

Espediente-zenbakia: 2024032 Harmonizatua

Kontratazioaren xedea: Europar Batasuneko NextGenerationEU funtsek finantzatutako Berreskuratze, Eraldaketa eta Erresilientzia Planaren esparruan “Zibersegurtasuneko Jazoeren Simulakroaren” zerbitzuak eskaintzeko esparru-hitzarmena.

Dokumentua: Preskripzio teknikoen plegua.

1. SARRERA

Euskadiko eraldaketa digitala bultzatzeko Eusko Jaurlaritzaren oinarritzko tresna da “Euskadi 2025 Eraldaketa Digitaleko Estrategia”, eta 2021eko martxoaren 30ean onartu zuen Gobernu Kontseiluak.

Eusko Jaurlaritzaren Industria, Trantsizio Energetiko eta Jasangarritasunaren Sailak bultzatutako estrategia honek eraldaketa digitalerako eredu berri bat ezartzen duen erronkari lagunduko dio, parte hartzen duten eragile guztien laguntza sinergiko, proaktibo eta koordinatuarekin.

Erakunde guztien egungo eta etorkizuneko hazkundea bultzatzera bideratuta daude teknologia digitalak, baita funtzio, gaitasun multzo eta laneko profil berrien eskaria handitzera ere. Automatizazioaren gorakadaren aurrean, enpresek haien lan-indarra berregituratu behar dute. Horretarako, profil tradizionalenak gutxitu eta horien ordean profil teknologikoagoak txertatu behar dituzte, edo azpikontratazioa areagotu behar dute lan espezifikoetarako.

EEDE 2025 hiru dimentsiotan egituratzen da eta aukera ematen du Eusko Jaurlaritzak estrategiaren indarraldian zehar finkatu dituen elementuak eta lehentasunak definitzeko. Hauek dira dimentsio horiek: **palanka teknologikoak**, **laguntzeko gaitasunak** eta **aplikazio-eremuak**. Hiru dimentsio horiek ez dute modu isolatuan jarduten, sistema moduan baizik, eta Euskadirentzako balioa sortzeko ikuspegitik erreparatu behar zaie. Hortik aurrera, palanka teknologikoak aukeratzeko kontuan hartu da epe labur, ertain eta luzean hiru trantsizioetan planteatzen diren erronketan izan dezaketen rol disruptiboa. Erraztaileak teknologia digitalak hedatzea sustatzeko eta azkartzeko bitartekoak, kanalak edo gaitasunak dira.

Identifikatutako “palanka teknologiko” horietako bat da “ZIBERSEGURTASUNA ETA KONFIANTZA DIGITALA”.



Zibersegurtasunak erasoen, kalteen edo baimenik gabeko sarbideen sareak, gailuak, programak eta datuak babesteko neurri eta jarduketak biltzen ditu. Jarduera produktiboaren digitalizazioan izandako sustapena eta garapena eta, zehazki, sarera konektatutako gailuen hazkunde esponentziala, zein informazioaren eta komunikazioen teknologien gero eta sofistikazio handiagoa direla eta, beharrezkoa da enpresen segurtasun digitalean eragitea eta babesteko tresnak hobetzea.

Zibersegurtasuna aplikazioen eta sistema informatikoen garapenean finkatutako jarduketa da eta enpresa erabiltzaileen barruan funtsezko funtzioa da. Horregatik, industrian inpaktu handia duten eta disrupziorako potentzial esanguratsua duten joera berriak sortu dira, jarraian zehaztuko dugun moduan:

- Hautemateko soluzio berriak eta zabaldutako erantzunak, mehatxuak hautematea hobetzeko eta jazoerei erantzuteko gaitasun hobea eskaintzeko.
- Segurtasun-prozesuen automatizazioa.
- Segurtasuneko erantzukizun berriak, AAre erabileraren bidez.
- Chief Security Officer, CSO, figura sortu zen, erakundearen segurtasun fisiko eta teknologikoaz arduratzeko.
- Pribatutasunaren gaineko garrantzi handiagoa erakundeetan.
- Bezeroekin eta hornitzaileekin izandako interakzio guztietan osotasuna bermatzeko konfiantzazko ekipoak eta segurtasun digitalak.
- Hodeiko segurtasun-zerbitzuak geroz eta ohikoagoak.
- Babes berbera erakundearen bizi-ziklo osoarentzat, baina hodeiko aplikazio natiboen edo cloud native app-en baldintzak kontuan hartuta.
- VPNak edo Sare Pribatu Birtualak zero konfiantzako sareekin, Zero Trust, ordezkatzen hasi dira. Sare horietan beharrezkoa da identitatea zorrotz egiaztatzea, kokapena edozein izanik ere, eta pertsonak zein gailuak izanda ere.

