0 AURREKARIAK

BiscayTIK Bizkaiko Foru Aldundiak sustatutako proiektua da, nazioarte mailan izaera berritzaile eta aitzindari nabarmena duena, helburutzat honako hauek dituelarik: komunikazio kanal berri baten bidez, Internet bidez, Administrazioa herritarrengana hurbilaraztea bien arteko elkarrekintza erraztuz; horrez gain, Bizkaiko Udaletako barne-kudeaketa eta herritarrekiko harremana hobetzeko tresna informatikoak homogeneizatzea; eta Bizkaia informazio teknologietan eta Udal Administrazioaren ezagupenean nazioarteko erreferentzia bilakatzea.

Helburu hau betetzeko, proiektuak hiru ardatz ditu,

- Herritarrentzako posta elektroniko zerbitzua.
- Udalerrientzat programa informatikoak eta herritar bideratzea duen web ataria.
- Nazioarteko erreferentziadun Teknologia Zentro bat sortzea.

Azken urteotan, informazioaren segurtasunak protagonismoa hartu du sistema seguru, fidagarri eta erresilienteen mendekotasun unibertsalagatik, eta sektore publiko zein pribatura iritsi da, orain arte ezezaguna zen arau-esparru batean garatuz. Bai Europako araudiak, Europako Parlamentuaren eta Kontseiluaren 2019ko apirilaren 17ko 2019/881 (EB) Erregelamenduak, ENISAri (Zibersegurtasunerako Europar Batasunaren Agentzia) eta informazioaren eta komunikazioaren teknologien zibersegurtasunaren ziurtapenari buruzkoak, bai SENetik eratorritako araudiak, ikuspegi bateratua dute, europazalea, eta informazio-sistemen zibersegurtasun-maila handitzen dute. Informazioaren teknologien bilakaerak, batez ere sektore publikoko eragile guztien nahitaezko presentziari lotutako Interneten garapenak, eragin du informazio-sareek eta -sistemek gaur egun berebiziko garrantzia izatea gure gizartean, eta haien fidagarritasuna eta segurtasuna funtsezko alderdiak dira jarduera ekonomiko eta sozialen garapen normalerako.

Egoera horrek balio izan du ohartzeko erakunde batean zer-nolako garrantzia izan dezaketen informazio-sare eta -sistemei eragiten dieten gorabeherek eguneroko jarduerak aldatzen dituztenean, eta hori mehatxu larria da; izan ere, gertakari horiek ustekabekoak badira eta nahita egindako ekintzetatik badatoz, herritarren konfiantza kaltetu dezakete, eta, azken batean, kalte larriak eragin diezazkiokete ekonomiari eta gizarteari, erakundeen osotasunari berari eragiteko aukerarekin.

Sektore publiko osoan informazioaren teknologiek hedapen horizontala eta interkonektatua dutela kontuan hartuta, mehatxu eta arrisku gehiago eragiten baititu horrek, arrisku horiek arintzeko neurri eraginkorrak hartzeko osotasuna behatuko duen plangintza bat egin behar dela ikus daiteke, ekintza isolatuak saihestuz. Halaber, zeharkako izaera horrek eraginkortasuna galtzeko arriskua sortzen du, baldin eta informazioaren segurtasunaren arloko betekizunak modu independentean definitzen badira eragindako eremu bakoitzerako.

Beraz, BiscayTIK Fundazioak egokitzat jotzen du proiektu bat ezartzea, ikuspegi integral batekin, informazio-sistemei eragiten dieten mehatxuen aurkako babesa hobetzeko azterlan bat egin ahal izateko, Bizkaiko Lurralde Historikoko (BLH) toki-erakundeentzat arlo horretan egindako jardueren koordinazioa errazteko.

1 XEDEA

Lehiaketa honen xedea da BiscayTIK proiektuari atxikita dauden Bizkaiko Lurralde Historikoko tokiko entitateetarako segurtasuneko operazio-zentro bat ezartzeko ekintza plana definitzeko aholkularitza-zerbitzuak kontratatzea.

2 ZEHAZTAPEN TEKNIKOAK

Adjudikaziodunak gaitasun nahikoa izan beharko du entitate kontratatzaileari aholkularitza eta proiektuen kudeaketa eskaini ahal izateko, eta berehala jarriko ditu kontratuaren esku BiscayTIK proiektuari atxikita dauden Bizkaiko Lurralde Historikoko tokiko entitateetarako segurtasuneko operazio-zentro bat ezartzeko ekintza plana definitzeko aholkularitza-zerbitzuak barne hartzen dituen gai guztietako adituak.

Esleipendunak zerbitzua kalitatez, zehaztasunez eta eraginkortasunez eman beharko du, eta indarrean dauden eta, zuzenean edo zeharka, hori arautzen duten xedapen legalak, erregelamenduzko xedapenak, arauak eta espezifikazioak betez.

