BILBAO BIZKAIA UR PARTZUERGOKO SEGURTASUN-ERAGIKETEN ZENTROKO ZERBITZUAK KONTRATATZEKO PRESKRIPZIO TEKNIKO PARTIKULARREN AGIRIA “EUROPAR BATASUNAREN NEXT GENERATION SUSPERTZE ETA ERRESILIENTZIARAKO MEKANISMOAREN FUNTSEKIN FINANTZATUA, ZEHAZKI, «ITSASERTZA ETA BALIABIDE HIDRIKOAK ZAINTZEA» 5. OSAGAIAREN «AZPIEGITUREN ARAZKETA-, SANEAMENDU-, EFIZIENTZIA-, AURREZPEN-, BERRERABILPEN- ETA SEGURTASUN-JARDUKETAK GAUZATZEA» 1. INBERTSIOAREN (C5.I1) ESPARRUAN”

# AURKIBIDEA

1 AURREKARIAK ..... 4
2 XEDEA ..... 4
3 ARAUDI ESPEZIFIKOA ..... 4
4 ZERBITZUEN DESKRIBAPENA ..... 5
4.1 Segurtasun-eragiketen zentroa (SEZ) ..... 5
4.1.1 Ziberinteligentzia ..... 6
4.1.2 Segurtasuna monitorizatzea ..... 7
4.1.3 Segurtasun-gorabeheren kudeaketa ..... 10
4.1.4 Segurtasun-auditorien eta kalteberatasunen analisien zerbitzua ..... 12
4.2 Baliabide teknikoak eta giza baliabideak. ..... 15
4.2.1 Proiektuburua ..... 16
4.2.2 Zibersegurtasuneko Eragiketa Zentroari (SEZ) atxikitako langileak ..... 16
4.2.3 Azken gogoetak ..... 18
4.3 Ikuskapena eta kontrola ..... 19
4.3.1 Informatzeko betebeharra ..... 20
4.3.2 Zerbitzua emateko mailak ..... 21
4.4 Azpikontratazioa ..... 21
4.5 Proiektuaren faseak ..... 21
4.5.1 Ezarpen-fasea ..... 22
4.5.2 Zerbitzu osoko fasea ..... 22
4.5.3 Zerbitzuak itzultzeko fasea ..... 22
4.6 Lan-metodologia ..... 23
4.7 Beste baldintza batzuk ..... 23
4.7.1 Zerbitzua emateko lekua ..... 23
4.7.2 Zerbitzua emateko ordutegia ..... 24
4.7.3 BBUPeko sistemetan sartzea ..... 24
4.8 Kontratua suntsiarazteko arrazoiak ..... 25
4.9 Informazioaren konfidentzialtasuna ..... 26

4.10 Lanen dokumentazioa ..... 27
4.11 Zigorrak eta zehapenak ..... 27
5 IRAUPENA ..... 28

# 1 AURREKARIAK

Bilbao Bizkaia Ur Partzuergoak (aurrerantzean, BBUP), hainbat enpresa espezializaturekin batera, segurtasun-eragiketen zentroari lotutako zerbitzuak planifikatu, garatu eta mantentzen ditu.

Mehatxuak eta erasoak gero eta handiagoak eta konplexuagoak direnez, eta informazioaren segurtasunaren eta zibersegurtasunaren alorrean Espainian zein nazioartean gero eta gorabehera gehiago daudenez, beharrezkoa da horietan espezializatutako kanpoko zerbitzuak kontratatzea, arriskuen prebentzioa eta gorabehera baten aurrean erantzun egokia ziurtatuko dutenak.

# 2 XEDEA

Dokumentu honen helburua da SEZ zerbitzuak zerbitzu-modalitatean kontratatzeko bete behar dituen zereginak eta ezaugarriak zehaztea.

# 3 ARAUDI ESPEZIFIKOA

Jarraian, kontratazioaren helburuarekin zerikusia duten arau eta erregulazioen zerrenda bat jasotzen da, zehatza ez dena:

- 43/2021 Errege Dekretua.
- 311/2022 Errege Dekretua, Segurtasunaren Eskema Nazionala arautzen duena.
- 8/2011 Legea, apirilaren 28koa, Azpiegitura kritikoak babesteko neurriak ezartzen dituena.
- 12/2018 Errege Lege Dekretua, irailaren 7koa, Informazio Sare eta Sistemen Segurtasunarena.
- 43/2021 Errege Dekretua, urtarrilaren 26koa, Informazio Sare eta Sistemen Segurtasunaren irailaren 7ko 12/2018 Errege Lege Dekretua garatzen duena.
- 704/2011 Errege Dekretua, maiatzaren 20koa, Azpiegitura Kritikoak Babesteko Araudia onartzen duena.
- «Zibergorabeheren jakinarazpen eta kudeaketarako gida nazionala», Barne Ministerioak argitaratua.
- 2016/679 (EB) Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2016ko apirilaren 27koa, datu pertsonalen tratamenduari eta datu horien zirkulazio askeari

dagokienez pertsona fisikoak babesteari buruzkoa (Datuak Babesteko Erregelamendu Orokorra).

- 3/2018 Lege Organikoa, Datuak Babesteari eta Eskubide Digitalak Bermatzeari buruzkoa (DBEDBLO).
- UNE-EN ISO/IEC 27001:2017 araua. Informazioaren teknologia. Segurtasun-teknikak. Informazioaren segurtasuna kudeatzeko sistemak. Baldintzak. (eta ISO/IEC 27000 serieko ondorengoak, informazioaren segurtasuna kudeatzeko sistemei buruzkoak.
- Information Technology Infrastructure Library (ITIL)

# 4 ZERBITZUEN DESKRIBAPENA

Adjudikaziodunak kontratu honen esparruan egin beharreko lanen irismena informazioaren segurtasuneko eta zibersegurtasuneko zerbitzuak ematea izango da, BBUPen Segurtasun Logikoko arloari laguntzeko. Horretarako, segurtasun-eragiketen zentro bat (aurrerantzean SEZ) izango du.

Ondoren, adjudikaziodunak eman beharko dituen zerbitzuak xehetasunez deskribatzen dira. IV. eranskinean, hornitzaileak bete beharreko gutxieneko estandarrak (zerbitzu-mailako akordioak) jasotzen dira.

## 4.1 Segurtasun-eragiketen zentroa (SEZ)

SEZek etengabeko zerbitzua (24x7) eskainiko du segurtasun-gorabeherak monitorizatu, gainbegiratu, detektatu eta kudeatzeko, hau da, prebentzio-segurtasunean eta segurtasun erreaktiboan zentratuko da bere jarduera.

BBUPen ezarritako prozeduren arabera jardun behar du beti. Jardueraren erregistroa, kontrola eta jarraipena egiteko, BBUPek gorabeherak kudeatzeko duen tresna erabiliko da, bai eta agintari nazionalek (LUCIA, CCN-CERT edo beste erakunde batzuek, behar izanez gero) ezartzen dituzten zibergorabeherak jakinarazteko tresnak ere.

Baldintza-agiri honen esparruan hedatzen den Zibersegurtasuneko Operazio Zentroa Zibersegurtasuneko Operazio Zentroen Sare Nazionalean sartuko da. Estatuko sare horretan integratutako zentroak Zibergorabeheren Jakinarazpen eta Jarraipenerako Plataforma Nazionalaren bidez koordinatuko dira. Plataforma hori, hain zuzen ere, Informazio Sare eta Sistemen Segurtasunaren irailaren 7ko 12/2018 Errege Lege Dekretua garatzen duen urtarrilaren 26ko 43/2021 Errege Dekretuaren 11. artikuluan aurreikusita dago.

SEZek, gutxienez, ondoren aipatzen diren zerbitzuak emango ditu (ez da zehatza zerrenda). Eskaintzaileak zerrenda hori handitu ahal izango du, bai edukiari dagokionez, bai irismenari dagokionez.

### 4.1.1 Ziberinteligentzia

Adjudikaziodunak inteligentzia digitaleko zerbitzu bat emango du datuak eta informazioa hainbat iturritatik biltzeko, eta ikertu egingo du, eta emaitzak aztertu, BBUPi eragin diezaioketen online mehatxuak lehenbailehen detektatzeko. Hauek dira, gutxienez, mehatxuok:

- Informazio-ihesak; datu pertsonalak egotea (bertako langileenak edo BBUPek zaindutako hirugarrenen datuenak), kredentzialak lapurtzea, dokumentu konfidentzialak lapurtzea edo iragaztea, datu-baseetan egotea, konprometitutako sistemei buruzko informazioa eta abar.
- Aktiboak babestea.
- Mehatxu aurreratu iraunkorrak.
- Mugimendu sozialak eta hacktibistak.
- VIP babesa.
- Marka, presentzia eta lineako ospea babestea.

Aztertu beharreko iturriek, gutxienez, hauek izan behar dute:

- Webgune konbentzionalak, hizkuntza eta kokapen geografikoa gorabehera.
- Bilaketa-motorrak: Google, Bing, Altavista, Yahoo, besteak beste.
- Foroak.
- Datu-base publikoak (EAO, OEPM, BOPI eta abar) eta datu-base pribatuak (einforma, erregistratzaileak eta abar).
- Interneten argitaratutako barne-informazioa: Fabrikatzaileen arrakasta-kasuak, aurkezpen publikoak, BBUPen baliabideetan argitaratutako metadatuak, *news*-zerbitzariak, foroak eta abar.
- Sare sozialak (Facebook, Linkedin, Twitter eta abar).
- Threat Intelligence datu-baseak.
- Spam-zerrenda beltzak
- DNS zerbitzariak.
- Domeinuez jabetzea (*Cybersquatting*).
- Mugikorretako aplikazioen *market*ak.
- P2P sareak (Emule, Bit Torrent eta abar).
- TOR sarea eta sare alternatiboak (I2P, Freenet eta abar).
- *Underground* kanalak eta foroak.
- URLak laburtzeko zerbitzuak (Tiny URLak), malware- eta spam-zerrendak, domeinu-erregistratzaileak eta abar.

- *Online pastea*k (Pastebin eta antzekoak), IRCak, *Botneta*k, *Carding Market*ak eta abar.
- Aurreko bilaketa-eremuetan bildutako dokumentuetako metadatuak.

Zerbitzuak honako hauek emango ditu:

- Etengabe, alerta goiztiarrak gorabehera edo kalteberatasun guztietarako, baita zero egunekoak ere, BBUPen segurtasuna arriskuan jar dezaketenak.
- Aldian behin:
  - Inteligentziako analistak egindako hileroko txostena, denbora-tarte horretan sortutako alerta esanguratsu guztien xehetasunekin.
  - Lau hilean behingo goi-mailako txostena, denbora-tarte horretako aurkikuntza garrantzitsuenak zehazten dituena eta sektorearen testuinguru globalaren ikuspegia ematen duena (antzeko beste erakunde batzuei dagokienez, jarduerari, tamainari, kokapen geografikoari eta beste ezaugarri esanguratsu batzuei dagokienez).
- Eskatuz gero, gorabehera jakin bati buruzko xehetasun txostena, beharrezkoa bada.

### 4.1.2 Segurtasuna monitorizatzea

Adjudikaziodunak etengabe gainbegiratuko du BBUPen azpiegitura teknologikoaren egoera, eta dagozkion alertak sortuko ditu konpainiaren segurtasunari eragin diezaioketen gertaeretan. Honako hauek dira egin beharreko lan nagusiak:

- Segurtasun-gertaeren monitorizazio eta gainbegiratze proaktiboa, segurtasun-gertaeren korrelatzaile baten bidez (SIEM). Adjudikaziodunak zerbitzuaren parte gisa eman beharko du tresna hori.
- Gertaerak monitorizatzea eta modu proaktiboan gainbegiratzea, zerbitzuaren eskura jartzen diren eta SIEMen sartuta ez dauden BBUPen segurtasun-tresnen gainean zuzenean.
- Denbora errealean bildutako gertaeren prozesamendua eta korrelazioa, eraso baten adierazle izan daitezkeen gertaera garrantzitsuak aldez aurretik detektatzeko, bai eta positibo faltsuak ezeztatzeko analisi eta egiaztapena ere.
- Betetze-mailaren eta jardunaren adierazleak prestatzea.

#### *4.1.2.1 Informazioaren segurtasuneko gertaerak korrelazioan jartzeko plataforma.*

Adjudikaziodunak plataforma bat eskaini behar du BBUPen informazio- eta telekomunikazio-sistemak osatzen dituzten hardware- edo software-osagaiek sortutako segurtasun-alertak denbora errealean jasotzeko eta aztertzeko. Plataforma hori SaaS modalitatean eskainiko da (softwarea zerbitzu gisa), eta BBUPek ez du hardwarerik edo lizentziarik erosiko. Zerbitzuak barne hartuko ditu bere azpiegituran ostatatutako zerbitzua emateko beharrezkoak diren hardware eta software guztien hornidura, haren aldizkako eguneratzeak, administrazioa eta 24x7 modalitateko azpiegituraren eragiketa, agiri honetan zehaztutakoaren arabera. BBUPeko

segurtasun-langileek plataforma funtzionalki erabili ahal izango dute (gertaerak bilatzeko eta korrelazioan jartzeko sekuentziak sortzea, aginte-koadroak egitea, alertak konfiguratzea eta sortzea eta abar).