Zibersegurtasunarekin lotutako arazoak edo erronkak etengabe aldatzen dira; izan ere, ziberasoen bolumena eta zailtasuna handituz doa. Hortaz, zibersegurtasunaren gaitasunak eta garapenak bilakaera berbera izango dute. Beste teknologia batzuen garapenak, erabilerak edo agerpenak aukerak eta erronkak dakartza zibersegurtasunarentzat. Alde batetik, AAK erantzunaren abiadura azkartu du eta hobeto hautematen ditu ziberasoak automatikoki hauteman eta blokeatu ahal izateko anomaliak. Beste alde batetik, konputazio kuantikoak erronka berriak ekarri ditu kriptografia kuantikoarekin lotuta, teknologia hori erabiltzen duten erasoan aurrean kalteberatasunak murrizteko. Zibersegurtasun kuantikoak hainbat erronka planteatzen ditu, hala nola gako kuantikoak banatzea, segurtasun kuantikoko algoritmoak eta ausazko zenbaki kuantikoen sortzaileak. Era berean, zibersegurtasuna funtsezkoa da informazio-sistemen edo Datuak Prozesatzeko Zentroen barne funtzionamendurako, datu sentiberak biltegiratu eta trukatzeko dituelako.

Azkenik, zibersegurtasunaren gaitasunak 5G sareetara egokitu dira eta ezinbesteko hainbat aplikazioen bizkarrezurra bihurtu dira, hala nola ibilgailu autonomoena. Hortaz, sare horien osotasunak eta eskuragarritasunak kalteberatasun-puntu handiak ditu.

Testuinguru horretan, beharrezkoa da enpresak entrenatuta egotea izan ditzaketen zibersegurtasuneko jazoerak kudeatzeko. Enpresak bi motatan sailka daitezke arlo horretan. Dagoeneko zibersegurtasuneko jazoera bat jasan dutenak, eta jasango dutenak.

Egungo proiektua “Zibersegurtasuneko jazoeren simulakroa” egitean datza, ingurune kontrolatu batean. Horrek aukera emango du enpresaren ahulguneak hautemateko eta, ondoren, gure sistemen eta ekipoen kalteberatasunak murrizteko erabakiak hartu ahal izateko. Erabaki horiekin ez dira amaituko zibersegurtasuneko jazoera bat jasateko aukerak, baina jazoera horiek gure enpresari eragin diezazkioketen kalteak arintzeko balioko dute.

Zerbitzu hori DIGITALIZAZIOAREN ETA ADIMEN ARTIFIZIALAREN ESTATU IDAZKARITZAREN RETECH DEIALDIAREN (ESPEZIALIZAZIO TEKNOLOGIKORAKO LURRALDEEN SAREAK) BARRUAN EGINDAKO HITZARMENAREN ETA LANKIDETZAREN barruan sartzen da. 2023ko azaroan sinatu zuten hitzarmen hori, besteak beste, SPRI-ENPRESEN GARAPENERAKO EUSKAL AGENTZIAK eta INCIBEK (S.M.E. ESPAINIAKO ZIBERSEGURTASUNeko INSTITUTU NAZIONALA M.P., S.A.).

