

PRESKIPZIO TEKNIKO PARTIKULARREN BALDINTZA AGIRIA, GIPUZKOAKO MAKINA-ERREMINTAREN SEKTOREKO PRODUKTU INDUSTRIALAK EBALUATZEKO ETA ETORKIZUNeko ZIBERSEGURTASUN ZIURTAGIRIA SORTZEKO (ZIUR2023-02 ESPEDIENTEA)

I.- PRESKIPZIO TEKNIKOEN BALDINTZA AGIRIAREN TESTUINGURUA

Baldintza agiri honen xedea da, Sektore Publikoko Kontratuei buruzko 9/2017 Legearen 124. artikulua zehazten duenari jarraikiz, prestazioak emateko prozesua arautuko duten preskripzio tekniko bereziak definitzea, horien irismen objektiboa zehaztuz, bai eta aholkularitza zerbitzua emateko kontuan hartu beharko diren gutxieneko betekizun eta baldintza tekniko orokorrak ezartzea ere.

II.- ZERBITZUAREN XEDEA ETA IRISMENA

Proiektu honen bidez, ZIURek ebaluaziora bideraturiko ekimen bat garatu nahi du, etorkizunean produktu industrial ziberseguruaren ziurtagiri bat sortu ahal izateko. Horretarako, ZIURek *metodologia* bat definitu du, eta, haren bidez, IEC 62443 arauaren arabera *ebalatu eta ziurtatu ahal izango dira produktu industrialak*, betiere arau horretako segurtasun baldintzei eta segurtasun maileri jarraikiz.

Metodologia diseinatzeko orduan, funtsezko alderdi hauek hartu dira kontuan:

- *Eskarirako balioa ematea*, eskaintzaren bidez produktuen ziurtapena sustatzeko.
- *Metodologia fidagarria* izatea, lurraldeko ekosistema integratuko duen *elkarlaneko ebaluazio sistema* espezializatu bat sustatuko duena.
- *ZIUR integrazio horren funtsezko elementu gisa posizionatzea*.

Lizitazio honen **xedea** da produktu industrialak ebaluatzeke zerbitzu bat lortzea —bereziki, makina-erremintakoak—. Ebaluazio hori baldintza teknikoen agirian definitutako diren gaitasun teknikoak eta giza gaitasunak dituen laborategi ebaluatzaile batek egingo du, betiere ZIURek zehaztutako metodologiei jarraituz, zeina enpresa lizitatzailen eskura jarriko baita, aldez aurretik berariaz eskatuta, lizitazioaren proposamenak aurkezteko epearen lehen hamabost egunetan berariaz eskatu ondoren.

Laborategi ebaluatzailearekin batera, positiboki baloratuko da —balio-judizioaren bidez baloratu beharreko irizpidearen bidez— enpresa lizitatzailerek aurkeztutako proposamenean jasota egotea ebaluaziorako prestatzeko eta ebaluatutako enpresari laguntzeko zerbitzu bat, enpresa independente batek laborategi ebaluatzaileari eskainia.

Hau da, puntuazio handiagoa emango da baldin eta desberdinak badira prestaketari/laguntzari lotutako zerbitzuak eskaintzen dituen enpresa eta laborategi ebaluatzaileari lotutako zerbitzuak egiten dituenak. Horren helburua da independentziari eustea bi prozesuetan.

Ebaluazioa prestatzeko eta ebaluatutako enpresari laguntzeko fasea eta laborategi ebaluatzaileak egin beharreko fasea enpresa berak eskaintzen baditu, ordea, inplikaturako bi lantaldeek pertsona desberdinez osaturik egon beharko dute.

Hauek dira proiektuaren **helburuak**:

- ZIURek definitutako ebaluazio metodologiari buruzko pilotu bat egitea eta produktu industrialen zibersegurtasuna ebaluatzeko etorkizuneko tresna gisa baliagarria ote den aztertzea.
- Aztertutako industria produktuek zibersegurtasunaren aldetik ageri duten betetze maila eta heldutasuna identifikatzea.
- Lurraldeko enpresa ehunaren industria produktuak ebaluatzeko gaitasunak identifikatzea.
- Makina-erremintaren sektoreari laguntza eskaintzea, merkatuak zibersegurtasunaren arloan eskatuko dizkieten beharrak ezagutzeko, bai eta araudi eskakizunen berri emateko ere.