Plataforma hori SEZek hornitu, instalatu, konfiguratu, optimizatu, operatu eta kudeatuko du. Segurtasun-informazioa eta -gertaerak dituzten erregistroak eta *log*ak bildu eta zentralizatuko ditu, eta gertaera horiek normalizatu, kategorizatu, gehitu, korrelazioan jarri eta biltegiratuko ditu, hasierako atxikipen-aldian 365 egunez, segurtasun-gorabeherak detektatuz eta alertak sortuz. Erabakiak modu proaktiboan hartzeko tresna bat izango du, eta web-kontsola irisgarri bakarra eskainiko du, BBUPek kontsultak egin eta txostenak eta aginte-koadroak sor ditzan definitutako arrisku-politika eta -metriketatik abiatuta.

Zerbitzu horren ustiapenak aukera eman behar du segurtasun-alertak detektatzeko eta horiek konpontzeko eta dokumentatzeko behar den ahaleginaren artean oreka mantentzeko.

Oro har, hauxe egin beharko da laborategian:

- Gertaeren analisia ia denbora errealean ematea.
- Hainbat iturri eta sistematatik datorren informazio konplexua korrelazioan jartzea eta aztertzea (ingurune heterogeneoak, hala nola sare-aktiboak, segurtasun-gailuak, sistema eragileak, aplikazioak, datu-baseak eta sarbideak eta identitateak kudeatzeko produktuak).
- Jardueren oinarrizko lerro bat sortzeko eta anomaliak detektatzeko aukera ematea, aplikazioei, ostalariei, erabiltzaileei eta abarri lotutako portaera-aldaketak identifikatzeko.
- Hautemandako anomalietan eta sare-fluxuen portaeran eta segurtasun-gertaeretan izandako aldaketetan oinarritutako alertak sortzea, eta BBUPek definitutako anomaliak gehitu ahal izatea.
- Alertak ematea ezarritako politiken arabera (adibidez, baimendu gabeko berehalako mezularitzako trafikoa, baimendu gabeko hodeiko biltegiratzea, baimendu gabeko protokoloen erabilera eta abar) eta arriskutsuak izan daitezkeen aplikazioen arabera (file sharing, P2P eta abar).
- Alertak konfiguratu eta transmititzea, hainbat mekanismoren bidez, ticketingeko beste soluzio batzuetarako eta hirugarrenen tresnetarako.
- Hirugarrenen segurtasun-tresnekin sinergiak ezartzea (inteligentziako *feed*ak, Cyber Threat Intelligence plataformak eta abar).
- Integratutako kalteberatasunak edo hirugarrenenak eskaneatzeko tresnek emandako emaitzak korrelazioan jartzea.
- Gainbegiratutako iturri edo gailu baten erregistro-bilketa eteten denean alerta ematea eta monitorizatzea.
- Sareko aktiboak automatikoki aurkitzea eta sailkatzea, hainbat eskaneatze-teknikaren bidez (*ping*a, ataken eta sistema eragileen *fingerprinting*a eta abar) eta kanpoko aktiboen biltegiei kontsulta egiteko tekniken bidez (direktorio aktiboa, LDAP, CMDB eta abar).

- Erabiltzaileak aktibo bakoitzaren arabera autentifikatzeko jardueraren historiko bati eustea eta hura mantentzea, auditoria- eta trazabilitate-txostenak sortzeko.

- Denboran gehitutako balioak korrelazioan jartzea ahalbidetzea (adibidez, alerta bat bidaltzea jatorrizko IP batek konfiguratutako datu-bolumen bat baino gehiago bidaltzen duenean konfiguratutako denbora-leiho batetik helburuko IP batean argitaratutako zerbitzu bakar batera).
- Trafiko-profilei buruzko informazioa ematea, byte-kopurua, paketeen maiztasuna, aplikazio bakoitzeko komunikazio-aktiboen kopurua, atakak, protokoloak, mehatxuak edo sareko beste monitorizazio-puntu batzuk kontuan hartuta.
- Modulu edo tresna aurreratuak izatea (ikaste automatikoa, *big data*ren analisiak, adimen artifiziala eta beste batzuk) «0-day» motako mehatxuekin, mehatxu ezezagunekin, mehatxu iraunkor aurreratuekin, albo-mugimenduekin, *endpoint*aren konpromisoarekin, informazioa kanporatzearekin, jarduera susmagarriarekin, oro har, eta abarrekin zerikusia duten gertaerak detektatzeko.
- Aztertutako portaera-ereduetatik (gertaerak zein sare-jarduera) dinamikoki autoikastea eta segurtasun-gorabehera bat ekar lezakeen ezohiko jardueraz ohartaraztea.
- DoS (*Denial of Service*) eta DDoS (*Distribute Denial of Service*) motako erasoak detektatzeko gai izatea.
- Sarean behatutako mehatxu jakin batekin lotutako trafikoa detektatzeko eta erakusteko gai izatea.
- Sarearen diseinu logikoari lotutako trafiko-profilen sorrerari eustea, bai IP helbide indibidualari dagokionez, bai sare-mailari dagokionez (adibidez, azpisarea/CIDR).
- Eskualde geografikoetan eta denbora errealean Internetetik datozen edo Internetera zuzentzen diren komunikazioak profilatzeko gai izatea.
- Tokiko trafikotik eta Interneteko jatorria eta helburua duen trafikotik argi eta garbi bereizitako profil independenteak sortzea ahalbidetzea.
- IP helbideetan, IP helbide-multzoetan, jatorri/helmuga IP helbide-bikoteetan eta abarretan oinarritutako trafiko-profilen sorrera onartzea.
- Biltegiratutako segurtasun-gertaeren eta sare-fluxuen xehetasunetara sartzeko aukera ematea, gutxienez hamabi hilabetez.

SIEM soluzioak zerbitzua bermearekin emateko beharrezkoak diren elementu eta modulu guztiak barne hartuko ditu.

SEZ arduratuko da segurtasuna monitorizatzeko zerbitzua ematen duen plataformaren heldutasuna hobetzeko etengabeko azterketaz eta aholkularitzaz, eta, horretarako, etengabeko hobekuntzako ziklo bat proposatuko du, iturri berriak sartzeko eta hauek garatzeko: erabilera-kasuak, korrelazio- eta detekzio-arauak, objektu estandarrak eta *ad hoc* objektuak, iragazkiak,

txosten estandarrak eta *custom*-txostenak, alertak, zerrendak, ezagutzari buruzko datu-baseko elementuak (gorabeherak eta egindako jarduerak barne) garatzeko, zerbitzu hori ematen duen plataforma ahalik eta gehien aprobetxatu ahal izateko.

*Log*ak, konfiguratu ondoren, eskuragarri egongo dira auzitegiko kontsultak eta analisiak egiteko, gorabeherak arin ikertzeko, mehatxu iraunkor aurreratuen adierazleak bilatzeko eta betetze-mailaren ikuskaritzek detektatutako ahuleziak gainditzen laguntzeko.
Datu historikoetarako sarbidea eta ekitaldi bakoitzaren xehetasunak ikusteko aukera konbinatuko dira.

Plataformak aukera emango du BBUPek monitorizazioa egiteko erabiltzea erabakitzen dituen informazio-iturriak sartzeko; hala, erraza eta gardena izango da denborak aurrera egin ahala azpiegituran gerta daitezkeen aldaketen ondorioz iturri berriak sartzea. Informazio-iturriak edozein unetan sar daitezke zerbitzua ematen den bitartean, kontuan hartuta BBUPen azpiegitura etengabe ari dela eboluzionatzen eta garatzen. Adjudikaziodunaren teknikariak arduratuko dira BBUPek eskatzen dituen informazio-iturri berriak sartzeaz, eta, horretarako, BBUPeko teknikariekin koordinatuta lan egingo dute. Plataformak bateragarria izan behar du hainbat motatako gailu eta produktuekin eta fabrikatzaileekin, eta gutxienez 1.500 EPS (40 GB/egun) jasan behar ditu.

### 4.1.3 Segurtasun-gorabeheren kudeaketa

Monitorizazio-zerbitzuaren bidez gorabehera bat detektatzen denean, edo ezarritako kanalen baten bidez jakinarazten zaionean, SEZek gorabeheraren kudeaketa osoa egingo du, eta, gutxienez, jarduera hauek egingo ditu:

- Monitorizazio-zerbitzuaren bidez detektatzen diren segurtasun-gorabeherak erregistratzea, sailkatzea, baloratzea, lehenestea eta mailakatzea, Segurtasuneko edo BBUPeko IKTetako langileek jakinarazten badituzte edo zibersegurtasun-gorabeherei erantzuteko Estatuko, eskualdeko edo tokiko erakundeek (CERTSIS) jakinarazten badituzte.
- Segurtasun-gertaerei dagozkien alertak ematea, bai barnekoen kasuan, bai hirugarrenen kasuan (Estatuko agintariak eta/edo beste erakunde batzuk).
- Segurtasun-gorabeherak jakinaraztea eta dokumentatzea, Zibergorabeherak jakinarazteko eta kudeatzeko Estatuko gidaren eta BBUPen ezarritako protokoloen arabera.
- Segurtasun-gorabeherei eusteko neurriak hartzea, edo jarraibide zehatzak ematea BBUPeko IKT arloko langileek aplika ditzaten, ezarritako protokoloen arabera, eta haien eraginkortasuna egiaztatzea.
- Segurtasun-gorabeherak ikertzea, sartzeko baimena duen BBUPen azpiegitura teknologikoari buruzko ebidentziak aurkituz eta bilduz, edo ebidentziak biltzeko eskatuz Informazioaren Segurtasuneko Bulego Teknikoari (hemendik aurrera, ISBT) eta BBUPeko IKT taldeari, eta, gero, haiek aztertuz.

- Kode gaiztoaren analisia egitea.
- Ikerketa forentsea.
- Gorabehera ixteko txostena eta gorabeheraren osteko txostena egitea, ikasitako lezioak eta ekintza-planen proposamenak barne, etorkizunean antzeko gorabeherak berriro gerta ez daitezen edo gorabeherei erantzuteko eta haiek kudeatzeko mekanismoak hobetzeko.
- Zerbitzuari buruzko aldizkako txostenak egitea eta definitutako metrikak eta adierazleak eguneratzea.

Adjudikaziodunak beharrezko tresnak eta gaitasunak izan beharko ditu malwarea analizatzeko, auzitegiko ikerketak egiteko eta ebidentzia digitalak biltzeko zerbitzuak emateko, hala nola:

- *Sandbox*ak eta emaitzak korrelazioan jartzeko tresnak, kode gaiztoko laginen analisi automatizaturako.
- Kode gaiztoaren alderantzizko ingeniaritzarako ingurunea, analisi estatikoa eta dinamikoa egiteko, eta Konpromiso Adierazleak (IOC - Indicator of Compromise) sortzeko, sarea detektatzeko sinadura gisa edo ostalarian erabiltzeko adierazle gisa.
- Diskoen analisi forentsea egiteko tresnak (ezabatutako fitxategiak berreskuratzea, datu-indexatzailea)
- Ebidentziak eskuratzeko *in situ* esku-hartzeak egiteko materiala (auzitegiko materiala eskuratzeko materiala, disko-klonagailuak, ebidentziak modu seguruan manipulatzeko *writeblocker*-gailuak, auzitegiko erosketa-prozesuaren erregistro dokumentala egiteko GPS lokalizazioa duten argazki-kamerak eta abar).

Gorabeheraren bizi-zikloa BBUPen ezarritako prozeduren arabera kudeatuko da. Adjudikaziodunak proposatuko ditu lortutako ebidentziak peritatzeko, biltzeko, biltegiratzeko eta zaintzeko prozesua berme osoz hornitzeko mekanismoak eta protokoloak, behar izanez gero, esparru legal eta juridikoan aurkeztu, onartu eta balio osoa izan dezaten.

Horrez gain, adjudikaziodunak eguneratuta eta frogatuta eduki behar ditu gorabeherei erantzuteko prozedurak, honako zeregin hauen bidez:

- Segurtasun-gorabeherak kudeatzeko definitutako prozedurak, eskuliburuak eta tresnak aldizka berrikustea.
- Erakundean urteko ziberekitaldi bat prestatzea eta gauzatzea.
- BBUPek parte hartzea erabakitzen duen ziberariketa publiko edo pribatuetan parte hartzeko laguntza.

Segurtasun Gorabeherak Kudeatzeko Zerbitzuari erantzuteko, adjudikaziodunak honako hauek izan beharko ditu, gutxienez:

- 24x7 Harremanetarako Puntu Bakarra (Service Desk); gorabeherei, kontsultei, eskaerei eta jakinarazpenen kudeaketari erantzuteko. Adjudikaziodunak komunikazio-bide segurua (zifratua, erredundantea) emango du.
- Lehen esku-hartzeko taldea: gorabeherak detektatzeko, identifikatzeko eta baloratzeko, bai eta soluziorako proposamenak, euste-neurriak eta/edo beharrezkotzat jotzen diren konpentsazio-neurriak dokumentu bidez emateko ere.
- Zerbitzuaren kudeatzailea; zerbitzua ikuskatzeaz eta jarraitzeaz, txostenak aurkezteaz eta emaitzez arduratzen dena.

### 4.1.4 Segurtasun-auditorien eta kalteberatasunen analisien zerbitzua

Zerbitzu honen helburua da BBUPen informazio-sare eta -sistemetan kanpoko eta barneko erasoen aurrean dauden kalteberatasunak edo segurtasun-akatsak identifikatzea, informazio-sistemak (IT) eta sistema industrialak (OT) kontuan hartuta.

Segurtasun-ikuskapenak eta kalteberatasunen azterketak egiteko, nazioartean onartutako lan-metodologiak erabiliko dira erreferentzia gisa (hala nola OSSTMM, OWAS, WASC eta abar). Detektatutako eta egiaztatutako kalteberatasunen balorazio objektiboa egiteko, CVSS (Common Vulnerability Scoring System) metodologia erabiliko da.

