



## ZIURTAPEN PRAKTIKEN DEKLARAZIOA

Erreferentzia: IZENPE-ZPD  
Bertsio zkia.: v 5.03  
Data: 2015ko martxoaren 10an

---

© IZENPE 2015

Dokumentu hau IZENPErena da. Osotasunean soilik erreproduzi daiteke.

■ Beato Tomás de Zumárraga  
71 - 1ª Planta  
01008  
Vitoria - Gasteiz

[www.izenpe.com](http://www.izenpe.com)  
[info@izenpe.com](mailto:info@izenpe.com)  
Tel.: 945 017 490



# Aurkibidea

## Edukia

<b>1</b>	<b>Sarrera</b>	<b>12</b>
1.1	Aurkezpena	13
1.2	Identifikazioa	15
1.3	PKI gako publikoko azpiegituraren parte-hartzaileak	15
1.3.1.	Ziurtapen-agintaritzak	15
1.3.2.	Erregistro-entitateak	22
1.3.3.	Ziurtagirien erabiltzaile diren azken entitateak	22
1.3.4.	Denbora zigilatzeke zerbitzuen azken entitate erabiltzaileak	23
1.3.5.	Konfiantzako hirugarren batzuk	23
1.4	Ziurtagiriaren erabilerak	23
1.4.1.	Ziurtagiriaren erabilera egokiak	24
1.4.2.	Ziurtagiriaren erabilera debekatuak	25
1.5	Politikak	25
1.5.1.	Dokumentazioaren kudeaketaz arduratzen den entitatea	25
1.5.2.	Harremanetarako datuak	26
1.5.3.	Ziurtapen Praktiken Deklarazioaren egokitzapenaren arduradunak	26
1.5.4.	Ziurtapen Praktiken Deklarazioa onartzeko prozedura	26
1.6	Definizioak eta akronimoak	26
1.6.1.	Definizioak	26
1.6.2.	Akronimoak	30
<b>2</b>	<b>Argitalpena eta informazio-biltegiaren arduradunak</b>	<b>32</b>
2.1	Informazio-biltegia	32



2.2	Ziurtapen-informazioaren argitalpena	32
2.2.1.	Argitalpen- eta jakinarazte-politika	32
2.2.2.	Ziurtapen Praktiken Deklarazioan argitaratzen ez diren elementuak	33
2.3	Argitalpen-maiztasuna	33
2.4	Biltegirako sarrera kontrolatzea	33
<b>3</b>	<b>Izenak</b>	<b>34</b>
3.1.1.	Izen motak	34
3.1.2.	Izenen formatuak interpretatzeko arauak	34
3.1.3.	Izen-bakartasuna	34
3.1.4.	Izenen eta marka erregistratuen tratamenduaren arloko gatazkak ebaztea	34
3.2	Identitatea balidatzea	35
3.2.1.	Gako pribatuaren jabetza frogatzeko metodoak	35
3.2.2.	Antolakundearen nortasuna kautotzea	35
3.2.3.	Pertsona fisiko eskatzailearen nortasuna kautotzea	35
3.3	Gakoak berriro jaulkitzeko eskaerarako identifikatzea eta kautotzea	35
3.4	Ezeztatzeko eskaerarako identifikatzea eta kautotzea	35
<b>4</b>	<b>Ziurtagirien bizi-zikloaren baldintza operatiboak</b>	<b>36</b>
4.1	Ziurtagiria eskatzea	36
4.1.1.	Eskaeraren egiaztapena	36
4.1.2.	Inskribatzeko prozesua eta erantzukizunak.	36
4.2	Eskaerak prozesatzea	37
4.2.1.	Identifikatzeko eta kautotzeko eginkizunak egitea	37
4.2.2.	Eskaerak onartzea edo baztertzea	37
4.3	Ziurtagiria jaulkitzea	37
4.3.1.	CAren jardunak ziurtagiriak jaulkitzean	38



4.3.2.	Jaulkipena jakinaraztea harpidedunari	39
4.4	Ziurtagiria onartzea	39
4.4.1.	Ziurtagiria onartzeko prozesua	40
4.4.2.	CAk ziurtagiria argitaratzea	40
4.4.3.	CAk beste entitate batzuei ziurtagiria jaulki izana jakinaraztea	40
4.5	Gako-parea eta ziurtagiriaren erabilera	40
4.5.1.	Harpidedunaren gako pribatua eta ziurtagiriaren erabilera	40
4.5.2.	Ziurtagirietan konfiantza duten hirugarren batzuek gako publikoa eta ziurtagiria erabiltzea	42
4.6	Ziurtagiria gako aldaketarik gabe berritzea	42
4.7	Ziurtagiria gakoak aldatuta berritzea	42
4.7.1.	Ziurtagiria berritzeko zirkunstantziak	43
4.7.2.	Nork eska dezake	43
4.7.3.	Berritzeko eskaeren tratamendua	43
4.7.4.	Harpidedunari jakinaraztea	43
4.7.5.	Ziurtagiri berritua onartzeko prozedura	43
4.7.6.	Ziurtagiria argitaratzea	43
4.7.7.	Beste entitate batzuei jakinaraztea	44
4.8	Ziurtagiria aldatzea	44
4.9	Ezeztatzea	44
4.9.1.	Ezeztatzeko zirkunstantziak	44
4.9.2.	Nork eska dezake ziurtagiria ezeztatzea	45
4.9.3.	Ezeztatzeko eskaeren tratamendua	45
4.9.4.	Ezeztatzea prozesatzeko CAren epea	45
4.9.5.	Konfiantzako hirugarren batzuek ezeztatzeak egiaztatzeko betebeharra	46
4.9.6.	CRLak sortzeko maiztasuna	46
4.9.7.	CRLak sortzen direnetik argitaratzen direnera arte emandako denbora	46



4.9.8.	Ziurtagirien egoera online egiaztatzeko sistemaren erabilgarritasuna	46
4.9.9.	On line ezeztatzea egiaztatzeko eskakizunak	46
4.9.10.	Ezeztatzeak ohartarazteko eskura dauden beste modu batzuk	47
4.9.11.	Arriskupean dagoen gakoaren eskakizun bereziak	47
4.10	Ziurtagirien egoera-zerbitzuak	47
4.10.1.	Ezaugarri operatiboak	47
4.10.2.	Zerbitzuaren erabilgarritasuna	47
4.11	Harpidetzari amaiera ematea	47
4.12	Gakoak zaintzea eta berreskuratzea	47
<b>5</b>	<b>Segurtasun fisikoaren, prozeduren eta langileen kontrolak</b>	<b>48</b>
5.1.1.	Instalazioen kokalekua eta eraikuntza	48
5.1.2.	Sarbide fisikoa	48
5.1.3.	Elektrizitatea eta aire egokitua	48
5.1.4.	Urarekiko erresistentzia	49
5.1.5.	Suteen prebentzioa eta horien aurkako babesa	49
5.1.6.	Euskarrien biltegitratzea	49
5.1.7.	Hondakinen tratamendua	49
5.1.8.	Instalazioetatik kanpoko babeskopia	49
5.2	Prozeduren kontrolak	49
5.2.1.	Konfiantzazko funtzioak	49
5.2.2.	Zeregin bakoitzerako pertsona kopurua	50
5.2.3.	Eginkizun bakoitzean identifikatzea eta kautotzea	50
5.2.4.	Eginkizunetan bereiztea zereginak	50
5.3	Langileen kontrolak	50
5.3.1.	Historialei, kalifikazioei, esperientziari eta kautotzeei buruzko baldintzak	50
5.3.2.	Historiala ikertzeko prozedurak	50



5.3.3.	Trebakuntza-baldintzak	50
5.3.4.	Trebakuntza eguneratzeko baldintzak eta maiztasuna	51
5.3.5.	Lan-txandaketen segida eta maiztasuna	51
5.3.6.	Baimendu gabeko konexioen zigorrak	51
5.3.7.	Langileak kontratatzeke baldintzak	51
5.3.8.	Langileei dokumentazioa ematea	51
5.4	Audit	51
5.4.1.	Erregistratutako gertaera motak	51
5.4.2.	Log fitxategien prozesamenduaren maiztasuna	52
5.4.3.	Audit logaren atxikipen-aldia	52
5.4.4.	Audit logaren babesa	52
5.4.5.	Audit-logaren backup prozedura	52
5.4.6.	Log fitxategiak biltzea	52
5.4.7.	Log fitxategiak sortzea eragin duen ekintzaren jakinarazpena	52
5.4.8.	Puntu ahulen azterketa	52
5.5	Erregistroak artxibatzea	52
5.5.1.	Artxibatutako erregistroen mota	52
5.5.2.	Fitxategiaren atxikipen-aldia	52
5.5.3.	Artxiboaren babesa	53
5.5.4.	Artxiboaren backup prozedurak	53
5.5.5.	Erregistroen denbora zigilatzeke eskakizunak	53
5.5.6.	Artxibatzeke sistema	53
5.5.7.	Artxiboaren informazioa lortzeke eta egiaztatzeke prozedurak	53
5.6	Gakoak aldatzea	53
5.7	Larrialdietarako plana	53
5.7.1.	Gertakariak kudeatzeke prozedurak	53



5.7.2.	Datu eta software ustelen aurrean jarduteko plana	54
5.7.3.	Gako pribatuaren konpromisoaren aurreko prozedura	55
5.7.4.	Hondamendi baten ondoren, negozioaren jarraipena	55
5.8	CAren edo RArean amaiera	55
5.8.1.	Ziurtapen-entitatea	55
5.8.2.	Erregistro-entitatea.	56
<b>6</b>	<b>Segurtasun teknikoaren kontrolak</b>	<b>57</b>
6.1	Gako-parea sortu eta instalatzea	57
6.1.1.	Gako-parea sortzea	57
6.1.2.	Gako pribatua harpidedunari banatzea	57
6.1.3.	Gako publikoa ziurtagiriaren jaulkitzaileari banatzea	57
6.1.4.	Ziurtapen-entitatearen gako publikoa ziurtagirien erabiltzaileei banatzea	58
6.1.5.	Gakoen tamainak eta erabilitako algoritmoak	58
6.1.6.	Ziurtapen-sinaduretako algoritmoak	58
6.1.7.	Gakoen erabilera baimenduak (KeyUsage field X.509v3)	59
6.2	Gako pribatua babestea	59
6.2.1.	Modulu kriptografikoen estandarrak	59
6.2.2.	Gako pribatua pertsona batek baino gehiagok kontrolatzea (m-tik n)	59
6.2.3.	Gako pribatuaren zaintza	59
6.2.4.	Gako pribatuaren babeskopia	60
6.2.5.	Gako pribatua artxibatzea	60
6.2.6.	Gako pribatuaren transferentzia, modulu kriptografikora edo modulu kriptografikotik	60
6.2.7.	Gako pribatua modulu kriptografikoan biltegitzea	60
6.2.8.	Gako pribatua aktibatzeke metodoa	61
6.2.9.	Gako pribatua desaktibatzeke metodoa	61
6.2.10.	Gako pribatua deuseztatzeko metodoa	61



6.2.11.	Modulu kriptografikoaren kalifikazioa	61
6.3	Gako-parea kudeatzearen beste alderdi batzuk	61
6.3.1.	Gako publikoa artxibatzea	61
6.3.2.	Gako publikoa eta pribatua erabiltzekoaldiak	61
6.4	Aktibatzeke datuak	61
6.4.1.	Aktibatzeke datuak sortzea eta instalatzea	61
6.4.2.	Aktibatzeke datuak babestea	62
6.4.3.	Aktibatzeke datuen beste alderdi batzuk	62
6.5	Segurtasun informatikoaren kontrolak	62
6.5.1.	Segurtasun informatikorako berariazko eskakizun teknikoak	62
6.5.2.	Segurtasun informatikoaren mailaren ebaluazioa	63
6.6	Bizi-zikloaren kontrol teknikoak	63
6.6.1.	Sistemen garapen-kontrolak	63
6.6.2.	Segurtasunaren kudeaketa-kontrolak	64
6.6.3.	Bizi-zikloaren segurtasun-kontrolak	64
6.7	Sareko segurtasunaren kontrolak	64
6.8	Denbora-iturria	64
<b>7</b>	<b>Ziurtagiriaren profilak eta ezeztatutako ziurtagiriaren zerrendaren profilak</b>	<b>65</b>
7.1	Ziurtagiriaren profila	65
7.1.1.	Bertsio-zenbakia	65
7.1.2.	Ziurtagiriaren luzapenak	65
7.1.3.	Algoritmo-objektuen identifikatzailea	68
7.1.4.	Izenen formatuak	68
7.1.5.	Izenen murrizpenak	68
7.1.6.	Ziurtagiriaren politikaren objektu-identifikatzailea	68
7.1.7.	“Politika-murrizpenak” luzapenaren erabilera	68



7.1.8.	Politika kalifikatzaileen sintaxia eta semantika	69
7.1.9.	“certificate policy” luzapenerako tratamendu semantikoa	69
7.2	Ezeztatutako ziurtagirien zerrendaren profila	69
7.2.1.	Bertsio-zenbakia	69
7.2.2.	Zerrendako elementuen ezeztatutako ziurtagirien eta luzapenen zerrenda	69
7.3	OCSP profila	70
7.3.1.	Bertsio-zenbakia	70
7.3.2.	OCSParen luzapenak	70
<b>8</b>	<b>Denbora Zigilatze Zerbitzuaren Praktiken Deklarazioa (TSA)</b>	<b>71</b>
8.1	TSAREN dibulgazio-deklarazioa	71
<b>9</b>	<b>Bete beharreko ikuskapenak</b>	<b>72</b>
9.1	Ikuskapenaren maiztasuna	72
9.2	Ikuskatzailearen kualifikazioa	72
9.3	Ikuskatzailearen eta ikuskatutako enpresaren arteko harremana	72
9.4	Ikuskapenaren mende dauden elementuak	72
9.5	Urritasunen ondoriozko erabakiak hartzea	72
9.6	Emaitzen berri ematea	72
<b>10</b>	<b>Beste lege eta jarduera gai batzuk</b>	<b>73</b>
10.1	Tarifak	73
10.1.1.	Ziurtagiriak jaulkitzeko edo berritzeko tarifak	73
10.1.2.	Ziurtagirien egoerari buruzko informazioa eskuratzeko tarifa	73
10.1.3.	Beste zenbait zerbitzutarako tarifak	73
10.1.4.	Itzultze-politika	73
10.2	Finantza-erantzukizunak	73
10.3	Informazioaren konfidentziasuna	73