Proiektuaren emaitza gisa, Gipuzkoako industria enpresek **onura** hauek izango dituzte:

- Gaitasun zientifiko-teknologikoak eta industrialak lerrokatzea.
- Gure industria sarearen lehiakortasuna indartzea.
- Gipuzkoa zibersegurtasun industrialean erreferentzia bihurtzeko urratsak egitea – Produktu Industrialaren Ebaluazioa.

Irismena

Zerbitzuaren barruan, **makina-erremintaren sektoreko 4 enpresa desberdinetako 4 industria produkturen segurtasun ebaluazioa egitea aurreikusten da**, eta hauek dira hasiera batean aurreikusitako faseak:

1. Ebaluazioa prestatu aurreko zerbitzua eskaintzea eta ebaluatutako enpresei laguntzea.
2. Ebaluazio egoeraren dokumentazioa.
3. Produktu eragiketaren parametroak adostea.
4. Egin beharreko probak hautatzea eta ebaluazioak diseinatzea.
5. Aurreko puntuetan egindako probetan lortutako emaitzak aztertzea eta diseinua hobetzeko proposamena egitea.
6. Enpresa bakoitzari laguntzeko zerbitzu teknikoa, konpontze planean proposatutako hobekuntzak ezartzen laguntzeko.

Lizitatzaillearen kontura izango dira zerbitzuari lotutako kostu guztiak, zerbitzutik erator daitezkeen garraioari eta joan-etorriei lotutakoak barne, adibidez:

- **Parte hartzen duten 4 enpresetako langileak laborategi ebaluatzailearen instalazioetara joatea. Lau enpresak Gipuzkoan egongo dira.**
- **Aztertuko diren makinak laborategi ebaluatzaileara garraiatzea parte hartzen duten 4 enpresetatik.**

III.- ZERBITZUAREN DESKRIBAPENA

Atal honetan, kontratuaren xedea osatzen duten eta adjudikaziodunak eman beharko dituen ezaugarri teknikoak deskribatzen dira. Ondoren agertzen den zerrenda ez da kontratatutako zerbitzuaren ezaugarrien zerrenda zehatza, ZIURek eskatutako jarduera orokorrak baizik, betiere barnean harturik egin beharreko zereginen alderdiak eta esperotako emaitzak.

Adjudikaziodunak eskaintzan aurkeztu eta deskribatu beharko ditu proiektuaren emaitza onena ziurtatzeko erabiliko dituen ezagutzak, metodologiak, tresnak eta giza taldea, guztia ere ezaugarrien koadroan eta administrazio klausula partikularren baldintza agiriko klausula orokorretan ezarritako baldintzetan.

Zerbitzuan hainbat eragilek esku hartzea aurreikusten da:

- **Fabrikatzailea.** Ebaluazio prozesuari ekiteko, fabrikatzaileak produktuaren ziurtagiria eskatzen du eta horretarako beharrezko dokumentazioa ematen du. ZIUReko langileek aukeratuko dituzte prozesuan parte hartuko duten lau fabrikatzaileak. IEEC62443 arauan oinarrituta, sakon aztertzen dira produktuaren ezaugarriak eta berezitasunak.
- **Prestatzeko/laguntzeko zerbitzua.** Araudia ebaluazioaren kasu partikularrean doitzen da, eta kontroletan mamitzen da.
- **Laborategi ebaluatzailea.** Laborategi independente batean egiten dira ezarritako saiakuntzak, dagozkion kontrolak betetzen direla egiaztatzeko.

Gorago adierazi den bezala, prestaketarekin/laguntzarekin lotutako zerbitzuak gauzatzen dituen lantaldeak ez du izan behar laborategi ebaluatzailearekin lotutako zerbitzuak eskaintzen dituen. Horren helburua da independentziari eustea bi prozesuetan.

Erreferentzia esparruari eta ebaluazio metodologiari dagokienez, ZIURek definiturik dauka erreferentzia framework bat, ebaluazioak eta testak egiteko, IEC 63443 4-1 eta 62443 4-2 arauetan oinarritua, eta lizitatzaillearen eskura ipintzen du. Horretarako, ziur@ziur.eus helbide elektronikora idatzita egin behar da eskaera, metodologia eta egin beharreko proben berri izateko.