Hurrengo ataletan, eskatutako zerbitzuen gutxieneko irismena deskribatzen da.

#### *4.1.4.1 Segurtasun perimetralaren ikuskapena*

Zerbitzu honek hilean behin auditoria perimetrala egitea aurreikusten du, eta gutxieneko irismen hau izango du:

- Informazio publikoa biltzea hainbat iturritatik (ziberinteligentziako zerbitzuak egindako jarduera, dagokion atalean zehazten denaren arabera).
- Erakundeak Internetera begira dituen eta zibereraso bat jasan dezaketen aktibo eta baliabide guztien zerrenda (IP tarteak, ekipamendua, zerbitzu aktiboak, ataka irekiak, DNS, posta-zerbitzariak eta abar).
- Aktibo horien kalteberatasunak, konfigurazio-akatsak eta segurtasun-akatsak detektatzea eta identifikatzea, tresna automatizatuak erabiliz, eta eskuz egiaztatzea positibo faltsuak baztertzeko.
- Txosten tekniko batean, aurkitutako kalteberatasun guztiak zehaztea: kalteberatasunaren identifikazioa eta deskribapena, kaltetutako aktiboak, arrisku-maila, CVSSren balorazioa (baldin badago), ebidentziak, erreferentzia dokumentalak, arintze-planak eta gomendioak.
- Txosten exekutiboa egitea.

Zerbitzua 40 (azpi)domeinu desberdinetarako aurreikusita dago.

#### *4.1.4.2 Barne-auditoria*

##### 4.1.4.2.1 Kalteberatasunen analisia

Zerbitzua ematen den bitartean, adjudikaziodunak tresna bat izango du BBUPen barne-sarean kalteberatasunak automatikoki identifikatzeko. Tresna hori merkatuan dauden tresnetako bat izan daiteke (Nessus, Qualys eta abar), edo Open Source (OpenVAS eta abar). Adjudikaziodunak jarri behar ditu tresna eta ekipoa. Kontratua indarrean dagoen bitartean, BBUPen instalazioetan koka daiteke tresna. Horretarako, adjudikaziodunak beharrezkoak diren instalazio-lanak egin behar ditu, BBUPeko teknikariekin koordinatuta, edo, bestela, adjudikaziodunaren instalazioetan egon behar du. Kasu horretan, BBUPek emandako linea dedikatu baten bidez egin behar da lana. Nolanahi ere, BBUPeko Segurtasun Logikoaren arloko teknikariek tresna administratzeko kontsolarako sarbidea izango dute, eta, behar izanez gero, kontsola erabiltzeko aukera izango dute.

Probak BBUPeko teknikariekin koordinatuta egingo dira beti, eta kontrol zorrotza egingo da, zerbitzua degradatzea eragin dezaketen egoerak saihesteko.

Tresnaren mantentze- eta eguneratze-lan guztiak adjudikaziodunaren teknikariek egingo dituzte.

Kalteberatasunen azterketa bakoitzaren emaitza gisa, adjudikaziodunak hauek egin behar ditu:

- Aurkitutako kalteberatasun guztiak zehaztuko dituen txosten tekniko bat: kalteberatasunaren identifikazioa eta deskribapena, eragindako aktiboak, arrisku-maila, CVSS balorazioa (halakorik badago), ebidentziak, erreferentzia dokumentalak, arintze-planak eta gomendioak zehaztuta.
- Aurkikuntza nagusien laburpena goi-mailan jasotzen duen txosten exekutiboa.

Kalteberatasunen azterketa osoa egin behar da (ingurune korporatiboa eta industriala), gutxienez, hiru hilean behin. Horretarako, adjudikaziodunak programazio bat egingo du, eta BBUPeko proiektu-arduradunak onartu egin beharko du.

##### 4.1.4.2.1 Segurtasun-testa (*hacking* etikoa)

Urtero, zerbitzua ematen den bitartean, adjudikaziodunak segurtasuneko barne-test bat (*hacking* etikoa) egingo du. Zerbitzuaren hasieran, lehenengo segurtasun-testa egingo da. Test horren bidez, erakundearen egoeraren ikuspegi orokorra lortuko da, eta erreferentzia gisa erabiliko da kontratua egiten den bitartean egiten diren segurtasun-jardueren eraginkortasuna

baloratzeko. Segurtasun-testek barnean hartuko dituzte informazioaren eta komunikazioaren teknologien arloko ekipamenduak, sistemak eta sareak,
bai eta komunikazioak (telekomunikazio-sistema eta -sare korporatiboak) eta eragiketa-teknologiak (SCADA sare eta sistemak eta prozesu industrialen kontrol-sistemak) ere. Horretarako, bi alorretan behar bezala gaitutako langileak izan behar ditu adjudikaziodunak.

*Hacking* etikoko probak hauek izango dira:

- «Kutxa beltz» motako testak. Auditoria-taldeak ez du helburuei buruzko informaziorik izango, baina kalteberatasunak aztertuz lortutako informazioa erabili ahal izango du, informazio hori erasotzaile izan daitekeen norbaiten eskuetan egon daitekeela jotzen baita. Analisi automatizatuak egingo dira, eskaner espezifikoekin eta eskuzko berrikuspenekin osatuta, aurkikuntzetan sakontzeko eta positibo faltsuak baztertzeko.

- «Kutxa zuri» motako testak; BBUPek emandako informaziotik abiatuta, auditore-taldeak konpainiaren informazio-sareen eta -sistemen arkitektura aztertuko du, izan daitezkeen ahuleziak edo segurtasun-akatsak detektatzeko.

- Ingeniaritza sozialeko probak; tipologia desberdinekoak egingo dira, gutxienez ere honako hauek:

  - Mezu elektronikoak bidaltzea asmo txarreko erasoak simulatuz (Phishing); sinesgarritasun-maila desberdinekin (igorlearen domeinua ordeztuz eta ordeztu gabe, gaztelaniaz edo beste hizkuntza batean eta abar).
  - Telefono deiak egitea, BBUPi (Vishing) buruzko informazio garrantzitsua lortzeko. Dei horiek bertako langileei, enpresa hornitzaileetako langileei edo BBUPeko hirugarren kolaboratzaileei zuzenduta egon daitezke.
  - BBUPen bulegoetara fisikoki sartzen saiatzea, engainu-teknikak erabiliz.

  Proba horiek BBUPek proiektuaren arduradunarekin adostu behar ditu aldez aurretik, langile, hornitzaile eta antzeko pertsona fisikoei eragiten baitiete zuzenean.

Sistemen kalteberatasuna ez izan arren BBUPen segurtasun-araudia betetzen ez duten kalteberatasunak ere identifikatuko dira.

*Hacking* etikoaren testen emaitza gisa, adjudikaziodunak hau egingo du:

- Txosten tekniko bat, aurkitutako segurtasun-akats guztien xehetasunekin, eta honako hauek zehaztuta: identifikazioa, deskribapena, eragindako aktiboak, arrisku-maila, ebidentziak, dokumentu-erreferentziak, arintze-planak eta gomendioak.

- Aurkikuntza nagusien laburpena goi-mailan jasotzen duen txosten exekutiboa.

#### *4.1.4.3 Kode-auditoria*

Adjudikaziodunak bere irismenean sartuko du BBUPek eskatzen dituen aplikazioei buruzko kode-ikuskapenen zerbitzua. Ikuskatu beharreko aplikazioak BBUPek eta adjudikaziodunak horretarako egingo dituzten bilera espezifikoetan zehaztuko dira. Zerbitzu horrek, gutxienez, honako hauek hartuko ditu barne kontratuak irauten duen bitartean:

- Web-zerbitzu oso baten auditoria
- Gailu mugikorretarako aplikazio baten auditoria (Android eta iOS, lotutako web-zerbitzuak barne, baldin badaude).

Auditoriek nazioartean onartutako estandar hauek izango dituzte oinarri: CWE (Common Weakness Enumeration), Open Web Application Security Project (OWASP), Open Source Security Testing Methodology Manual (OSSTMM) eta abar.

Kode-auditoriak honako hauek jasoko ditu:

- Dokumentazioaren hasierako azterketa eta berrikuspena: aplikazio bakoitza eta bere erabilerak eta bertan dauden informazio-fluxuak ezagutzeko eta aztertzeko helburuarekin.
- Analisi estatikoa: adjudikaziodunak zerbitzua emateko emandako tresna automatizatuen bidez, iturburu-kodea egiaztatuko da, ohiko kalteberatasunak identifikatzen dituzten ereduak bilatzeko: Cross-Site Scripting (XSS), SQL injekzioak, tokiko edo urruneko inklusioak, komandoak exekutatzea, informazio-ihesak eta abar.
- Iturburu-kodearen eskuzko berrikuspena: analisi estatikoaren osagarri gisa, positibo faltsuak ezabatzeko edo tresna automatizatuen irismenetik kanpo egon daitezkeen kalteberatasunak edo arazoak detektatzeko.
- Analisi dinamikoa: arreta berezia jarriz aplikazioaren sarrera-puntu posibleetan, irteeren emaitzen sorkuntzan, erroreen manipulazioan eta abarrean.
- Emaitzen txostena.

## 4.2 Baliabide teknikoak eta giza baliabideak.

Zibersegurtasuneko Eragiketa Zentroaren lana gauzatzeko ardura duten profesionalek (talde nagusia) osatuko dute Segurtasuneko Talde Teknikoa. Diziplina anitzeko talde bat behar da, prestakuntza eta esperientzia dituena segurtasun teknikoan, antolakuntzako segurtasunean eta

lege-segurtasunean. Lanen izaerari egokitutako kualifikazioa, ezagutza eta esperientzia izan beharko dituzte, atal honetan eskatzen den moduan.

Dokumentu honetan deskribatutako zerbitzuak emateko behar diren baliabideak egokiak izango dira definitutako lanak bermearekin egiteko, jarraian zehazten diren irizpideak kontuan hartuta.

### 4.2.1 Proiektuburua

- Informazioaren Teknologien, Konputazioaren, Telekomunikazioen edo Industriaren arloko goi-mailako unibertsitate-titulua.
- Gutxienez sei urteko esperientzia izan behar du gai hauei buruzko proiektuak kudeatzen eta koordinatzen: informazio-sistemen segurtasuna, segurtasuneko plan zuzentzaileak, segurtasuneko bulego teknikoak, zibergorabeherei erantzuteko lantaldeak, informazioaren segurtasuneko plan estrategikoak, negozio-jarraitutasuneko planak eta abar.
- Azken bost (5) urteetan kontratu honetakoen antzekoak edo berdinak diren bi (2) proiektu zuzendu behar izan ditu gutxienez.
- Proiektuak kudeatzeko metodologiak (PMI edo beste batzuk) ezagutzen dituela egiaztatu beharko du, prestakuntza-ziurtagirien bidez.
- III. eranskinean («Segurtasun-ziurtagiriak») jasotako bi (2) segurtasun-ziurtagiri, gutxienez, izan behar ditu.

### 4.2.2 Zibersegurtasuneko Eragiketa Zentroari (SEZ) atxikitako langileak

#### *4.2.2.1 SEZeko arduraduna*

- Informazioaren Teknologien, Konputazioaren, Telekomunikazioen edo Industriaren alorreko erdi- edo goi-mailako unibertsitate-titulua izatea.

- Gutxienez bost urteko esperientzia izango du arlo hauetan:

  - Gorabehera informatikoen aurrean erantzuteko ekipoak kudeatzea (SEZ, CERTSI)
  - Segurtasun-tresnak (NGF, WAF, SIEM, MDM, *antimalware*a, *antispam*a eta abar) diseinatzea, administratzea eta erabiltzea.
  - Alerta goiztiarreko sistemak eta tresnak kudeatzea eta erabiltzea.
  - Zibergorabeherak kudeatzea.
  - Eragiketetako, txostenetako eta bezeroarentzako laguntzako tiketen jarraipena eta kontrola.

Gainera, gai hauei buruzko ezagutza orokorra izan behar du:

- Segurtasun-auditoria teknikoak egitea.
- Kalteberatasunen analisia eta kudeaketa
- Windows eta Linux sistema eragileak administratzea eta gotortzea.
- Komunikazio-sareak eta -hardwarea segurtasunez diseinatzea eta administratzea.
- Web-atariak programatzea, administratzea eta gotortzea.
- Malwarea eta iruzur elektronikoa aztertzea.
- Analisi forentsea.
- Segurtasuna gailu mugikorretan (Android eta iOS).

#### *4.2.2.2 SEZeko teknikariak*

SEZ osatzen duten teknikarien kasuan, gutxienez urtebeteko esperientzia egiaztatu beharko da arlo hauetan:

- Gorabehera informatikoen aurrean erantzuteko taldeetako kide izatea (SEZ, CERTSI)

- Segurtasun-tresnak (NGF, WAF, SIEM, MDM, *antimalware*a, *antispam*a eta abar) diseinatzea, administratzea eta erabiltzea.
- Alerta goiztiarreko sistemak eta tresnak kudeatzea eta erabiltzea.
- Zibergorabeherak kudeatzea.

Enpresa lizitatzaileek urrunetik eta aurrez aurre laguntza emateko (gorabehera larriren bat izanez gero) proposatutako lantaldea garatuko dute beren eskaintzetan, langileen lan-baldintza egokiak bermatuta (txandakatzeak, oporrak, atsedenaldiak, bajak eta abar).