Eusko Jaurlaritzak deialdi horretan aurkeztu zuen RED-ARGOS PROIEKTUA izeneko proiektuaren helburu estrategikoak hauek dira, besteak beste:

- Zibersegurtasun-industria indartzea berrikuntza publiko-pribatuko ekosistema batekin, esperimentaziorako I+G+b jarduerak garatuz eta banatutako ezagutzaren azpiegitura logiko edo fisikoen sare bat sortuz, osagarritasuna, enpresentzako transferentzia, espezializazio teknologikoa, soluzioak merkatura iristea eta balio-kate osoan produktuak sortzea eskainiko duena.
- Zibersegurtasunaren iragazkortasuna hobetzea sektore ekonomiko guztietan, globalki hartzea errazteko.
- Eskualdeen arteko lankidetzak sustatzea, haztea eta sendotzea, proposamenean parte hartzen duen autonomia-erkidego bakoitzaren indarguneetan oinarrituta, zibersegurtasunaren arloan trakzio-efektu handiagoa lortzeko, aukera ekonomiko, profesional eta enpresarial gisa.
- Erkidego mailan dauden gaitasunak hobetzea, espezializatu ahal izateko azpiegitura, ekipamendu eta baliabide berriak gehituz.
- Zibersegurtasuneko neurri orokorren ezarpena handitzea, diseinutik hasi eta gainerako etapa guztietan. Konponbide berriak garatzea.
- Zibersegurtasuneko atzemateko eta trebatzeko estrategien garapenarekin talentua erakartzea eta sortzea, bai eskaintzari, bai eskariari dagokionez, prestakuntza-planen eta konpetentzia eta profil profesionalekin espezializatutako ibilbideen bitartez, betiere, zibersegurtasunaren garapena azkartzeko.
- Zibersegurtasuneko ekintzailatza sustatzea eta batez ere ETE-etan bizkortzea, ikusgarritasun eta merkaturako iritsiera hobeara eramateko.

2. KONTRATAZIOAREN HELBURUA

Esparru-akordio honen xedea da Zibersegurtasunean espezializatutako enpresak hautatzea, SPRI-Enpresa Garapenerako Euskal Agentziarentzat (aurrerantzean, "SPRI") zibersegurtasuneko gertakarien simulazio-zerbitzuak emateko, hitzarmenak irauten duen bitartean.

Lehiaketa publiko honetako esleipendunen zerbitzuen eskaintza SPRIren eskari bidez egingo da eta, aldi berean, baita SPRIk jarduera EAEn duten enpresetatik jasotzen dituen eskarien erantzun gisa ere, "Zibersegurtasuneko jazoeren simulakroen" jardunaldiak antolatzeko. Jardunaldi horiek "in company" egin ahal izango dira enpresa bateko talde zuzendarientzat, baita hainbat enpresarentzako formatu irekian ere, SPRIk jarduera horietarako eskuragarri jartzen dituen instalazioetan. Baldintzak berberak izango dira jarduera-zentroa EAEn duten enpresa guztientzat. Simulakro horiek enpresak zibersegurtasuneko arloan dituen kalteberatasunak murriztu ahal izateko erabakiak hartzeko gaitasuna duten zuzendaritza-taldeetako pertsonaiei zuzenduta egongo dira batik bat. Informazioaren eta Komunikazioen Teknologien saileko pertsonak beti hartu beharko dute parte simulakro horietan. Halaber, arlo teknikoko pertsonak inplikatzeko dituen simulakroak antolatu ahal izango ditu SPRIk. SPRIk eskatutako esleipendunek eskainiko dituzte zerbitzu horiek eta eskaera hori bere eskariaren eta enpresek SPRIren webguneko ZIBERSEGURTASUNEKO JAZOEREN ZERBITZUAREN bitartez aldeztatik aurretik egindako eskariaren arabera egingo du erakundeak. Simulakro horiek hainbat enpresarentzako batera egindako deialdi irekien bidez ere antolatu ahal izango ditu SPRIk eta EAEko 17 enpresa-klusterrei dagokienez jazoera espezifikoen simulakroak egin ahal izango dira.