Arduradun bat izendatu beharko da, eta une oro izango du ardura kontratuaren xede diren jarduerak behar bezala doazela ikuskatzeko.

Esleipendunak zerbitzua ematen duten langileen kontrola eta ikuskapena gauzatuko du, eta gaixotasun, opor edo hutsegite kasuetan kualifikatutako beste langile batekin ordeztuko du.

Zerbitzua hainbat kanaletatik eman ahal izango da: posta bidez, telematikoki, telefonoz edo aurrez aurre.

Hala ere, lanak BiscayTIK Fundazioak eskatuta egingo dira, BiscayTIK Fundazioak bestelako kontratuak beste esleipendunekin egiteko aukera kaltetu gabe, baldintza-orriaren xede diren gaiei dagokienez.

2.1 Prestazioaren deskribapen orokorra.

Baliabide elektronikoak erabiliz egindako mehatxuen pertzepzioa errealitate onargarri, unibertsal eta sinesgarri bihurtu da, ezagutza orokorraren parte da, eta erakunde publikoen eta herritarren aurkako eraso-tresna indartsua da haiekiko harremanetan; beraz, zibersegurtasuna erakunde publiko ororen lehentasunezko jardun-eremu bihurtu behar da. Horregatik, beharrezkoa da administrazio publiko guztien informazio-sistemen eta komunikazio- eta azpiegitura-sareen segurtasuna eskainiko duten bermeak mantentzea, zibersegurtasun eta erresilientzia maila egokia lortzeko estrategia bat sortuz eta helburu horiekin koherenteak izango diren informazio- eta telekomunikazio-sistemak ezarriz.

Administrazio elektronikoaren eremua deritzonaren sorreratik, segurtasunaren eskema nazionalak aipamen berezia izan du araudi erregulatzailean. Herritarrek Zerbitzu Publikoetan Sarbide Elektronikoa izateari buruzko ekainaren 22ko 11/2007 Legearen 42.2 artikuluak Segurtasunerako Eskema Nazionala sortzea ezartzen zuen. Eskema horren helburua informazioa behar bezala babesteko aukera emango duten bitarteko elektronikoak erabiltzeko segurtasun-politikaren printzipioak eta betekizunak ezartzea izango litzateke. Administrazio elektronikoaren eremuan Segurtasunerako Eskema Nazionala arautzen duen urtarrilaren 8ko 3/2010 Errege Dekretua onartu zenean hasi zen kontzeptu hori lantzen, eta haren ibilbidea zalantzan zegoen aldi batean hasi zen, batez ere toki-eremuan, arau horren hirugarren xedapen iragankorrean deskribatutako ezarpen-marjina zabala kontuan hartuta. Sektore Publikoaren Araubide Juridikoaren urriaren 1eko 40/2015 Legearen eta Administrazio Publikoen Administrazio Prozedura Erkidearen urriaren 1eko 39/2015 Legearen blokeak 11/2007 Legea indargabetu zituenez, derrigortasuna modu uniformean ezarri zen, eta premiaz egokitu behar izan zen, urriaren 23ko 951/2015 Errege Dekretua onetsiz, 3/2010 Errege Dekretua aldatzen duena, herritarrek

konfiantza izan dezaten bitarteko elektroniko bidez eskuragarri dauden zerbitzu publikoetan ere administrazioaren bulegoetara pertsonalki hurbiltzen direnean dituzten zerbitzuen segurtasun-baldintza berak izango dituztela, araugintza-aginduak zehaztuz, sakonduz eta hobeto betetzen lagunduz.

Prebentzio-, babes-, monitorizazio-, detekzio- eta erantzun-segurtasuneko zerbitzu horiek ziberespazioan integratu eta eskainiko dira zibersegurtasuneko bulego zentralizatutik, eta tokiko erakundeari aukera emango diote eguneroko informazio- eta komunikazio-sistemen erabileran mehatxuak zaintzeko eta antzemateko gaitasuna handitzeko, baita edozein erasoren aurrean erantzuteko gaitasuna hobetzeko ere.

Ondorioz, eta arestian zehaztutakoagatik, BiscayTIK Fundazioak beharrezkotzat jotzen du BLHko toki-erakundeei segurtasun-zerbitzu bat ematea, SENa betetzen laguntzeko eta zibersegurtasuneko neurri indartuak, teknikoak zein antolamendukoak, inplementatzeko. Horretarako, bulego zentralizatu bat ezarriko da, atxikitako toki-erakunde guztiek behar horiei erantzun diezaieten. Horregatik, beharrezkotzat jotzen da aholkularitza bat egitea zentro hori deskribatzeko eta ekintza-plan xehatua definitzeko, ondoren bulego hori ezartzeko.