#### *4.2.2.3 Segurtasuneko talde teknikoa*

Kontratu honen esparruan egin beharreko gainerako lanetarako (*hacking* etikoa, analisi forentsea, ebidentziak biltzea eta zibergorabeherei *in situ* arreta ematea eta abar), adjudikaziodunak proposatutako langileak SEZeko teknikarien taldeko kide izan daitezke, edo ez. Nolanahi ere, langile horiek honako hauek izan behar dituzte:

- Informazioaren Teknologien, Konputazioaren, Telekomunikazioen edo Industriaren alorreko erdi- edo goi-mailako unibertsitate-titulua izatea.

- Gutxienez, bi urteko esperientzia izan behar dute honako hauetan:

  - Segurtasun-auditoria teknikoak egitea.
  - Kalteberatasunen analisia eta kudeaketa
  - Windows eta Linux sistema eragileak administratzea eta gotortzea.

- Komunikazio-sareak eta -hardwarea segurtasunez diseinatzea eta administratzea.
- Web-atariak programatzea, administratzea eta gotortzea.
- Malwarea eta iruzur elektronikoa aztertzea.
- Analisi forentsea.
- Segurtasuna gailu mugikorretan (Android eta iOS).
- Softwarea segurtasunez garatzea.

Zehazki, segurtasun-testak (*hacking* etikoa) egiteko proposatutako profiletako batek gutxienez bi urteko esperientzia egiaztatua izan behar du OT inguruneetan (eragiketa-teknologiak) segurtasun-ikuskapen teknikoak egiten.

### 4.2.3 Azken gogoetak.

**Profil profesional bakoitzaren deskribapenean adierazitako eskakizunak gutxieneko errekerimendutzat hartzen dira, eta, beraz, baztertu egingo dira haiek egiaztatzen ez dituzten eskaintzak. Funtsezko kontratu-betebeharra izango da profil profesional horiek kontratura atxikitzea kontratuaren iraupen osoan; beraz, betebehar hori ez betetzeak kontratua aldez aurretik suntsiaraztea ekar dezake.**

Enpresa lizitatzaileek proiektuari atxikitako teknikarien izenak haien profiletan bakarrik zehaztu beharko dituzte, eta ez dute profil desberdinekoak ez diren beste teknikaririk sartuko. Adjudikaziodun izanez gero, kontratua formalizatu ondoren lanak egiteko sartuko den pertsona-taldeak eskaintza adjudikaziodunean zerrendatutako osagaiekin osatuta egon beharko du. Betebehar hori arrazoi justifikaturik gabe betetzen ez bada, kontratua suntsiarazi ahal izango da, eta fidantza galdu.

I. eranskinean, proiektuari atxikitako langileei eta enpresa lizitatzaileari buruzko informazioa emateko erabili beharreko txantiloiak daude. Nabarmentzekoa da eskaintzan aurkeztutako profil profesionalak, beraien kualifikazioekin, lotesleak izango direla eskaintzailearentzat, eskaintzaren adjudikaziodun izanez gero. Era berean, eskatutako esperientzia eta prestakuntza egiaztatzen duten agiriak aurkeztu beharko dira, baita lizitatzailearen plantillakoa dela egiaztatzen dutenak ere, azken TC2aren kopiaren bidez. Horretan, eskaintzan proposatutako pertsonen datuak adierazi beharko dira, errazago aurkitu ahal izateko. BBUPek eskubidea du kualifikazio- eta esperientzia-eskakizun horiek betetzen direla egiaztatzeko. Eskatutako gutxienekoa egiaztatzen ez duten eskaintzak baztertu egingo dira, eta egiaztatu gabeko alderdiak ez dira kontuan hartuko. Lizitatzaileari beste proba batzuk eskatzeko eskubidea du BBUPek, aurkeztutako frogak aski ez direla uste badu. Administrazio Klausula Partikularren Agiriko 1. eranskinean adierazten da noiz aurkeztu behar den informazio hori.

Kontratua adjudikatu nahi zaion pertsonaren bat ez bada agertzen lizitatzailearen plantillan eskaintza aurkezteko unean, lizitatzaileak eta proposatutako langileak sinatutako dokumentu bat erantsi beharko da, zeinean biek konpromisoa hartuko duten eskaintza adjudikaziodun

gertatzen bada pertsona horri plantillan alta emango zaiola kontratua formalizatu aurreko baldintza gisa. Hala egin ezean, adjudikazioa ezeztatu egingo da.

Proiektuak arrakasta izan dezan, BBUPen ustez, funtsezkoa da proiektuari esleitutako lantaldean jarraitzea. Beraz, langileen kudeaketa adjudikaziodunaren ardura dela uste badu ere, komeni da langileen txandakatze-maila mugatua izatea, eta hori kontuan hartuko da langileei dagozkien zerbitzu-mailako akordioetan.

Lantaldearen osaera ezin izango da aldatu BBUPen berariazko baimenik gabe. Baimen hori emateko, proposatutako ordezkoak ordeztu nahi den taldeko kideak duen prestakuntza tekniko eta esperientzia bera edo handiagoa izan behar du. Aldaketarik egin nahi izanez gero, idatziz eskatu beharko da, gutxienez hamabost egun naturaleko aurrerapenarekin.

Lan-ingurunera eta proiektura egokitzeko egon daitezkeen arazoak, taldeko kideak ordeztearen ondoriozkoak, gainjartze-aldien bidez konpondu beharko dira, kostu gehigarririk gabe eta zerbitzuan eraginik izango ez duen trantsizioa bermatzeko behar den denboran. Adjudikaziodunak ziurtatu beharko du ordeztutako baliabidearen ezagutza lantaldearen gainerakoari transferituko zaiola.

Lanak egiteko atxikita dagoen taldeko kideren bat aldatzean ez badira aipatu prozedura eta baldintzak betetzen, BBUPek ahalmena izango du aldaketa hori planifikatu gabeko txandakatze gisa kalifikatzeko.

## 4.3 Ikuskapena eta kontrola

Uztailaren 13ko 20/2012 Errege Dekretuaren lehenengo xedapen gehigarriaren ondorioetarako, gogorarazten da BBUPen eta adjudikaziodunaren arteko merkataritza-harreman bat sortzea besterik ez dakarrela BBUPen kontrol-sistemen aplikazioen euskarri- eta mantentze-zerbitzuak kontratatzeak, eta adjudikaziodunak kontratatutako zerbitzuak independentzia eta autonomia osoz garatuko dituela haiek egiteko giza baliabideak eta baliabide materialak antolatzeari dagokionez, eta ez dela inolako lan-harremanik sortuko kontratistako langileen eta BBUPen artean.

Hori horrela izanik, BBUPek kontratatutako zerbitzuen kalitatea eta egokitasuna kontrolatzeko izendatutako ikuskatzaileak ez du ahalmenik izango kontratistako langileek egiten dituzten lanak antolatu, kontrolatu edo esleitzeko. Zerbitzuaren beharren berri ematera eta adostutako baldintzen arabera adjudikaziodunak solaskide izendatutako pertsonari egokitzera mugatuko da elkarrizketa; ez du kontratatutako zerbitzuan esku sartuko.

Proiektuaren zuzendaritza-figura eta -organo hauek ezarri dira:

- Kontratuaren ikuskatzailea (BBUPen arduraduna).
- Proiektuburua (adjudikaziodunak kontratuaren ardura izango du).

Kontratuaren gainbegiralea BBUPek izendatutako teknikari bat izango da, eta funtzio nagusi hauek izango ditu:

- Lanen gauzatzea eta garapena zuzendu, gainbegiratu eta koordinatzea, eta eraginkortasun- eta kalitate-mailaz arduratzea.
- Funtzionamendu-arauak eta dokumentu honetan ezarritako baldintzak betearaztea.
- Lanak egiteko plangintzak onartzea.
- Proiektuburuak lanak egin bitartean egindako proposamen teknikoak onartzen diren ala ez erabakitzea.
- Lanak egiteko programaren jarraipena ziurtatzea.
- Zerbitzuari eskatutako jarduerak eta lanak egiteko erabilitako metodologian edo prozeduretan edozein aldaketa egiteko baimena ematea.
- Jarduera-txostenak berrikustea eta baliozkotzea.
- Ezarritako zerbitzu-mailako akordioak betetzen direla zaintzea eta ez-betetzeen ondoriozko zigorrak aplikatzea.
- Proiektuaren gauzatzea ekonomikoki kontrolatzea eta ordainketak onartzea.

Adjudikaziodunak proiektuburu bat izendatuko du, eta hauek izango dira haren funtzio nagusiak:

- Zerbitzuak ematen dituzten langileak zuzentzea, eta horretarako behar diren aginduak eta jarraibideak ematea.
- BBUPekin zerbitzuak ematen dituzten giza baliabideekiko harreman zuzeneko funtzioak betetzea.
- BBUPen proiektuaren arduradunari proposatzea BBUPen segurtasun-sistemak optimizatzeko beharrezkotzat jotzen dituen aldaketak edo hobekuntzak.
- Lanen kalitate-maila ziurtatzea.
- Beste lantalde batzuekin hizketakide izatea eta horiek koordinatzea planifikatutako jardueretan parte hartu behar dutenean.

### 4.3.1 Informatzeko betebeharra

Kontratuaren xede diren lanak egiten diren bitartean, adjudikaziodunak BBUPek izendatutako proiektuaren gainbegiratze-teknikariari hark eskatutako informazioa eta dokumentazioa eman behar dizkio, lanak zer egoeratan egiten diren eta sor daitezkeen arazoak eta haiek konpontzeko erabilitako baliabideak erabat ezagut ditzan.

Jardueraren jarraipenari buruzko txostena aurkeztu behar da hilero. Txosten horretan, alderdi hauek jaso behar dira, besteak beste:

- Erantzundako segurtasun-gorabeheren txostena.

- Epe horretan egindako lanak eta lortutako emaitzak.
- Hurrengo aldirako planifikatutako lanak.
- Esleitutako zereginak gauzatzeari eragiten dioten gorabehera teknikoak eta lantaldearenak, baita horiek konpontzeko proposamenak edo alternatibak ere.

Halaber, adjudikaziodunaren proiektuburua behartuta dago BBUPek proiektuaren jarraipena egiteko ezartzen dituen bileretara joatera, eta adjudikaziodunari behar besteko aurrerapenarekin hitzordua jartzeko konpromisoa hartzen du.

### 4.3.2 Zerbitzua emateko mailak

BBUPeko solaskideek arretaz jokatuko dute, eta IV. eranskinean jasotako zerbitzu-mailen arabera, prozeduran ezarritako kanalen bidez jakinarazitako segurtasun-gorabeheren komunikazioei (sailkapena, lehenespena, bideratzea eta kudeaketa) erantzungo diete. Adjudikaziodunaren erantzun-denboran ez dira kontuan hartuko hirugarrenei egotz dakizkiekeenak eta egin beharreko jarduerak eragozten dituztenak. Argibide gisa, gorabehera kritikotzat hartuko dira honako hauek:

- Barne-prozeduren arabera ezarritako konpainiaren sistema kritikoei eragiten dietenak edo eragiteko arrisku handia dakartenak.
- Sistema, sail edo pertsona kopuru handi batean inpaktu esanguratsua eragiten dutenak, haien eragiketari eragiten badiote (erabiltzaile aktiboen % 10i baino gehiagori eragitea).

- Konpainiaren informazio konfidentzial edo sentikorrari eragiten diotenak, bereziki datu pertsonalak babesteko arauen mende dagoenari.
- Erakundearen barruan hedatzeko aukera handia eta kalte handiak eragitea edo zerbitzuak etetea dakartenak.
- Bezeroei informazioa emateko sistema elektronikoei eta, agian, bezeroei eragiten dietenak.
- Pertsonen segurtasun fisikoa arriskuan jar dezaketenak.

## 4.4 Azpikontratazioa

BBUPek gizartearentzako funtsezkoa den zerbitzu bat hornitzen duenez, kritikotzat jotzen dira SEZek egin behar dituen zeregin guztiak, erabiltzen den informazioaren sentikortasunagatik eta SEZko eta BBUPeko teknikarien arteko zuzeneko interakzioagatik. Koordinazio egokia, arina eta eraginkorra lortzea da helburua, hauteman daitezkeen segurtasun informatikoko akatsen edo zibergorabeheren kudeaketan eta konponketan, eta, beraz, debekatuta dago azpikontratatzea.

## 4.5 Proiektuaren faseak

Proiektua kontratuaren denbora-esparruan garatzeko plangintza bat egin beharko da. Enpresa eskaintzaileek proiektu-plan bat proposatuko dute, maila handiko faseetan egituratua, eta eman beharreko zerbitzuen gutxieneko multzoa izango du. Hona hemen bakoitzaren gutxieneko irismena osatuko duten faseak eta zerbitzuak:

### 4.5.1 Ezarpen-fasea

Fase horretan, adjudikazioduna zerbitzuak bere gain hartzen hasiko da: lantaldeak integratuko ditu; azpiegituren, ingurune teknikoen, lan-prozeduren, tresnen eta BBUPen estandarren berri izango du; eta ezagutza transferitzeko eta zerbitzua behar bezala emateko behar diren jarduerak eta dokumentazioa prestatuko ditu.

Fase honetan sartzen dira gertaerak monitorizatzeko sistema (hardwarea, softwarea eta komunikazioak) ezartzeko lanak, BBUPeko teknikariekin koordinatuta, bai eta hasierako auditoria perimetraleko eta barne-auditoriako zerbitzuak (*hacking* etikoa) eta kalteberatasunen analisia ere, zerbitzuaren hasierako egoerarekin oinarrizko lerro bat ezartzea ahalbidetuko dutenak.

