BCSCren zibersegurtasun-gorabeherei erantzuteko eta horiei buruzko aholkularitza emateko linea kudeatzeko zerbitzua kontratatzeko baldintza teknikoen agiria.

Espediente Zk: 2023026 Harmonizatua

Kontratazioaren xedea: BCSCren zibersegurtasun-gorabeherei erantzuteko eta horiei buruzko aholkularitza emateko linea kudeatzeko zerbitzua.

Dokumentua: Baldintza Teknikoen Agiria

1. TESTUINGURUA

Basque CYBERSECURITY Centre (aurrerantzean, BCSC) ekimena SPRI-Enpresa Garapenerako Euskal Agentziaren (aurrerantzean, SPRI) barruan dago, eta Eusko Jaurlaritzako Ekonomiaren Garapen eta Azpiegitura Sailaren mende dago. Euskadiko herritarren, enpresen eta erakunde publikoen zibersegurtasuna eta konfiantza digitala garatzeko erreferentziazko erakundea da BCSC, batez ere eskualdeko ekonomiaren sektore estrategikoentzat.

BCSC Eusko Jaurlaritzaren tresna bat da euskal gizartean zibersegurtasunaren kultura handitzeko, eta zerbitzu espezializatuen eskaintzaileen eta eskatzaileen arteko topagune izan nahi du. Horrela, berrikuntzarako aukera sortzen da, enpresen lehiakortasuna sustatzen da eta herritarrek jarduera digital seguruagoa izateko ohiturak gara ditzaten errazten da.

Helburuak lortzeko, BCSC zeharkako ekimena da, eta hasieratik Eusko Jaurlaritzako lau sailek hartzen dute parte: ekonomiaren Garapen eta Azpiegitura Sailak, Segurtasun Sailak, Gobernantza Publiko eta Autogobernu Sailak eta Hezkuntza Sailak. Jarduera horretan sartzen dira ikerketa-proiektuak, ekintzailetza-ekimenak eta estatuko eta nazioarteko beste eragile eskudun batzuekin koordinatutako lankidetza. Izan ere, Zientzia, Teknologia eta Berrikuntzaren Euskal Sareko eragileekin lankidetza estuan lan egiten da. Eragile horiek Batzorde Iraunkorreko kide dira.

Beraz, BCSCren misioa da euskal gizartean zibersegurtasuna sustatzea eta garatzea, Euskadiko enpresa-jarduera dinamizatzea eta erreferente izango den sektore profesional bat sortzea ahalbidetzea. Testuinguru horretan, berrikuntza teknologikoaren, ikerketaren eta fabrikazio aurreratuko industriara eta beste sektore batzuetara transferentzia teknologikoaren arloetan eragile osagarrien arteko lankidetza-proiektuak gauzatzea bultzatzen da.

BCSCk hainbat zerbitzu eskaintzen ditu Gertakariei Erantzuteko Talde gisa (aurrerantzean, CERT, ingelesezko siglengatik "Computer Emergency Response Team"), eta Euskal Autonomia Erkidegoan lan egiten du, mehatxu berriak goiz detektatzeko eta ohartarazteko gaitasuna handitzeko, informazioaren segurtasun-gorabeherei erantzuteko eta aztertzeko, eta euskal gizartearen beharrei erantzuteko prebentzio-neurriak diseinatzeko.

2. KONTRATAZIOAREN XEDEA

Kontratuaren xedea zibersegurtasuneko gorabeherei erantzuteko zerbitzu bati dagokio. Zerbitzu horrek aholkularitza eskainiko die Zibersegurtasuneko Euskal Zentroaren (aurrerantzean, BCSC) xede-publiko guztiei, horretarako ezarritako bideen bidez.

Gaur egun, honako hauek dira zentroaren publiko objektiboak: erakunde pribatuak zein publikoak, eta herritarrak.

3. BETEKIZUN TEKNIKOAK

3.1 OHARRAK

Atal honetan kontratuaren xedea osatzen duten eta esleipendunak eman beharko dituen ezaugarri teknikoak deskribatzen dira. Zerrenda ez da kontratatutako zerbitzuaren ezaugarrien zerrenda zehatza, BCSCk eskatutako jarduera orokorrak baizik, egin beharreko zereginen alderdiak eta espero diren emaitzak estaliz.

Baldintza horiek gutxienekotzat hartu behar dira (kontrakorik adierazi ezean), eta lizitatzaileek eskaintzak luzatu ahal izango dituzte.

Lizitatzaileak proiektuaren emaitza optimoa ziurtatzeko erabiliko dituen ezagutzak, metodologiak, tresnak eta giza taldea aurkeztu eta deskribatu beharko ditu.