Zibersegurtasun ebaluazioen bidez (*security testing*), baliozkotu nahi da segurtasun kontrolek esperotakoaren arabera funtzionatzen dutela. Segurtasun eskakizunen dokumentutik abiatuta, ebaluatzen da produktu horrek betetzen ote duen zehaztapena dimentsio bakoitzerako. Ebaluazio horiek prozedura bati jarraikiz, errepikatzeko moduan eta kanpoko eragile batek egiaztatuz egiteko, IEC 62443 arauak segurtasun maila batzuk definitzen ditu (*security levels*), baita ebaluatu beharreko praktikak ere.

Adierazi behar da ZIUREk definitutako metodologiak, IEC 62443 arauak bezala, zenbait segurtasun maila ezartzen dituela (SL, *Security Levels*), erasoaren jatorriaren eta izan ditzakeen ondorioen arabera.

- 0 maila: ez da segurtasun babesik behar produktuarentzat.
- 1. segurtasun maila: nahi gabeko gertakarietatik babestu behar da.
- 2. segurtasun maila: nahita gertatutako gertakarietatik babestu behar da, motibazio edo ezagutza txikia duten erasotzaileak saihesteko baliabideekin.
- 3. segurtasun maila: nahita gertatutako gertakarien aurkako babesa eskatzen du, IACS ezagutzak (*Industrial Automation and Control System*) dituzten erasotzaileek egindako erasoetatik babesteko, besteak beste, hacktivistak eta ziberterroristak.
- 4. segurtasun maila: nahita gertatutako gertakarien aurkako babesa eskatzen du, eta, horretarako, baliabide oso aurreratuak, baliabide handiak, ezagutza aurreratuak eta motibazio handia behar da; esate baterako, erakunde kriminalak eta ziberarmadak izatea.

Horri dagokionez, produktu industrialen ebaluazioaren irismena 1. segurtasun mailarako (SL1) definitutakoaren arabera ezartzen da.

Ebaluazio hori hainbat esparrutan egiten da; konparazio baterako, erabilera industrialeko protokoloak ebaluatzen diren eremu orokorrakoak (OPC-UA, Profinet, Modbus, eta abar), edo produktu industrial baten esparru zehatzak —izan litezke fabrikatzaileak berak garatutako aplikazioak, adibidez—. Bereizketa hori eginda, proba orokorretarako dauden testatze tresnak erabil daitezke; fabrikatzailearen aplikazioaren ebaluazioaren emaitza, berriz, probetako ingeniarien ezagutzaren eta esperientziaren araberakoa izango da.

Lizitatzzailearen kontura izango dira ebaluazioa egiteko eskatzen diren hardware eta software lizentzia guztiak.

IV.- PROBA LABORATEGIAREN BALDINTZA TEKNIKOAK

Probak behar bezala eta ZIUREk espero duen kalitatearekin gauzatzeko, prozedura bati jarraikiz, errepikatze moduan eta kanpoko eragile batek egiaztatuz eta kostuei eutsiz, beharrezkoa da ebaluaziorako tresna komertzialak erabiltzea.

Zibersegurtasun industrialak ebaluatzeko tresnen egungo egoera kontuan hartuta, lizitatzzaileak egiaztaturiko laborategiak funtzionalitate hauek eskaintzeko behar adina tresna izan behar ditu:

- Web sarteak probatzeko tresna.
 - Tresna horrek erreferentzia esparru estandarizatu edo *de facto* bat erabili behar du testak egiteko, adibidez, Open Web Application Security Project (OWASP) edo antzekoa.
- Komunikazio protokoloen testu erreminta.