Fase honek gehienez bost hilabete iraungo du, kontratua erabat martxan jartzeko.

### 4.5.2 Zerbitzu osoko fasea

Ezarpen-fasearen ondoren, adjudikaziodunak zerbitzu osoa eman beharko du, agiri honetan eta kontratuan ezarritako baldintzak betez.

### 4.5.3 Zerbitzuak itzultzeko fasea

Fase hori zerbitzua amaitzea erabakitzen denean egin beharko da, dela kontraturako ezarritako hasierako epea bete delako, dela, kontratua ez betetzea oinarri hartuta, alderdietako batek kontratua suntsiarazi duelako.

Fase honetan, adjudikaziodunak baliabideak konprometituko ditu, eta zerbitzua BBUPi edo hark izendatzen duenari itzultzeko behar diren jarduerak egin, ardura eta lankidetza osoz. Jarduera horien artean, proiektuan egin den eta BBUPek bere esku ez duen dokumentazio guztia (prozedurak, txostenak eta abar) itzultzea dago, bai eta ekitaldien monitorizazio- eta korrelazio-plataformarekin lotutako informazio guztia ere, bereziki, urtebetez erregistratutako korrelazio-arauak eta gertaerak, formatu estandarrean, beste plataforma batean berrerabili ahal izateko.

Itzultzeko fasea zerbitzua amaitzeko aurreikusitako data baino gutxienez hiru hilabete lehenago hasi beharko da, dela osorik, kontraturako ezarritako hasierako epea edo haren luzapenen epea bete delako, dela zati batean, kontratua suntsiarazi delako. Zerbitzuak itzultzeaz gain, itzultzeko fasean horiek gauzatzea adjudikaziodunaren ardura izango da, ondorio guztietarako.

## 4.6 Lan-metodologia

Informazioaren segurtasuneko eta IKTetako zerbitzuen kudeaketa etengabeko hobekuntza bermatzen duen prozesu-eredu batera bideratzen ari da BBUP. Hori lortzeko, agiri honetan eskatutakotik eratorritako jarduera guztiak ISO 27001 arauan eta ITILen jasotako jardunbide egokien multzoan eskainitako ikuspegitik landu beharko dira.

Kontratua indarrean dagoen bitartean, adjudikaziodunak BBUPek onartutako prozedurak, prozesuak eta metodologiak errespetatu beharko ditu, edozein formatan.

## 4.7 Beste baldintza batzuk

### 4.7.1 Zerbitzua emateko lekua

Proiektuan aurreikusitako aurrez aurreko lanak BBUPen bulego nagusietan egingo dira, helbide honetan:

BBUPen bulego nagusiak
San Bizente kalea, 8, Albia eraikina, 1. solairua
48001 Bilbo

Ez da baztertzen bilera edo elkarrizketa puntualen bat egitea konpainiaren beste egoitza batzuetan edo hirugarrenen instalazioetan, informazio osagarriren bat lortzeko edo *hacking* etikoaren zerbitzuetan aurreikusitako ingeniaritza sozialeko jardueraren bat egiteko.

Lan ez-presentziala, SEZ zerbitzuari dagokiona, adjudikaziodunaren bulegoetan egingo da, beren ezaugarriengatik BBUPen instalazioetan osorik edo partzialki garatu behar diren zerbitzuak izan ezik (adibidez, segimendu-bilerak, *hacking* etikoko probak edo bereziki larriak diren gorabeherak konpontzea).

BBUPeko arduradunaren eta adjudikaziodunaren proiektuburuaren arteko segimendu-bilerak BBUPen egoitzan edo adjudikaziodunaren egoitzan egin daitezke, BBUPeko proiektu-arduradunak beharrezkotzat jotzen duenaren arabera eta lizitatzailearen eskaintzan jasota egon behar da.

Segurtasun-gorabehera larri bati aurre egiteko, enpresa adjudikaziodunak BBUPera gehienez ere bi orduko epean joan behar da BBUPera. Eskaintza teknikoan, gaitasun hori behar bezala dokumentatu beharko da.

Kontratistak agiri honen II. eranskina bete beharko du, laneko arriskuen prebentzioari dagokiona.

### 4.7.2 Zerbitzua emateko ordutegia

Zibersegurtasuneko Eragiketa Zentroaren (SEZ) jarduera eskema honen arabera emango da:

- Urruneko zerbitzua: Haren lana 24x7 ordutegian egingo da, eta gehiena enpresa adjudikaziodunaren bulegoetan egingo da, ezaugarriak direla-eta BBUPen instalazioetan osorik edo partzialki garatu behar diren zerbitzuen kasuan izan ezik (adibidez, *hacking* etikoko probak).
- Aurrez aurreko arreta: segurtasun-gorabehera larriren bat izanez gero, SEZeko langile espezializatuek BBUPen instalazioetara joan behar dute. Horretarako, lizitatzaileak urtean gutxienez hogei orduko aurrez aurreko zerbitzua ematea aurreikusi behar du. Adjudikaziodunak lantaldea dimentsionatu egin behar du, baldintza-agirian emandako informazioarekin bat eta egin beharreko jarduera-motaren arabera duen esperientziarekin bat.

### 4.7.3 BBUPeko sistemetan sartzea

Adjudikaziodunak konexio pribatua ezarri behar du BBUPen datuen sare korporatiboarekin, kontratu honetan zehaztutako lanek hala eskatzen dutenean.

Adjudikaziodunaren erakundearen eta BBUPen arteko komunikazioen interkonexioa egiteko, adjudikaziodunak Interneteko bi linea eskaini behar ditu, telekomunikazio-operadore desberdinenak, zerbitzuaren jarraitutasuna eskaini eta bermatzeko, eta eskuragarritasun handia ziurtatzeko.

Operadore-linea horien sare-ekipoak beharrezkoak dira BBUPen bulegoetan, eta Bilboko bulegoetako datu-prozesaketako zentroetan instalatuko dira, bi kokaleku desberdinetan, edo BBUPen beste kokapen batean, lanak egiten ari diren bitartean BBUPeko teknikariek hala zehazten badute.

Bi alderdien arteko komunikazioek IPSec tunelen bidez tunelizatuta egon beharko dute, bi alderdien artean trafiko segurua bidaliko dela bermatzeko.

BBUPek erabakiko du, adjudikaziodunak proposamena egin ondoren, komunikazio-lineen ezaugarrien eta edukieraren azken definizioa, konexioaren zirkulazio-baldintzak eta -bolumena aztertu ondoren.

Adjudikaziodunak behar diren segurtasun-neurriak hartu beharko ditu zerbitzuaren soluzioa horretarako baimena duten langileek (adjudikaziodunek eta BBUPeko langileek) bakarrik erabil dezaketela bermatzeko, eta beste zerbitzu batzuetako gainerako bezeroengandik isolatuta eduki behar du.

Baldintza-agiri honen irismenaren barruan dago, eta kostu gehigarririk gabe, baldintza horiek betetzeko behar diren elementu fisiko, lizentzia eta konfigurazio guztiak ematea.

## 4.8 Kontratua suntsiarazteko arrazoiak

Jarraian adierazten diren kasuek funtsezko betebeharrak ez betetzea dakarte, eta, beraz, dokumentu honetako beste edozein ataletan berariaz adierazten direnak eta AKPAn jasotzen direnak alde batera utzi gabe, kontratua suntsiaraz daiteke, kasuaren inguruabarrak kontuan hartuta:

- Adjudikaziodunak informazio faltsua edo zehaztugabea ematea, baita lizitazio-prozesuan edo proiektuaren edozein fasetan emandakoaren kasuan ere.
- Faltsutasuna hautematea eskainitako taldearen ezagutza-mailaren eta lanak egitean erakutsitako ezagutza errealen artean, edo zerbitzua modu nabarmen ez-eraginkorrean edo arduragabean ematea.
- Kontratatutako zerbitzua eskaintzan hitzartutako kualifikazio eta esperientziako giza baliabideekin emateko funtsezko kontratu-betebeharra ez betetzea.
- BBUPeko proiektuko-ikuskatzailearen eskakizunei behin eta berriz ez erantzutea, bereziki:
  - Aurrez aurreko arreta-zerbitzuaren ordutegiak arrazoirik gabe ez betetzea.
  - Jasotako telefono-deiei edo mezu elektronikoei behin eta berriz eta arrazoirik gabe ez erantzutea.
  - Zerbitzu-mailako akordioak behin eta berriz ez betetzea.
- Dokumentu honetako 4.10 atala («Informazioaren konfidentzialtasuna») edozein alderditan urratzea.

## 4.9 Informazioaren konfidentzialtasuna

BBUPek uste du proiektuan erabiltzen den informazio eta dokumentazio guztia, edozein motatakoa (elektronikoa, idatzia edo inprimatua, ikusizkoa, ahozkoa…), erabat konfidentziala dela. Beraz, printzipio hori urratuz gero, zehapena ezarriko da, agiri honetako dagokion atalean ezarritako baldintzen arabera, eta kontratua berehala suntsitzeko arrazoia ere izan daiteke, hala erabakitzen bada. Hori guztia erantzukizun penalak edo beste edozein eratakoak alde batera utzi gabe.

Kontratu honen esparruan erabiltzen den informazio eta dokumentazio guztia BBUPen jabetzakoa da. Adjudikaziodunak konpromisoa hartzen du informazio hori ez zabaltzeko eta ez hedatzeko edo erabiltzeko, kontratuari lotutako jarduerez eta BBUPek idatziz baimendu dituenez gain. Halaber, konpromisoa hartzen du informazio hori amaitzean eskura duen dokumentazioa itzultzeko, baita formatu elektronikoan edo lehendik dagoen edo etorkizunean egongo den beste edozein bitartekoren bidez gordetakoa ere. Betebehar hori mugagabea izango da, lanak adjudikatzen diren unetik hasita.

Adjudikaziodunak BBUPi jakinarazi behar dio proiektuan parte hartzen duen erakundeko langileen zerrenda, eta aldez aurretik baimena eskatu behar die informazio hori erabili behar dutenei. Halaber, proiektuan zehar harreman horretan gerta daitekeen edozein aldaketaren berri eman behar dio.

Aurrekoez gain, adjudikaziodunaren langileek betebehar hauek izango dituzte:

- BBUPen barne-arauetara egokitzea, eta zorrotz betetzea, segurtasun-politikei dagokienez, bai eta proiektu honetan aplika daitekeen beste edozein arauetara ere.

- Informazio konfidentziala zuhurtasun zorrotzez gordetzea eta behar bezala babestea, bere esku dagoen bitartean.

- Informazio konfidentziala erakunde barruan jasotzeko baimena duten pertsonen artean baino ez zabaltzea.

- Informazio konfidentziala behar bezala erabiltzen trebatzea langileak, bai eta hartu dituzten erantzukizunen inguruan trebatzea ere.

Zerbitzua ematen hasi aurretik, ezinbesteko baldintza izango da BBUPen Informazioaren Segurtasuna Kudeatzeko Sisteman (ISKS) aurreikusitako baldintzak betetzea, bereziki:

- Hirugarrenen arriskuak ebaluatzeko galdetegia
- Konfidentzialtasun-konpromisoa

- Erabilera-arauak onartzea

Kontratua gauzatzeko, adjudikaziodunak BBUPek emandako datuen datu pertsonaletarako sarbidea izan behar du eta datu horiek tratatu behar ditu (zehazki, BBUPen sareen eta informazio-sistemen erabiltzaileen datuak, hala nola izena, abizena, NANa, nabigazio-datu orokorrak, hala nola URLa eta deskargatutako fitxategien izena, gaia, bidalitako edo jasotako mezu elektronikoen bidaltzailea edo hartzailea). Horrenbestez, bere gain hartuko ditu Europako Parlamentuaren eta Kontseiluaren 2016ko apirilaren 27ko 2016/679 (EB) Erregelamenduak (pertsona fisikoak babesteari buruzkoa, datu pertsonalen tratamenduari eta datu horien zirkulazio askeari dagokienez) tratamenduaren arduradunentzat xedatzen dituen eginkizun eta betebeharrak. Erregelamendu horren 28. artikulua betez, datu pertsonaletarako sarbide eta tratamendu hori kontratua adjudikatu ondoren formalizatuko den kontratu berezi batean arautuko da (tratamenduaren arduradunaren kontratua). Adjudikaziodunak, zerbitzuaren zati gisa, datu pertsonaletarako sarbidea izan dezan baldintzak idatziz arautuko dira kontratu horretan, eta espresuki ezartzen da adjudikaziodunak, tratamenduaren arduradun den aldetik, tratamenduaren arduradunaren jarraibideen arabera tratatuko dituela datuak, eta ez dituela aplikatuko edo erabiliko kontratuan ageri ez den beste xede baterako, eta ez dizkiela komunikatuko beste pertsona batzuei, ezta gorde ditzaten ere. Kontratuan, halaber, tratamenduaren arduradunak ezarri behar dituen segurtasun-neurriak zehaztuko dira. Gainera, tratamenduaren Arriskuen Ebaluazioa egin beharko du (edo BBUPi hura egiten lagundu beharko dio, hala eskatuz gero), eta, azterketa horren emaitzaren arabera, Pribatutasunean duen Inpaktuaren Ebaluazioa egin beharko du.

## 4.10 Lanen dokumentazioa

Zerbitzuaren parte gisa sortzen den dokumentazioaren bertsio berriak eman behar dizkio adjudikaziodunak BBUPi.

