakunde horiei ere Informazioaren Segurtasunerako Politika honen berri izango zaie. Informazioa emateko eta Informazioaren Segurtasun Batzordeak koordinatzeko bideak finkatuko dira, eta segurtasun alorreko gorabeherei erantzuteko jarduketa prozedurak ezarriko dira.

DonostiaTIKek hirugarrenen zerbitzuak erabiltzen dituenean edo informazioa hirugarrenei lagatzen dienean, zerbitzu edo informazio horiei dagozkien Segurtasun Araudiaren eta Segurtasun Politikaren berri emango zaie haiei ere. Hirugarrenek aipatu araudian finkatutako eginbeharrak bete beharko dituzte, eta, horretarako, beren prozedura propioak garatu ahal izango dituzte. Gorabeheren berri emateko eta gorabeherak konpontzeko berariazko prozedurak ezarriko dira. Hirugarrenen langileak segurtasunaren alorrean ongi kontzientziatuta egotea bermatuko da, gutxienez Segurtasun Politika honetan finkatutako maila berean.

Orobat, entitate publikoei zerbitzuak ematen dizkieten edo soluzioak ematen dizkieten sektore pribatuko eragileek, Segurtasun Eskema Nazionala betetzea galdagarria zaienek, Segurtasun Eskema Nazionalarekiko adostasun adierazpena erakusteko moduan egon beharko dute, OINARRIZKO kategoriako sistemak direnean, edo

Segurtasun Eskema Nazionalarekiko adostasun ziurtagiria, kategoria ERTAIN edo ALTUkoak direnean.

Segurtasun politika honen alderdiren bat hirugarren batek bete ezin badu aurreko paragrafoetan eskatutako moduan, SENaren Segurtasun arduradunaren txosten bat eskatuko da, sortzen diren arriskuak eta horiek tratatzeko moduak zehazten dituena. Txosten hori ukitutako informazioaren eta zerbitzuen arduradunek sinatu beharko dute, aurrera jarraitu aurretik.

12. KOORDINAZIOA ETA INTERPRETAZIOA

Politika honetan jasota dauden jarduketak garatzeko garaian, DonostiaTIKek Donostiako Udalarekin koordinatuta beteko ditu bere funtzioak, Informazioaren Segurtasun Batzordearen bidez.

Informazioaren Segurtasun Batzordeak interpretaziorako irizpideak ezarri ahalko ditu, politika hau aplikatzeko. Irizpide horiek kontraesanean badaude Udalaren Politikaren irizpideekin, azkenok izango dute lehentasuna, bi politikak modu koordinatuan aplikatu eta erakundearen xedeak betetze aldera.

Politika hau eta gerora egin daitezkeen aldaketa guztiak Udalari jakinaraziko zaizkio, bertako Informazioaren Segurtasun Batzordeen bidez, Udalaren Segurtasun Politikan jasotakoaren aurka aplika ez dadin, udal informazioaren segurtasunerako esparru orokor moduan.