4. EGIN BEHARREKO LANEN DESKRIBAPENA

4.1. Aholkularitza eta gertakariei erantzutea

Gaur egun, gorabeherak jakinarazteko bide hauek daude gaituta, eta zerbitzuaren esleipendunak erantzungo ditu:

- **Postontziak:** Postontzi bat, zibersegurtasuneko gorabeherak sartzeko bide nagusia (incidencias@bcsc.eus).
- **Telefono bidezko arreta**: 900 104 891 telefonoaren bidez.
- **Bilaketa proaktiboa:** 3.2.2 atalean zehazten da jarduera: balizko mehatxu eta arriskuen bilaketa proaktiboa.

Behin gertakariak jasota, emailen kasuetan, modu automatikoan prozesatuko dira ticketing tresnan; horrek berehalako erantzun automatikoa bidali beharko dio igorleei, jaso izanaren adierazpen gisa esleitutako identifikatzailea adieraziz. Deien kasuan, 1. mailako talde teknikoak tresnan erregistratuko ditu, eta, kasu bietan, aztertu eta CCN-STIC 817 gidan jasota dagoen eta BCSCk erabiltzen duen taxonomian oinarrituz sailkatuko ditu, eta aholkularitza emango da, jakinarazi duen pertsona edo entitatea laguntzeko egokienak diren jarduketa-jarraibideak emanez. Era berean, dagokion

kasuetan arriskua arindu / desegiteko beharrezkoak diren jakinarazpen- eta koordinazio-lanak egingo dira, eta, azkenik, jarraipena egingo da, horien eraginkortasun-maila zehazteko.

Anali xehatuagoa behar bada edo nola jardun argi ez badago, 1. mailako talde teknikoak esperientzia gehiago duen 2. mailako talde tekniko bati bidaliko dio, eta, azkenik, beharrezkoa bada, BCSCren talde teknikoari aholkularitza eskatuko zaio.

Ondoren, 2022an kudeatutako gertakarien tipologiak adierazten dira:

Tipologia	Ehunekoa
I	% 55,63
Eduki neurrigabekoa	% 16,83
Bidegabe sartzea	% 11,26
Bidegabe sartzeko saiakera	% 4,66
Programa gaiztoak	% 3,41
Sistema zaurgarriak	% 2,27
Erabilgarritasuna	% 1,25
Informazioaren segurtasuna	% 1,25
Informazioa eskuratzea	% 0,68
Bestelakoak	% 2,73

Zerbitzua etengabe hobetzen jarraitzeko, **zerbitzuaren esleipendunak aldizka berrikusi eta eguneratuko ditu zerbitzuaren ezagutzari buruzko datu-basea eta zerbitzuaren operatiboa, baita honako hauen arabera jarraitu beharreko prozedurak: jasotako gertakariaren mota (playbook-ak), bidalitako prozedura, larrialdi-protokoloa aktibatzeko prozedura, behin adostuta emaitzen ereduak, etab. BCSCk horretarako sarbidea emango du.**

Zerbitzuaren operatiboan adierazten den bezala, **2 eragiketa-maila** aurreikusten dira:

- 1. mailak egin beharreko zereginak:
  - BCSCk zerbitzurako gaitutako kanalei erantzutea.
  - Gertakariak ticketing tresnan erregistratzea, dagokien kategorizazioaren arabera.
  - Gorabeherak aztertzea eta erantzun egoki bat prestatzea, ezagutzaren datu-basea laguntza gisa erabiliz. Erantzun horren helburua izango da zibersegurtasunari buruzko prebentzioari eta erantzunari buruz

aholkatzea.

- Egiaztapen eta azterketa egokiak egitea mehatxua arindu / konpontzeko.
- Jakinarazpen egokiak egitea mehatxua arindu / konpontzeko.
- Gertakarien jarraipena egitea.
- Erantzun egokia nola eman ez jakitean, gertakariak 2. mailako taldeari bidaltzea.
- 2. mailarekin koordinazio-maila handia izatea.
- Istripuak ticketing tresnan ixtea, konpondu ondoren.

- 2. mailak egin beharreko zereginak:
  - 1. mailak bidalitako gertakarietan aholkatzea eta horiek konpontzea.
  - 1. mailarekin koordinazio-maila handia izatea.
  - 1. mailak egiten duen gertakarien kudeaketa berrikustea eta horren kalitatea ebaluatu eta hobetzeko aldeak zehaztea.
  - 1. mailan prestatzea, zerbitzua ematean bikaintasun-maila handia mantentzeko beharrezkoa denean.
  - Erantzun egokia nola eman ez jakitean, gertakariak BCSCri bidaltzea.
  - Zibersegurtasuneko gertakarietatik eratorri litezkeen mehatxu eta arriskuak modu proaktiboan bilatzeko taldeari laguntza ematea.
  - BCSCrekin koordinazio-maila handia izatea.
- 1. eta 2. mailen gainetik zerbitzuaren koordinatzaile teknikoa dago, eta honako eginkizun hauek beteko ditu:
  - Etengabe eta ikuspuntu teknikotik emandako zerbitzuaren kalitatea eta erabilgarritasuna ebaluatzea.
  - Zerbitzua zuzendu eta hobetzeko ekintzak proposatzea eta horien jarraipena egitea.
  - Ezagutzaren datu-basea eguneratuta mantentzea; horrek prozedurak, playbook-ak, txantiloiak, etab. garatzea dakar.
  - 1. eta 2. mailaren arteko koordinazioa, barneko eta kanpoko bezeroentzat zerbitzua modu eraginkor eta antolatuan emateko.
  - Zibersegurtasuneko gertakarietatik eratorri litezkeen mehatxu eta arriskuak modu proaktiboan bilatzeko taldeari laguntza ematea.
  - BCSCaren eta 1. eta 2. mailako talde teknikoen arteko bitartekaria izatea.