## 4.11 Zigorrak eta zehapenak

Honako zigor hauek ezarri ahal izango dira, Administrazio Publikoen Administrazio Klausula Partikularren Agirian ezarritakoak baztertu gabe:

- Ezarritako zerbitzu-mailak ez betetzea IV. eranskineko («Zerbitzu-mailako akordioak») tauletan jasotakoaren arabera zigortuko da, baldin eta arrazoiak adjudikaziodunari egotz badakizkioke.

- Adjudikaziodunak konfidentzialtasun-klausula betetzen ez badu, adjudikazioaren zenbatekoaren % 30eko zehapen ekonomikoa izango du, eta, gainera, kontratua suntsiarazi ahal izango da, BBUPek hala baderitzo.

- Adjudikaziodunak zerbitzua giza baliabideekin eta eskatutako kualifikazio eta esperientziarekin emateko betebeharra betetzen ez badu, laurehun euroko (400 €) zehapena ezarriko zaio kontratua betetzen ez duen egun eta giza baliabide bakoitzeko, kontratua arrazoi horregatik suntsiarazteko aukerari kalte egin gabe.

Zehapen ekonomikoa ezartzeak edo kontratua suntsiarazteak ez dio BBUPi eragozten adjudikaziodunari bere kontratu-betebeharrak bete ditzan eskatzea, ez eta hark izan ditzakeen kalte-galeren ordaina eskatzea ere, eta ez luke salbuetsiko bestelako erantzukizun penaletik edo bestelakotik.

# 5 IRAUPENA

Kontratuak urtebeteko iraupena izango du, eta urtebeteko ondoz ondoko bi luzapen egin ahal izango dira.

Luzapenak hautazkoak izango dira BBUPen, eta nahitaezkoak adjudikaziodunarentzat, baldin eta kontratua amaitzeko data baino gutxienez bi hilabete lehenago jakinarazten bada.

Hala eta guztiz ere, behar iraunkor bati erantzuten dioten zerbitzuak direnez, kontratua amaitzen denean BBUPek kontratua luzatu ahal izango du, kontratistarentzat nahitaez, harik eta beste adjudikaziodun batek zerbitzua bere gain hartzen duenera arte. Luzapen horrek ezingo du sei hilabete baino gehiago iraun, eta kasu horretan ez da aplikatuko lehen aipatutako aurreabisu-epea.

Lanak hasteko akta sinatzen denean hasiko dira epeak kontatzen. Kontratuaren ikuskatzaileak adierazten duen egunean egin behar da akta, eta inoiz ez du 30 egun baino gehiago iraungo, kontratua sinatzen den egunetik kontatzen hasita.

Adjudikazio-prezioa ez da berrikusiko, ezta kontratua luzatuz gero ere.

05 de marzo de 2025

Izenpetua:

Marian Mena Domínguez
Kontratuaren kudeatzailea

Jose Luis Unzueta Portillo
Informatikako zuzendariordea

# I. ERANSKINA

# LANTALDEA EBALUATZEKO DOKUMENTAZIOA AURKEZTEKO TXANTILOIAK: CURRICULUM VITAEA

**Informazio pertsonala**

Izena **[abizenak, Izena]**
Helbidea
Nazionalitatea
Jaiotza-data**[eguna/hilabetea/urtea]**

**Laneko esperientzia**

| Datak (noiztik noiz arte) | Iraupena | Enplegatzailearen izena eta helbidea | Enpresa edo sektore mota | Betetako lanpostu edo kargua | Jarduera eta ardura nagusiak |
|---|---|---|---|---|---|
| [Berrienetik hasi eta informazio bera erantsi betetako lanpostu bakoitzerako] | [Urteak hamartarrekin adierazita] | | | | [Orokorrean] |

**Parte hartu duen proiektuak**

| Proiektuaren izenburua | Proiektuaren deskribapena | Erakunde enplegatzailea | Erakunde hartzailea | Egindako jarduera | Iraupena | Erabilitako metodologia eta tresnak |
|---|---|---|---|---|---|---|
| [Adierazi proiektu honen xedearen antzekoak bakarrik] | | [«Lan-esperientzia» atalean identifikatuta dagoen bezala | | [Egindako funtzioen deskribapena] | [Hilabetetan adierazita] | |

**Hezkuntza eta prestakuntza (arautua)**

| Datak (noiztik noiz arte) | Prestakuntza eskaini duen erakundearen izena eta mota | Jorratutako gai edo gaitasun okupazional nagusiak | Lortutako kualifikazioaren titulua |
|---|---|---|---|
| [Azken hilabetetik hasi eta beheko lerroetan informazio bera gehitu proiektuaren xedearekin lotura duen egindako ikastaro bakoitzeko] | | | |

**Prestakuntza osagarria**

| Datak (noiztik noiz arte) | Prestakuntzaren ordu-kopurua | Prestakuntza eskaini duen erakundearen izena eta mota | Jorratutako gai edo gaitasun okupazional nagusiak | Lortutako ziurtagiria |
|---|---|---|---|---|
| [Azken hilabetetik hasi eta beheko lerroetan informazio bera gehitu proiektuaren xedearekin lotura duen egindako ikastaro bakoitzeko] | | | | [Hala badagokio] |
| **Informazio gehigarria** | [Txertatu hemen proiektu honen xederako esanguratsutzat jotzen den edozein informazio] | | | |

# II. ERANSKINA

# LANEKO ARRISKUEN PREBENTZIOA

# ERANSKINA: LANEKO ARRISKUEN PREBENTZIOA

## 1 PREBENTZIO- ETA BABES-NEURRIAK

Enpresa adjudikaziodunak Laneko Arriskuen Prebentzioari buruzko Legearen 14. artikuluan aurreikusitako prebentzio-betebeharra osatzen duten neurriak aplikatuko ditu, printzipio hauen arabera: a) Arriskuak saihestea.

b) Saihetsezinak diren arriskuak ebaluatzea.
c) Arriskuen jatorriaren aurka borrokatzea.
d) Lana pertsonarentzat moldatzea, bereziki lanpostuak betetzeko orduan, baita laneko eta ekoizpeneko ekipamendu eta metodoei egokitzea ere, lan monotono eta errepikakorra arintzeko, eta horrek osasunean dituen ondorioak gutxitzeko.
e) Teknikaren bilakaera aintzat hartzea.
f) Arriskutsua denaren ordez, arrisku gutxikoa edo arriskurik gabekoa dena ezartzea.
g) Prebentzioa planifikatzea.
h) Langileei jarraibide egokiak ematea.

## 2 PREBENTZIO-MODALITATEA

Enpresa adjudikaziodunak laneko arriskuen prebentzioa antolatzeko eredua, prebentzio-jarduerak egiteko hartutakoa, egiaztatu behar dio BBUPi, laneko arriskuen prebentzioaren arloko arduraduna edo arduradunak barne. Kanpoko prebentzio-zerbitzu batekin sinatutako hitzarmena bada aukeratutako eredua, indarrean dagoen kontratuaren kopia aurkeztu behar du enpresa adjudikaziodunak.

Aldi berean, dagokion lan-istripu eta gaixotasun profesionalen mutualitateari igorriko dio elkartze-kontratua.

## 3 ARRISKUAK EBALUATZEA ETA JARDUERAK PLANIFIKATZEA

Enpresa adjudikaziodunak agiri honen xede diren langileen arriskuen ebaluazioa eta prebentzio-jardueren plangintza izan behar ditu, 31/1995 Legearen 16. artikuluaren arabera. Egin ondoren, enpresa adjudikaziodunak BBUPen esku jarri behar du dokumentazio hori, kontrolatzeko.

## 4 BBUP-EN ZENTROETAKO ARRISKUEN EBALUAZIOA

Lanak hasi baino lehen, enpresa adjudikaziodunak BBUPen gainbegiraleak preskripzio-agiri honen xede diren langileen lantokiek/instalazioek dituzten arriskuei buruzko informazioa emango dio.

Lanak egingo diren instalazioetan arrisku larriak edo oso larriak badaude, informazio hori idatziz entregatu beharko da, eta enpresa kontratistak informazio hori jaso duela sinatu beharko du.

## 5 LARRIALDI-NEURRIAK

Enpresa adjudikaziodunak, BBUPen lantokietara sartzean, agiri honen xede diren langileak sartuko diren lantoki/instalazioetan kontuan hartu beharreko larrialdi-neurriei buruzko informazioa jasoko du.

## 6 OSASUNA ZAINTZEA

Enpresa adjudikaziodunak bere langileei bermatu behar die osasun-egoera aldizka zainduko zaiela, lanak dituen arriskuen arabera, eta azterketa espezifikoetarako protokoloak aplikatuko zaizkiela, beharrezkoa denean.

Enpresa adjudikaziodunak nahitaez aurkeztu behar dizkio BBUPi, hark hala eskatuz gero, hark osasun-zaintzaren arloan hartutako modalitatea egiaztatzeko agiriak, bai eta langile guztien azterketa medikoak ere, «GAI» kalifikazioarekin, bete beharreko lanpostuaren arabera.

## 7 PRESTAKUNTZA ETA INFORMAZIOA

Enpresa adjudikaziodunak bermatuko du langileak behar bezala trebatuta eta prestatuta daudela laneko arriskuen prebentzioaren eta lehen sorospenen arloan, eta horretarako egindako ekintzen berri emango du agiri bidez. Gainera, enpresa adjudikaziodunak BBUPen esku jarriko du bere langileei enpresan egindako arriskuen ebaluazioa eta prebentzioko ekintza-plana azaldu izana egiaztatzen duen dokumentazioa, eta gai horri buruzko trebakuntza espezifikoa dutela egiaztatzen duena.

Enpresa kontratistak, enpresa-jarduerak koordinatzeko betebeharra betetzeko, prebentzioaren arloan ematen zaion informazio guztia eman behar die agiri honen xede diren lanetarako izendatutako langileei, eta BBUPen esku jarri behar ditu informazio horren hedapenari dagozkion erregistroak.

## *8 NORBERA BABESTEKO EKIPOAK*

Enpresa adjudikaziodunak egin behar duen arriskuen ebaluazioko prebentzioko ekintza-planaren arabera, enpresa horren ardura da norbera babesteko ekipoak (NBEak) ematea, agiri honen xede diren lanak egiteko, bai eta langileek horiek erabiltzea ere. Norbera babesteko ekipoak dira langileak bere segurtasuna edo osasuna arriskuan jar dezakeen arrisku batetik edo batzuetatik babesteko eraman edo heldu behar duen edozein ekipamendu, bai eta horretarako osagarri edo gehigarri oro ere.

Enpresa adjudikaziodunak BBUPen esku jarri behar du langileei NBEak entregatu izanaren erregistroa. Halaber, NBEen mantentze-lanak eta berrikuspena egingo ditu, fabrikatzailearen jarraibideen arabera, eta BBUPek haien emaitzak egiaztatuko ditu, hala eskatzen duenean.

## *9 EZBEHAR-TASAREN AZTERKETA ETA KONTROLA*

Istripurik gertatuz gero, enpresa adjudikaziodunak berehala jakinarazi behar dio BBUPi, eta ahalik eta lasterren bidali behar dio dagokion ikerketa-txostena.

## *10 PREBENTZIO-AUDITORIA*

Enpresa adjudikaziodunaren prebentzio-modalitatea kanpoko prebentzio-zerbitzu batekin hitzartuta ez badago, eta Prebentzio Zerbitzuen Araudiaren 29. artikuluaren arabera, BBUPek laneko arriskuen prebentzioko auditoriaren nahitaezko txostena eta dagokion zuzenketa-ekintzen plana izan behar ditu eskura.

## *11 TEKNIKARI ARDURADUNA*

Enpresa adjudikaziodunak lan-arriskuen prebentzioaren arloko teknikari solaskide bat izendatuko du, BBUPekin lan-arriskuen prebentzioaren arloan. Berdin dio zer antolaketa-mota den eta zer baliabide behar diren hartutako prebentzio-jarduerak egiteko.

## *12 ENPRESA-JARDUEREN KOORDINAZIOA*

171/2004 Errege Dekretua betez, BBUP, Laneko Arriskuak Prebenitzeko Kudeaketa Sistemaren barruan,
Enpresa Jarduerak Koordinatzeko Prozedura (GE 018.11) ezartzen ari da, eta prozedura horren aplikazioa da zerbitzu-kontratazioetan lehentasunezko koordinazio-bitartekoa. Hori betetzea nahitaezkoa izango da enpresa adjudikaziodunarentzat.

Komeni dela iritziz gero, BBUPek eta enpresa adjudikaziodunak beste koordinazio-bitarteko osagarri batzuk ezarri ahal izango dituzte. Kasu horietan, enpresa adjudikaziodunak idatziz egiaztatuko du agiri honen xede diren lanak egiteko esleitutako langileei 31/1995 Legearen 18.1 artikuluan ezarritako koordinazio-bitartekoen berri eman diela.

## *13 KUDEAKETA*

Laneko arriskuen prebentzioaren arloko dokumentazio guztia, bai baldintza-agiriari dagokiona, bai BBUPek enpresa kontratistari eskatzen dion beste edozein, kontratua-gainbegiralearen edo BBUPek enpresa-jardueren koordinazioaren arduradun gisa dituen pertsonen eskura egongo da.
Enpresa-jarduerak koordinatzea.

Kontratistak plataforma horretan egiaztatu behar du laneko arriskuen prebentzioari buruzko baldintza orokorrak eta langileei, makinei, lan-ekipoei, ibilgailuei eta baliabide osagarriei buruzko baldintza espezifikoak formalki betetzen dituela, laneko arriskuen prebentzioari buruzko eranskin honetan adierazitakoaren arabera.