- Tresna horrek helburu orokorreko komunikazio protokoloak aztertu behar ditu. Azterketa horren emaitzak lotuta egon beharko du CVE (Common Vulnerabilities and Exposures) kalteberatasunen txosten estandarizatuarekin.
- Industria komunikazioko protokoloak probatzeko tresna.
 - Tresna horrek alderdi hauek estali behar ditu: komunikazio baliogabeak edo gaizki eratuak testatzea (*fuzzing* izenez ezagutzen dena), trafiko handiaren testa egitea (zerbitzuaren ukapen proba bezala ezagutzen dena) eta OT protokoloetan ezagutzen diren kalteberatasunak egiaztatzea.
 - Gutxienez, komunikazio protokolo hauek jasan behar ditu:
 - EtherNet/IP (CIP)
 - Foundation Fieldbus (FF-HSE)
 - MMS
 - Modbus TCP/IP
 - OPC UA
 - PROFINET IO
 - DNP3
 - MMS (IEC 61850/ICCP)
 - Modbus TCP/IP
 - SES-92
 - ZigBee SE (802.15.4)

Nolanahi ere, lizitatzailerak probak egiteko proposatutako laborategiak proiektuaren xederako gutxienerako baldintzak betetzen dituela egiaztatzeke, proposamenak ebaluazioa egingo den laborategia osatzen duten hardware eta software tresnen zerrenda xehatua jaso behar du, baita horien kokaleku fisikoa ere.

Eskaini beharreko laborategi zerbitzuek, IEC 62443 araua erreferentziatzen hartuta, gutxienez test hauek egin behar dituzte:

- 1. proba: Aztertu beharreko produktuaren segurtasun eskakizunen testa.
 - Proba funtzionala: testak, arauaren eskakizunak kontuan hartuta, modu objektiboan ebaluatuko du betetzen den ala ez (gainditzeko/ez gainditzeko ebidentziak), **bai kanpotik, bai barrutik**.
- 2. proba: Mehatxuak arintzeko testa.
 - Sartze probak: **barne funtzionaltasuna** modu erdiautomatikoan ebaluatzen duen testa, eta, horretarako, baimendu gabeko sarbide tekniken bidez kontrolatutako eraso egoera bat simulatzen da, benetako segurtasun arrakalak ezagutzeko.
- 3. proba: Kalteberatasunen testa.

- Atakak eskaneatzea: **produktuaren kanpo konektibitatea** ebaluatzen duen testa; erabiltzen ez diren kanal posibleak identifikatzea; kanal horiek sistemarekin kontrolatu gabeko interakzio puntu gisa balio dezakete.
 - Sareko kalteberatasunak eskaneatzea: produktuaren kanpo konektibitatea ebaluatzen duen testa; komunikazio protokoloen inplementazioan **ezagutzen diren akatsak identifikatuz**.
 - *Fuzzinga*: produktuaren kanpo funtzionaltasuna ebaluatzen duen testa, komunikazio protokoloen inplementazioan **ezagutzen EZ diren akatsak identifikatzen dituen**a.
 - Sarearen estres testa: **produktuaren kanpo konektibitatea** ebaluatzen duen testa, haren interfazeak estresatuz, eta, horrela, haren funtzionamenduari eraginez; zerbitzuaren ukapen motako erasoetan erabiltzen diren tekniken antzekoa da (zerbitzuaren ukapena). Proba horrek balio handia du; izan ere, detekta dezakegu ea sistemaren kontrol portaerek (erabilgarritasuna) kalterik jasaten duten oso sofistikatuak ez diren erasoen aurrean.
- 4. proba: Sartze testa.
 - Sartze logikoko testa: **barne funtzionaltasuna eskuz ebaluatzen duen testa**, eta, horretarako, baimendu gabeko sarbide tekniken bidez kontrolatutako eraso egoera bat simulatzen da, benetako segurtasun arrakalak ezagutzeko.
 - 5. proba: Testatzaileen independentzia.
 - Testatzaileen independentzia lortzen da ez dagoelako inolako filiazio harremanik produktuak fabrikatzen dituzten enpresen eta proba ingeniarien artean.

V.- METODOLOGIA ETA LAN PLANA

Enpresa lizitatzailerak eginiko proposamenean metodologia eta lan plana jaso beharko ditu, zerbitzuaren mugari garrantzitsuenak eta datak adierazita. Era berean, entregagaien zerrenda zehaztu beharko da, horietako bakoitzak izango duenaren gutxi gorabeherako deskribapen eta egiturarekin. Hori horrela, entregagai hauek prestatu beharko dira gutxienez:

V.1.- Ebaluazioa prestatu aurreko zerbitzua eta ebaluatutako enpresei laguntzea

Ebaluazioa fabrikatzaileak emaniko alde aurreko prestaketa prozesu batekin hasten da. Prozesu horretan, funtsezko parametroak definitzen dira, ebaluazioaren esparruan eskakizunen irismena eta aplikagarritasuna baldintzatzen dutenak, probak egingo zaizkien kontrolak diseinatzeko.