Azken batean, aholkularitzaren emaitzak behar diren tresna tekniko eta antolaketa-tresna guztiak emango dizkio BiscayTIKi (planak, prozesuak, ereduak eta abar) Bizkaiko Lurralde Historikoko toki-erakundeetarako SENaren gutxieneko neurriak betetzeko zibersegurtasuneko operazio-zentro bat ezarri ahal izateko.

2.2 Zerbitzuaren irismen-zereginen deskribapena

Jarraian, zerbitzuarekin zerikusia duten jarduera nagusiak zerrendatu dira, zehatzak eta osoak izan nahi gabe ere, lizitazioan eskatu daitekeen lan-esparrua deskribatu nahi da, besterik ez.

Azken helburua lortzeko, eta zehaztapen teknikoen txosten honetan deskribatutako xedeak lortzeko, aholkularitzaren fase guztiak kontuan hartuko dituen proposamen tekniko bat egin beharko da. Proposamen horretan, zereginak, arduradunak eta entregagaiak adieraziko dira, hasieratik zibersegurtasuneko bulegoa ezartzeko eman beharreko urrats zehatzak zehaztuko dituen plan zuzentzailea lortu arte. Horrela, gutxienez, honako hauek jaso beharko dira:

2.2.1 Toki-erakundeen hasierako diagnostikoa zibersegurtasunaren arloan (AS IS)

Fase honetan, informazioaren segurtasunaren eta pribatutasunaren kudeaketaren egungo egoera zehaztu beharko da Bizkaiko toki-erakunde guztietan; horrela, Bizkaiko erakunde-motak eta heldutasun-maila identifikatuko dira, Maila ertaineko informazio-sistemarako SENaen ezarritako betekizunak zenbateraino betetzen diren kontuan hartuta.

Horrela, hasierako argazki bat lortuko da, hurrengo faserako sarrera gisa balioko duena, eta funtsezkoa izango dena GAPa identifikatzeko, egungo benetako egoeraren eta nahi den etorkizuneko egoeraren artean. Gainera, informazio hori baliagarria izango da inplementatu beharreko zerbitzuak eta neurriak identifikatzeko, zerbitzu multzokatuak sortzeko horiek elkartzea komeni den ala ez, arau-esparruaren arabera behar diren segurtasun-mailak, elkartzeko aukera emango duen edo emango ez duen toki-erakundeen arteko homogeneotasuna edo heterogeneotasuna, eta zerbitzu bakoitza eskaintzeko toki-erakundeen tipologiak sortzea.

Era berean, etorkizuneko eredua baldintzatu dezaketen arazoak, bateraezintasunak, mendekotasunak eta abar identifikatu beharko dira, betiere, kontuan hartuta zerbitzuaren azken helburua dela zerbitzua Bizkaiko Lurralde Historikoko toki-erakunde guztietara iristea. Hori dela eta, ekintza-plan bat prestatu beharko da, baldintza horiek toki-erakunde bat ere zerbitzutik kanpo utz ez dezaten.

2.2.2 Eredu objektiboa (TO BE) eta ekintza-plana definitzea

Fase honen helburua BiscayTIKeko segurtasun-operazioen zentroaren agertoki objektiboa eta funtzio zehatzak puntuz puntu definitzea eta diseinatzea da, eta ibilbide-orria ezartzea, egungo egoeratik behin betiko helburu-eredura iristeko.

Fase honetan, zehatz-mehatz definituko dira bulegoaren katalogoa osatzen duten zerbitzu guztiak, bai eta balizko erakunde hartzaileak ere; horrela, zerbitzu, entitate eta ad hoc beharren matrize bat sartuko da horietako bakoitzerako, hasierako egoeraren diagnostiko-txostenean oinarrituta. Era berean, kudeaketa, jarraipena eta etengabeko hobekuntzara bideratutako prozedura eta plan guzti-guztiak definituko dira, bai eta proposatutako kanpoko eta barruko txostenak ere.

Zibersegurtasuneko operazio-bulegoa ezartzeko ekintza-planak honako hauek zehaztu beharko ditu: plana barne hartzen duen ekimen bakoitzerako egin beharreko ekintza zehatzak, identifikatutako ekintza bakoitza ezartzeko planak, ekintza horien denbora-plangintza, bakoitzarentzat beharrezkoak diren baliabideak, fundazioaren edo kanpoko beste bulego batzuen dedikazioa, eta proposatutako planaren ezarpenaren zenbatespen ekonomikoa. Gainera, hori ezartzeko estrategia bat planteatu beharko da, identifikatutako zerbitzuetan eta zerbitzu horiek jasoko dituzten toki-erakundeetan oinarrituta.

Azkenik, etorkizuneko zerbitzuaren kudeaketa- eta gobernantza-eredua adierazi beharko da, zerbitzuaren antolaketa-, operazio- eta kudeaketa-eredua deskribatuz.