Noizean behin, aholkularitza-lanak eta gertakerei erantzuteko lanak egiten dituen Gehienez 3 jarduera egingo dira urtean.

Hilabete batean zehar erregistratu eta kontratuaren xede izan daitezkeen gertakarien

- Utzitako balioa BCSCk agiri honetan parte hartu ahal izateko eskatzen duen gutxienekoa da, esleipendunak gertatzen den gorabehera orori erantzuteko duen betebeharraren kaltetan izan gabe.

- Hilabete bakoitzean benetan kudeatutako eskaeren kopuruak ez du eraginik izango fakturazioan.
- Hilabete batean zehar gutxieneko eskaera kopurua gainditzen bada, zerbitzu-mailako akordioen etendura hartuko da kontuan, testuingurua aztertu ondoren.

Horrela, ziurtatu behar den gaitasuna (konprometitutako hileko gutxieneko intzidenteen kopurua) **250 gertakarietakoa da**; nolanahi ere, adierazi den bezala, gutxi gorabeherako kopurua da, eta esleipendunak kopuru hori gainditzen duen gertakari orori erantzun behar dio. Kopuru txikiagoa konprometitzen duten eskaintzaileak lizitaziotik kanpo geratuko dira, baldintza-agiriko funtsezko gutxieneko baldintza hori delako. Zenbatetsi da urtero gutxienez % 25eko igoera dagoela gertakarien kopuruan.

Kontratistak egungo kopurua kudeatzeko azpiegitura bat izan beharko du, harremanetarako telefonoaren deiak erantzuteko, elkarrizketak grabatzeko, grabatutako lokuzioak erreproduzitzeko, testu-mezuak bidaltzeko eta zerbitzuaren gogobetetzea ebaluatzeko inkestak egiteko gaitasunarekin, bai eta gertakariak erregistratzeko plataforma bat ere, egungo datu-basea inportatu ahal izateko; zeregin hori zerbitzua hasi bezain laster egingo da. Era berean, plataformak aukera emango du informazioa esportatzeko; izan ere, zerbitzuan zehar, BCSCk gertakariak kudeatzeko ezartzen duen tresnara migratuko da.

Zerbitzua 24x7 formatuan eta formatu elebidunean eskainiko da: euskaraz eta gaztelaniaz, 5. atalean zehaztutako zerbitzu-mailari buruzko akordioa betez. Zerbitzuko dokumentu guztiak BCSCren erakunde-nortasunaren eskuliburuaren arabera egingo dira, bere markarekin.

4.2. Larrialdietarako / alertetarako protokoloa aktibatzea

Zerbitzuaren esleipendunak 4.1. atalean (Aholkularitza eta gertakariei erantzutea) deskribatutako zereginak egiteko aurkeztutako talde teknikoak, BCSCk eskatuta, larrialdiko/alertako protokoloa aktibatuko du hala eskatzen duten egoerei erantzuteko. Ildo horretan, testu-mezuak bidaliko dira edo, dagokionaren arabera, BCSCk zehaztutako harremanetarako guneetara deituko da, protokolo hori aktibatu dela jakinarazteko, eta egoera horri erantzuteko behar diren jakinarazpen guztiak egingo dira. Erabili beharreko plataforma eta horren funtzionalitate nagusiak adierazi beharko dira. Zerbitzua 4.1. Aholkularitza eta gertakariei erantzuteko zerbitzuaren 24x7 formatu berean eskainiko da.