Halaber, enpresa adjudikaziodunak erantzun egin behar die BBUPek laneko arriskuen prebentzioa kudeatzeko sistema aplikatuz egiten dizkion eskaerei.

| ENPRESEN zerrenda | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Enpresa kontratistaren datuak | | | | | | | | | Proiektuarekiko duen lotura | | SerCAE plataformako harremanetarako pertsona | | |
| Sozietate-izena | IFK | Enpresa mota | Enpresaren jarduera mota (erantzun bat baino gehiago eman daitezke) | | | | | | Hasiera-data | Amaiera-data | Izena eta abizenak | Helbide elektronikoa | Telefono-zenbakia |
| | | | Segurtasuna eta osasuna koordinatzeko enpresa | Eraikuntza-jarduera | Amiantoari loturiko jarduera (fibrozementua) | Arrisku elektrikoa duen jarduera | Beste jarduera bat | | | | | | |

## *14 EZ-BETETZEAGATIKO ZIGORRAK*

Laneko arriskuen prebentzioari buruzko araudia ez betetzeagatik adjudikaziodunak izan ditzakeen beste legezko erantzukizun batzuk gorabehera, eranskin honetan jasotako betebeharrak ez betetzea honela kalifikatu eta zigortuko da:

- Hutsegite arina, 100 eurotik 300 eurora bitarteko zigorra dakarrena: eranskin honen 2., 4., 9., 10., 11. eta 12. ataletan jasotako betebeharrak ez betetzea.

- Hutsegite larria, 301 eurotik 1.500 eurora bitarteko zigorra dakarrena: eranskin honetako 5., 6., 7., 8. eta 13. ataletan jasotako betebeharrak ez betetzea.

- Hutsegite oso larria, 1.501 eurotik 6.000 eurora bitarteko zigorra dakarrena: eranskin honen 3. eta 14. ataletan jasotako betebeharrak ez betetzea.

Urtebeteko epean (edo kontratua egikaritzeko epean, epe hori laburragoa bada) hiru (3) hutsegite arin egitea hutsegite larri bat egitearen baliokidea izango da.

Urtebeteko epean (edo kontratua gauzatzeko epean, txikiagoa bada) hutsegite oso larri bat (1) edo bi (2) hutsegite larri egiten badira, BBUPek kontratua suntsiarazteko eskubidea izango du, eta behin betiko fidantza galduko du.

1. OHARRA: ***Eranskin honetan eskatzen diren dokumentu guztiak BBUPi bidali behar zaizkio, enpresa adjudikaziodunak izendatzen duen arduradunak sinatuta.***

2. OHARRA: ***Kontratua esleitu ondoren, enpresa adjudikaziodunak BBUPeko arriskuak, prebentzio-neurriak, jarraibideak, prozedurak edo prozesuak aldatu direla ikusten badu, eta aldaketa horiek agiri honen xede diren lanak egiteko izendatutako langileen segurtasunari eta osasunari eragiten badiete, BBUPen kontratuaren gainbegiraleari jakinarazi behar dio.***

Prebentzioburua - BBUP

| | ENPRESA-JARDUERAK ENPRESA KONTRATISTEKIN KOORDINATZEKO PROTOKOLOA | Espedientea Zenbakia |
|---|---|---|

## Prebentzio-antolakuntza

**Enpresaren datu orokorrak**

| **Sozietate-izena** | **Sozietatearen egoitza** |
|---|---|
| | |

| **Probintzia** | **Udalerria** | **Posta-kodea** | **Telefono-zenbakia** |
|---|---|---|---|
| | | | |

**a) Enpresariak bere gain hartzea**

Enpresariaren izena:

**b) Langile bat edo gehiago izendatzea** (zehaztu langile-kopurua, laneko arriskuen prebentzioko prestakuntza-mailaren arabera)

| Oinarrizko maila | | Bitarteko maila | | Goi-maila | |
|---|---|---|---|---|---|

**c) Prebentzio-zerbitzu propioa eta/edo enpresaz kanpoko prebentzio-zerbitzua**

| Espezialitatea | Propioa | Kanpokoa | KPZren izena | Espezialitatea | Propioa | Kanpokoa | KPZren izena |
|---|---|---|---|---|---|---|---|
| Laneko segurtasuna | ☐ | ☐ | | Ergonomia eta psikosoziologia | ☐ | ☐ | |
| Higiene industriala | ☐ | ☐ | | Laneko Medikuntza | ☐ | ☐ | |

## Prebentzioa kudeatzea

| **Enpresak honako xedapen hauek betetzen direla bermatzen du:** | **BAI** | **EZ** | **E.A.** |
|---|---|---|---|
| Kontratu honen xede diren jarduera guztien arriskuen ebaluazioa egina izatea. | | | |
| Arriskuen ebaluazioan oinarritutako prebentzio-plangintza egin izana. | | | |
| Laneko arriskuen prebentzioari buruzko legezko ikuskapena eginda izatea (prebentzio-zerbitzu propioen kasuan bakarrik): | ☐ | ☐ | ☐ |
| **Kontratu honen xede diren lanetan parte hartzen duten langileei dagokienez, enpresak hau bermatzen du:** | **BAI** | **EZ** | **E.A.** |
| Arriskuei eta prebentzio- eta babes-neurriei buruzko prebentzio-informazioa jaso dute. | | | |
| Beren lanpostutik eratorritako arriskuei buruzko prestakuntza espezifikoa dute. | | | |
| Garabiak, *dumper*-ak eta obran erabiltzen diren gainerako makinak erabiltzeko ardura duten langile guztiek prestakuntza espezifikoaren ziurtagiriak dituztela egiaztatzen duen agiria. | ☐ | ☐ | ☐ |
| Lanerako babes kolektiboko eta norbere babeserako (NBE) baliabide egokiak dituzte. | | | |
| Ohiko lanerako behar den gaitasun medikoaren ziurtagiria dute. | | | |
| Lanbide-prestakuntzako ziurtagiriak dituzte, lan arautuak egin behar izanez gero. | ☐ | ☐ | ☐ |
| **Kontratistak lan-ekipoak, norbera babesteko ekipoak (NBE) edo produktu kimikoak hornitu behar baditu, honako hauek bermatu behar du:** | **BAI** | **EZ** | **E.A.** |
| Erabili beharreko lan-ekipoen CE adostasun-adierazpena duela, edo, halakorik ez badu, 1215/1997 Errege Dekretura egokitzen dela ziurtatzen duen agiria. | ☐ | ☐ | ☐ |

| | | | |
|---|---|---|---|
| Langileei emandako NBEen CE onespen-adierazpena duela. | | | |
| Erabili beharreko produktu kimikoen segurtasun-fitxak daudela. | | | |
| **Kontratistaren laneko arriskuak prebenitzeko plana:** | **BAI** | **EZ** | **E.A.** |
| Laneko arriskuak prebenitzeko kudeaketa sistema du ezarrita. | | | |
| Laneko Arriskuak Prebenitzeko Eskuliburua du. | | | |
| Laneko arriskuak prebenitzeko politika du. | | | |
| Laneko arriskuen prebentzioaren arloko ardurak eta funtzioak zehaztu ditu idatziz. | | | |
| Azpikontratistei eta langile autonomoei laneko arriskuen prebentzioaren arloko betebehar guztiak bete dituztela egiaztatzen duten agiriak eskatu dizkie. | ☐ | ☐ | ☐ |
| Enpresa azpikontratisten eta langile autonomoen aldetik, laneko arriskuen ebaluazioa jaso izana lanetarako. | ☐ | ☐ | ☐ |
| Arriskuen prebentzio-ekintza garatzeko idatzizko prozedurak edo jarraibideak ditu, eta prebentzio-baliabideak izendatzen ditu, eskuragarri izan behar diren guztietan. | ☐ | ☐ | ☐ |

**Prebentzio-arloko arduraduna naizen aldetik, ziurtatzen dut lehen adierazitako datuak betetzen ditudala, eta BBUPen eskura jartzen ditut egiaztagiriak.**

| | | |
|---|---|---|
| Izena eta izenpea: | Kargua:<br><br>Telefono-zenbakia: | Data: |

**1. OHARRA: Lanak adjudikatu ondoren, enpresa adjudikaziodunak BBUPeko arriskuak, prebentzio-neurriak, jarraibideak, prozedurak edo prozesuak aldatu direla ikusten badu, eta aldaketa horiek agiri honen xede diren lanak egiteko izendatutako langileen segurtasunari eta osasunari eragiten badiete, BBUPen kontratatutako zerbitzuen ikuskatzaileari jakinarazi beharko dio.**
**2. OHARRA: BBUPen laneko arriskuak prebenitzeko politika eskuragarri dago lantoki guztietan.**

## PARTE HARTZEN DUTEN LANGILEEN ZERRENDA.

*Eguneratze-data:*

| ***LANGILEAREN IZENA*** | **NAN:** | **ENPRESA** |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Lanez arduratzen den enpresaren zigilua

Izenpetua:
Kargua:
Enpresa:

## ZERBITZUAN ERABILITAKO MAKINEN ETA BALIABIDE OSAGARRIEN ZERRENDA

*Eguneratze-data:*

| ***MODELOA*** | **MATRIKULA EDO IDENTIFIKAZIO-ZENBAKIA*** | **MUNTAKETA-ENPRESA*** | **AZKEN IKUSKAPENAREN DATA*** | **HURRENGO BERRIKUSPENAREN DATA*** | **CE MARKA**** | **ENPRESA KONTRATATZAILEA*** |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

Lanez arduratzen den enpresaren zigilua

Enpresa:

* Aplikatzekoa denean ** Bestela, 1215 ED aplikatu beharko da.

Izenpetua:

Kargua:

# KUDEAKETA-SISTEMA INTEGRATUAREN POLITIKA (04 Ber.)

Uraren ziklo integralari dagozkion arlo guztietan herritarrei zuzendutako jarduera garatzen duen enpresa den aldetik, BBUPek jotzen du kalitatea kudeaketako funtsezko faktorea dela bere zerbitzuen prestazioan. Horretarako, hierarkia-mailen bidez, honako hauek kudeatzeko sistema integratu bat ezarri du: kalitatea, kontsumoko uraren segurtasun planak, laneko arriskuen prebentzioa, ingurumenaren babesa eta ikerketa, garapena eta berrikuntza, eta energia.

Politika honetan adierazitako printzipioen bidez, BBUPeko Zuzendaritzak konpromisoa hartzen du bere bezero eta erabiltzaileen beharrei egokitutako zerbitzua emateko, ingurumena babesteko, uraren erabilera jasangarriari laguntzeko, pertsonen osotasuna bermatzeko, arriskuak desagerrarazteko eta arriskuak murrizteko, I+G+B sustatzeko, uraren kaltegabetasuna bermatzeko hornikuntza-sistema orokor osoan, eta bere instalazioen eta prozesuen energia-eraginkortasuna hobetzeko, alderdi interesdun guztien beharrak eta espektatibak betetzeko: bezeroak, erabiltzaileak, akziodunak, erakundeko pertsonak, kolaboratzaileak, hornitzaileak eta gizartea, oro har. Hauek dira printzipioak:

- Kudeaketa-sistema integratua definitzea, ezartzea eta mantentzea, eraginkorra, dinamikoa eta erakundearentzat egokia dena, politika honen arabera. Sistema horrek helburuak eta helmugak aldian-aldian ezartzeko aukera emango du, bai eta betetze-maila kontrolatu eta ebaluatzekoa ere, eraginkortasuna eta lana etengabe hobetzeko.

- Gure jarduerari aplika dakizkiokeen legezko eta arauzko baldintzak eta izenpetutako bestelako betekizunak betetzea, bai eta erreferentziako arauetan ezarritako betekizunak ere, horiek ezagutu eta eguneratuta edukitzeko prozedurak ezarriz.
- Langileen prestakuntza, sentsibilizazioa eta informazioa bermatzea, beren jarduerak behar bezala garatzeak duen garrantziari buruz kontzientziatzeko, erakundearen helburuak lortzeko kontsulta, parte-hartze eta inplikazio aktiboa eta jokabide sortzaile eta berritzaileak azpimarratuz.
- Gure kolaboratzaileak, kontratistak eta hornitzaileak etengabeko hobekuntzara zuzendutako konpromiso aktiboan integratzea eta inguruko administrazio, erakunde eta komunitateekin gardentasunez jokatzea.
- Laneko istripu-tasa murrizteko jarduerak sustatzea, lan-baldintza seguruak eta osasungarriak eskaintzea lesioak eta osasunaren narriadura prebenitzeko, bai eta gure isurien, emisioen eta kontsumoen inpaktuak minimizatzeko jarduerak sustatzea ere. Horretarako, eskuragarri dauden baliabide tekniko eta ekonomikoak kontuan hartu behar dira, eta kontroleko, zaintzako, zuzenketako eta larrialdien aurrean jarduteko prozedura egokiak ezarri, hondakinak eta baliabide naturalak berrerabiltzea, birziklatzea eta behar bezala kudeatzea sustatu behar da.
- Enpresan energiaren erabilera egokia sustatzea, diseinua hobetzea erakundeko instalazioen eta prozesuen energia-eraginkortasun handiagoa lortzeko, eta energetikoki eraginkorrak diren produktuak eta zerbitzuak erostea.
- Politika honekin bat datozen I+G+B proiektuei ekitea, aliantza onuragarriak bultzatzea eta, oro har, proiektu horien emaitzak babesteko neurriak ezartzea.
- Helburuak eta xedeak lortzeko beharrezko informazioa eta baliabideak eskuragarri daudela ziurtatzea.
- Kontsumitzaileari ahalik eta segurtasun eta konfiantza handiena eskaintzea, arriskuen analisiko eta kontrol-puntu kritikoen sistema zorrotz bat aplikatuz. Sistema hori hornikuntza-sistema orokorraren etapa guztietan kontrol higieniko-sanitario eta uraren kalitatearen kontrol iraunkor eta zorrotz batean oinarritzen da, bai eta, oro har, arriskua kudeatzeko sistema batean ere.
- Kudeaketa-sistema integratuaren oinarria, oro har, desadostasunak eta, bereziki, kutsadura, kalteak eta erakundeko pertsonen osasun-narriadura prebenitzea da. Hori dela eta, sistemaren funtzionamendu egokia arriskuan jartzen duen edozein egoera erreal edo potentzial zuzendaritzari jakinarazteko (ezarritako bideak erabiliz) askatasuna eta erantzukizuna dute erakundeko pertsona guztiek.