Eskaintzek, gutxienez, argi eta garbi zehaztu beharko dute irismenaren ulermena, bai eta zehaztapen teknikoen txosten honetan zehaztutako helburu guztiak lortzeko proposatutako ikuspegi osoa ere. Halaber, identifikatutako fase bakoitzean edo lizitatzaileak proposatutako fase bakoitzean erabili beharreko metodologia identifikatu eta deskribatuko da, bai eta egiteko konpromisoa duten zeregin zehatzak, antolaketa eta lan-taldea, eta proposatutako proiektu-plana ere. Gantt-en diagrama batean irudikatuko da, eta gutxienez honako hauek jasoko ditu: jarduerak, mugarriak, epeak, entregagaiak eta proposatutako fase bakoitzari esleitutako ekipoa.

Zerbitzuaren beharrak direla eta, eta kontuan hartuta toki-entitateek zibersegurtasunaren arloan hasierako diagnostikoa egiteko fasea (AS IS) eta toki-entitateekin harremanak izateko beharra, zerbitzua ele bitan eman beharko da (euskaraz eta gaztelaniaz), bai elkarrizketa mailan, bai dokumentu mailan.

2.2.3 Bateragarritasun-baldintza bereziak

Ekintza-planaren eta helburu-ereduaren (TO BE) definiziotik ezin izango dira sortu adjudikaziodunaren ezaugarri teknikoei bakarrik egokitzen zaizkien soluzio hain zehatz eta mugatuak, eredu eta ekintza-plan hori ezartzeko balizko kontratuari dagokionez. Ekintza-planaren eta helburu ereduaren (TO BE) definizioaren emaitza zehaztu beharko da ezaugarri orokorrak, eskakizun orokorrak edo interes publikoei hobeto erantzutea bermatuko duten formula abstraktuak sartzeko orduan, eta edonola ere ezin izango dute adjudikaziodunaren aldeko abantailarik ekarri, eredu hori ezartzeko balizko kontratu bat adjudikatzeari dagokionez.

Kontratuaren adjudikaziodunak helburu-eredua eta ekintza-plana ezartzeko balizko beste lizitazio batean parte hartu ahal izango du. Lizitazio horretan, honako neurri hauek hartuko dira:

- Interesa duten enpresa lizitatzaileen esku jarriko da kontratu honen adjudikaziodunak emandako ekintza-planaren eta helburu-ereduaren definizioari eta diagnostikoari buruzko dokumentazioa, dagokion informazio konfidentziala gordeta, gainerako lizitatzaileek eskaintza prestatzeko informazio gisa erabil dezaten.
- Dokumentazio horren egilea izan den adjudikazioduna identifikatuko da.

- Eskaintzak aurkezteko epe egoki bat ezarriko da.

3 KONTROLA ETA JARRAIPENA

Atal honetan proposatu behar diren eginkizunen helburua aldi oro zerbitzuaren egoerari buruzko ikuspegia izatea da. Horrela, gerta litezkeen desbideratzeak zehazteko eta behar diren ekintza zuzentzaileak aplikatzeko aukera ematen du.

Helburu hori betetzeko oinarrizko tresnak jarraipena egiteko txostenak dira. Txosten horiek dagozkien bilera eta batzordeetan aztertuko dira.

Lizitatzaileak bere proposamen teknikoan, ahalik eta erarik xehatuenean, proposatzen duen jarraipeneko kontrol-eredua deskribatu beharko du, zerbitzua ematean aplikatzeko

Enpresa esleipendunak arduradun bakarra ezarriko du BiscayTIK Fundazioarekin; hark BiscayTIK Fundazioaren agindu orokorrak jasoko ditu, eta ardura horren bitartekaritzat jokatuko du. Hauek izango ditu bere gain:

- Zerbitzu-mailaren akordioaren (ZMA) azpian dauden garapeneko eta mantentze-lanetako zerbitzu guztien kontrola eta jarraipena, enpresa esleipendunaren ardurapean gauzatu beharreko zerbitzuei dagokienez.
- BiscayTIK Fundazioarekiko harremanak zentralizatzea eta koordinatzea.
- BiscayTIK Fundazioarekin antolatutako bileretako aktak egitea, eta, bertan, hartutako erabakien berri ematea. Hasiera batean, astean behin egingo dira bilerak, eta abian dauden zereginen jarraipena egitea izango da helburu nagusia, baita desbideraketak eta zereginon aurrerapeneko puntu kritikoak edo geldiarazleak antzematea ere.

Lantaldeko koordinatzaileak Fundación BiscayTIK Fundazioak eskatuz gero Fundación BiscayTIK Fundazioaren egoitzan egon behako du bi ordutan, asko jota.