4.3. Zibersegurtasuneko gertakarietatik eratorri litezkeen mehatxu eta arriskuak modu proaktiboan bilatzeko taldea

Zerbitzua 8x5 formatuan eskainiko da, eta zibersegurtasuneko gertakari posibleak modu Ildo horretan, honako zeregin hauek egitea aurreikusten da:

- **Automatizazioa eta orkestrazioa:** BCSCren adimen-eredua etengabe hobetzea dakar, intzidenteak modu proaktiboan eta erreaktiboan detektatzeko gaitasunak etengabe hobetzeko.
    - Zereginak:

- Linux zerbitzarien kudeaketa.
- ELK-a mantentzea.
- Adimen-ereduaren bilakaeran laguntzea: analisia, erabiltze-kasuen diseinu eta inplementazioa, horiek eguneratzea, hobekuntza-proposamena, inplementazioa, etab.
- Kibanan aginte-koadroak egin eta mantentzea, Euskadin zibersegurtasunaren egoerari buruzko adierazleekin.
- Monitorizazio-, analisi- eta abar-tresnak zabaltzea, konfiguratzea eta mantentzea.
- Hainbat zerbitzutako HJA ugarirekin elkarreragitea, hala nola Shodan, Zoomeye, Phishtank, MISP, OTX, Minemeld, etab.
- Neurriko scriptak garatzea.
- Interfazeak diseinatzea.
- Dokumentazio teknikoa egin eta eguneratzea, hala nola erabilera-kasuenak eta jarduteko prozedurenak.
- BCSCko CERTak eskaintzen dituen zerbitzuei laguntzea.

- **Identifikazio proaktiboa eta arreta goiztiarra:** BSC adimenaren etengabeko ustiapena dakar, zibersegurtasuneko gertakariak modu proaktiboan identifikatzeko, bai eta gertakari potentzialak ekar ditzaketen arriskuak ere. Gertakari horiek zerbitzuaren esleipendunak emandako talde teknikora bidaliko dira, 4.1 atalean (aholkularitza eta gertakariei erantzuna) deskribatutako zereginak egiteko, dagokion arintze edo konponbidea emateko neurri egokiak har ditzaten.
  - Zereginak:
    - BCSCren adimen-ereduari dagozkion tresnekin elkarreragitea, informazioa ustiatzeko, gertakariak identifikatze aldera.
    - Honako hauek aztertzea, argitaratzea eta zabaltzea:
      - abisuen eta alerten jakinarazpenak.
      - segurtasun-buletinak.
      - hirugarrenek pairatutako zibersegurtasuneko gertakariei buruzko txostenak.
      - adimen-ereduaren informazioan oinarritutako txostenak.
    - Mitre ATT&CKen frameworkaren bidez mehatxuak eta erasoak identifikatzea.
    - Gertakarietara aurreratzeko, horiek detektatzeko eta horiei erantzuteko eragin daitekeen adimena lantzea: yara, snort, sigma eta abarren arauak.
    - Mehatxuei buruzko informazio partekatzeko tresnak elikatzea.

- Dokumentazio teknikoa eta jarduketa-prozedurak egitea eta eguneratzea.
- BCSCko CERTak eskaintzen dituen zerbitzuei laguntzea.

4.4. Zibersegurtasuneko gertakariak prebenitzen eta horiei aurre egiten lagunduko duten materialak sortzea

Lehen adierazitako zereginetan oinarrituta, esleipendunak mehatxuei, malware-familiei, ahultasunei eta abarri buruzko txosten teknikoak proposatu, ikertu eta egingo ditu, horien alerta goiztiarra egiteko. Txostenak euskaraz eta gaztelaniaz egingo dira, BCSCren identitate korporatiboari buruzko eskuliburua jarraituz.

2 txosten mota egitea aurreikusten da:

- *Bakunak:* eskuarki, ahulezien edo mehatxuen analisiari dagozkio, ikuspegi orokor batetik. Modu proaktiboan eta eskaeraren arabera egingo dira, eta 3 edo 4 orduko dedikazioa izango dute. Urtean mota horretako 35 txosten egitea aurreikusten da.
- Konplexuak: Malware-familien, aktore maltzurren eta abarren analisiari dagokio, haien portaerari, hedapenari, arintze-neurriei eta abarri buruzko ikuspegi zehatz batekin. Azterketa hori erreaktiboa izango da, BCSCk eskatuta, eta urtean mota horretako 14 txosten egitea aurreikusten da. Hortaz, hilean behin egingo dira, eta 2 azterketa gehigarri aurreikusten dira ziklotik kanpo, ezohiko egoeretarako.

Baliozkotu ondoren, esleipendunak BCSCren webgunean argitaratuko ditu txostenak. Bi motetako txostenen adibideak kontsulta daitezke zentroaren webgunean.

5. Zerbitzu-mailari buruzko akordioa

Lizitatzaileak konpromisoa hartuko du 4.1 zerbitzuak (aholkularitza eta gertakariei erantzutea) eta 4.2 zerbitzuak (larrialdi-/alerta-protokoloa aktibatzea) 24x7 ereduaren arabera ematen direla bermatzeko, ondoren zehazten diren gutxieneko mailekin.