10.3.1. Informazio konfidentzialaren irismena	73
10.3.2. Irismenaren barruan ez dagoen informazioa	74
10.3.3. Informazio konfidentziala babesteko erantzukizuna	75
10.4 Datu pertsonalak babestea	75
10.4.1. Sarrera	75
10.4.2. Aplikazio-esparrua	75
10.4.3. Datu pertsonalak babesteko segurtasun-antolamendua.	76
10.4.4. Segurtasun-antolamenduaren eredia	76
10.4.5. Segurtasuna antolatzeko unitateen sailkapena	77
10.4.6. Datu pertsonalak dituzten fitxategien egitura	78
10.4.7. Segurtasuneko arauak eta prozedurak	78
10.5 Jabetza intelektualeko eskubideak	80
10.5.1. Ziurtagirien jabetza	80
10.5.2. Ziurtapen Praktikaren jabetza	80
10.5.3. Izenen gaineko informazioaren jabetza	80
10.5.4. Gakoen eta horiei dagokien materialaren jabetza	80
10.6 Betebeharrak eta bermeak	80
10.6.1. Zerbitzua egiteko betebeharrak	80
10.6.2. Jardun fidagarriko betebeharrak	81
10.6.3. Identifikazio-betebeharrak	82
10.6.4. Erabiltzaileei eman beharreko informazioa: betebeharrak	82
10.6.5. Egiatzapen-programak: betebeharrak	83
10.6.6. Ziurtapen-zerbitzuaren arautze juridikoa: betebeharrak	83
10.6.7. Erregistro-entitatearen betebeharrak	84
10.6.8. Ziurtagiri-eskatzailearen betebeharrak	84
10.6.9. Ziurtagiri-harpidedunaren betebeharrak	85



10.6.10. Ziurtagirien erabiltzaile egiaztatzailearen betebeharrak	86
10.6.11. Denbora-zigiluak jaulkitzen dituen entitatearen betebeharrak	86
10.6.12. Denbora-zigiluen harpidedunaren betebeharrak	87
10.6.13. Denbora-zigiluak egiaztatzen dituzten hirugarren aldean betebeharrak	87
10.6.14. Argitalpen Zerbitzuaren betebeharrak	87
10.7 Erantzukizunak	87
10.7.1. Ziurtapen-agintaritzaren erantzukizunak	87
10.7.2. Denbora zigilatze agintaritzaren erantzukizuna	88
10.7.3. Erregistro-agintaritzaren erantzukizunak	88
10.7.4. Harpidedunen betebeharrak	89
10.7.5. Ziurtagirietan konfiantza duten hirugarrenen erantzukizunak	90
10.8 Kalte-ordainak	90
10.9 Baliozkotze-aldia	90
10.9.1. Epea	90
10.9.2. Amaiera	90
10.9.3. Amaieraren ondorioak	90
10.10 Banako jakinarazpenak eta komunikazioa parte-hartzaileekin	90
10.11 Zuzenketak	91
10.11.1. Aldaketetarako prozedura	91
10.11.2. Jakinarazteko aldia eta mekanismoa	91
10.11.3. OIDA zer zirkunstantzian aldatu behar den	91
10.12 Erreklamazioak eta auzien ebazpena	91
10.13 Aplikatzeko den araudia	92
10.14 Aplikatzekoa den araudia betetzea	92
10.15 Askotariko estipulazioak	92



## 1 Sarrera

---

Euskal administrazio publikoak informazioaren gizartea sustatu nahi izan du, eta helburua herritarren jarduera ekonomiko eta sozialetan informazioaren eta komunikazioaren teknologiak guztiz barneratzea da. Ildo horretan, herritarrei administrazioarekin harremanetan jartzeko aukera emango dieten tresnak bideratu nahi izan dira –betiere segurtasuna bermatuz–, informazioaren pribatutasuna, pertsonen intimitatea eta euren eskubideak babestea helburu.

Eusko Jaurlaritzak eta Foru Aldundiek elkarreraginkortasuna bermatuko duen ziurtapen eta sinadura elektronikorako sistema komuna elkarrekin garatzea erabaki zuten, beren sozietate informatikoen bitartez. Horrela, ematen diren ziurtagiriak administrazio batzuen zein besteen aplikazio eta prozeduretan baliagarriak izan daitezzen lortu nahi zen.

Elkarlanerako borondate horren ondorioz, 2002ko ekainean “Ziurtapen eta Zerbitzu Enpresa- Empresa de Certificación y Servicios, IZENPE, SA” merkataritza-sozietatea eratu zuten goraxeago adierazitako sozietate informatikoei (aurrerantzean IZENPE deituko diogu).

Euskal administrazio publikoetako sozietate informatikoei ziurtapen elektronikoa garatzeko duten interesa kudeatzeko tresna edo antolakunde komuna da IZENPE, eta herritarren eta administrazioaren arteko harremana errazteko tresna ezin hobea dela erakutsi du.

Ildo horretan, sinadura elektronikoari buruzko abenduaren 19ko 59/2003 Legearen 4. artikuluan jasotzen denez, Administrazioek edo haien mende dauden organismo edo sozietateek egin ahal izango dituzte ziurtapen-zerbitzuak.

Horrela, IZENPE euskal Administrazioen mende dagoen ziurtapen-entitatea da, eta hauek dira bere helburu sozialak:

- Telekomunikazio-sareen bidezko gobernu elektronikoaren erabilera sustatzea eta gobernu elektronikoaren garapena indartzea, betiere transakzioen segurtasun, konfidentzialtasun, benetakotasun eta atzerazintasuneko bermeekin.
- Segurtasun-zerbitzuak nahiz zerbitzu tekniko eta administratiboak ematea teknika eta bitarteko elektronikoak, informatikoak eta telematikoak erabiltzen diren komunikazioetan.

Era berean, ziurtapen elektronikoa modu eraginkorrean garatu eta barneratzeko helburuarekin, informazioaren segurtasuna kudeatuko duen sistema bat ezarri du, Azpiegitura Erabiltzeko eta Mantentzeko eta Ziurtapen Digitalak Balidatu eta Ezeztatzeko prozesuetarako ISO 27001 estandarren arabera.

IZENPEk ETSIren (Telekomunikazioetako Estandarren Europako Institutuaren) estandarren adierazpenak jarraitzen ditu, eta honako bi arau hauen zehaztapen teknikoak (TS) arabera lortu du ziurtapena: sinadura sortzeko gailu seguru batean (QCP Public + SSCD) sortutako ziurtagiri kualifikatuak jaulkitzeko 101 456 arauaren zehaztapen teknikoak arabera; eta ziurtagiri kualifikatuak eta ez kualifikatuak jaulkitzeko 102 042 arauaren arabera. Balidazio hedatuko ziurtagirien politikari (EVCP) jarraitzen dioten zerbitzari seguruko ziurtagirietarako, eta erakundearen balidazio-politikari (OVCP) jarraitzen dioten zerbitzari seguruko ziurtagirietarako, CA/Browser Forum-ek onartutako gidei ere jarraituko zaie.



TS 101 456 eta TS 102 042 arauen ezartzen diren TS zehaztapen teknikoek ziurtapenen kudeaketa eta praktikari buruzko oinarritzko baldintzak zehazten dituzte, eta baldintza horiek bete behar dituzte ziurtagiri kualifikatuak eta kualifikatu gabeak jaulkitzen dituzten entitateek, baldin eta jaulkitzen dituzten ziurtagiriak Europako Parlamentuko eta Kontseiluko 1999/93/EE zuzentarauaren lege-esparruaren arabekoak –zuzentarau hori Espainiako erregimen juridikoan sinadura elektronikoari buruzko 1999/93 legearen bitartez sartu zen– eta, ondoren, identifikazio elektronikoari eta barne-merkatuko transakzio elektronikoetarako konfiantzako zerbitzuei buruzko 910/2104 araudiaren (eIDAS) arabekoak badira.

## 1.1 Aurkezpena

IZENPEk gako publikoen azpiegitura bat kudeatzen du, erabiltzen duten entitate publikoei honako zerbitzu hauek eskaintzeko:

- *Ziurtapen Digitaleko Zerbitzua*, IZENPEk ziurtagiri kualifikatuak nahiz legez kualifikatuta ez dauden ziurtagiri arruntak jaulkitzen ditu, *abenduaren 19ko sinadura elektronikoari buruzko 59/2003 Legeari* jarraituta.
- *Denbora Zigiluen Zerbitzuak* entitate erabiltzaileari aukera ematen dio bermatzeko denbora-tarte jakin batean informazio jakin bat bazegoela.
- *Egiaztapen Aurreratuko Zerbitzuak* zerbitzua erabiltzen duen entitateari aukera ematen dio IZENPEk jaulkitako ziurtagiriak erabiltzeko. Horretarako, ziurtagirien egoera begiratzen du, OCSP (Online Certificate Status Protocol) protokoloaren bidez.
- Egiaztapen Zerbitzuak zerbitzua erabiltzen duen entitateari aukera ematen dio IZENPEk jaulkitako ziurtagiriak erabiltzeko. Horretarako, ziurtagirien egoera begiratzen du, CRL (Certificate Revocation List) protokoloaren bidez.
- ZAIN sinadura-zerbitzuen plataforma konfiantzako zerbitzuen plataforma bat da, segurtasun-zerbitzu global eta estandarizatuen multzoa hartzen duena barne (kautotzea, baimentzea, sinadura elektronikoa eta datuen babes), web-zerbitzu gisa.
- IZENPEk dohainik eskaintzen du id@zki. Nabigatzaile baten barruan integratu ahal izateko applet itxura duen Java aplikazio bat, elektronikoki sinatzeko eta zifratzeko funtzionaltasuna duena.
- IZENPEren sinadura-euskarriko zerbitzua ohiko sinadura-euskarriaren bertsio digitala da. Pertsona batek sinatu behar dituen dokumentuak jasotzeko azpil batean datza.
- ZIURRA komunikazio ziurtatuko zerbitzuak konfiantzako hirugarren gisa (“notario digital” gisa) jarduten du, eta, hartara, mezu elektronikoko edo SMS bat igorri dela eta hartzaileak mezu hori hartu duela fede ematen du.
- Argitalpena Jasota Uzteko eta Egiaztatzeko Zerbitzuak aukera ematen du kontratazio publiko batean barnean hartzen den informazioaren hedapen publikoaren hasierako unea fedez egiaztatzeko.

EGOITZA hodeian ziurtagiriak gordetzeko zerbitzuak aukera ematen du azken erabiltzailearen ziurtagiriak modu seguruan gordetzeko.



Ziurtapen Praktiken Deklarazio honen nahiz *Ziurtagiri bakoitzerako berariazko dokumentazioa* dokumentuaren baitan, IZENPEk honako ziurtagiri hauek jaulkitzen ditu:

EREMUA	ZIURTAGIRIA
<b>Pertsona fisikokoa</b>	
<b>Herritarra</b>	- Herritarra
<b>Eremu korporatiboa</b>	- Entitate publikoetako langileena - Eusko Jaurlaritzako langileena - Ziurtagiri korporatibo kualifikatua - Onartu gabeko ziurtagiri korporatiboa - Kualifikatutako ziurtagiri korporatibo pribatua - Onartu gabeko ziurtagiri korporatibo pribatua
<b>Besterik</b>	- Identifikatzaile sanitarioa - Euskal Etxeak
<b>Pertsona juridikokoa</b>	
<b>Entitatea eta nortasun juridikorik gabeko entitatea</b>	- Entitatearena - Nortasun juridikorik gabeko entitatearena
<b>Administrazio-organoa eta zigilu elektronikoa</b>	- Administrazio-organoarena - Zigilu elektronikoa.
<b>Gailukoa</b>	
<b>SSL eta egoitza elektronikoa</b>	- SSL - SSL EV - Egoitza elektronikoa - EV egoitza elektronikoarena
<b>Gailu informatikoa eta kode-sinadura</b>	- Aplikazioa - Kode-sinadura

IZENPEk jaulkitako ziurtagiri mota bakoitzari dagozkion xehetasunak *Ziurtagiri bakoitzerako berariazko dokumentazioa* dokumentuan arautzen dira. Dokumentu hori *Ziurtapen Praktiken Deklarazioa* dokumentu honekin batera dator.



## 1.2 Identifikazioa

IZENPEk egiztatze-praktiken deklarazio honekin bat etorritz jaulkitako ziurtagiri mota bakoitza bereizita eta banaka identifikatu ahal izateko, aipatutako ziurtagiri mota bakoitzari objektu-identifikatzaile (OID) bat esleitzen dio. Identifikatzaile hori ziurtagirian dagokion atalean agertuko da.

OID hori honako sekuentzia honekin hasten da beti: 1.3.6.1.4.1.14777.

## 1.3 PKI gako publikoko azpiegituraren parte-hartzaileak

Ziurtapen-entitatearen administrazioan eta jardunean honako hauek hartzen dute parte:

- Ziurtapen-agintaritzek.
- Erregistro-entitateak.
- Ziurtagirien erabiltzaileak.

#

### 1.3.1. Ziurtapen-agintaritzak

IZENPEk honako ziurtapen-agintaritza hauek ditu:

- Oinarrizko ziurtapen-agintaritza
- Mendeko ziurtapen-agintaritza

#### OINARRIZKO ZIURTAPEN AGINTARITZA

Mendeko ziurtapen-agintaritzei ziurtagiriak jaulkitzen dizkien ziurtapen-agintaritza da.

IZENPEk honako oinarrizko ziurtapen-agintaritza hauek ditu:

Oinarrizko CA 2007

SHA-1

Subject	CN = Izenpe.com O = IZENPE S.A. C = ES
Validity dates	from 13/12/2007 until 13/12/2037
Thumbprint	30 77 9e 93 15 02 2e 94 85 6a 3f f8 bc f8 15 b0 82 f9 ae fd
Subject alternative name	Nombre RFC822=info@izenpe.com Dirección del directorio: STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8



SHA-256

Subject	CN = Izenpe.com O = IZENPE S.A. C = ES
Validity dates	from 13/12/2007 until 13/12/2037
Thumbprint	2f 78 3d 25 52 18 a7 4a 65 39 71 b5 2c a2 9c 45 15 6f e9 19
Subject alternative name	Nombre RFC822=info@izenpe.com Dirección del directorio: STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8

#### MEENDEKO ZIURTAPEN AGINTARITZAK

Azken entitateei ziurtagiri elektronikoak jaulkitzen dizkieten ziurtapen-agintaritzak dira.

- Herritar eta Erakundeen kualifikatutako CAk
- Herritar eta Erakundeen onartu gabeko CAk
- Herri Administrazioen onartu gabeko CAk
- Herri Administrazioen kualifikatutako CAk
- Eusko Jaurlaritzako langileen CA
- CA SSL EV

#### 2003ko mendeko ziurtapen-agintaritzak.

CA horiek IZENPEren oinarrizko CA berrira migratu dira.