Lanak bukatutakoan, Hornitzaileak egindakoa fakturatuko du onartutako balorazioan ezartzen denaren arabera. BiscayTIK Fundazioak aurkeztutako lanak aztertuko ditu aldez aurretik onartutakoarekin bat datozela egiaztatzeko eta, azkenik, bere oniritzia emango die.

Fundación BiscayTIK Fundazioak egindako lanen gaineko kalitate kontrola egitea beretzat gordetzen du. Horrela, gutxieneko baldintzak betetzen ez dituztenak gaitzetsi ahalko ditu, bere irizpide propioei jarraiki. Hori guztia Fundación BiscayTIK Fundazioak atzerapenen edo kontrataturiko zerbitzuen kalitate baxuaren ondotik jar ditzakeen penalizazioen kaltetan izan gabe egingo da. Halaber, kontratua ebazteko arrazoi justifikatua izan daiteke.

4 BALDINTZA BEREZIAK

Enpresa lizitatzaileek ezin izango dute hizkera sexistarik erabili, proposamenak prestatu eta aurkezteko orduan. Era berean, kontratua indarrean dagoen bitartean, enpresa esleipendunak ezin izango du hizkera sexistarik erabili, idatziz edo modu digitalean sortutako behin betiko edozein dokumentutan; era berean, datuak sexuaren arabera banandu beharko ditu, pertsonei buruz sortzen diren estatistika guztietan. Eta hori, Emakumeen eta Gizonen Berdintasunerako otsailaren 18ko 4/2005 Legeko 2.3 artikuluak dioena betez, non errespetatu beharreko printzipio orokorrak adierazten baitira.

4.1 Lantalde eta betekizunak

Esleipendunak beharrezko giza baliabideak eta baliabide materialak jarri beharko ditu, egokitzen dizkioten zerbitzuak modu egokian egiteko.

Esleipendunak mugikortasun geografiko osoa izango du eta Fundación BiscayTIK Fundazioek eskatutako tokietan eman beharko du zerbitzua. Lantalde osoa edo zati bat lekualdatu behar badu, ez du kargu osagarririk kobratuko. Halaber, esleipendunak Fundación BiscayTIK Fundazioak beste enpresa edo erakundeekin adosten dituen bileretara joateko konpromisoa hartzen du.

Kontratuak dirauen bitartean, lantaldearen osaketan egin daitezkeen aldaketek ezin izango dituzte memoria deskribatzailean adierazitako ezaugarriak aldatu. Edonola ere, aldaketa horiek BiscayTIK Fundazioari jakinarazi beharko zaizkio aldez aurretik eta BiscayTIK Fundazioaren berariazko baimena izan beharko du

Esleipendunak lantaldea etengabe prestaturik mantentzeko ardura hartuko du, Fundación BiscayTIK Fundazioak eskaturiko teknologia/funtzionalitate horietan. Prestakuntza horren kostua, enpresa esleipendunak prestakuntza hori jasotzeko jartzen dituen langileen dedikazioa bezala, haren konturakoa izango da.

Enpresa esleipenduneko langileek beharrezko dituzten ekipamendua, baimenak, komunikazioak eta joan-etorriak enpresak berak ordaindu beharko ditu.

Esleipendunak zerbitzua ematen duten langileen kontrola eta ikuskapena gauzatuko du, eta gaixotasun, opor edo hutsegite kasuetan kualifikatutako beste langile batekin ordeztuko du.

Lantaldearen barruan honako tipologia hauen araberako rolak egongo dira:

- Proiektu-burua: Fundación BiscayTIK Fundazioarekin koordinazio-lanak egingo ditu. Pertsona hori BiscayTIK Fundazioarekiko arduradun bakarra izango da, eta ez du zertan arduraldi esklusiboa izan; egin beharreko lanak planifikatzeaz, horien jarraipena egiteaz eta kontrolatzeaz arduratuko da, bai eta haien kalitate-maila egiaztatzeaz ere. Pertsona horrek BiscayTIK Fundazioaren jarraibide orokorrak jasoko ditu, eta erantzukizun horren solaskide gisa esku hartuko du. Gainera, kontratu horren xede diren lanen profil egituratzailea izango da.
- Segurtasunean aditua den aholkularitza: beren ardura izango da kontratua behar bezala gauzatzea eta bertan sartzen diren lanak burutzea, eta aurreikusitako entregagaien onarpena bermatuko dute kontratua gauzatzen den bitartean.