Simulakro bakoitzaren prezioa SPRIk enpresei eskaini dizkien "zibersegurtasuneko jazoeren simulakro moten" eta SPRIk zibersegurtasuneko jazoeren simulakro mota horietako bakoitza kudeatzeko eta egiteko esleitutako ordu-kopuruaren arabera zehaztuko da, enpresa edo enpresa-kolektibo bakoitzaren ezaugarrien eta arlo horretan dituzten beharren arabera. Jazoeren simulakroen tipologia aldatuz joan ahal izango da bilakaera teknologikoaren eta zibersegurtasunak hainbat enpresa-sektoretan duen egoera orokorraren arabera. Jazoeren simulakroen tipologiaren diseinuan eta bilakaeran, EAEn dauden 17 klusterren behar espezifikoak izango dira kontuan. Jarduna ezingo da 7 ordutik gorakoa izan aholkulari bakoitzaren kasuan eta gehienez ere bi aholkulari izango dira simulakro bakoitzean. SPRIk zibersegurtasuneko jazoeren simulakro mota bakoitzerako zehazten dituen jarraibideen eta oinarritzko egituren arabera exekutatu beharko dituzte esleipendunek zibersegurtasuneko jazoeren simulakroak.

Era berean, hautatutako enpresa kontratista bakar batek ere ezingo du enpresa onuradunei diagnostiko-zerbitzua eskaintzeko 350.000 eurotik gorako zerbitzurik egin

(BEZik gabe), plegu honetan adierazitakoan oinarrituta. Kontratisten kopurua 10etik beherakoa bada, kontratistak oinarritutako kontratuak esleitzeko gehieneko zenbatekoa honela kalkulatu da: kontratuaren balio zenbatetsia zati kontratisten kopurua (adibidez, 8 kontratista, esleipenaren gehieneko balioa 437.500 euro).

Gehienez ere 20 kontratista aukeratuko dira.

Esparru Akordioaren eta kontratu bakoitzaren xede diren jarduerak EAEren barruan gauzatuko dira.

Behin-behineko irismena 2026ko martxoaren 31 bitartekoa izango da, Esparru Hitzarmena formalizatu eta hurrengo egun baliodunetik hasita. Oinarritutako kontratuak Esparru Akordioaren iraupenaren barruan esleituko dira, eta iraupen handiagoa eduki ahal izango dute, hiru hilabete gehiagokoa gehienez ere.

3. EGINGO DIREN JARDUEREN HELBURUAK ETA DESKRIBAPENA

3.1. Helburua

Zibersegurtasuneko jazoeren simulakroen zerbitzuak eskaintzea.

3.2. Kontratuaren xede diren jarduerak

Esleipendunei esleituko zaizkien zereginak zibersegurtasuneko jazoeren simulakroak kudeatzeko eta exekutatzeko beharrezkoak diren guztiak izango dira. Hauek izango dira, gutxi gorabehera:

- Zerbitzu bakoitzaren helburuak ezagutzea, bere beharrak identifikatzea eta bere beharretara hobekien egokitzen den simulakroaren tipologia definitzea.
- SPRIrekin lankidetzan aritzea zibersegurtasuneko jazoeren simulakro motak definitzeko.
- SPRIk deialdi irekiaren bidez EAEko enpresei eskaintzen dizkien zibersegurtasuneko jazoeren simulakroak kudeatzea eta exekutatzeko, SPRIk horretarako gaitutako instalazioetan.
- SPRIri eskaera indibiduala egiten dioten enpresen zibersegurtasuneko jazoeren simulakroak kudeatzea eta exekutatzeko, bai *in company*, bai SPRIk horretarako gaitzen dituen instalazioetan, EAE barruan.
- Egindako simulazioen emaitzei buruzko txostena egitea, bai eta haien ahultasunak murrizteko egin beharreko jarduketaren proposamenak ere.
- SPRIrentzat txostenak egitea, egindako simulakroen emaitzei buruz.
- Eskatutako zibersegurtasuneko simulakro mota exekutatzeko. Mota hori SPRIk diseinatuko du. Esparru Hitzarmenean eskatutako profil profesional bakoitzari egotzi

beharreko gehieneko ordu-kopurua ezarriko da simulakro bakoitzarentzat. Jarduna ezingo da 7 ordutik gorakoa izan aholkulari bakoitzaren kasuan eta gehienez ere bi aholkulari izango dira simulakro bakoitzean.