Kodea	Deskribapena	Xede-balioa	Gutxieneko betetze-ehunekoa
1	Erantzute-denbora. Ez da kasuaren identifikatzailearen esleipenaren eta hartu-agiriaren hasierako erantzuna (automatikoa izan behar du), baizik eta hasierako aholkularitza eskaintzen den lekua.	2 ordu	% 95
2	Larrialdi-protokoloa aktibatzea eta bidalketan identifikatutako pertsona guztiekin harremanetan	30 minutu	% 100

	jartzea		

Lizitatzaileak konpromisoa hartzen du 4.1 zeregina (aholkularitza eta gertakariei erantzutea) emateko kalitatearen jarraipena egiteko konpromisoa hartzen du. Horretarako, hilero jakinaraziko ditu zerbitzuaren kalitate-adierazleak, taula honen arabera egindako akatsak zenbatuta lortuko dituenak:

Maila	Motak
Baxua	Soil barne-mailan eragiten duten eta erraz konpondu ahal diren akatsak. Gertakaria txarto sailkatzea. Osatu gabeko esparruak dituen gertakaria. Akatsak eragin txikia dauka edo ez dauka eraginik. Bidaltzea ez dago justifikatuta.
Ertaina	Barne-eremura mugatzen ez diren ondorioak dituzten akatsak, hirugarrenei eragiten baitiete. BCSCk egindako informazio-eskaerak, informazio hori dagoeneko eman bada edo eskuragarri badago datu-base ezagun batean. Gomendio errepikakorrak edo ez-aplikagarriak, edo kontsultarekin zerikusia ez dutenak bidaltzea. Erantzuna txantiloi lehenetsiarekin bidaltzea, dituen iruzkinak ezabatu gabe edo informazioa eguneratu gabe. Erantzunean akats ortotipografikoak edo gramatikalak egotea.
Altua	Informazio konfidentziala bidaltzea hartzaile okerrei. Baja-eskaera egitea sistema legitimoetan. Kudeaketa-akatsak, baldin eta kanpoko ondorioak badituzte eta hirugarrenei kalte handiak eragiteko gaitasuna badute. Guztiz okerrak diren eskaerak edo gomendioak bidaltzea. Kudeaketa okerraren ondoriozko kexa justifikatua. Positibo faltsuen jakinarazpenak erakunde ordezkagarriei.

Ebaluazio horren ondorio gisa, zerbitzua ematea aurreikusten da, gutxieneko maila hauen arabera:

Kodea	Deskribapena	Xedearen betetze-ehunekoa	Gutxieneko betetze-ehunekoa
3	Maila baxuko akatsak	% 90	% 75

4	Maila ertaineko akatsak	% 90	% 75
5	Maila altuko akatsak	% 100	% 95

Lizitatzaileak konpromisoa hartzen du 4.4. zerbitzua (Zibersegurtasuneko gertakariak prebenitzen eta horiei aurre egiten lagunduko duten materialak sortzea) jarraian zehazten diren gutxieneko mailen arabera zehazten dira.

Kodea	Deskribapena	Xede-balioa	Gutxieneko betetze-ehunekoa
6	Txosten bakunak egitea eta entregatzea	3 ordu	% 90
7	Txosten konplexuak egitea eta entregatzea	21 egun	% 100

Kode bakoitzari aplikatu beharreko zigorraren zenbatekoa metagarria izango da. Hartara, kalkulurako oinarri gisa hartu da hileko fakturazioari dagokion zenbatekoa.

SPRIk jarraian deskribatzen den zigor-eredua aplikatzeko gaitasuna gordetzen du. Zigorraren zenbatekoa proportzionala izango da ez-betetzearen larritasunarekiko eta ezingo da izan kontratuaren esleipendunaren prezioaren % 10 baino handiagoa:

- 1. kodea
  - Betetzea >= % 95: Zigorrik gabe.
  - % 95 > Betetzea >= % 80: Hileko fakturazioaren % 1eko zigorra.
  - Betetzea < % 70 Hileko fakturazioaren % 3ko zigorra.
  - Adierazle horretan lehenengo arau-hausteak ez du zigorrik jasoko; ohartarazpena erregistratuko da, hurrengo hilabeteetan zigorren eredua aktibatuko duena.
  - Zigorra aktibatzeko behar diren mota horretako gutxieneko eskaerak: 10 eskaera.
- 2. kodea.
  - % 100 > Betetzea: Hileko fakturazioaren % 10eko zigorra ezarritako epean erantzun gabeko eskaera bakoitzeko.
  - Zigorra aktibatzeko behar diren mota horretako gutxieneko eskaerak: 1 eskaera.
- 3. kodea.
  - Betetzea >= % 75: Zigorrik gabe.
  - % 75 > Betetzea >= % 70: Hileko fakturazioaren % 1eko zigorra.
  - Betetzea < % 70 Hileko fakturazioaren % 3ko zigorra.
  - Adierazle horretan lehenengo arau-hausteak ez du zigorrik jasoko; ohartarazpena erregistratuko da, hurrengo hilabeteetan zigorren eredua aktibatuko duena.

- Zigorra aktibatzeko behar diren mota horretako gutxieneko eskaerak: 10 hutsegite.