Zerbitzua emateko, enpresa lizitatzaileak lanak egiteko behar den gaitasun teknikoa duen lantalde bat izan beharko du. Beharrezkotzat jotzen da gutxienez honako hauek osatuko duten lantalde bat:

- Gutxienez proiektu-buruaren profila duen pertsona bat (1), proiektu honen eremuko proiektuen kudeaketan gutxienez bost (5) urteko esperientzia egiaztatua duena, eta segurtasun-aholkularitzetan esperientzia duena, horien erreferentzia-esparrua Segurtasunerako Eskema Nazionala edo erreferentziazko beste estandar bat izan bada. Informatikako lizentziatura- edo ingeniaritza-titulua edo antzekoa izan behar du gutxienez, bai eta lanbide-ziurtagiri hauek ere:
    - Nahitaez, hauetako bat:
        - PMP (Project Management Professional) edo PRINCE2 (Projects In Controlled Environments) edo ITIL (Service Management Foundation Certification) edo antzekoa.
    - Baloratu ahal izango dira:
        - CISA (Certified Information Systems Auditor).

        - CRISC (Certified in Risk and Information Systems Control).
        - CISSP – ISSMP (Information Systems Security Management Professional).
        - CISSP – ISSAP (Information Systems Security Arquitecture Professional).
        - Lead Auditor ISO 27001 (AENOR, SGS, Bureau Veritas, BSI edo antzeko ziurtapen-erakunderen batek emana).
        - Lead Implementer ISO 27001 (AENOR, SGS, Bureau Veritas, BSI edo antzeko ziurtapen-erakunderen batek emana).
        - Aurrekoen antzeko beste batzuk.
- Segurtasunean aditua den aholkularitza-profila duten bi (2) pertsona, gutxienez hiru (3) urteko lanbide-esperientzia dutenak proiektu honen esparruko segurtasun-aholkularitzetan. Informatikako lizentziatura- edo ingeniaritza-titulua edo antzekoa eduki behar du gutxienez, baita honako lanbide-ziurtagiri hauek ere proposatutako aholkulari bakoitzaren kasuan:
    - Nahitaez, hauetako bat:
        - CISA (Certified Information Systems Auditor)
        - CRISC (Certified in Risk and Information Systems Control).
        - CISSP (Certified Information Systems Security Professional).
        - CISM (Certified Information Security Manager).
        - CISSP – ISSAP (Information Systems Security Arquitecture Professional).
        - Lead Auditor ISO 27001 (AENOR, SGS, Bureau Veritas, BSI edo antzeko ziurtapen-erakunderen batek emana).
        - Lead Implementer ISO 27001 (AENOR, SGS, Bureau Veritas, BSI edo antzeko ziurtapen-erakunderen batek emana).
        - Aurrekoen antzeko beste batzuk.

Lantaldeko kide batek, gutxienez, gaztelaniaz eta euskaraz hitz egin beharko du jatorrizko hizkuntza gisa, eta solaskide izan ahalko da proiektuaren irismeneko edozein eremutan.

Gutxieneko gaitasun tekniko gisa eskatzen den lantaldean baino pertsona gehiago egon ahal izango dira enpresa lizitatzaileak eskaintzan proposatzen duen lantaldean. Txosten honetako I. eranskineko 1. eta 2. xehetasun-taulak bete beharko dira proiektuaren lantaldea osatzen duten pertsona guztien kasuan. Puntu hori baloratzeko orduan, puntuaziorik altuena emango zaio hobeto dimentsionatuta dagoen lantalde bat proposatzen duen enpresa lizitatzaileari.

Lan-taldea osatzen duten profil guztien artean, CISA (Certified Information Systems Auditor) eta Lead Auditor ISO 27001 ziurtagiriak bete beharko dira gutxienez.

Hornitzaileak proposatutako lantaldeak karatulako 16.b ataletan eskatutako baldintzak bete beharko ditu.

4.2 Proiektuaren entregagaiak

Enpresa lizitatzaileak argi eta garbi adierazi beharko du zein diren bere proposamenak barne hartzen duen proiektuaren emaitza entregagarriak, eta nahitaezkoa izango da hasierako egoeraren diagnostiko-txostena eta amaierako plan xehatua egitea BLHko toki-erakundeetarako zibersegurtasuneko bulego zentralizatua ezartzeko, bai eta zentro horren diseinuari erantzungo dion txosten bat ere.

Enpresa lizitatzaileak aholkularitzaren irismenaren barruan egingo dituen dokumentu guztien aurkibideen proposamen bat aurkeztu beharko da eskaintzetan. Proposatutako entregagarriak eta indizeen xehetasun-maila eskaintza teknikoan baloratuko dira. Puntu hori baloratzeko, puntuazio handiagoa emango zaio entregagarri horietan kalitate eta xehetasun hobea proposatzen duen lizitatzaileari.

4.3 Entregatzeko plangintza eta mugarriak

Karatulako 5. paragrafoan adierazitako gehieneko epean egin beharko ditu lizitatzaileak kontratu honen xede diren lanak. Lizitatzaileak plangintza xehatua egin beharko du proposamenean. Gantt diagrama batean adieraziko du hori, eta bertan, proiektuaren xede diren entregagaiak entregatzeko faseak, epeak, giza baliabideak, lan-kargak eta mugarriak ageriko dira.