#### Herritar eta Erakundeen kualifikatutako CAk

Subject	E = <a href="mailto:Info@Izenpe.com">Info@Izenpe.com</a> CN = Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades OU = NZZ Ziurtagiri publikoa - Certificado publico SCI L = Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz O = IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8 C = ES
Validity dates	from 4/2/2003 until 4/2/2013
SHA1 thumbprint	b9 ca b0 0e 41 38 06 aa 3f ea 3a 5b 28 f9 bb 39 e7 ef 15 0a

#### Herritar eta Erakundeen onartu gabeko CAk

Subject	E = <a href="mailto:Info@Izenpe.com">Info@Izenpe.com</a> CN = Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (2) L = Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz
---------	---



	O = IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8 C = ES
Validity dates	from 14/6/2006 until 30/1/2018
SHA1 thumbprint	b0 6d b1 3a 6d ee 5a 3b 02 52 94 16 e0 b8 8c f2 26 8b 93 64

#### Herri Administrazioen kualifikatutako CAk

Subject	E = <a href="mailto:Info@izenpe.com">Info@izenpe.com</a> CN = EAEko HAetako langileen CA - CA personal de AAPP vascas OU = AZZ Ziurtagiri publikoa - Certificado publico SCA L = Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz O = IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8 C = ES
Validity dates	From 8/4/2003 until 8/4/2013
SHA1 thumbprint	85 6b ee 62 fc 8e 99 b9 a6 5c 15 29 02 09 be f9 87 ed e4 e4

#### Herri Administrazioen onartu gabeko CAk

Subject	E = <a href="mailto:Info@izenpe.com">Info@izenpe.com</a> CN = EAEko Herri Administrazioen CA - CA AAPP Vascas OU = AZZ Ziurtagiri publikoa - Certificado publico SCA L = Avda del Mediterraneo Etorbidea 3 - 01010 Vitoria-Gasteiz O = IZENPE S.A. - CIF A-01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8 C = ES
Validity dates	From 4/2/2003 until 4/2/2013
SHA1 thumbprint	7b 11 62 cc 37 dc 3d 43 db ef 46 b9 d6 05 fb 6f 93 f2 18 38

#### 2009ko mendeko ziurtapen-agintaritzak

##### Herritar eta Erakundearen kualifikatutako CAk

##### SHA1

Subject	CN = Herritar eta Erakundearen CA - CA de Ciudadanos y Entidades (4) OU = NZZ Ziurtagiri publikoa - Certificado publico SCI O = IZENPE S.A. C = ES
Subject alternative name	Dirección URL=http://www.izenpe.com



	Nombre RFC822=info@izenpe.com Dirección del directorio: STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From 24 de febrero de 2009 9:05:46 until domingo, 13 de diciembre de 2037 0:00:00
SHA1 thumbprint	9f dc e9 42 9b 3d 7e 59 49 9d c3 f8 3c 93 66 65 22 69 a7 59

#### SHA 256

Subject	CN = Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (4) OU = NZZ Ziurtagiri publikoa - Certificado publico SCI O = IZENPE S.A. C = ES
SubjectAlternativeName	Dirección URL=http://www.izenpe.com Nombre RFC822=info@izenpe.com Dirección del directorio: STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From miércoles, 20 de octubre de 2010 9:16:02 until domingo, 13 de diciembre de 2037 0:00:00
thumbprint	08 d8 d6 2a 1a 15 36 c5 3a 0f 9a 18 35 bf 82 c9 f0 96 83 23

#### Herritar eta Erakundeen onartu gabeko CAK

##### SHA1

Subject	CN = Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (3) OU = NZZ Ziurtagiri publikoa - Certificado publico SCI O = IZENPE S.A. C = ES
Subject alternative name	Dirección URL=http://www.izenpe.com Nombre RFC822=info@izenpe.com Dirección del directorio: STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From miércoles, 30 de enero de 2008 10:54:24 until domingo, 13 de diciembre de 2037 0:00:00



SHA1 thumbprint	06 fb ac 35 ae 18 fc bf 22 29 78 8d d1 2d ac 89 8e 74 52 ae
-----------------	---

#### SHA 256

Subject	CN = Herritar eta Erakundeen CA - CA de Ciudadanos y Entidades (3) OU = NZZ Ziurtagiri publikoa - Certificado publico SCI O = IZENPE S.A. C = ES
SubjectAlternativeName	Dirección URL=http://www.izenpe.com Nombre RFC822=info@izenpe.com Dirección del directorio: STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From miércoles, 20 de octubre de 2010 9:18:07 until domingo, 13 de diciembre de 2037 0:00:00
thumbprint	87 56 60 a3 5c b1 03 d7 e0 bb 00 44 24 f1 6d bf bf 21 e0 b4

#### Herri Administrazioen kualifikatutako CAk

##### SHA1

Subject	CN = EAeko HAetako langileen CA - CA personal de AAPP vascas (2) OU = AZZ Ziurtagiri publikoa - Certificado publico SCA O = IZENPE S.A. C = ES
Subject alternative name	Dirección URL=http://www.izenpe.com Nombre RFC822=info@izenpe.com Dirección del directorio: STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From martes, 24 de febrero de 2009 9:03:29 until domingo, 13 de diciembre de 2037 0:00:00
SHA1 thumbprint	e5 c8 62 ed dc f1 14 c8 26 61 98 4a d6 48 ad f2 3f 51 10 fc

##### SHA 256

Subject	CN = EAeko HAetako langileen CA - CA personal de AAPP vascas (2) OU = AZZ Ziurtagiri publikoa - Certificado publico SCA O = IZENPE S.A.
---------	---



	C = ES
SubjectAlternativeName	Dirección URL=http://www.izenpe.com Nombre RFC822=info@izenpe.com Dirección del directorio: STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From miércoles, 20 de octubre de 2010 9:22:40 until domingo, 13 de diciembre de 2037 0:00:00
thumbprint	93 a1 44 6b 61 99 4b 5b 0e 99 d0 5b 14 cd bb 32 2e 6c 17 64

### Herri Administrazioen CA onartu gabeak

#### SHA1

Subject	CN = EAeko Herri Administrazioen CA - CA AAPP Vascas (2) OU = AZZ Ziurtagiri publikoa - Certificado publico SCA O = IZENPE S.A. C = ES
Subject alternative name	Dirección URL=http://www.izenpe.com Nombre RFC822=info@izenpe.com Dirección del directorio: STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From martes, 24 de febrero de 2009 9:00:23 until domingo, 13 de diciembre de 2037 0:00:00
SHA1 thumbprint	7f 58 bb 8f 87 11 c0 49 61 28 cf 71 63 4b 77 95 0a dd d3 2c

#### SHA 256

Subject	CN = EAeko Herri Administrazioen CA - CA AAPP Vascas (2) OU = AZZ Ziurtagiri publikoa - Certificado publico SCA O = IZENPE S.A. C = ES
SubjectAlternativeName	Dirección URL=http://www.izenpe.com Nombre RFC822=info@izenpe.com Dirección del directorio: STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz



	O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From miércoles, 20 de octubre de 2010 9:23:33 until domingo, 13 de diciembre de 2037 0:00:00
thumbprint	f7 9c da 11 e7 91 74 19 a0 41 8d b8 4b a7 43 c5 31 3a d7 f0

## Eusko Jaurlaritzako langileen CA

### SHA1

Subject	CN = Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco OU = Ziurtagiri publikoa - Certificado publico O = IZENPE S.A. C = ES
Subject alternative name	Dirección URL=http://www.izenpe.com Nombre RFC822=info@izenpe.com Dirección del directorio: STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From jueves, 11 de febrero de 2010 11:43:40 until martes, 11 de febrero de 2020 11:43:40
SHA1 thumbprint	4a 17 ed d4 9e d4 cc 39 24 3a be 74 b8 92 df aa 00 68 6a 80

### SHA 256

Subject	CN = Eusko Jaurlaritzako langileen CA - CA personal Gobierno Vasco OU = Ziurtagiri publikoa - Certificado publico O = IZENPE S.A. C = ES
SubjectAlternativeName	Dirección URL=http://www.izenpe.com Nombre RFC822=info@izenpe.com Dirección del directorio: STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From jueves, 11 de febrero de 2010 11:45:37 until martes, 11 de febrero de 2020 11:45:37
thumbprint	25 e9 d1 6d f8 d6 4a 60 73 40 8c be 24 8e 52 9c 23 9e 32 92



CA SSL EV

SHA 256

Subject	CN = CA de Certificados SSL EV OU = BZ Ziurtagiri publikoa - Certificado publico EV O = IZENPE S.A. C = ES
SubjectAlternativeName	Dirección URL=http://www.izenpe.com Nombre RFC822=info@izenpe.com Dirección del directorio: STREET=Avda del Mediterraneo Etorbidea 14 - 01010 Vitoria-Gasteiz O=IZENPE S.A. - CIF A01337260-RMerc.Vitoria-Gasteiz T1055 F62 S8
Validity dates	From miércoles, 20 de octubre de 2010 9:28:56 until martes, 20 de octubre de 2020 9:28:56
thumbprint	6c 48 4d 0f 4d b2 95 ec 67 eb b3 e0 5e 3d c2 14 49 2a 9a b8

### 1.3.2. Erregistro-entitateak

Ziurtapen-praktiken deklarazio hau IZENPEk ziurtagiriak jaulki eta kudeatzeko prozeduretan baliatzen dituen erregistro-entitateei aplikatuko zaie.

Erregistro Entitateak ziurtagirien gakoan eskatzaileak, harpidedunak eta edukitzaileak identifikatuko dituzten entitateak dira; horrez gain, ziurtagirietan jasotzen diren zirkunstantziak egiaztatzen dituen dokumentazioa ziurtatzen dute, eta ziurtagiriak jaulkitzeko, ezetzatzeko eta berritzeko eskaerak balidatzen eta onartzen dituzte.

Erregistro-entitateak izango dira, IZENPE bera edota IZENPErekin dagokion lege-tresna sinatzen duen entitate erabiltzailea.

### 1.3.3. Ziurtagirien erabiltzaile diren azken entitateak

Ziurtagirien erabiltzaile diren azken entitateak ziurtagiri digitalak jaulki, kudeatu eta erabiltzeko zerbitzuak jasotzen dituzten pertsona eta erakundeak dira.

Honako entitate hauek izango dira ziurtapen-sistemaren azken entitate erabiltzaileak:

- Ziurtagirien eskatzaileak
- Ziurtagiriaren sinatzailea
- Ziurtagirien harpidedunak
- Gakoan edukitzaileak

Ziurtagiri bakoitzerako xehetasunak *Ziurtagiri bakoitzerako berariazko dokumentazioan* zehazten dira.



Ziurtagirien eskatzaileak, ziurtagiri oro pertsona batek eskatu behar du, bere izenean edo erakunderen baten izenean.

Sinatzailea, sinadura sortzeko gailua duen pertsona, eta nor bere izenean edota ordezkatzeko duen pertsona fisiko edo juridikoaren izenean jarduten du.

Ziurtagirien harpidedunak, ziurtagirian identifikatutako pertsona fisikoak edo juridikoak dira harpidedunak.

Gakoen edukitzaileak, sinadura digitaleko gakoak dituzten edo horien gaineko arduraren duten pertsona fisikoak dira.

#### **1.3.4. Denbora zigilatzeke zerbitzuen azken entitate erabiltzaileak**

Denbora zigilatzeke zerbitzuen azken entitate erabiltzaileak dira denbora zigiluak jaulkitzeke zerbitzu horien pertsona hartzaileak edo erakunde hartzaileak.

#### **1.3.5. Konfiantzako hirugarren batzuk**

Ziurtapen Praktiken Deklarazio honen barruan, IZENPEk jaulkitako ziurtagiriak eta denbora-zigiluak jasotzen dituzten pertsona fisiko edo juridikoak ziurtagirietan eta denbora-zigiluetan konfiantza duten hirugarren batzuk dira; beraz, ziurtagiri eta denbora-zigilu horietan konfiantza izatea erabakitzen dutenean, ziurtapen-praktiken deklarazio honetan jasotako aplikatuko zaie.

Hirugarrenek ziurtagirietan eta denbora-zigiluetan jartzen duten konfiantza harpidedunekiko harremanetan ziurtagiri horietaz egiten duten erabilera objektiboaren arabera izaten dela jotzen da.

Aipatutako erabilera egiten denean, honako hau egiaztatu behar da bereziki: hirugarrenak mezuei erantsitako ziurtagiri edo sinadura digitaletan konfiantzarik ez duela adierazten duen deklaraziorik ez dagoela, hirugarrenak ziurtagiri eta sinadura digitaletan konfiantza izan zuela finkatzeko, betiere ziurtagiriak baliozkoak badira, sinadurak ziurtagiriak indarrean zeudela sortuak badira eta ziurtagiri jakin batean konfiantza izateko gainerako baldintzak betetzen badira.

Hirugarrenek arduraz erabili behar dituzte ziurtagiri eta denbora-zigilu mota guztiak eta fede onez eta leialtasunez jardun behar dute. Halaber, ez dute izan behar ziurtagiriaren edo denbora-zigiluaren kategoriari dagokion konfiantza-esparruaren barruan bidalitako mezuei uko egitea helburu duten iruzur- edo zabarkeria-jarrerarik.

### **1.4 Ziurtagiriaren erabilerak**

Jarraian IZENPEk jaulkitako ziurtagiriekin zer baimentzen den eta zer debekatzen den zehaztuko da.



### 1.4.1. Ziurtagiriaren erabilera egokiak

#### Ziurtagiri kualifikatua

Ziurtagiri Onartuen erabilerari dagokionez:

Sinadura elektronikoko ziurtagiri onartuek harpidedunaren identitatea eta gako pribatuaren edukitzailearen identitatea bermatzen dituzte. Sinadura sortzeko gailu seguruekin erabiltzen direnean, ezin hobeak dira kualifikatutako sinadura elektronikoa euskarria emateko, hau da, ziurtagiri kualifikatua oinarritzen den eta gailu seguruaren bidez sortu den sinadura elektronikoa aurreratuari euskarria emateko. Hori dela eta, sinadura elektronikoa buruzko Legearen 3.4. artikularekin bat etorriz, lege-ondorioetarako eskuz idatzitako sinaduraren baliokidetzat jotzen da, beste eskakizunik bete behar izan gabe.