- 4. kodea.
  - Betetzea >= % 75: Zigorrik gabe.
  - % 75 > Betetzea >= % 70: Hileko fakturazioaren % 1eko zigorra.
  - Betetzea Hileko fakturazioaren % 3ko zigorra.
  - Adierazle horretan lehenengo arau-hausteak ez du zigorrik jasoko; ohartarazpena erregistratuko da, hurrengo hilabeteetan zigorren eredua aktibatuko duena.
  - Zigorra aktibatzeko behar diren mota horretako gutxieneko eskaerak: 10 hutsegite.
- 5. kodea.
  - Betetzea >= % 95: Zigorrik gabe.
  - % 95 > Betetzea >= % 90: Hileko fakturazioaren % 2ko zigorra.
  - Betetzea < % 90 Hileko fakturazioaren % 5eko zigorra.
  - Zigorra aktibatzeko behar diren mota horretako gutxieneko eskaerak: 1 hutsegite.
- 6. kodea.
  - Betetzea < % 90 Hileko fakturazioaren % 1eko zigorra ezarritako epean erantzun gabeko eskaera bakoitzeko.
  - Zigorra aktibatzeko behar diren mota horretako gutxieneko eskaerak: 3 eskaera.
- 7. kodea.
  - Betetzea < % 100 Hileko fakturazioaren % 1eko zigorra ezarritako epean erantzun gabeko eskaera bakoitzeko.
  - Zigorra aktibatzeko behar diren mota horretako gutxieneko eskaerak: 3 eskaera.

Adierazle horretan 1., 3., 6. eta 7. kodeak ez betetzeak ez du zigorrik jasoko; ohartarazpena erregistratuko da, hurrengo hilabeteetan zigorren eredua aktibatuko duena.

2., 4. eta 5. kodeei dagokionez, idatzizko hirugarren jakinarazpenaren ondoren kontratua gaizki ematen jarraitzen bada edo berriz gertatzen bada, kontratazio-organoak kontratua suntsiarazi dezake.

6. Gertakarien jakinarazpena

Zerbitzuaren eta eskura dauden datuen izaera sentikorra dela eta, esleipendunak detektatzen badu kontratuaren xede diren zerbitzuen emakidan inpaktua edo eragina izan ahal duen zibersegurtasuneko eragin bat, gertakaria berehala jakinarazi beharko dio kontratuaren arduradun gisa izendatutako BCSCko pertsonari.

Era berean, BCSCk gertakari horri buruzko informazio zehatza eskatu ahalko dio kontratistari; informazio hori behar bezala kudeatuko da, «need to know» politikari

jarraituz. Zabaltze kontrolatua behar izatekotan, horretarako aldez aurreko baimena eskatuko da.

7. Metodologia eta lan-plangintza

Lizitatzaileak proposamen bat egin beharko du, **metodologia, lan-plana eta kronograma jasoko dituena, eta zerbitzuaren mugarri garrantzitsuenak adieraziko ditu, data eta zerbitzua emateko erabilitako tresnak eta guzti**.

Metodologiak halabeharrez honako alderdi hauek jaso beharko ditu:

- **Zerbitzua emateko operatibo orokorra, honako hauek barne hartuta:**
  - **Hasierako fasea:** zerbitzuaren ezarpena, prestakuntza eta martxan jartzea. Hasierako epe bat aurreikusi ahal da deien plataforma eta ticketing-tresna ezartzeko; lantaldeari prestakuntza espezifikoa emateko; egungo eragiketak, playbook-ak, txantiloiak eta abar berrikusteko eta eguneratzeko. Epe hori gehienez ere 4 astekoa izango da.
  - **Zerbitzuaren jarraipena:** hilero, kontratistak zerbitzuaren jarraipen-txosten bat entregatuko du, eta bilera bat egingo da, zerbitzuaren jarduna ebaluatzeko eta hobekuntza-puntuak identifikatzeko. Kontratistak, zerbitzuaren aurreko txostenetan oinarrituta, txosten-proposamen bat egingo du, eta BCSCk baliozkotze-prozesu bat gainditu beharko du. Proposamen horrek 5. atalari (zerbitzu-mailako akordioa) dagozkion metrika espezifikoak gehituko ditu.
  - **Proiektua ixteko eta itzultzeko fasea:** proiektua amaitzean, kontratistak amaierako memoria bat aurkeztu beharko du, egindako lanen benetako irismena justifikatzeko txosten gisa balioko duena, eta alderdi hauek jasoko dituena, besteak beste: entregagaien xehetasuna, kontsumitutako baliabideak, lortutako helburuak eta mugarriak, eta hurrengo hilabeteetan zerbitzuan lortu beharreko jardueren eta helburuen gomendioen proposamena. Halaber, kudeatutako gertakariei buruzko ticketing-tresnaren informazio guztia entregatu beharko du, baita zerbitzuaren irismenaren barruan egindako informazio guztia ere, eta bermatu beharko du bere ekipo informatikoetan egon daitezkeen fitxategi guztiak ezabatzen direla, baldin eta edozein datu pertsonal badute.
- **Zerbitzuaren barruan jasotako ataza bakoitzaren deskribapena eta xehetasuna.**
- **Zerbitzu-mailari buruzko akordioa betetzen dela bermatzea.**
- **Zerbitzuaren etengabeko hobekuntza:**
  - **Kontingentzia-plan** bat eskatzen da, gutxieneko zerbitzua bermatzeko ahots- eta datu-komunikazioek eta sistema informatiko nagusiek huts egiten badute, edo langileak ordezkatuz gero. Zerbitzuaren prestazioari