- Adibide moduan, hauek izan daitezke simulakro motak:
 - Ransomware
 - Azpiegitura kritikoa
 - Zuzendutako erasoak
 - Beste batzuk
- Enpresen tamainaren eta haien jarduera-sektoreen arabera diseinatuko dira simulakro-motak, eta ahalegin berezia egingo da enpresa txiki eta ertainei zuzendutako simulakroak diseinatzeko, batez ere, industria-sektoreetakoei, zerbitzu aurreratuei eta energiaren arlokoiei zuzendutakoak.
- Zerbitzua hedatzeko ekintzak egitea SPRIrentzat.
- SPRIk simulakro-mota bakoitzarentzako ezartzen duen metodologiara egokitu beharko dute exekuzioa esparru-hitzarmeneko enpresa esleipendunek. Adibide modura, alderdi hauek hartuko dira kontuan:
 - Zuzendaritzako ekipoentzako simulakro espezifikoak diseinatzea, betiere, IKT saileko ekipoak inplikatur.
 - Simulakroak krisi-batzordeetako kideei zuzenduta egon beharko dira eta erabakiak hartzera bideratuko dira.
 - INCIBE edo ZIUR moduko erakundeek egiten dituzten ekintzekin benchmark egiteko eta sinergiak bilatzeko aukera.
 - Profil teknikoei, role playei eta abarri zuzendutako jarduketak berrikustea.
 - Simulakroak diseinatzea hainbat formatutan: jazoeren simulakroa egitea ekoizpen-fabrika batean rol-joko narratibo baten bidez (storytelling), simulakroak egitea hainbat profilentzat, hainbat orduko saio batean edo batzuetan.
- SPRIrekin lankidetzan aritzea zerbitzuaren aginte-koadroak ezartzeko eta kudeatzeko.
- Klusterrekin lankidetzan aritzea kontratu honen arloan, SPRIK hala eskatuz gero.

Esparru Akordioan oinarritutako kontratuak gauzatzean, Zerbitzuak bi hizkuntza ofizialetan emango direla bermatu beharko da; izan ere, prestazioa EAEn jarduerazentroa duen edozein enpresatan edo enpresa-taldetan gauzatu ahal izango da. Halaber, ekintza guztietan hizkuntzaren erabilera eta irudien tratamendu ez sexista egingo duela bermatuko du kontratistak. Hori guztia, Euskal Sektore Publikoan euskararen erabilera normalizatzeko otsailaren 22ko 19/2024 DEKRETUAN eta Emakumeen eta Gizonen Benetako berdintasunari buruzko martxoaren 22ko 3/2007 Lege Organikoan aurreikusitakoaren arabera.

Hizkuntza-koofizialtasunarekin eta hizkuntzaren eta irudien erabilera ez sexistarekin lotutako betebeharrak betetzea ezinbestekoa eta funtsezkoa da Zerbitzua ongi emateko. Hortaz, Esparru Akordioan oinarritutako kontratuetako bakoitza eta Esparru Akordioa bera gauzatzeko funtsezko baldintzak dira, eta ez betetzeak (hau da, Zerbitzu bat hizkuntza ofizialetako batean ez ematea, SPRIk edo enpresa batek hala eskatu

ondoren; edo hizkuntzaren eta irudien erabilera ez bat etortzea Emakumeen eta Gizonen Benetako Berdintasunari buruzko martxoaren 22ko 3/2007 Lege Organikoak ezarritakoarekin) honako ondorioak izan ditzake:

- Kontratuari dagokion zenbatekoaren % 10era arteko zigorra jasotzea, hizkuntzaren eta irudien erabilera ez sexistaren baldintza bete ezean.
- Esparru-akordioa suntsiarazteko arrazoia izango da, baldin eta oinarritzko kontratua esleitzen zaion kontratistak ezin badu prestazioa SPRIk edo enpresak eskatutako hizkuntza ofizialean gauzatu.