Sinadura elektronikoko ziurtagiri kualifikatuak, dagokion ziurtagiri motan hala definitzen bada, kautotze-mezuak sinatzeko ere erabil daitezke, bereziki SSL edo TLS bezeroen testiguak, S/MIME posta elektronikoa segurua, gako-berreskurapen gabeko zifratzeak eta beste zenbait. Sinadura digital horrek sinadura-ziurtagiriaren harpidedunaren identitatea bermatzen du.

Kualifikatutako ziurtagiriek Telekomunikazioko Arauen Europako Institutuaren (ETSI) TS 101 456 arau teknikoa betetzen dute.

#### Onartu gabeko ziurtagiria

Onartu gabeko ziurtagiriek harpidedunaren eta, hala bada, gako pribatuaren edukitzailearen identitatea bermatzen dute. Era berean, nahikoa segurua den sinadurak sortzeko gailu batekin batera erabili behar dira.

Sinadura elektronikoko onartu gabeko ziurtagiriak, dagokion ziurtagiri motan hala definitzen bada, kautotze-mezuak sinatzeko ere erabil daitezke, bereziki SSL edo TLS bezeroen testiguak, S/MIME posta elektronikoa segurua, gako-berreskurapen gabeko zifratzeak eta beste zenbait. Horrelakoetan, ez da sinatzaileak eskuz idatzitako sinaduraren baliokide izaten. Hala ere, sinadura digital horrek sinadura-ziurtagiriaren harpidedunaren identitatea bermatzen du.

Horrez gain, ziurtagiri horiek sinadura elektronikoa aurreraturako eta kautotzeko hainbat modutarako ere balio dute, sinadura-gako pribatua modu fidagarrian babesten duten aplikazio informatikoekin batera erabiliz gero.

Egoitzako eta EV Egoitzako ziurtagiriak webguneak modu fidagarrian identifikatzeko jaulkitzen dira.

Egoitza eta ziurtagiri elektronikoko ziurtagiriak egoitza elektronikoa eta dokumentuen zigitatze elektronikoa identifikatzeko jaulkitzen dira, betiere *Zerbitzu Publikoetarako Hiritarren Sarrera Elektronikoa buruzko ekainaren 22ko 11/2007 Legean* aurreikusitakoaren arabera.

Erabilera orokorreko ziurtagiriek Telekomunikazioko Arauen Europako Institutuaren (ETSI) TS 102 042 arau teknikoa betetzen dute.

#### Gailu informatikoko ziurtagiria

Gailu informatikoen eragiketaz arduratzen diren entitateei zerbitzari seguruko ziurtagiriak (SSL DV, SSL OV, SSL EV, Egoitza eta Egoitza EV) eta aplikazio-ziurtagiriak jaulkitzen zaizkie.



Mota horretako ziurtagiriek CA/Browser Forum-en kualifikatutako eta ETSIren TS 102 042 arau teknikoaren arabera ikuskatutako arauari jarraitzen diete, balidatze hedatuko politikarako zein oinarritzorako.

#### **Kode-sinaduraren ziurtagiria.**

Titular diren entitateei ematen zaie, software horren osagaien baten egiazkotasuna eta osotasuna bermatzeko.

#### **Ziurtagirien erabilera-esparrua**

Erabilera-esparruari dagokionez bi kasu bereizten dira:

- IZENPEk jaulkitako eta herritarrei, oro har, zuzendutako ziurtagiriak harpidedunek erabiliko dituzte, edo, hala badagokio, gakoan edukitzaileek, Nortasun Ziurtapen Digitaleko ziurtagiriak entitate publiko erabiltzaileekiko harremanetan, baita ziurtagiri horren erabilera onartu duten erakunde publiko eta pribatuekiko harremanetan ere.

Ziurtagiri bakoitzaren erabilpen-esparruari dagozkion xehetasunak Ziurtagiri bakoitzerako berariazko dokumentazioan kontsulta daitezke.

- IZENPEk jaulkitako eta entitate erabiltzaileek eskatutako ziurtagiriak antolakundearen eta betetzen den karguaren edo lanpostuaren berezko eskumenen barruan erabiliko dira. Dena den, gakoan edukitzaileek beste erabilera batzuetarako erabili ahal izango dituzte ziurtagiri horiek, baina beti aurreko a) idatz zatian adierazten diren erabilera-mugak errespetatzen badira.

Ziurtagiri bakoitzaren erabilpen-esparruari dagozkion xehetasunak Ziurtagiri bakoitzerako berariazko dokumentazioan kontsulta daitezke.

#### **1.4.2. Ziurtagiriaren erabilera debekatuak**

Berezkoa duten zereginerako eta ezarritako helbururako erabili behar dira ziurtagiriak, eta ez beste inongo zeregin eta eginkizunetarako.

Era berean, ziurtagiriak aplikatzekoa den legearen arabera soilik erabili beharko dira.

Ziurtapen Praktiken Deklarazio honen erregulazioaren mende dauden ziurtagiriak ezin izango dira erabili entitate-erregistro gisa izapideak egiteko.

Ziurtagiriak ez dira diseinatu egoera arriskutsuetan kontrol-ekipo gisara edo hutsegiteen aurkako jardueretan erabiltzeko (instalazio nuklearren funtzionamenduan, nabigazio-sistemetan, airetiko komunikazioetan, armamentuaren kontrol-sistemetan...). Jarduera horietan, akats batek heriotza, zauriak edo ingurumen-kalte larriak eragin ditzake.

## **1.5 Politikak**

### **1.5.1. Dokumentazioaren kudeaketaz arduratzen den entitatea**

IZENPE (Mediterraneoaren hiribidea 14, Gasteiz eta IFZ: 01337260) da ziurtapen-praktiken deklarazio hau aplikagarri duten ziurtagiri publikoak ematen dituen ziurtapen-entitatea.



### 1.5.2. Harremanetarako datuak

Zerbitzu-egilearen izena	Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, SA
Posta-helbidea:	Tomas Zumarraga Dohatsuaren kalea, 71-1. 01008 Vitoria-Gasteiz
Posta elektronikoko helbidea:	<a href="mailto:info@izenpe.com">info@izenpe.com</a>
Telefonia	902 542 542

### 1.5.3. Ziurtapen Praktiken Deklarazioaren egokitzapenaren arduradunak

IZENPEren administrazio-kontseilua arduratzen da Ziurtapen Praktiken Deklarazio hau onartzeaz, baita hari egin beharreko aldaketak onartzeaz ere.

### 1.5.4. Ziurtapen Praktiken Deklarazioa onartzeko prozedura

Dokumentu honetan egindako azken aldaketak IZENPEren Administrazio Kontseiluak onetsiko ditu, ezarritako baldintzak betetzen direla egiaztatu eta gero.

## 1.6 Definizioak eta akronimoak

### 1.6.1. Definizioak

- **Datuak Babesteko Espainiako Agentzia (APD):** zuzenbide publikoko ente bat da, berezko izaera juridikoa du eta ahalmen publiko eta pribatu osoa. Askatasun osoz burutzen ditu bere funtzioak, Administrazio Publikoen mende egon gabe. Helburu nagusia datuak babesteari buruzko legedia betetzen dela zaintzea eta legediaren aplikazioa kontrolatzea da.
- **Ziurtapen Agintaritza (CA):** Ziurtapen Agintaritza behar diren ziurtagiriak jaulkitzen dituen entitatea da, Erregistro Agintaritzak hala eskatu ondoren, modu automatizatuan eta Tokiko Erregistro Autoritatearen baieztapena jaso ondoren.
- **Erregistro Agintaritza (RA):** Erregistro Agintaritzak erabiltzaileen altak kudeatzen ditu (baita ezeztapenak eta bajak ere) gako publikodun azpiegitura batean. Erabiltzaileak Erregistro Agintaritzara joan behar du gako publikodun ziurtagiri bat eskatzeko, Erregistro Agintaritzarekin lotuta dagoen Ziurtapen Agintaritzaren bermearekin.
- **Denbora zigilatzeako agintaritza (TSA):** denbora-zigiluko tokenak jaulkitzen dituen agintaritza.
- Azken finean, ziurtagirien gakoak eskatzaileak, harpidedunak eta edukitzaileak identifikatuko dituzten entitateak dira; horrez gain, ziurtagirietan jasotzen diren zirkunstantziak egiaztatzen dituen dokumentazioa ziurtatzen dute, eta ziurtagiriak jaulkitzeko, ezeztatze eta berritzeko eskaerak balidatzen eta onartzen dituzte.



- **Ziurtagiria:** Ziurtapen Zerbitzuen Egileak elektronikoki sinatutako dokumentu elektronikoa da, sinadura egiaztatzeko datuak sinatzailearekin lotzen ditu eta haren identitatea baieztatzen du.
- **Oinarrizko ziurtagiria:** harpidedun gisa IZENPEren hierarkiako Ziurtapen Agintaritza bat duen ziurtagiria. Agintaritza horren sinadura egiaztatzeko datuak Ziurtapen Zerbitzuen Egile gisa daude sinatuta, agintaritzarenak diren sinadura sortzeko datuekin. IZENPEko entitate jaulkitzaileek hierarkia bat osatzen dute, horrela, oinarrizko entitate bat dago, komuna edozein ziurtagiritarako, eta mendeko entitate bat baino gehiago, ziurtagiri mota desberdinetarako.
- **Ziurtagiri kualifikatua:** Ziurtapen Zerbitzuen Egile batek emandako ziurtagiri elektronikoak dira. Ziurtapen Zerbitzuen Egile horrek sinadura elektronikoari buruzko abenduaren 19ko 59/2003 Legean ezarritako baldintzak betetzen ditu, identitateari eta eskatzaileen inguruko bestelakoei dagokienez, eta ematen dituzten ziurtapen-zerbitzuen bermeei dagokienez.
- **Erabilera orokorreko ziurtagiriak:** ziurtagiri arruntak dira, legez ziurtagiri aitortutzat jotzen ez direnak. Harpidedunaren eta, hala badagokio, sinadura-gakoaren edukitzailearen identitatea bermatzen dute. Era berean, nahikoa segurua den sinadurak sortzeko gailu batekin batera erabili behar dira.
- **Gakoa:** zifratze- eta deszifratze-eragiketak kontrolatzeko erabilitako sinbolo-sekuentzia.
- **Konfidentziasuna:** konfidentziasuna dokumentu elektroniko bat pertsona-zerrenda jakin bati izan ezik gainerako erabiliztaile guztiei eskuraezin egiteko gaitasuna da. Horrela, komunikazioak beste batzuek entzun ezin izateko moduan egitea eta dokumentuak adierazitako hartzaileak soilik irakurri ahal izateko moduan igortzea lortu dezakegu.
- **Kriptografia:** kriptografia matematikaren adar bat da, eta aztertzeko duena da nola eraldatu informazio irakurgarria zuzenean ezin irakurtzeko moduan, hau da, irakurtzeko deszifratu behar izateko moduan.
- **Sinadura sortzeko datuak (Gako Pribatua):** gako pribatua zenbaki bakar eta sekretua da eta pertsona bakar bati dagokio, horrela, pertsona bere gako pribatuaren bitartez identifika daiteke. Gakoa asimetrikoa da gako publikoarekiko. Gako batek beste gako batek sinatu edo zifratu duena egiaztatu eta deszifratu dezake.
- **Sinadura Egiaztatzeko Datuak (Gako Publikoa):** gako publikoa pertsona bakar bati dagokion zenbaki bakarra da baina, gako pribatua ez bezala, edonork jakin dezake. Prozedura matematikoen bitartez gako pribatuarekin lotu eta sinadura digitalak zifratzeko eta egiaztatzeko balio du.
- **Ziurtapen Praktiken Deklarazioa (ZPD):** IZENPEk edonorentzat eskuragarri duen deklarazioa, erraz lortu daitekeena, elektronikoki eta dohainik.
- ZPDak segurtasun-dokumentuaren balioa du eta bertan zehazten dira –sinadura elektronikoari buruzko 59/2003 Legeari eta haren garapen-xedapenei jarraiki– zein diren Ziurtapen Zerbitzuen Egileen betebeharrak, sinadura sortzeko nahiz egiaztatzeko datuak kudeatzeari dagokionez eta ziurtagiri elektronikoak kudeatzeari dagokionez, hala nola, zein diren aplikagarri diren baldintzak ziurtagiria eskatzean, jaulkitzean,



erabiltzean, eteteen nahiz iraungitzean, zein diren segurtasun-neurri teknikoak eta antolakuntzari dagozkionak, zein diren ziurtagirien indarraldiari buruzko profilak eta informazio-mekanismoak. Bertan zehazten da, halaber, koordinazio-prozedurak izan behar direla dagozkien erregistro-publikoekin, ziurtagirietan aipatzen den ahalmenaren indarraldiari buruzko informazioa –erregistro horietan aginduz jaso beharko dira– berehala elkarri trukatzeko.

- **Ziurtagirien direktorioa:** ITU-Tren X.500 estandarren arabera informazio-biltegia. Horrela, IZENPEk ziurtagirien direktorio eguneratua mantentzen du eta direktorio horrek egindako ziurtagiriak, horiek indarrean dauden edo beren indarraldia eten edo iraungi den emango du aditzera.
- **Sinadura sortzeko gailu segurua:** sinadura sortzeko datuak aplikatzeko balio duen gailua da. Espainiako aplikazio-arau espezifikoetan ezarritakoei jarraitzen dio, baita Europako Parlamentuko 1999/93/EE Zuzentarauan bildutakoei eta sinadura elektronikoari esparru komuna ezartzen dion 1999ko abenduaren 13ko Europako Kontseiluko arauan ezarritakoari ere.
- **Sinadura elektronikoa:** datu multzo elektronikoa, beste batzuekin batera idatzia edota beste horiei lotua, eta sinatzailea identifikatzeko modu gisa erabil daiteke.
- **Sinadura elektronikoa aurreratua:** sinatzailea identifikatzen duen sinadura elektronikoa da, eta sinatutako datuen ostean egondako edozein aldaketa hauteman dezake. Sinatzaile bakarrarekiko eta sinadurak berak biltzen dituen datuekiko lotura du, eta sinatzailea bakarrik ezagutu dezakeen moduan sortzen da.
- **Sinadura elektronikoa kualifikatua:** sinadura elektronikoa kualifikatua ziurtagiri onartu batean oinarritzen den eta sinadura sortzeko gailu seguru baten bidez sortu den sinadura elektronikoa aurreratua da.
- **Sinatzailea:** sinadura sortzeko gailua duen pertsona, eta nor bere izenean edota ordezkatzan duen pertsona fisiko edo juridikoaren izenean jarduten du.
- **Hash edo hatz-marka:** mezu bati hash funtzioa aplikatu ostean lortzen den emaitza, tamaina zehatzekoa, eta hasierako datuetara modu unibokoan lotuta dagoena.
- **HSM (segurtasun-modulu kriptografikoa):** gako kriptografikoak sortu eta babesten dituen segurtasunerako gailua.
- **Gako Publikoen Azpiegitura (PKI, Public Key Infrastructure):** PKIak ziurtagiri-sistema zein entitatek osatuko duten zehazten du, entitate horiek zein betekizun betetzen duten, zein arau eta protokolori jarraitu behar zaion sistema barnean lan egiteko, informazio digitala nola kodetzen den eta nola transmititzen den, eta zein izango den azpiegiturak kudeatzen dituen objektu eta dokumentuetako informazioa. Horrek guztiak Gako Publikoko teknologia izango du oinarri (bi gako).
- **Abenduaren 13ko 15/1999 Lege Organikoa, datu pertsonalak babesteari buruzkoa:** Lege Organikoa honen helburua da datu pertsonalak baliatzerakoan pertsona fisikoaren askatasun publikoak eta oinarrizko eskubideak bermatu eta babestea, batez ere, pertsona horien ohorea eta intimitate pertsonal eta familiara.
- **Ezetzatutako Ziurtagirien Zerrenda (CRLak):** IZENPEk jaulkitzen dituen ziurtagiri ezetzatuek edo etendakoek osatzen duten zerrenda da, eta berehalako ezetzatze bat gertatzen den bezain laster geratzen da jasota zerrendan. Bada beste web-zerbitzu



iraunkor bat ere, IZENPEk ezeztatutako ziurtagirien eguneratze inkremental telematikoa kontsultatzeko aukera eskaintzen duena. Ezeztatutako Ziurtagirien Zerrendak argitaratzeari dagokionez, sarbide azkarra eta segurua bermatzen zaie erabiltzaileei eta ziurtagirien harpidedunei.