Plangintzaren hobekuntza eta haren xehetasuna baloratuko da.

4.4 Lanen kontrola

BiscayTIK Fundazioak egindako lanen gaineko kalitate kontrola egitea beretzat gordetzen du. Horrela, gutxieneko baldintzak betetzen ez dituztenak gaitzetsi ahalko ditu, bere irizpide propioei jarraiki. Hori guztia BiscayTIK Fundazioak atzerapenen edo kontrataturiko zerbitzuen kalitate baxuaren ondotik jar ditzakeen penalizazioen kaltetan izan gabe egingo da. Halaber, kontratua ebazteko arrazoi justifikatua izan daiteke.

Enpresa esleipendunak irtenbide mekanizatuak jarriko ditu zerbitzuaren kudeaketa eta jarraipenerako.

4.5 Jabetza intelektuala

Esleipendunak BiscayTIK Fundazioari lagako dizkio kontratu honen baitan eratutako plan, sorkuntza eta dokumentu guztien egile-eskubideak eta jabetza intelektualeko eskubideak. Jabetza intelektualari dagozkion eskubideen lagapenak ez du denbora-mugarik izango eta esleipendunak kobratuko duen ordainsariaren barne dagoela ulertuko da. Ondore horietarako, BiscayTIK Fundazioak esleipendunaren lana orokorki aldatzeko, eraldatzeko, erreproduzitzeko, banatzeko, argitaratzeko, erakusteko, erabiltzeko eta ustiatzeko eskubidea izango du.

Esleipendunak ezin izango du ikerketa osoa edo zati bat erabili, ez zuzenean ezta zeharka ere, munduko edozein lekutan egin lezakeen beste enkargu batean.

Lizitatzaileak BiscayTIK Fundazioari eman beharko dizkio fitxategi guztien iturriak, baita erabilitako baliabide teknologiko guztiak ere.

4.6 Bermea

Gutxienez 3 hilabeteko bermea eskatuko da egindako lanentzat.

4.7 Genero ikuspegia

Dagozkien proposamenak egin eta aurkezteko, enpresa lizitatzaileek hizkera ez sexista erabili beharko dute. Halaber, enpresa esleipendunak, kontratua indarrean den bitartean, hizkera ez sexista erabili beharko du behin betiko dokumentu guztietan, izan idatziak edo digitalak, eta, pertsonei dagokien edozein estatistika egiteko, datuak sexuen arabera banandu beharko ditu. Hori guztia Emakumeen eta gizonen berdintasunerako otsailaren

18ko 4/2005 Legearen 2.3 artikuluari jarraikiz, zeinean errespetatu beharreko printzipio orokorrak zehazten baitira.

Enpresa esleipendunak kontratuaren helburu den prestazioa egin izanaren azken justifikazioan, hala badagokio, txosten bat aurkeztu beharko du, kontratazioan generoak izan duen eraginari buruz, adierazleak eta datuak sexuen arabera banatuta, hala erabiltzaileenak nola onuradunenak, edo zerbitzua ematen duten langileenak, aplikatutako berdintasun-neurriak ebaluatzeko aukera izateko.