Kudeaketa Sistema Integratuaren Eskuliburuan eta hortik eratorritako gainerako dokumentazioan definitzen eta garatzen da kudeaketa-sistema integratua, eta, beraz, nahitaez bete behar dute kudeaketa-sistema integratuko jarduerak gauzatzeko erantzukizuna duten pertsona guztiek.

# III. ERANSKINA

# SEGURTASUN-EGIAZTAGIRIAK

- EC-Council erakundearen segurtasun-egiaztagiriak
- Information Systems Audit and Control Association (ISACA) erakundearen segurtasun-egiaztagiriak
- International Information System Security Certification Consortium $(ISC)^2$ erakundearen segurtasun-egiaztagiriak
- CompTIA erakundearen segurtasun-egiaztagiriak
- Global Information Assurance Certification (GIAC) erakundearen segurtasun-egiaztagiriak
- Institute for Security and Open Methodologies (ISECOM) erakundearen segurtasun-egiaztagiriak
- BS 25999/UNE-ISO 22301 Lead Auditor
- CERT-Certified Computer Security Incident Handler Certification
- CISSP: Certified Information Systems Security Professional
- CHFJ: Computer Hacking Forensic Investigator ✓ CISMP: Information Security Management Principles.
- CNDA: Certified Network Security Arquitect
- CompTIA Security+
- CompTIA Advanced Security Practitioner
- ECSA: Certified Security Analyst
- ENSA: Network Security Administrator
- CCFE: Certified Computer Forensics Examiner
- CCNA Security: Cisco Certified Network Professional Security
- CCTHP: Certified Cyber Threat Hunting Professional
- CDDP: Certified Data Privacy Professional
- CDP: Certified Protection Professional
- CDRP: Certified Data Recovery Professional
- CEPT: Certified Expert Penetration Tester
- CEREA: Certified Expert Reverse Engineering Analyst
- CMWAPT: Certified Mobile and Web Application Penetration Tester
- CMFE: Certified Mobile Forensics Examiner
- CPT: Certified Penetration Tester
- CRTOP: Certified Red Team Operations Professional
- CREA: Certified Reverse Engineering Analyst
- CSSA: Certified SCADA Security Architect
- CSAP: Certified Security Awareness Practitioner ✓ CGEIT: Certified in the Governance of Enterprise IT ✓ CISA: Certified Information Systems Auditor.
- CISM: Certified Information Security Manager.
- CPP: Certified Protection Professional
- CREST: Penetration Testing Certifications
- CRISC: Certified in Risk and Information Systems Control
- CCSP: Cisco Certified Security Professional
- EC-Council Certified Ethical Hacker
- EC-Council Computer Hacking Forensic Investigator

- EC-Council Certified Security Analyst
- EC-Council Licensed Penetration Tester
- EC-Council Network Security Administrator
- EC-Council Certified Incident Handler
- EC-Council Certified Security Specialist
- EC-council Certified Disaster Recovery
- EC-Council Chief Information Security Officer
- GIAC: Global Information Assurance Certification
- GPEN: GIAC Certified Penetration Tester
- GWAPT: GIAC Web Application Pentration Tester
- GXPN: GIAC Exploit Researcher and Advanced Penetration Tester
- GCIH: GIAC Certified Incident Handler
- ISO/IEC 27001 Lead Auditor
- ISO/IEC 27001 Expert Implementator
- OCSP: Offensive Security Certified Professional
- OPSA: OSSTM Professional Security Analyst
- OPST: OSSTM Professional Security Tester
- OPSE: OSSTM Professional Security Expert
- OWSE: OSSTM Wireless Security Expert
- OSWP: Offensive Security Wireless Professional
- SSCP: Systems Security Certified Practitioner
- SANS Instituteren ziurtagiriak
- Certified Ethical Hacker (CEH)
- CompTIA Cybersecurity Analyst (CySA+)
- SANS Threat Hunting and Incident Response (THIR)
- Informazioaren segurtasunari edo antzeko gaiei buruzko unibertsitate-masterren batean (ofiziala edo propioa) trebatzea (zibersegurtasuna, segurtasun informatikoa).
- EC-Council, ISACA, $(ISC)^2$, CompTIA edo GIAC erakundeen bestelako egiaztagiri batzuk, baldintza-agiriaren xedearekin lotura zuzena dutenak.

# IV. ERANSKINA

# ZERBITZU-MAILAKO AKORDIOA

## *Ezarpena*

| Esparrua | Zerbitzu-mailako akordioa | Xehetasuna | Balio objektiboa | Neurketa | Irizpidea | Zehapena |
|---|---|---|---|---|---|---|
| **SEZ** | **«Ezarpen-fasea» betetzea** | «Ezarpen-faserako» ezarritako epean atzeratutako egun naturalak, adjudikaziodunari egozteko modukoak. | 0 | Ezarpen-fasearen epearen amaiera | - Atzeratutako egun bakoitzeko | 200 € |

- Zigorrak metagarriak dira.
- Egunak lanegunak dira.

## *Monitorizazio-zerbitzua (alertak eta txostenak)*

| Zerbitzu-mailako akordioa | Xehetasuna | Balio objektiboa | | Betetze-mailaren gutxieneko ehunekoa | Neurketa | Irizpidea | Zehapena |
|---|---|---|---|---|---|---|---|
| **Monitorizazio- eta erantzun-zerbitzua** | | | | | | | |
| **Alertei arreta emateko denbora** | **Sortutako alertei erantzuteko gehieneko denbora** | Kritikak | Berehalako arreta | % 95 | Hilero | Zerbitzu-mailako akordioaren ez-betetze bakoitzeko | 900 € |
| | | Oso handiak / handiak | <4 ordu | % 95 | Hilero | Zerbitzu-mailako akordioaren ez-betetze bakoitzeko | 500 € |
| | | Ertainak | <8 ordu | % 90 | Hilero | Zerbitzu-mailako akordioaren ez-betetze bakoitzeko | 300 € |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | Txikiak | <48 ordu | % 90 | Hilero | Zerbitzu-mailako akordioaren ez-betetze bakoitzeko | 100 € |
| **Gorabeherak jakinarazteko denbora** | **Gorabehera bat jakinarazteko gehienezko denbora, detektatzen denetik** | Kritikoak | Ordubete | % 95 | Hilero | Zerbitzu-mailako akordioaren ez-betetze bakoitzeko | 900 € |
| | | Oso handiak / handiak | 4 ordu | % 95 | Hilero | Zerbitzu-mailako akordioaren ez-betetze bakoitzeko | 500 € |
| | | Bitartekoak | 8 ordu | % 90 | Hilero | Zerbitzu-mailako akordioaren ez-betetze bakoitzeko | 300 € |
| | | Baxuak | 48 ordu | % 90 | Hilero | Zerbitzu-mailako akordioaren ez-betetze bakoitzeko | 100 € |
| **Gorabeherei erantzuteko denbora** | **Erantzuteko gehieneko denbora, gorabehera bat jakinarazten denetik** | Kritikoak | 15 minutu | % 95 | Hilero | Zerbitzu-mailako akordioaren ez-betetze bakoitzeko | 900 € |
| | | Oso handiak / handiak | 30 minutu | % 95 | Hilero | Zerbitzu-mailako akordioaren ez-betetze bakoitzeko | 500 € |
| | | Bitartekoak | 2 ordu | % 90 | Hilero | Zerbitzu-mailako akordioaren ez-betetze bakoitzeko | 300 € |
| | | Baxuak | 2 ordu | % 90 | Hilero | Zerbitzu-mailako akordioaren ez-betetze bakoitzeko | 100 € |
| **Gomendioa proposatzeko denbora** | **Gorabehera detektatzen denetik hura arintzeko gomendio bat proposatu arte igaro beharreko gehieneko denbora** | Kritikoak | 2 ordu | % 95 | Hilero | Zerbitzu-mailako akordioaren ez-betetze bakoitzeko | 900 € |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | Oso handiak / handiak | 4 eta 16 ordu artean | % 95 | Hilero | Zerbitzu-mailako akordioaren ez-betetze bakoitzeko | 500 € |
| | | Bitartekoak | 16 eta 160 ordu artean | % 90 | Hilero | Zerbitzu-mailako akordioaren ez-betetze bakoitzeko | 300 € |
| | | Baxuak | Kasuan-kasuan | % 90 | Hilero | Zerbitzu-mailako akordioaren ez-betetze bakoitzeko | 100 € |
| **Zerbitzuaren eskuragarritasuna** | **SEZaren atariaren eskuragarritasuna** | % 100 | | % 99,99 | Hilero | Zerbitzu-mailako akordioaren ez-betetze bakoitzeko | 300 |

| Zerbitzu-mailako akordioa | Konpromiso-balioa | Gutxieneko betetze-ehunekoa | Neurketa | Irizpidea | Zehapena |
|---|---|---|---|---|---|
| **Alerta kritikoko txostena entregatzea** | <=30 minutu | % 95 | Lau hilean behin | - Zerbitzu-mailako akordioaren ez-betetze bakoitzeko. - Atzerapenaren 10 minutu bakoitzeko, esku-hartze bakoitzaren gainean. | 600 €<br>100 € |
| **Alerta oso handi edo handiaren txostena entregatzea** | <=ordubete | % 90 | Lau hilean behin | - Zerbitzu-mailako akordioaren ez-betetze bakoitzeko. - Atzerapenaren 20 minutu bakoitzeko, esku-hartze bakoitzaren gainean. | 300 €<br>100 € |
| **Zerbitzua emateari buruzko hileko txostena entregatzea** | Hurrengo hilabeteko lehen 5 egunak | % 95 | Lau hilean behin | - Zerbitzu-mailako akordioaren ez-betetze bakoitzeko. - Atzerapen-egun bakoitzeko, entrega bakoitzean. | 200 €<br>100 € |

| | | | | | |
|---|---|---|---|---|---|
| **SIEM plataforman txosten edo aginte-koadro berria (*dashboard*) diseinatzea eta ezartzea, eskaeraren arabera (gehienez 3, hileko)** | 10 egun (eskatu ondoren) | % 95 | Lau hilean behin | - Zerbitzu-mailako akordioaren ez-betetze bakoitzeko. - Atzerapen-egun bakoitzeko, entrega bakoitzean. | 200 €<br>100 € |

- Egunak lanegunak dira.
- Zigorrak metagarriak dira.

## *Forentsea*

| Zerbitzu-mailako akordioa | Gorabeheraren larritasun-maila | Konpromiso-balioa | Ordutegia | Gutxieneko betetze-ehunekoa | Neurketa | Irizpidea | Zehapena |
|---|---|---|---|---|---|---|---|
| **Azterketa forentsea egiten hasteko erantzun-denbora** | Kritikoa / oso handia | 3 ordu | 24x7 | % 95 | Lau hilean behin | - Zerbitzu-mailako akordioaren ez-betetze bakoitzeko<br>- Eskatutako esku-hartze bakoitzean konpromisoaren balioaren gainean atzeratzen den ordu bakoitzeko | 600 €<br>200 € |

- «Analisi forentseko lanei ekiteko erantzun-denbora» hau da: analisi-eskaera bat jakinarazten denetik espezialista bat lan forentseari ekiteko bezeroaren instalazioetara joaten den gehieneko denborara arte igarotzen den denbora. - Zigorrak metagarriak dira.

## *Kalteberatasunen analisia eta hacking etikoa*

| Zerbitzu-mailako akordioa | Konpromiso-balioa | Gutxieneko betetze-ehunekoa | Neurketa | Irizpidea | Zehapena |
|---|---|---|---|---|---|
| **Barne-kalteberatasunen txostena entregatzea** | Analisi programatuaren data amaitu eta 5 egunera | % 95 | Urtero | - Zerbitzu-mailako akordioaren ez-betetze bakoitzeko. - Atzerapen-egun bakoitzeko, entrega bakoitzean. | 300 €<br>100 € |
| **Kalteberatasunen auditoria perimetralaren txostena entregatzea** | Hurrengo hilabeteko lehen 5 egunak | % 95 | Urtero | - Zerbitzu-mailako akordioaren ez-betetze bakoitzeko. - Atzerapen-egun bakoitzeko, entrega bakoitzean. | 300 €<br>100 € |
| **Segurtasun-testaren txostena entregatzea (*hacking* etikoa)** | 15 egun, probak amaitu ondoren | % 100 | Urtero | - Zerbitzu-mailako akordioaren ez-betetze bakoitzeko. - Atzerapen-egun bakoitzeko, entrega bakoitzean. | 300 €<br>100 € |

- Egunak lanegunak dira.
- Zigorrak metagarriak dira.