- **Ziurtagiriaren serie-zenbakia:** balio osoa eta bakarra da, eta modu unibokoan dago edozein Ziurtapen Zerbitzuen Egilek jaulkitako ziurtagiri bati lotuta.
- **OCSP (Online Certificate Status Protocol):** ziurtagiri elektronikoa indarrean dagoen ala ez frogatzen duen protokolo informatikoa da.
- **OID (Object Identifier):** aldagai oso ez negatiboez –puntu batez banatuta– osatzen duten sekuentzia. Erregistratutako objektuei egokitu dakieke, eta bakarrik dira gainerako OID guztien artean.
- **PIN (Personal Identification Number):** mekanismo honen beraren babespean dagoen baliabide batera sartu behar duen subjektuak bakarrik ezagutu behar duen karaktere-sekuentzia.
- **PKCS (Public-Key Cryptography Standards):** estandarrik ohikoena da informazioa, hala nola, ziurtagiriak edo sinatutako fitxategiak kodetzeko. Programatzaileek edo analisigileek konbentzio edo estandar horiei “formatu” edo “lay-out” deitzen diete. PKCSk “Public Key Cryptography Standards” esan nahi du.
- **PKCS#10 (Certification Request Syntax Standard):** ziurtagiria eskatzeko estandarra. Gako publiko baten ziurtapena eskatzeko Ziurtapen Agintaritza bati bidaltzen zaizkion mezuen formatua zehazten du.
- **PKCS #12 (Personal Information Exchange Syntax Standard):** informazio pertsonala elkarbanatzeko sintaxiaren estandarra. Gako pribatuak gako publikoko ziurtagiriarekin batera eta kode simetrikoaz babestuta biltzeko oro har erabiltzen den fitxategiaren formatua zehazten du.
- **Ziurtapen-politika:** Ziurtapen Praktiken Deklarazioari erantsitako dokumentua da, eta bertan jasotzen da zein den ziurtagirien aplikazio-eremua, karaktere teknikoak, ziurtapen-zerbitzuak ematerakoan jarraitutako prozeduretarako arauak, baita ziurtagirien erabilpen-baldintzak ere.
- **Gakoen edukitzaileak:** kautotzeko gakoak eta sinadura digitala dituzten eta horiek zaintzeaz arduratzen diren pertsona fisikoak izango dira.
- **Ziurtapen Zerbitzuen Egilea (ZZE):** ziurtagiri elektronikoak jaulkitzen dituen edota sinadura elektronikoarekin lotutako bestelako zerbitzuak ematen dituen pertsona fisiko edo juridikoa da.
- **Egiatzapen Aurreratuko Zerbitzua:** zerbitzu honek aukera ematen dio zerbitzuaren Entitate Erabiltzaileari IZENPEk jaulkitako ziurtagiriak erabiltzeko. Horretarako, ziurtagirien egoera begiratzen du, OCSP (Online Certificate Status Protocol) protokoloaren bidez.
- **PUK (Personal Unblocking Key):** baliabide baterako sarbidea desblokeatzeko erabiltzen den baliabidera sartuko den subjektuak bakarrik dakien karaktere-sekuentzia.



- **Argitalpen Zerbitzua:** ziurtapen-sistemearekin lotutako dokumentazioa argitaratzen duen zerbitzua da, eta ziurtagirien erabiltzaile guztientzat egon behar du erabilgarri.
- **Denbora Zigiluen Zerbitzua:** Denbora Zigiluen Zerbitzuak entitate erabiltzaileari aukera ematen dio bermatzeko denbora-tarte jakin batean informazio jakin bat bazegoela.
- **Zerbitzari segurua:** Web-zerbitzari bat da eta, bertan, komunikazioa zifratuta doa batetik bestera, modu seguruan. Eragiketa hori egin ahal izateko, zerbitzariak ziurtagiri bat izan beharko du.
- **Ziurtagiriaren eskatzailea:** nork bere buruaren izenean, edota erakunde batenean, ziurtagiri bat jaulkitzea eskatzen duen pertsona da.
- **SSL (Secure Socket Layer):** protokolo honek bide ematen du zifratutako informazioa Interneteko nabigatzaile baten eta zerbitzari baten artean transmititzeko.
- **Ziurtagiriaren harpideduna:** Ziurtapen Zerbitzuen Egileak ziurtatutako gako publikoaren bitartez identitate pertsonala elektronikoki sinatutako datuei lotua duen pertsona.
- **Txartel kriptografikoa:** Sinadura Sortzeko Gailu Seguru gisa hartzen den txartela da, eta harpidedunak, besteak beste sinatzeko eta kautotzeko erabiltzen diren gako pribatuak biltzeko, sinadura elektronikoa sortzeko eta datu-mezuak desfzifratzeko erabil dezake.
- **Hirugarrengogan konfiantza duten hirugarren batzuk:** IZENPEk jaulkitako ziurtagiriak jasotzen dituzten pertsona fisikoak edo juridikoak dira. Ziurtagirietan konfiantza duten hirugarren batzuk dira eta, hirugarrenak diren heinean, Ziurtapen Praktiken Deklarazioan ezarritakoa zaie aplikagarri, baldin eta ondorioetarako ziurtagiri horietan benetan konfiantza badute.
- **Ziurtagirien erabiltzaileak:** Ziurtagirien erabiltzaile diren azken entitateak ziurtagiri digitalak jaulki, kudeatu eta erabiltzeko zerbitzuak jasotzen dituzten pertsona eta erakundeak dira.

### 1.6.2. Akronimoak

**ARL:** Ziurtapen Agintaritzak Ezeztatzeko Zerrenda.

**CA:** Ziurtapen Agintaritzak.

**CA/B:** CAs and Browser

**CN:** Common Name (izen arrunta).

**CRL:** Certificate Revocation List (ezeztatutako ziurtagirien zerrenda).

**DN:** Distinguished Name (izen bereizgarria).

**ZPD:** Ziurtapen Praktiken Deklarazioa

**DSCF:** Sinadura sortzeko gailu segurua.

**ETSI:** European Telecommunications Standards Institute

**GN:** Given Name (izena).



**HSM:** Hardware Security Module (segurtasun-modulu kriptografikoa).

**SEL:** Sinadura elektronikoari buruzko abenduaren 19ko 59/2003 Legea.

**LRA:** tokiko erregistro-agintaritza.

**OCSP:** Online Certificate Status Protocol (Ezeztatutako Ziurtagirien Argitalpen Zerbitzua, data eta ordu batetik aurrera).

**OID:** Object Identifier (objektu-identifikatzaile bakarra).

**PIN:** Personal Identification Number (identifikazio pertsonaleko zenbakia).

**PKCS:** Public Key Cryptography Standards (RSA Laborategiek garatutako PKI estandarrak).

**PKI:** Public Key Infrastructure (gako publikoen azpiegitura)

**ZZE:** Ziurtapen Zerbitzuen Egilea

**PUK:** Personal Unblocking Key (desblokeatze-kodea).

**RA:** Erregistro-agintaritza.

**SSL:** Secure Socket Layer

**TSA:** Time Stamping agintaritza-zerbitzua



## 2 Argitalpena eta informazio-biltegiaren arduradunak

---

### 2.1 Informazio-biltegia

IZENPEk informazio publikoko biltegia du <http://www.izenpe.com> helbidean, eta asteko zazpi egunetan eta eguneko 24 orduetan dago eskuragarri.

### 2.2 Ziurtapen-informazioaren argitalpena

IZENPEren Argitalpen Zerbitzuaren bitartez ziurtapen digitalari buruzko informazioa eta zerbitzu osagarriari buruzko informazioa argitaratzen da.

Informazio hori [www.izenpe.com](http://www.izenpe.com) web-orrian dago eskuragarri, 24 orduetan eta asteko 7 egunetan.

IZENPEk,

- On line informazioaren eskuragarritasuna bermatzen du.  
Dena den, dokumentu horren bertsio osoa, paperezko euskarrian, eman ahal da ikuskapenak, inspektzioak edo ziurtapen-zerbitzuen beste egile batzuekin ziurtapen gurutzatuak egin behar direnean, edo gakoak edukitzaileak edo hirugarren batek hala eskatzen dutenean.
- Jaulkitako ziurtagirien erregistroa azkar eta modu seguruan kontsultatzeko aukera eskaintzen du. Ziurtagirietan konfiantza duten hirugarrenek ere kontsulta dezakete erregistroa.
- Ziurtagirien sistema eguneratua mantentzen du eta sistema horrek egindako ziurtagiriak, horiek indarrean dauden edo beren indarraldia eten edo iraungi den emango du aditzera.
- Ezeztatutako Ziurtagirien Zerrendak (CRLak) jaulkitzen ditu eta, erabiltzailearentzako eskuragarri egonez gero, ziurtagiriak denbora errealean egiaztatzeko zerbitzuak eskaintzen ditu, Online Certificate Status Protocol-aren bidez (OCSP).
- Ezeztatutako Ziurtagirien Zerrendak argitaratzeari dagokionez, sarbide azkarra, segurua eta doakoa bermatzen zaie erabiltzaileei eta ziurtagirien harpidedunei.

#### 2.2.1. Argitalpen- eta jakinarazte-politika

Zerbitzuaren zehaztapenetan edo baldintzetan egindako aldaketak IZENPEren web-orri nagusiaren ([www.izenpe.com](http://www.izenpe.com)) bidez jakinaraziko dizkie IZENPEk erabiltzaileei.

30 egunez egingo da aldaketen aipamena, eta bertan jasoaraziko da aldatu den dokumentua, eguneratze-dokumentua eta bertsio berria.

30 egunera, egindako aldaketen aipamena kenduko da , baita bertsio zaharra dokumentaziotik ere. Azken hori IZENPEk gordeko du gutxienez 15 urtez, eta kontsultatu ahal izango dira interesatuen justifikazio arrazoituaren ondoren.



### **2.2.2. Ziurtapen Praktiken Deklarazioan argitaratzen ez diren elementuak**

Ziurtapen Praktiken Deklarazio honetako 9.3. atalean lehendik dauden osagaiei, azpiosagaiei eta elementuei, baina horien konfidentzialtasuna gordetzeko publikoarentzat erabilgarri ez daudenei, egiten zaie erreferentzia.

## **2.3 Argitalpen-maiztasuna**

Ziurtapen Praktiken Deklarazioa onartzen den unean ematen da argitara. Ziurtapen Praktiken Deklarazioan egin beharreko aldaketak dokumentu honek dioenaren arabera egin behar dira.

Ziurtagirien egoerari buruzko informazioa dokumentu honetako 4.9.6, 4.9.7 eta 4.9.9 atalek diotenaren arabera argitaratu behar da.

## **2.4 Biltegirako sarrera kontrolatzea**

IZENPEk bere biltegian argitaratutako informazioa irakurtzen uzten du, baina kontrolak ezartzen ditu baimenik gabeko jendeak Zerbitzu horretan erregistrorik sar ez dezan, lehendik zeudenak alda edo ezaba ez ditzan, eta horko informazioaren osotasuna eta egiazkotasuna babesteko.

IZENPEk sistema fidagarriak erabiltzen ditu informazio-biltegiara sartzeko. Horrela:

- Baimendutako jendeak bakarrik erants dezake informazioa edo egin ditzake aldaketak.
- Informazioaren egiazkotasuna egiaztatzea badago.
- Ziurtagiriak kontsultarako daude eskuragarri.
- Segurtasun-baldintzei eragiten dien aldaketa oro antzeman egiten da.



## 3 Izenak

---

### 3.1.1. Izen motak

Azken entitateko ziurtagiri guztiek izen bereizgarri bat daukate Subject Name eremuan.

Ziurtagiriaren subject eremuko izen bereizgarria osatzen duten ezaugarriak ziurtagiriaren profilaren atalean bildutakoak dira.

*Common Name* eremuaren balio kautotua gakoan edukitzailearen izena da.

Batzuetan, *subjectAltName* eremua erabiltzen da subjektua identifikatzeko izena (Subject Name eremuko ez bezalakoa) edukitzeko.

#### Igorlea (SEL legearen 11.2 c) artikulua eskakizuna)

Eremu honetan egoten da IZENPEren identifikazioa, hori baita ziurtagiria izenpetu eta jaulki duen ziurtapen-entitatea.

Eremu horrek ezin du zuriz egon, eta nahitaez eduki behar du hainbat ezaugarri dituen izen bereizgarria (DN) –izen bat edo etiketa bat eta hori dagokion balioa–.

Mendeko CAen issuer eremua bat dator ziurtagiri horiek jaulki dituen CAren subject eremuarekin.

#### Gaia (SEL legearen 11.2 e) artikulua eskakizuna)

Harpidedunaren edo IZENPEk jaulkitako ziurtagiriaren titularraren identifikazioa egoten da eremu honetan (horren Issuer eremuan identifikatutako CA).