4. ESKATZEN DIREN LANTALDEA ETA PROFIL PROFESIONALAK

Lizitatzailleek beren proposamen teknikoan eskaintzen duten lantaldeak langile kualifikatuak izan beharko ditu, eta Zibersegurtasuneko teknikari espezialistek osatu beharko dute. Bereziki, proposatzen den lantaldeak baldintza hauek bete beharko ditu, gutxienez:

- a- Eman beharreko zerbitzuen arduradun nagusi eta SPRIko arduradunarekin solaskide gisa jardungo duen pertsona bat izendatzea (proiektuaren aholkulari-burua). Pertsona horrek ezagutza eta esperientzia nahikoak izango ditu agiri honen xedearen antzeko zereginetan, hau da, Zibersegurtasunaren eremuan.
- b- 3. atalean deskribatutako lanak egiteko, proiektuaren aholkulari nagusiaz gain, beharrezkoa da esleipendun bakoitzak gutxienez 2 pertsonako talde gehigarria izatea (2 aholkulari tekniko espezialista, teknikari laguntzaile gisa jarduteko), esperientzia duena zibersegurtasunaren arloan.
- c- Proposatutako lantaldeko pertsona batek, gutxienez, enpresei zerbitzua euskaraz emateko aukera izan beharko du, enpresek hala eskatzen dutenean. Hortaz, proposatutako lantaldeko kide batek, gutxienez, euskarako C1 maila edo baliokidea duela ziurtatu behar da eskaintza teknikoan.
- d- SPRIin kontratuaren ardura duenak zuzenean gainbegiratu du esleipendunaren lantaldeak egindako lana.

SPRIk kontratistari iradoki ahal izango dio Zerbitzuetan jende gehiago sartzea unean uneko beharren arabera, betiere haien profilak lantaldean proposatutako pertsonen antzekoak badira. Kontratistak iradokizuna baloratzeko konpromisoa hartuko du.

Nolanahi ere, lantaldeak, gutxienez, profesionalen profil hauek izan behar ditu:

- Industria Ingeniaritzan, Informatika Ingeniaritzan, Telekomunikazio Ingeniaritzan, Fisikan, Matematikan edo baliokideetan goi-mailako prestakuntza duen eta Zibersegurtasunean prestakuntza espezifikoa duen pertsona bat, proiektuaren aholkulari buru eta SPRIrekin solaskide nagusi gisa jardungo duena.

- Bi pertsonak, horietako batek, gutxienez, goi-mailako prestakuntza dute Industria Ingeniaritzan, Informatika Ingeniaritzan, Telekomunikazio Ingeniaritzan, Fisikan, Matematikan edo antzekoetan, eta prestakuntza espezifikoak dute Zibersegurtasunean, aholkulari aditu espezialista gisa, laguntza-teknikari moduan. Bigarren pertsonari ez zaio eskatuko goi-mailako prestakuntza izatea, baina bai zibersegurtasunaren arloko ezagutzak egiaztatzea.

Proposatutako lantaldeko kideek gutxienez honako esperientzia hau izan beharko dute, eta jarraian zehaztutako funtzioak bete behar dituzte:

Profil profesionala	Rolak eta esperientzia-urteak
1 proiektuaren aholkulari buru	Aholkularitzan eta proiektuen kudeaketan esperientzia izatea, eta gutxienez 5 urteko esperientzia izatea zerbitzu honen xede den arloan. Lidergoa: Diziplina anitzeko taldeak gidatzeko eta proiektuak zuzentzeko gai izan behar du, sorreratik ezarpeneraino. Kudeaketa-trebetasunak: Proiektuak kudeatzeko trebetasun sendoak izan behar ditu, plangintza, baliabideen esleipena, arriskuen kudeaketa eta aurrekontua barne, eta SPRIko taldearekin proiektua deskargatzeko trebetasunak izan behar ditu. Komunikazio-trebetasun bikainak: Bezerekin, barne-ekipoekin eta beste stakeholder batzuekin eraginkortasunez komunikatzeko gai izan behar du. Emaitzetara bideratua: Profil horrek emaitzetara bideratutako ikuspegia izatea eta ezarritako epe eta aurrekontuen barruan proiektuaren helburuak betetzeko gai izatea espero da. Gaitasun analitikoa: Arazo konplexuak aztertze eta horiek konpontzeko irtenbide eraginkorrak garatzeko gai izan behar du.
2-Aholkulari teknikari espezialista	Gutxienez 2 urteko esperientzia aholkularitzan proiektuarekin lotutako arlo espezifikoan. Trebetasun teknikoak: Ezagutza tekniko sendoa izan behar du bere espezializazio-arloan, eta ezagutza hori SPRIrekin zerbitzua

gauzatzean sortzen diren arazoak konpontzeko aplikatzeko gai izan behar du.