Izenpetua: Alaitz Etxeandia Arteaga

BiscayTIK Fundazioko Zuzendari Nagusia

I.ERANSKINA – GIZA TALDEAREN KAUDIMENA

Gutxieneko baldintza teknikoak	Proposatutako balioa	Eskatutako balioa
Proiektu-buruaren profila duen pertsona bat (1), proiektu honen eremuko proiektuen kudeaketan gutxienez bost (5) urteko esperientzia egiaztatua duena, eta segurtasun-aholkularitzetan esperientzia duena, horien erreferentzia-esparrua Segurtasunerako Eskema Nazionala edo erreferentziazko beste estandar bat izan bada. Informatikako lizentziatura- edo ingeniaritza-titulua edo antzekoa izan behar du gutxienez, bai eta lanbide-ziurtagiri hauek ere:	(urteetan) Informatikako lizentziatura- edo ingeniaritza-titulua edo antzekoa (BAI / EZ) segurtasun-aholkularitzetan esperientzia (BAI / EZ) (gutxienez, 2 adierazi 1-xehetasun-taulan)	>=5 años SÍ SÍ
• Nahitaez, hauetako bat: o PMP (Project Management Professional) edo PRINCE2 (Projects In Controlled Environments) edo ITIL (Service Management Foundation Certification) edo antzekoa. • Baloratu ahal izango dira: o CISA (Certified Information Systems Auditor). o CRISC (Certified in Risk and Information Systems Control). o CISSP – ISSMP (Information Systems Security Management Professional). o CISSP – ISSAP (Information Systems Security Arquitecture Professional). o Lead Auditor ISO 27001 (AENOR, SGS, Bureau Veritas, BSI edo antzeko ziurtapen-erakunderen batek emana). o Lead Implementer ISO 27001 (AENOR, SGS, Bureau Veritas, BSI edo antzeko ziurtapen-erakunderen batek emana). o Aurrekoen antzeko beste batzuk..	Bete (BAI / EZ) (Bete 2-xehetasun-taulan) Bete (BAI / EZ) (Bete 2-xehetasun-taulan)	SÍ gutxienez bat N/A
Segurtasunean aditua den aholkularitza-profila duten bi (2) pertsona, gutxienez hiru (3) urteko lanbide-esperientzia dutenak proiektu honen esparruko segurtasun-aholkularitzetan. Informatikako lizentziatura- edo ingeniaritza-titulua edo antzekoa eduki behar du gutxienez, baita honako lanbide-ziurtagiri hauek ere proposatutako aholkulari bakoitzaren kasuan:	**Aholkulari 1** (urteetan) Informatikako lizentziatura- edo ingeniaritza-titulua edo antzekoa (BAI / EZ)	>=3 años SÍ
• Nahitaez, hauetako bat: o CISA (Certified Information Systems Auditor) o CRISC (Certified in Risk and Information Systems Control). o CISSP (Certified Information Systems Security Professional). o CISM (Certified Information Security Manager). o CISSP – ISSAP (Information Systems Security Arquitecture Professional). o Lead Auditor ISO 27001 (AENOR, SGS, Bureau Veritas, BSI edo antzeko ziurtapen-erakunderen batek emana).	Segurtasun-aholkularitzetan esperientzia (BAI / EZ) (SÍ / NO) (gutxienez, 2 adierazi 1-xehetasun-taulan) Ziurtagiriak (Bete 2-xehetasun-taulan)	SÍ

○ Lead Implementer ISO 27001 (AENOR, SGS, Bureau Veritas, BSI edo antzeko ziurtapen-erakunderen batek emana). ○ Aurrekoen antzeko beste batzuk.	Aholkulari 2 (urteetan) Informatikako lizentziatura- edo ingeniaritza-titulua edo antzekoa (BAI / EZ) Segurtasun-aholkularitzetan esperientzia (BAI / EZ) (SÍ / NO) (gutxienez, 2 adierazi 1-xehetasun-taulan) Ziurtagiriak (Bete 2-xehetasun-taulan)	>=3 años SÍ SÍ

1-Xehetasun-taula

Profila	Proiektuaren deskribapena	Bezeroa	Hasiera-data	Amaiera-data	Zenbatekoa (€ BEZik gabe)
Proiektu-burua			hilabete/urtea	hilabete/urtea	
			hilabete/urtea	hilabete/urtea	
	...	...	...	...	...
Aholkulari 1			hilabete/urtea	hilabete/urtea	
			hilabete/urtea	hilabete/urtea	
	...	...	...	...	...
Aholkulari 2			hilabete/urtea	hilabete/urtea	
			hilabete/urtea	hilabete/urtea	
	...	...	...	...	...

Adierazi, gutxienez, 2 (bi) proiektu profil bakoitzerako, gaitasun teknikoa osatzen duten profilen kasuetarako.

Honelako beste taula bereizi bat bete proposatutako proiektu-lantaldea osatzen duten gainerako profiletarako, nahiz eta gaitasun teknikoaren barruan egon ez.

2-Xehetasun-taula

Profila	Elebidun (SÍ / NO)	Titulu akademiko	Proiektuen Kudeaketako Ziurtagiria	Segurtasun Ziurtagiria
Proiektu-burua				
Aholkulari 1				
Aholkulari 2				

Adierazi profil bakoitzak dituen ziurtagiri guztiak. Ziurtagiri profesionalek indarrean egon beharko dute adjudikazioa egiten den unean, bai eta kontratua gauzatzen den bitartean ere.

Lantaldeko kide batek, gutxienez, gaztelaniaz eta euskaraz hitz egin beharko du jatorrizko hizkuntza gisa, eta solaskide izan ahalko da proiektuaren irismeneko edozein eremutan.

Lan-taldea osatzen duten profil guztien artean, CISA (Certified Information Systems Auditor) eta Lead Auditor ISO 27001 ziurtagiriak bete beharko dira gutxienez.

Honelako beste taula bereizi bat bete proposatutako proiektu-lantaldea osatzen duten gainerako profiletarako, nahiz eta gaitasun teknikoaren barruan egon ez.

Proposatzen den lantaldeak baldintza hauek ez betetzea baztertzeko arrazoia izango da. Edozein profiletarako, informazio hau berariaz EZ gehitzea ez-betetze gisa interpretatuko da.