Eremuak ez du hutsik egon behar; nahitaez eduki behar du izen bereizgarri bat (DN). Hainbat ezaugarri ditu izen bereizgarriak: izena edo etiketa, eta horri dagokion balioa.

*Ziurtagiri bakoitzerako berariazko dokumentazioan* ezartzen da ziurtagiri bakoitzaren profil zehatza.

### 3.1.2. Izenen formatuak interpretatzeko arauak

Erabaki gabe.

### 3.1.3. Izen-bakartasuna

Bakarrak dira harpidedunen eta, hala badagokie, gakoan edukitzaileen izenak ziurtagiri-mota bakoitzerako, IZENPEren Ziurtapen Praktiken Deklarazioaren barruan.

### 3.1.4. Izenen eta marka erregistratuen tratamenduaren arloko gatazkek ebaztea

Etorkizuneko harpidedunak hirugarrenen eskubideak urratzeko moduko izenik ez dute jarri behar ziurtagiri-eskatzaileek ziurtagiriak jaulkitzeko eskaeretan.

IZENPEk ez du erabakitzen ziurtagiri-eskatzaileak baduen eskubiderik ziurtagiri-eskaeran ageri den izenaren gainean. Halaber, ez du artekari- edo arbitro-lanik egiten, eta ez du beste inola ebazten pertsona-, erakunde- edo domeinu-izenen jabetzaren gaineko auzirik.



IZENPEk eskubidea dauka ziurtagiri-eskubiderik ez onartzeko izenei buruzko auziak direla eta.

## **Marka erregistratuen tratamendua**

IZENPEk ez du erabakitzen ziurtagiri-eskatzaileak baduen eskubiderik ziurtagiri-eskaeran egon daitezkeen marken gainean.

Halaber, ez du artekari- edo arbitro-lanik egiten, eta ez du beste inola ebazten marka edo izen komertzialen jabetzaren gaineko auzirik.

IZENPEk eskubidea dauka ziurtagiri-eskabiderik ez onartzeko marka edo izen komertzialei buruzko auziak direla eta.

## **3.2 Identitatea balidatzea**

### **3.2.1. Gako pribatuaren jabetza frogatzeko metodoak**

Gako-parea

- Erregistro-entitate batek sortua bada eta gakoak txartel kriptografiko batean kokatuta daudenean, honela frogatzen da gako pribatuaren jabetza: gailu kriptografikoa entregatzeko eta onartzeko prozedura fidagarriaren indarrez, horri dagokion ziurtagiriaren bitartez, eta barruan duen gako-pareari esker.
- Erregistro-entitate batek sortua bada eta gakoak HSM batean kokatuta daudenean, honela frogatzen da gako pribatuaren jabetza: HSMan zaintzeko prozedura fidagarriaren indarrez, eta gakoak harpidedunak soilik eskuratzeko prozedura fidagarriaren bitartez.
- Ziurtagiriaren gakoan edukitzaileak sortua bada, honela frogatzen da gako pribatuaren jabetza: ziurtagiria behar bezala erabiliz.

### **3.2.2. Antolakundearen nortasuna kautotzea**

Ikusi *Ziurtagiri bakoitzerako berariazko dokumentazioan*.

### **3.2.3. Pertsona fisiko eskatzailearen nortasuna kautotzea**

Ikusi *Ziurtagiri bakoitzerako berariazko dokumentazioan*.

## **3.3 Gakoak berriro jaulkitzeko eskaeratarako identifikatzea eta kautotzea**

IZENPEk gakoak sortzen dituen ziurtagirietan, ziurtagiria ezeztatu eta beste bat jaulki ondoren, gakoak berriro egin behar dira beti.

## **3.4 Ezeztatzeko eskaeratarako identifikatzea eta kautotzea**

Ezeztatzeko eskaera bat kautotzeko baldintzak *Ziurtagiri bakoitzerako berariazko dokumentazioan* garatzen dira.



## 4 Ziurtagirien bizi-zikloaren baldintza operatiboak

---

Ziurtapen Praktiken Deklarazio honek ziurtagirietarako komunak diren baldintza operatiboak arautzen ditu.

Ziurtagiri mota bakoitzerako berariazko erregulazioa *Ziurtagiri bakoitzerako berariazko dokumentazioan* begiratu behar da.

### 4.1 Ziurtagiria eskatzea

Kontsultatu *Ziurtagiri bakoitzerako berariazko dokumentazioa*

Ziurtagiria edo dagokion dokumentazioa jaulkitzean eta/edo banatzean izandako akats teknikoen ondoriozko ezeztatzeak eragindako jaulkitzeen kasuan, ez da beharrezkoa izango ziurtagiria *jaulkitzeko* beste eskaera bat egitea.

Debekatuta dago gakoan edukitzaile beraren alde datu berberak dituen ziurtagiri bat baino gehiago jaulkitzea.

Horretarako, erregistro-entitateak egiaztatu egiten du –jaulkitze-prozesuari ekin aurretik– gakoan edukitzaile izango dena ez dela eskaera egin duen eta une horretan indarrean dagoen mota horretako beste ziurtagiri baten titularra.

Horretarako, zehaztasunez idatzi behar dira identifikazio-dokumentuetan bildutako datu identifikatzaileak, betiere ziurtagiriaren edukian finkatutako baldintza teknikoek eragiten dituzten leku-mugak kontuan izanik..

#### 4.1.1. Eskaeraren egiaztapena

Ziurtagiria jaulki aurretik, IZENPEk eskaera jasoarazitako datuak egiaztatuko ditu.

#### 4.1.2. Inskribatzeko prozesua eta erantzukizunak.

Erregistro-entitateek egingo dituzte ziurtagirian jasoarazi den informazioa identifikatzeko eta egiaztatzeko zereginak, eta ziurtagiri horiek jaulkitzeko, ezeztatzeko eta berritzeko eskaerak balidatuko eta onartuko dituzte.

IZENPEren berezko erregistro entitateek edota IZENPErekin dagokion lege-tresna sinatzen duten entitate erabiltzaileek honako betebeharrak hartu beharko dituzte bere gain:

- Eskatzailearen, harpidedunaren eta gakoan edukitzailearen nortasuna eta beste zenbait datu pertsonal egiaztatzea –ziurtagirien xedetarako garrantzizkoak direnak edo ziurtagirietan daudenak–, prozedura hauen arabera.
- Kudeatzen dituen ziurtagirien jaulkipenari, berritzeari, ezeztatzeari edo berraktibatzeari buruzko dokumentazio eta informazio guztia gordetzea.
- IZENPEri garaiz jakinaraztea ziurtagiriak azkar eta modu fidagarrian ezeztatzeko eskaeren berri.



- IZENPERi artxihoak erabiltzen uztea, baita jardueretarako erabiltzen diren prozeduren eta horretarako behar den informazioaren mantentze-lanen ikuskapena egiten ere.
- IZENPERi jakinaraztea ziurtagiriak jaulki, berritu edo berraktibatzeke eskaeren berri, baita hark jaulkitzen dituen ziurtagiriei buruzko beste zeinahi alderdiren berri ere.
- Garaiz begiratzea ziurtagirien iraunaldian eragina izan dezaketen ezeztatzeko zergatiak.
- Ziurtagiriak jaulki, berritu eta ezeztatzeko IZENPEk ezarritako prozedurak eta gai horretaz indarrean dagoen legeriak agindutakoa betetzea.
- Hala dagokionean, bere gain hartu ahal du eginkizun hau ere: gakoan edukitzailearen esku jartzea sinadura (gako pribatua) sortzeko eta sinadura elektronikoa (gako publikoa) egiaztatzeke prozedura teknikoak.

## 4.2 Eskaerak prozesatzea

### 4.2.1. Identifikatzeko eta kautotzeko eginkizunak egitea

IZENPERen erantzukizuna da harpideduna behar bezala identifikatzea. Prozesu hori ziurtagiria jaulki aurretik egin beharko da.

Dena den, ziurtagiri mota bakoitzerako xehetasunak *Ziurtagiri bakoitzerako berariazko dokumentazioan* begiratu behar dira.

### 4.2.2. Eskaerak onartzea edo baztertzea

Ziurtagiria eskatu ondoren, RAK eskatzaileak emandako informazioa egiaztatu beharko du, harpidedunaren identitatearen balidazioa barne.

Informazioa zuzena ez bada, RAK eskaerari ezezkoa emango dio eta eskatzailearekin harremanetan jarriko da arrazoa jakinarazteko. Zuzena bada, berriz, ziurtagiria jaulkitzeari ekingo zaio.

Eskaera hori zerbitzari bat kautotzeko domeinu-izen bat barnean hartzen duen ziurtagiri baterako denean, IZENPEk baimendutako CAen erregistroa (CAA erregistroa) aztertuko du, RFC 6844 arabera. CAA erregistro horiek badaude eta, erregistratuta ez dagoelako, IZENPERi ez badiote ziurtagiri horiek jaulkitzeko aukera ematen, IZENPEk ez du ziurtagiri hori jaulkiko, baina eskatzaileek eskaera egin ahal izango dute berriro, behin IZENPEk balizko gorabehera hori konpondu ahal izan duenean.

Dena den, ziurtagiri mota bakoitzerako xehetasunak *Ziurtagiri bakoitzerako berariazko dokumentazioan* begiratu behar dira.

## 4.3 Ziurtagiria jaulkitzea

Ziurtagiria egiteak berarekin dakar eskaeraren azken onarpena, eta osoa.

IZENPEk ziurtagiria jaulki eta emateari ekingo dio,



- Bertaratuta entregatzen den kasuetan, ziurtagiria jaulkitzeko unean, IZENPEk PINa eta PINa desblokeatzeko kodea (PUKa) eta telefono bidez identifikatzeko pasahitza adieraziko duen orria emango du.
  - Une horretan, ziurtagiria ematearen justifikatzailea sinatu beharko du eskatzaileak, jaulkitzeko eskaeraren bidez.
- Bertaratuta eskatu ez bada, ziurtagiria jaulkitzeko eskaeran finkatutako posta helbidera igorriko da ziurtagiria. Bi une bereiziko dira:
  - Ziurtagiria bidaltzea.
  - PINa, PINa desblokeatzeko kodea (PUKa) eta telefono bidez identifikatzeko pasahitza adieraziko duen orria bidaltzea.

Ez dira desblokeatzeko kodeak (PIN edo PUK) emango IZENPEk gakoak sortu ez dituen ziurtagirien kasuan.

Ziurtagiria jaulkitzeko eskaeratik hilabeteko epea pasa eta eskatzaileak ziurtagiria jaso ez badu, IZENPErekin jarri beharko da harremanetan.

Eskatzaileak Entrega eta Onarpen Orria sinatuta itzuli beharko dio IZENPERi.

#### **4.3.1. CAren jardunak ziurtagiriak jaulkitzean**

Ziurtagiriaren arabera, smartcard-ean, HSMan edota software-euskarrian jaulki daiteke.

I. Smartcard-ean jaulkitzerakoan jarraitu beharreko prozedura:

- Erregistro Entitateak egiaztatu egiten du eskatzaileek aurkeztutako dokumentuaren baliozkotasuna.
- Kautotze-lana amaitu ondoren, ziurtagiri bat jaulkitzeko eskatzen dio IZENPERi erregistro-entitateak.
- Eskaera erregistro-entitate baimendu batek bidali duela egiaztatu ondoren, IZENPEk ziurtagiria jaulkitzen du –ezarritako prozedurari jarraiki– eta erregistro-entitateari igortzen dio.
- Eskaera IZENPEk bidali duela egiaztatu ondoren, erregistro-entitateak sinadura sortzeko gailuan kargatzen du ziurtagiria, gailu kriptografikoak kudeatzeko prozesu seguru bat erabiliz.
- Segurtasun-arrazoiak direla medio (ziurtagirien gako pribatuaren konfidentzialtasuna) PIN bat eta PIN hori desblokeatzeko kode bat (PUK) sortzen dira, ausaz. Horiek konfidentzialtasuna gordetzeko moduan ematen zaizkio harpidedunari edo gakoaren edukitzaileari (baldin eta pertsona berbera ez badira).
- Modu seguruan eman behar zaizkio ziurtagiria eta gutunak (barruan PINa eta PUKa dituztenak) ziurtagiriaren harpidedunari edo gakoaren edukitzaileari.



- Arrazoiren batengatik IZENPEk ziurtagiria ez jaulkitzea erabakitzen badu (nahiz eta kautotze-prozedurak egokiak izan), erabaki horren arrazoiak jakinarazi egin behar zaizkio eskatzaileari.

## II. HSMan jaulkitzerakoan jarraitu beharreko prozedura:"

- Erregistro Entitateak egiaztatu egiten du eskatzaileek aurkeztutako dokumentuaren baliozkotasuna.
- Kautotze-lana amaitu ondoren, ziurtagiri bat jaulkitzeko eskatzen dio IZENPERi erregistro-entitateak.
- Eskaera erregistro-entitate baimendu batek bidali duela egiaztatu ondoren, IZENPEk ziurtagiria jaulkitzen du –ezarritako prozedurari jarraiki– eta erregistro-entitateari igortzen dio.
- Eskaera IZENPEk bidali duela egiaztatu ondoren, erregistro-entitateak sinadura sortzeko gailuan kargatzen du ziurtagiria, gailu kriptografikoak kudeatzeko prozesu seguru bat erabiliz.

Arrazoiren batengatik IZENPEk ziurtagiria ez jaulkitzea erabakitzen badu (nahiz eta kautotze-prozedurak egokiak izan), erabaki horren arrazoiak jakinarazi egin behar zaizkio eskatzaileari.

## III. Ziurtagiria software-euskarrian jaulki behar bada jarraitu beharreko prozedura:

- Erregistro Entitateak egiaztatu egiten du eskatzaileek aurkeztutako dokumentuaren baliozkotasuna.
- Eskaera-formularioarekin batera, eskatzaileak gako-parea sortu beharko du zerbitzarian bertan, eta IZENPERi eman beharko dio eskaera teknikoa..
- Dokumentazioa jaso ondoren jaulkiko du IZENPEk ziurtagiria.

Ziurtagiri bakoitza jaulkitzeko zehaztasunak *Ziurtagiri bakoitzerako berariazko dokumentazioan* begiratu behar dira.

### 4.3.2. Jaulkipena jakinaraztea harpidedunari

IZENPEk ziurtagiriaren jaulkipenaren berri emango dio harpidedunari.