Autonomia: Esleitutako zereginetan modu autonomoan lan egin ahal izatea espero da, nahiz eta esleipendunak eta SPRIk osatutako taldeetan eraginkortasunez lagundu ahal izango duen.

Komunikazio-trebetasunak: SPRIko taldearekin argi eta garbi komunikatzeko gai izan behar du, ahoz zein idatziz.

Moldagarritasuna: Lan-ingurune desberdinetara egokitzeko gai izan behar du, eta malgua izan behar du bere ikuspegian, proiektuaren erronkei heltzeko.

Gutxieneko taldeak osatzeko, esleipendunak baldintza hauek bete beharko ditu: kontratua behar bezala gauzatzeko behar dituen langileak jarri beharko ditu, eta indarrean dagoen legerian gaitasun tekniko eta profesionalari buruz jasotako eta Plegu honetan eskatutako baldintza orokor eta espezifikoak bete beharko dituzte; izan ere, giza baliabideak faktore erabakigarria dira zerbitzuaren kalitatean. Kontratuak irauten duen bitartean kontratua garatzeko behar diren pertsonak atxikita dauden profilaren araberrako curriculum-maila izango dute.

5. IKUSKAPENA ETA ZERBITZUAREN KONTROLA

Eman beharreko zerbitzuak SPRIren Eraldaketa Digitalaren Sailak gainbegiratu dituen, eta bereziki, kontratuaren arduradunak, eta kontratatutako lanen garapen egokia egiaztatzeko beharrezkotzat jotzen dituen azalpenak eta informazioa eskatu ahal izango ditu.

6. HAUTATUTAKO KONTRATISTEN ARTEAN OINARRITUTAKO KONTRATUAK ESLEITZEA

Zerbitzuak eskaintzeko, Esparru Hitzarmenetik eratorritako kontratuen segida bat egingo da “zibersegurtasuneko jazoeren simulakro” bakoitzarentzat, eta SPRIk eskatutakoan exekutatu da:

- (i) In company zerbitzuen kasuan, SPRIk hiru eskaintzak eskatuko ditu enpresen aurretiazko eskariaren oinarriaren gainean, eta Esparru Akordioaren esleipenean

erabilitako esleipen-irizpide bat edo batzuk erabili ahal izango dira. Halaber, haztapenak desberdinak izan daitezke.

- (ii) Hainbat enpresentzako irekiak diren zibersegurtasuneko jazoeren simulazio-egunei dagokienez, SPRIk txandakako txandetan egingo du banaketa, eta enpresa bakoitzari oinarritutako kontratu bat esleituko dio, proposamenen sailkapenaren ordenaren arabera (hau da, lehen zerbitzua lehen enpresa sailkatuari esleituko zaio, eta horrela hurrengo sailkatutako enpresa guztiekin). Puntuazio orokorrean berdinketarik balego, esleipendunen izen sozialaren ordena alfabetikoa jarraituko da. Eguna bat baldin badator aurretik esleitutako beste egun batekin, oinarritutako kontratua hurrengo enpresari esleituko zaio, ordena eta txandakako txanda berbera jarraituz.

Edonola ere, hautatutako kontratista bakar batek ere ezingo ditu 350.000 eurotik (BEZ gabe) gorako zerbitzuak gauzatu. Kontratisten kopurua 10etik beherakoa bada, kontratistak oinarritutako kontratuak esleitzeko gehieneko zenbatekoa honela kalkulatu da: kontratuaren balio zenbatetsia zati kontratisten kopurua (adibidez, 8 kontratista, esleipenaren gehieneko balioa 437.500 euro).

Oinarritutako kontratu bat gauzatzeko hautatutako kontratistak ezingo dio inola ere uko egin kontratua gauzatzeari, justifikaziorik gabe, eta SPRIk eskatutako zerbitzu guztiak eman beharko ditu. Esparru-akordio honen barruan aldez aurretik ezarritako egunekin bat etorritz gero, justifikatuta egongo da, baita kontratistak aurretik adierazitako gehieneko atalase ekonomikoa gainditzen badu ere.