eragiten dion edozein gertakari garrantzitsu berehala jakinarazi beharko zaio BCSCri, eta zerbitzuaren jarduera jakinarazteko hileroko txostenetan jaso beharko da.

- Zerbitzuaren **etengabeko hobekuntzarako plan** bat eskatzen da. Plan horrek lizitatzaileak zerbitzuaren bikaintasun-maila lortzen eta mantentzen lagunduko duten zenbait neurri aurreikusiko ditu. Neurri horiek, adibidez, honako hauek izan ahalko dira: posta elektronikoz, telefonoz eta abarrez kudeatutako gertakarien proba-deiak, analisiak eta ausazko ebaluazioa egitea.
- Era berean, zerbitzua ematen duen taldearentzat etengabeko **prestakuntza-plan** bat sartzea aurreikusten da, **zerbitzuaren hasieran eta hori ematen den bitartean** hainbat prestakuntza-ekintza jasoko dituena. Plan hori bereziki oinarritu behar da 4.1 jarduera (aholkularitza eta gertakariei erantzutea) egiten duen taldean, bai eta 4.3 jarduera (zibersegurtasun arloko gertakariak eragin ditzaketen mehatxu eta arrisku potentzialen bilaketa proaktiboa) egiten duen taldean ere**, eta bereziki garrantzitsua da azken hori. Horretarako, gutxienez 4 prestakuntza-ekintzaren ebidentziak aurkeztu beharko dira urtero, eta ez da barne-prestakuntzarik jasoko horretarako**.
- Azkenik, zerbitzua ematen duen plantillan aldaketarik egonez gero, **ordezkapen-plan** bat sartzea aurreikusten da. Hori bereziki garrantzitsua da 3.2.3 jarduera (zibersegurtasun arloko gertakariak eragin ditzaketen mehatxu eta arrisku potentzialen bilaketa proaktiboa) egiten duen taldearen kasuan.

8. Lantaldea

Enpresa esleipendunak etengabe esleituko dio proiektuari giza talde bat, 4. atalean (egin beharreko lanen deskribapena) deskribatutako lanez arduratuko dena. Lantaldea langile egokiz osatuta egongo da, eta zerbitzuaren xede diren zereginetan esperientzia izango dute. Alde horretatik, eskaintzaileek kontratua gauzatzeko erabilgarri dagoen **lantaldea zehaztu beharko dute**, eta baliabide bakoitzerako profil eta talde operatiboa adierazi beharko dute, bai eta **antzeko jardueretan izandako esperientzia ere**, zerbitzua behar bezala ematen dela ziurtatzeko.

Zereginetarako proposatutako **lantaldearen rolak eta erantzukizunak adierazi beharko dira**.

Proiektu hau gauzatzeko izendatutako langileei eskatu beharreko baldintzak eta gaitasunak hauek dira:

- **Proiektuaren arduraduna:** proiektuaren arduradun nagusia izango den pertsona bat izendatzea, horrelako lanetan behar besteko ezagutza eta esperientzia izango duena. Hala, ezinbestekoa izango da, zerbitzua emateko prestasuna eta arintasuna direla eta, Vitoria-Gasteizko 120 km-tik beherako erradioan dagoen lantoki batetik egitea. Langile horrek honako lan hauek egingo ditu nagusiki:
  - BCSCk izendatutako pertsona gisa aritzea.

- Jarraipen-txostenak egitea.
- Zerbitzuaren jarraipen-aktak egitea.
- SLAen ez-betetzeen berri ematea.
- Zerbitzuaren prestazio egokiari eragiten dion edozein gertakariren berri ematea.
- Etengabeko hobekuntza eta zerbitzuaren kalitatea zaintzea.

Gaitasunak eta esperientzia adierazi behar dira.