Laburbilduz, ebaluazioa mugatu egin behar da, argi eta garbi ezartzeko haren esparrua eta helburua. Fabrikatzaileak egingako prozesuaren ondorioz, ebaluatu beharreko kontrol guztiak lortuko dira.

Lehen fase horren barruan, azpifase hauek aurreikusten dira:

1. Irismena ezartzea. Ebaluazioa hastean, lehen urratsa irismena definitzea da; hau da, mugatu behar da zer hartuko den kontuan prozesuan. Irismenak gutxienez alderdi hauek definitu behar ditu: ebaluazioaren xede izango diren antolamendu unitateak, ebaluatu beharreko prozesuak edo osagaiak, eta ebaluazioaren arau estaldura.
2. Aplikagarritasun adierazpena. Aplikagarriak ez diren eskakizunetarako —ebaluazioaren xedearen izaera edo baldintzak direla eta—, adierazi behar da ez direla aplikagarriak, eta jakinaren gainean ipini behar da ebaluatzailea, arrazoiak emanez.
3. Lortu nahi den segurtasun maila. Ebaluazioa egitean kontuan hartu beharreko segurtasun maila zehaztu behar da. Araudi osorako segurtasun maila orokor bat hartu behar da, hargatik eragotzi gabe zenbait azpiataletarako segurtasun maila desberdinak ezartzeko aukera.
4. Adostasun adierazpena. Ebaluatzaileari adostasun adierazpen bat emango zaio aplikazio eremuko betekizun bakoitzerako. Adostasun adierazpen horrek azalduko du nola betetzen den aplikazio eremuan eskatutako segurtasun mailari dagokion baldintza.
5. Ebidentziak ematea. Ebaluazio prozesurako, segurtasun mailak eskatzen duen zorroztasun mailari egokitutako ebidentziak emango dira, ebaluatzaileak ondoren aintzat har ditzan, lotutako baldintza betetzen ote den aztertzeko. Ebidentziak ematea ez da izango beharrezkoa aplikatzen ez diren betekizunetarako.

Aurreko puntuetan deskribatutako jarduerak egiteko, garrantzitsua da alderdi hauek kontuan hartzea:

- Aipatutako puntu guztiak idatziz eman behar zaizkie ebaluatzaileari eta zerbitzu osagarrien erakundeari. Txosten horiek euskaraz eta gaztelaniaz egon behar dute idatzita.
- Ebaluatu beharreko helburuetako batzuek aurrez zehaztutako aplikagarritasun irizpideak dituzte, produktuaren ezaugarrien arabera, eta kasuak eskatzen badu bakarrik ebaluatuko dira.
- Zerbitzu osagarrien erakundeak ebaluatu beharreko kontrolak zehaztu ondoren emango dira ebidentziak.

V.2.- Ebaluazio egoeraren dokumentazioa

Hasieran, produktuaren fabrikatzaileak probatu beharreko aktiboetako/gailuei buruzko informazioa emango dio enpresa adjudikatzaileari (DUT, *Device Under Test* ere esaten zaio); esate baterako, kontrol funtzionamendu normala, salbuespenezko kontrol funtzionamendua eta gailuarekiko elkarreragin mekanismoen zerrenda bat. DUTak jasan dezakeen funtzionaltasun guztiekin egon behar du konfiguratuta, ahalik eta ebaluazio estaldura handiena bermatzeko eta, hartara, ahalik eta etekin handiena ateratzeko.

V.3.- Produktu eragiketaren parametroak adostea

Probetako ingeniariak dokumentazio hori eskuratu ondoren, aztertu egingo dituzte agiriok, eta dokumentu bat proposatuko dute testatzeko metodoekin eta kontrol funtzioak monitorizatzeko irizpideekin. Dokumentu horren parametroak proba ingeniarien eta produktuaren fabrikatzailearen artean adostuko dira.