## 4.4 Ziurtagiria onartzea

Ziurtagiria onartzeak berekin dakar harpideduna bat etortzea IZENPERen eta harpidedunaren eskubideak eta betekizunak zehazten dituen xehetasunekin eta baldintzekin, baita IZENPERen ziurtapen digitaleko zerbitzuen gidaritza teknikoa eta operatiboa egiten duen Ziurtapen Praktiken Deklarazio hau ezagutzea ere.



Harpidedunak edo gakoan edukitzaileak 15 eguneko epea du (ziurtagiria ematen zaionetik kontatzen hasita) ziurtagiriak behar bezala funtzionatzen duela egiaztatzeko eta, hala behar izanez gero, erregistro-entitateari itzultzeko.

Arrazoi teknikoengatik gaizki funtzionatzen duelako (besteak beste, ziurtagiriaren euskarriak gaizki funtzionatzen duelako, programak bateraezinak direlako, ziurtagiriko oker teknikoagatik, etab.) edo ziurtagiriko datuak oker daudelako itzultzen bada, IZENPEk ezeztatu egingo du ziurtagiria, eta beste bat jaulkiko du.

#### **4.4.1. Ziurtagiria onartzeko prozesua**

Ziurtagiria eskatzeko dokumentuaren arabera, erabilera-baldintzak eta harpidedunaren kontratua onartzen dira –biak nahitaez bete beharrekoak–, eta horren lekuko sinatu beharko du harpidedunak entrega- eta onarpen-orria.

#### **4.4.2. CAk ziurtagiria argitaratzea**

Harpidedunak ziurtagiria onartu eta sortu ostean, beharrezkoak diren ziurtagiri-biltegietan emango da argitara ziurtagiri hori.

#### **4.4.3. CAk beste entitate batzuei ziurtagiria jaulki izana jakinaraztea**

IZENPEk ez die beste entitate batzuei jakinaraziko ziurtagiriak jaulki dituela, IZENPEren Certificate Transparency Log Server zerbitzuan argitaratutako EV ziurtagiriak izan ezik.

### **4.5 Gako-parea eta ziurtagiriaren erabilera**

#### **4.5.1. Harpidedunaren gako pribatua eta ziurtagiriaren erabilera**

Bere gakoak zaintzen dituen harpidedunak,

- Ziurtagirien euskarriak ongi erabili eta gordeko direla bermatuko du.
- Ziurtagiria egokiro erabiliko du, eta, zehazki, ziurtagirien erabilera-mugak aintzat hartuko ditu.
- Arretaz zainduko du gako pribatua, baimendu gabeko erabilerak saihestearren, Ziurtapen Praktiken Deklarazioko 6.1, 6.2 eta 6.4 sailek agintzen dutenaren arabera.
- IZENPEri eta, harpidedunaren ustez, ziurtagirian konfiantza duen edonori hau jakinaraziko dio, justifikatzerik ez dagoen atzerapenik gabe:
  - Gako pribatua galdu, norbaitek ostu edo arriskuan jarri izana.
  - Gako pribatuaren kontrola galdu izana, aktibatze-datuak (gailu kriptografikoaren PIN kodea, adibidez) arriskuan jartzeagatik edo beste edozein arrazoirengatik.



- Ziurtagiriaren edukian dauden okerrak edo izandako aldaketak (harpidedunak dakizkienak edo jakin litzakeenak). Aldaketak ziurtagiria ezeztatzea badakar, horretarako eskaera egin behar du harpidedunak.
- Gako pribatua erabiltzeari utziko dio ziurtagiriaren balio-epea amaitu ondoren.
- Gakoen edukitzaileei jakinaraziko die zein betebeharrak dagozkien.
- Ez du ziurtagiri-zerbitzuen ezartze teknikoak kontrolatuko eta manipulatu, ezta atzeranzko ingeniartzako ekintzarik egingo ere, aurrez Ziurtapen Entitatearen idatzizko baimenik eduki gabe.
- Ez du ziurtagiri-zerbitzuen segurtasuna arriskuan nahita jarriko.
- Ez ditu ziurtagirietako gako publikoei dagozkien gako pribatuak erabiliko inongo ziurtagiri izenpetzeko, ziurtapen-entitatea balitz bezala.
- Ziurtagirian zerrendatutako gako publikoari dagokion gako pribatua erabiliz sinadura digitalak sortzen dituen ziurtagiri onartuen harpidedunak aitortu egin behar du, dagokion bitarteko juridikoaz, sinadura elektronikoko horiek eskuz idatzitako sinaduren baliokide direla, gailu kriptografikoa erabiltzen denean, betiere Sinadura Elektronikoari buruzko Legearen 3.4. artikulua agintzen duenaren arabera.

Bere gakoak IZENPEn gordetzen dituen harpidedunak,

- Ziurtagiria egokiro erabiliko du, eta, zehazki, ziurtagirien erabilera-mugak aintzat hartuko ditu.
- Arretaz zainduko du aktibatze gakoak, baimendu gabeko erabilerak saihestearren, Ziurtapen Praktiken Deklarazioko 6.1, 6.2 eta 6.4 sailek agintzen dutenaren arabera.
- IZENPEri eta, harpidedunaren ustez, ziurtagirian konfiantza duen edonori hau jakinaraziko dio, justifikatzerik ez dagoen atzerapenik gabe:
  - Gako pribatuaren kontrola galdu izana, aktibatze-datuak arriskuan jartzeagatik edo beste edozein arrazoiengatik.
  - Ziurtagiriaren edukian dauden okerrak edo izandako aldaketak (harpidedunak dakizkienak edo jakin litzakeenak). Aldaketak ziurtagiria ezeztatzea badakar, horretarako eskaera egin behar du harpidedunak.
- Gako pribatua erabiltzeari utziko dio ziurtagiriaren balio-epea amaitu ondoren.
- Gakoen edukitzaileei jakinaraziko die zein betebeharrak dagozkien.
- Ez du ziurtagiri-zerbitzuen ezartze teknikoak kontrolatuko eta manipulatu, ezta atzeranzko ingeniartzako ekintzarik egingo ere, aurrez Ziurtapen Entitatearen idatzizko baimenik eduki gabe.
- Ez du ziurtagiri-zerbitzuen segurtasuna arriskuan nahita jarriko.
- Ez ditu ziurtagirietako gako publikoei dagozkien gako pribatuak erabiliko inongo ziurtagiri izenpetzeko, ziurtapen-entitatea balitz bezala.



Ziurtagirian zerrendatutako gako publikoari dagokion gako pribatua erabiliz sinadura digitalak sortzen dituen ziurtagiri kualifikatuen harpidedunak aitortu egin behar du, dagokion bitarteko juridikoaz, sinadura elektronikorik eskuz idatzitako sinaduren baliokide direla, gailu kriptografikoa erabiltzen denean, betiere Sinadura Elektronikoari buruzko Legearen 3.4. artikulua agintzen duenaren arabera.

#### **4.5.2. Ziurtagirietan konfiantza duten hirugarren batzuek gako publikoa eta ziurtagiria erabiltzea**

Ziurtagirien erabiltzaile egiaztatzaileak honako betebeharrak dituzte:

- Eman nahi zaion erabilerarako ziurtagiria egokia den ala ez jakiteko, informazioa iturri independenteetatik jasotzea.
- Ziurtagiriak erabiltzeko baldintzak ezagutzea, Ziurtagiri Praktiken Deklarazioan aurreikusitakoaren arabera.
- Emandako ziurtagirien baliozkotasuna, etena edo ezeztapena egiaztatzea. Horretarako, ziurtagirien egoerari buruzko informazioa erabiliko da.
- Ziurtagirien hierarkiako ziurtagiri guztiak egiaztatzea, sinadura digitalean edo hierarkiako ziurtagiriren batean konfiantza jarri baino lehen.
- Kontuan izatea ziurtagiria erabiltzeko dauden mugak, nonahi daudelarik ere: ziurtagirian bertan nahiz egiaztatzailearen kontratuan.
- Kontuan izatea kontratuan edo beste nonbait finkatutako badaezpadako neurri guztiak, edozein delarik ere haren izaera juridikoa.
- Jakinaraztea ziurtagiriari buruzko gertaera edo egoera irregular guztiak, ziurtagiria ezeztatze arrazoia izan daitekeenak.
- Ziurtagiri-zerbitzuen ezartze teknikoak ez kontrolatzea, manipulatzeko edo atzerantzko ingeniartzako ekintzarik ez egitea, aurretik IZENPEren idatzizko baimenik gabe.
- Ziurtagiri-zerbitzuen segurtasuna arriskuan nahita ez jartzea.
- Ziurtagiri onartuen erabiltzailea behartuta dago aitortzera –dagokion tresna juridikoan– sinadura elektronikorik eskuz idatzitako sinaduren baliokideak direla, Sinadura Elektronikoari buruzko Legearen 3.4. artikulua arabera.

## **4.6 Ziurtagiria gako aldaketarik gabe berritzea**

IZENPEk ez du aukera hori aintzat hartzen.

## **4.7 Ziurtagiria gakoak aldatuta berritzea**

Ziurtagiria berritzeko, bai ezeztatu egin delako, bai indarraldia amaitu delako, ziurtagiri berria eskatu behar da, ziurtagiriak jaulkitzeko *Ziurtagiri bakoitzerako berariazko dokumentazioan* aurreikusitako prozesuari jarraituz.



Gailu kriptografikoan jaulkitako ziurtagiriak berritzea eskatu ahal izango da, ziurtagiri horiek iraungi aurreko hirurogei egunetan. Ziurtagiri berriaren indarraldia aurreko ziurtagiria iraungitzen den egunean bertan hasten da.

Segurtasun-arrazoia direla-eta, ziurtagiriren bat berritzen denean haren gakoak ere berritu egin behar dira, zifratze-ziurtagiriak –hala badagokie– izan ezik.

#### **4.7.1. Ziurtagiria berritzeko zirkunstantziak**

Ziurtagiria iraungi ez bada, baina RArean aurrean bertaratu eta identifikatu zen azken alditik 5 urte pasa badira, berritu ahal izango da ziurtagiria.

#### **4.7.2. Nork eska dezake**

Edozein harpidedunek eskatu ahal izango du haren ziurtagiria berritzea, baldin eta aurreko puntuan deskribatutako zirkunstantziak betetzen badira.

#### **4.7.3. Berritzeko eskaeren tratamendua**

Harpideduna IZENPErekin harremanetan jar daiteke bere ziurtagiria berritzea eskatzeko. IZENPEk eskaera nola formalizatu azalduko dio.

#### **4.7.4. Harpidedunari jakinaraztea**

Honako urrats hauek egingo dira:

- IZENPEk ziurtagiri bat iraungitzeaz dagoela egiaztatu ahal izango du.
- Harpidedunari ziurtagiria berritu dezakeela jakinaraziko zaio.
- Harpidedunak ziurtagiria berritzeko hitzordua eskatuko du, telefono bidez edo web-orriaren bidez. Gainera, eskaera bere ziurtagiria erabilia sinatu ahal izango du, bere ziurtagiria berritzea sinatuta.
- Ondoren, ziurtagiria sortuko da, ziurtagiria jaulkitzeko ohiko prozedurari jarraituta.
- Sortzen den ziurtagiria harpidedunari emango zaio.

#### **4.7.5. Ziurtagiri berritua onartzeko prozedura**

Berritzea eta entrega- eta onarpen-orria elektronikoki sinatzean onartuko da ziurtagiria (hala eginez gero).

#### **4.7.6. Ziurtagiria argitaratzea**

Ziurtagiria berritu ostean, ziurtagiri berria beharrezkotzat jotzen diren ziurtagiri-biltegietan eman ahal izango da argitara, aurreko ziurtagiria ordeztuta.



#### 4.7.7. Beste entitate batzuei jakinaraztea

4.4.3. puntuan jasotakoaren arabera.

### 4.8 Ziurtagiria aldatzea

Ziurtagiriko daturen bat aldatu behar izanez gero, IZENPEk ziurtagiria ezeztatuko du eta beste bat jaulkitzeari ekingo dio.

### 4.9 Ezeztatzea

#### 4.9.1. Ezeztatzeko zirkunstantziak

Honako egoera hauetan ezeztatuko ditu ziurtagiriak IZENPEk:

- Ziurtagiriak ezeztatzea sinatzaileak, edo hori ordezkutzen duen pertsona fisikoak edo juridikoak eskatuta edota hirugarren baimendu batek edo pertsona juridikoko ziurtagiri elektronikoa eskatu duen pertsona fisiko batek eskatuta.
- Sinatzailearen edo ziurtapen-zerbitzuen egilearen sinadura sortzeko datuak urratzen direnean edo arriskuan jartzen direnean, edo sinatzaileak edo hirugarren batek datu horiek bidegabe erabiltzen dituenean.
- Ebazpen judizial edo administratiboren batek hala agintzen duenean.
- Sinatzailearen nortasun juridikoa iraungitzea edo hiltzea, ordezkatuaren nortasun juridikoa iraungitzea edo hiltzea, sinatzailearengan edo ordezkatuarengan gerora ezintasun iraunkorra edo partziala agertzea, ordezkartzari amaiera ematea, ordezkaturako pertsona juridikoa desagitea, edo pertsona juridiko batek egindako ziurtagirietan islatzen diren sinadura sortzeko datuak zaindu eta erabiltzeko baldintzak aldatzea.
- IZENPEk jardura eteten badu, baldin eta, sinatzailearen aurretiko onespena dela medio, hark jaulkitako ziurtagiri elektronikoen kudeaketa ez bazaizkio transferitzen beste ziurtapen-zerbitzuen egileren bati.
- Ziurtagiria lortzeko emandako datuak aldatzea edo ziurtagiria emateko egiaztatutako zirkunstantziak aldatzea.
- Ziurtagiria galtzen bada edo lapurtzen badute, edo erabiltzeko ez dela geratzen bada ziurtagiriaren euskarria hondatu delako edo Ziurtapen Politikak aurreikusten ez duen beste euskarri batera aldatu delako.
- Aldeetakoren batek dagozkion betebeharrak betetzen ez dituenean.
- Ziurtagiria jaulkitzean akatsen bat gertatu bada, ezarritako prozedurari ez egokitzeagatik edo jaulkitze-prozesuan arazo teknikoak sortzeagatik.
- Sinadura sortzeko datuen hitzarmenetik kanpoko gorabeherak direla medio, IZENPEk jaulkitako ziurtagirien fidagarritasuna eta sistemen segurtasuna arriskuan jartzen bada.



- Ziurtagiria edo harekin lotzen den dokumentazioa jaulkitzean eta/edo banatzean akats teknikorik gertatzen bada.
- Ziurtagiria eskatu zen egunetik hiru hilabete iragan direnean eskatzaileak jaso duen arte.
- IZENPEk ziurtagiria jaulkitzeko eskaera bat jasotzen duenean, eta politika bereko eta bakartasun-irizpide bereko beste ziurtagiri bat dagoenean, ezeztatu egingo da indarrean dagoen ziurtagiria, baina eskatzaileak ezeztatzeko eskaera egin ondoren.