- **Zerbitzuaren koordinatzaile teknikoa:** zerbitzuaren kalitatea alderdi teknikoei dagokienez ebaluatuko duen pertsona bat izendatzea. Pertsona horrek hobekuntza esparruak proposatuko ditu eta lotura teknikoa izango da 1. eta 2. mailekin. Ezagutza eta esperientzia adieraziko dira, eta, gutxienez, 3 urteko esperientzia izan beharko da zibersegurtasuneko gorabeherak kudeatzen. Horrez gain, zerbitzua emateko prestasuna eta arintasuna direla eta, Vitoria-Gasteizko 120 km-tik beherako erradioan dagoen lantoki batetik egitea.
- **Gertakariei erantzuteko 1. mailako taldea:** langile elebidunak (euskaraz eta gaztelaniaz), ingeleseko oinarrizko gaitasuna dutenak, erabiltzaileei arreta ematearekin lotutako zereginetan esperientzia dutenak eta 3.2.1 atalean deskribatutako zereginetan esperientzia dutenak (aholkularitza eta gertakariei erantzutea). Horrez gain, zerbitzua emateko prestasuna eta arintasuna direla eta, Vitoria-Gasteizko 120 km-tik beherako erradioan dagoen lantoki batetik egitea. Zerbitzuari esleitutako profilak adierazi behar dira, baita kontratuaren xedean duten esperientzia eta hizkuntza-gaitasunak ere.
- **Gertakariei erantzuteko 2. mailako taldea:** 3.2.1 atalean deskribatutako zereginetan esperientzia handia duten langileak (aholkularitza eta gertakariei erantzutea). Zerbitzuari esleitutako profilak adierazi behar dira, baita kontratuaren xede diren zereginetan duten esperientzia ere.
- **Mehatxu eta arriskuen bilaketa proaktiboaz arduratzen den taldea:** zerbitzuaren esleipendunak bi baliabide erabiliko ditu 3.2.3 atalean zehaztutako zereginak egiteko, hau da, mehatxu eta arrisku potentzialen bilaketa proaktiboa egiteko. Bien gaitasunak eta esperientzia adierazi behar dira.
    - Baliabide batek automatizazio- eta orkestrazio-zereginetara bideratutako profil bat izan behar du. Profil horrek gutxienez 2 urteko esperientzia izan behar du ELK kudeatzen, APIen erabileraren, interfazeen diseinuaren, datu-baseen eta abarren arloko garapen-zereginetan, eta esperientzia izan behar du Linuxen, Bash eta Python programazioan, node.js, elk eta antzeko teknologietan.
    - Identifikazio proaktiboan eta alerta goiztiarrean deskribatutako zereginetarako dedikazio esklusiboa duten bi profil. Gutxienez 2 urteko esperientzia izan beharko dute zibersegurtasuneko mehatxuen adimen-modeloen informazioa ustiatzen; yara, snort eta sigma arauen bidez eragin daitekeen adimena garatzen, mehatxuak mitre att&ck bidez

bereizten, mehatxuak aztertzen eta alerta goiztiarreko edukia egiten (hala nola abisuak, alertak eta txostenak), playbook-ak egiten, etab.

Aurreko informazioarekin batera, EquipoTrabajo.xlsx. taula aurkeztu beharko da

GARRANTZITSUA: Proiektuaren arduradunaren ziurtagiriak bakarrik adieraziko dira, eta proiektuen kudeaketarekin zerikusia dutenak soilik.

4.1 atalean (aholkularitza eta gorabeherei erantzutea), 4..2 atalean (larrialdi-/alerta-protokoloa aktibatzea) eta 4.4 atalean (zibersegurtasuneko gertakariak prebenitzen eta horiei aurre egiten lagunduko duten materialak sortzea) deskribatutako zereginak egiten dituzten pertsonen lantokia enpresa esleipendunaren bulegoak eta instalazioak izango dira, eta VPN urrutiko konexioa izango dute BCSCren azpiegitura informatikoarekin, lanak egiteko beharrezkoa dena, eta horren bidez erregistratuko dira eskaerak eta horien xehetasuna.

4.3 atalean (Zibersegurtasuneko gertakariak eragin ditzaketen mehatxu eta arrisku potentzialen bilaketa proaktiboa) deskribatutako zereginak egiten dituzten pertsonen lantokia BCSCren bulegoak eta instalazioak izan daitezke, erakunde kontratatzaileak hala erabakitzen badu, lan egin behar den informazioaren izaera sentikorra dela eta. Horregatik guztiagatik, proposatutako lantaldeak dimentsionatuta eta prestatuta egon beharko du, eta beharrezko baliabideak izan beharko ditu BCSCren instalazio horietan kontratua normaltasun osoz gauzatzeko.

Lanak gauzatzeko kontratua formalizatu ondoren sartu beharreko lantaldeak esleipendunaren eskaintzan zehaztutakoa izan beharko du, eta horren arabera baloratu beharko da.

Proiektuko taldeak garatutako lanak zuzenean gainbegiratuko dituzte BCSCko langileek, eta egoki iritzitako azalpenak eta informazioak eskatu ahal izango dituzte kontratatutako lanak behar bezala egiten direla egiaztatzeko.