V.4.- Egin beharreko probak hautatzea eta ebaluazioak diseinatzea

Ebaluatu beharreko produktuaren berezitasunak kontuan hartuta, kasu bakoitzean aplikatzen diren testak aukeratuko dira, eta test hori nola egingo den deskribatuko da (ingurune operatiboa, neurtzeko tresnak, neurtzeko metodoa, emaitzak, eta abar).

Test horiek preskripzio teknikoen baldintza agiri honen IV. atalean ezarritako baldintzak bete behar dituzte, IEC 62443 arauaren 4-1 zatiko 5. praktikari jarraikiz. Test mota bakoitzak proba bat izan beharko du gutxienez, eta gomendagarria da ahalik eta proba mota gehien egitea.

V.5.- Egin beharreko probak hautatzea eta ebaluazioak diseinatzea

Diseinua egin ondoren, proba ingeniariak ebaluazio hori egingo dute laborategian.

V.6.- Aurreko puntuetan egindako probetan lortutako emaitzak aztertzea eta diseinua hobetzeko proposamena egitea.

Probak egin ondoren, testetan jasotako informazio guztia aztertuko da, emaitzen txostenak egiteko. Txosten horiek ebaluaturiko enpresei ez ezik ZIURi ere aurkeztuko zaizkie. Txosten guztiak euskaraz eta gaztelaniaz aurkeztu behar dira.

Haietan, lortutako emaitzen arabera, produktuaren diseinua hobetzeko proposamen bat sartu behar da, zibersegurtasun arloko heldutasuna hobetzeko.

V.7.- Enpresa bakoitzari laguntzeko zerbitzu teknikoa, konpontze planean proposatutako hobekuntzak ezartzen laguntzeko

Ebaluazioaz arduratuko den enpresa adjudikaziodunak laguntza zerbitzu tekniko bat txertatu behar du proiektuan, ebaluatuko dituzten 4 enpresetako bakoitzari aurreko atalean proposatutako hobekuntzak ezartzen laguntzeko, zeini bere produktuan.

Fase horiek aurreikusi behar dira, gutxienez, proiektuan jasotako 4 ebaluazioetako bakoitzerako.

VI.- LANTALDEAREN BETEKIZUNAK

Giza baliabideak nahitaez atxikitzeko ezarritako betekizunaz aparte:

- 1. faseko zerbitzuko lantaldeak —ebaluatutako enpresak prestatzeko eta laguntzeko preskripzio teknikoen baldintza agirian deskribatu da fase hori— lantalde bat aurkeztu beharko du, ebaluazio

zerbitzuaz arduratuko denaz bestelakoa. Lantalde horrek antzeko zerbitzuetan esperientzia duten 2 profesional izan behar ditu gutxienez.

- Ebaluazio zerbitzuari lotutako 2., 3., 4., 5., 6. eta 7. faseei lotutako zerbitzuko lantaldeak, ebaluazioa egiteko prozesua ez luzatzeko eta ebaluazio guztiak aldi berean kudeatu ahal izateko; proiektua gauzatzeko ezarritako denborak betez, gutxienez 4 proba ingeniari izan behar ditu.

VII.- LANAK IKUSKATZEA ETA KONTROLATZEA

Enpresa adjudikaziodunak erraztu egin beharko ditu ZIUR Fundazioari dagozkion lanak ikuskatzeko eta kontrolatzeko eginkizunak, eta zorrotz bete beharko ditu jasotzen dituen oharra eta gomendioak.

Nolanahi ere, ZIUR Fundazioaren irizpidearen arabera geratuko da jarraipena egiteko modua aldatzea (bilerak, aktak, txostenak, prozedurak...), baldin eta beharrezkotzat jotzen badu.

Era berean, kontratua behar bezala garatzeko eta betetzeko beharrezkotzat jotzen diren zerbitzuak eman beharko ditu, lan edo informazio bileretara joateari dagokionez, eta ez du izango ordainketa osagarririk jasotzeko eskubiderik horregatik. Betebehar horrek berme aldia amaitu arte iraungo du.

Donostia, 2023ko otsailaren 10a.



Koldo PECIÑA TXINTXURRETA
ZIUR FUNDAZIOA