#### **4.9.2. Nork eska dezake ziurtagiria ezeztatzea**

Ikusi *Ziurtagiri bakoitzerako berariazko dokumentazioan*.

#### **4.9.3. Ezeztatzeko eskaeren tratamendua**

Ezeztatzea eskatzen duenak IZENPEren aurrean bideratuko du *ziurtagiria ezeztatzeko eskaera*.

Ziurtagiria edozein unetan ezeztatu ahal izango da, eta ziurtagiria lapurtu edo galdu denean beti.

Ezeztatzeko eskaera kautotua eta ezeztapena justifikatzen duen informazioa erregistratu eta artxibatu egingo dira.

Ezeztapena eskatzailea, harpideduna edo gakoan edukitzailea ez den beste pertsona batek eskatuko balu –ezeztatu aurretik edo ezeztatzen den unean bertan–, IZENPEk gakoan edukitzaileari eta ziurtagiriaren harpidedunari jakinaraziko die ziurtagiria baliorik gabe geratuko dela, baita horren zergatia ere.

Eskatzaileak honako bide hauetatik ezeztatu ahal izango du ziurtagiria:

- Bertaratuta, IZENPEren aurrean.
- Telefono bidez, 902 542 542 telefonora deituta.
- Online, [www.izenpe.com](http://www.izenpe.com) web-orrian edo posta elektronikoko bidez, ziurtagiri onartu batekin elektronikoki sinatutako eskaera baliatuta.
- Posta bidez, ziurtagiria ezeztatzeko eskaera notario aurrean sinatua eta legitimatua igorrita.

Ziurtagiri motari dagokion berariazko dokumentazioa kontsultatu, identifikaziorako zer beharko den jakiteko.

#### **4.9.4. Ezeztatzea prozesatzeko CAren epea**

4.9.3 atalean adierazitakoa egin ostean, eta RAK ziurtagiria ezeztatzeko izapideak behar bezala egin ondoren, ezeztatzea gaur egungo legeriaren arabera izango da indarrean.



#### **4.9.5. Konfiantzako hirugarren batzuek ezeztatzeak egiaztatzeko betebeharra**

Ziurtagirien egoera egiaztatzea derrigorrezkoa da ziurtagirien erabilera bakoitzerako, bai ezeztatzen zerrenda (CRL) kontsultatuta, bai OCSP zerbitzuan kontsultatuta.

IZENPEk informazioa ematen die egiaztatzaileei, dagokion CRLa eta/edo OCSPa non eta nola aurkitu jakin dezaten.

#### **4.9.6. CRLak sortzeko maiztasuna**

Ezeztatutako Ziurtagirien Zerrenda (CRL, hemendik aurrera) berehala jaulkitzen du IZENPEk, ezeztapen bat egiten den une berean.

CRLan adierazten da beste CRL bat jaulkitzeko programatuta dagoen unea, aurreko CRLan adierazitako epea amaitu baino lehen ere CRL bat jaulkitzea badagoen arren. Ziurtagiririk berritzen ez bada, ziurtagiriak ezeztatze zerrenda egunero birsortuko da.

Azken entitatearen ziurtagirien CRLa 24 orduko gutxienez jaulkitzen da, edo ezeztatze bat gertatzen denean, eta 10 eguneko baliagarria.

CAen ziurtagirien (ARLen) CRLa 12 hilero jaulkitzen da edo ezeztatze bat gertatzen denean.

Ezeztatzen diren ziurtagiria CRLtik kenduko dira. Une horretatik aurrera, 15 urtez gorde behar da ezeztapena IZENPEren barne-erregistroan.

#### **4.9.7. CRLak sortzen direnetik argitaratzen direnera arte emandako denbora**

CRLa sortzen denetik 30 segundokoa da gehieneko latentzia-denbora.

#### **4.9.8. Ziurtagirien egoera online egiaztatzeko sistemaren erabilgarritasuna**

IZENPEk egiaztatze-zerbitzua eskaintzen die –denbora errealean– entitate erabiltzaileei OCSP (Online Certificate Status Protocol) protokoloaren bitartez; horrenbestez, erabilera-aplikazioek egiaztatzen dute ziurtagiriaren egoera.

Zerbitzua eguneko 24 orduetan erabili daiteke, asteko 7 egunetan.

#### **4.9.9. On line ezeztatzea egiaztatzeko eskakizunak**

CRLen zerbitzua, librea, erabiltzeak eskatuko du,

- Jaulkitako azken CRLa beti egiaztatzea –hori ziurtagirian bertan jasotzen den URL helbidean, “CRL Distribution Point” luzapenean, deskargatu ahal izango da–.
- Erabiltzaileak, horrez gain, hierarkiaren ziurtagiri-kate bidezko CRLak ere egiaztatzea.
- Erabiltzaileak ziurtagiriaren balidatze nahi den ziurtagiria jaulki duen agintaritzak sinatzen duela ezeztatze zerrenda.

Ezeztatzen diren ziurtagiriak CRLtik kenduko dira.

OCSP zerbitzua, librea, erabiltzeak eskatuko du,

- Ziurtagiriaren bertan agertzen den URL helbidea egiaztatzea, “Authority Info Access” luzapenean.



- Erabiltzaileak ziurtatzea balidatu nahi den ziurtagiria jaulki duen CAk sinatu duela erantzuna.

#### **4.9.10. Ezeztatzeak ohartarazteko eskura dauden beste modu batzuk**

Ziurtagiri kualifikatu bat ezeztatzen denean, IZENPEk informaziorako mezu elektronikoa bidaltzen dio ziurtagiriaren harpidedunari.

#### **4.9.11. Arriskupean dagoen gakoaren eskakizun bereziak**

Ziurtagiriaren gako pribatua arriskupean badago, gakoaren harpidedunak edo edukitzaileak IZENPERi eman behar dio horren berri, horrek ziurtagiria ezeztatzeko eskaera egin dezan eta ziurtagiriaren erabilera eten dadin.

IZENPEren CAREN gako pribatua arriskupean badago, dokumentu honen 5.7.3 atalak dioena egin behar da.

### **4.10 Ziurtagirien egoera-zerbitzuak**

#### **4.10.1. Ezaugarri operatiboak**

IZENPEk ezeztatutako ziurtagirien zerrendak (CRL) argitaratzeko doako zerbitzua eskaintzen du, horietara sartzeko mugarik gabe. Horrez gain, OCSP (Online Certificate Status Protocol) protokoloaren bidez ziurtagiriak balidatzeko zerbitzuak eskaintzen ditu.

#### **4.10.2. Zerbitzuaren erabilgarritasuna**

IZENPEk ziurtagiriak ezeztatzeko 24x7 zerbitzua eskaintzen die entitate erabiltzaileei (24 ordukoa asteko 7 egunetan).

### **4.11 Harpidetzari amaiera ematea**

Ziurtagiriaren indarraldia amaitzen denean edo ezeztatu denean, ematen zaio amaiera ziurtagiriari, eta ez da erabiltzeko baliagarria.

Berariazko dokumentazioan begiratu behar da ziurtagirien iraungipena.

### **4.12 Gakoak zaintzea eta berreskuratzea**

IZENPEk ez du zerbitzu hori eskaintzen.



## 5 Segurtasun fisikoaren, prozeduren eta langileen kontrolak

---

IZENPEk bere zerbitzuak ematen dituen toki horietan guztietan kontrolak egingo dira.

### 5.1.1. Instalazioen kokalekua eta eraikuntza

Informazioa prozesatzen den tokiek honako baldintza fisiko hauek betetzen dituzte:

- Informazioa prozesatzeko instalazioak dituen eraikina fisikoki sendoa da, kanpoko hormak eraikuntza sendokoak dira, eta segurtasun-kamerek etengabe zaintzen dute. Sartzeko baimena duten pertsonak bakarrik izango dute sarbidea.
- Ate eta leiho guztiak itxita eta babestuta daude, baimenik ez duen inor sartu ez dadin.

### 5.1.2. Sarbide fisikoa

#### IZENPEren instalazioak

IZENPEren instalazioek sarbide fisikorako kontrol-sistema osatu bat dute. Hauek dira sistema horren ezaugarriak:

- Segurtasun-perimetro bat, lur errealetik sabai errealeraino, baimenik gabeko inor sar ez dadin.
- Instalazioetarako sarbide fisikoko kontrola,
  - Horretarako baimena duten langileak soilik sar daitezke.
  - Aldiro ikuskatzen eta eguneratzen dira eremu segurura sartzeko baimenak.
  - Langile guztiek eraman behar dute identifikazio-elementuren bat, erraz ikusten dela, eta ez daramanari langileek eurek eskatzea bultzatzen du enpresak.
  - Gainbegiratu egiten dira IZENPEren jarduerarekin zerikusirik ez duten eta haren instalazioetan lanean aritzen diren langileak.

Sarbideen log fitxategi bat dago, leku seguruan gordeta.

IZENPEra sartzeko ateen sarbide-mekanismoak dauzkate.

IZENPEk ziurtapen-zerbitzua egiteko erabiltzen dituen elementuak monitorizatzen dituen telebista-zirkuitu itxi bat.

#### RAk

RAek erregistro-postuko segurtasun-dokumentuan definitzen diren beharrezko segurtasun-irizpideak betetzen dituzte.

### 5.1.3. Elektrizitatea eta aire egokitua

Datu Prozesaketarako Zentroak energia- eta aireztapen-sistema egokiak ditu, lantoki fidagarri bat izan dadila bermatzeko.



Era berean, IZENPEren instalazioek etengabeko elikadura-funtzionalitatea dute (SAI eta multzo elektrogenoa), energiarik gabe geratu edo aire egokituaren sistema hondatuz gero ekipoa behar bezainbat denboraz martxan edukitzen duena, sistemak modu ordenatuan itxi daitezten.

#### **5.1.4. Urarekiko erresistentzia**

Urak eragindako kalteetatik eratorritako arriskuak gutxitzeko, IZENPEk beharrezko neurriak hartu ditu.

#### **5.1.5. Suteen prebentzioa eta horien aurkako babesa**

IZENPEren Datu Prozesaketa Zentroak oztopo fisikoak ditu, lur errealetik sabai errealerainokoak, baita suteak automatikoki detektatzeko sistemak ere, honako helburu hauekin:

- Sutea hasi dela jakinaraztea IZENPEko zaintze-zerbitzuari eta langileei.
- Aireztatzeko-sistema deskonektatzea, suteen aurkako atek ixtea, elektrizitate-hornidura etetea eta itzaltze-sistema automatikoa abiaraztea.

#### **5.1.6. Euskarrien biltegitzea**

Babeskopien euskarriak modu seguruan biltzen dira.

#### **5.1.7. Hondakinen tratamendua**

Informazio-euskarriak deuseztatzeko prozedurak arautuko dituen politika ezarri da.

Informazio konfidentziala duten euskarriak deuseztatu egiten dira, deuseztatu eta gero berreskurazina izateko moduan.

#### **5.1.8. Instalazioetatik kanpoko babeskopia**

IZENPEk babeskopiak istripuetatik babestuta biltegitratzen ditu, eta kokaleku nagusian gerta daitekeen edozein hondamenditan kaltetuak ez gertatzeko moduko distantzia batean.

### **5.2 Prozeduren kontrolak**

#### **5.2.1. Konfiantzazko funtzioak**

“Konfiantzazko eginkizunak” dira behar bezala egin ezean istripuagatik edo asmo txarrez segurtasun-arazoak sor ditzaketan funtzioak dituztenak.

“Konfiantzazko eginkizun” bati dagozkion funtzioak behar bezala gauzatzen direnaren probabilitatea handitzeko asmoz, bi alderdi hartu behar dira kontuan:

- Lehenbizikoa erroreak saihesteko eta jarrera desegokiak debekatzeko teknologia diseinatzea eta konfiguratzeko da.
- Bigarrena funtzioak hainbat lagunen artean banatzea da asmo txarreko jardura gauzatzeko hainbat lagunekin adostea beharrezkoa izateko.



IZENPEk antolakundearen garatu diren rolen definizio osoa du. Horietarako guztietarako funtzioak eta erantzukizunak definitu dira, eta horietako bakoitzaren jarduna arautzen duten prozedura dokumentatuak bildu dira.

### **5.2.2. Zeregin bakoitzerako pertsona kopurua**

Sistemaren segurtasuna indartzeko, eginkizun bakoitzerako pertsona desberdinak esleitzen dira salbuespen batekin: operadorearen eginkizuna administratzaileak egin dezake.

Gainera, eginkizun baterako lagun bat baino gehiago esleitu daitezke.

### **5.2.3. Eginkizun bakoitzean identifikatzea eta kautotzea**

Konfiantzako eginkizunek behar bezain segurua den bitarteko batez kautotzea eskatzen dute, eta beti erabiltzaile pertsonalekin.

IZENPEk bakoitzaren eginkizunak zehazten dituen berariazko dokumentazioa du.

### **5.2.4. Eginkizunetan bereiztea zereginak**

IZENPEk CIMC (Certificate Issuing and Management Component) segurtasun-politikari jarraitzen dio, eta haren segurtasun-ereduan dago definituta.

## **5.3 Langileen kontrolak**

### **5.3.1. Historialei, kalifikazioei, esperientziari eta kautotzei buruzko baldintzak**

Egin behar dituen zerbitzuetan esperientzia eta kalifikazioak dituen langileak enplegatzen ditu IZENPEk.

Konfiantzako eginkizunak dituzten langileek ez dute IZENPEko eragiketen inpartzialtasunari kalte egin diezaioketen interesik.

### **5.3.2. Historiala ikertzeko prozedurak**

Ez da Espainiako araudiari jarraituta aplikatzen.

### **5.3.3. Trebakuntza-baldintzak**

IZENPEren langileek eskatutako trebakuntza jasoko dute, funtzioak betetzean beren trebetasuna ziurtatzeko. Trebakuntzan alderdi hauek sartuko dira:

- Ziurtapen Praktiken Deklarazioaren kopia bat emango zaie.
- Segurtasunaren gaineko kontzientziakzioa.
- Softwarearen eta hardwarearen funtzionamendua eginkizun jakin bakoitzerako.
- Segurtasun-prozedurak eginkizun jakin bakoitzerako.
- Funtzionamendu eta administratzioko prozedurak eginkizun jakin bakoitzerako.
- Hondamenak konpontzeko prozedurak.



#### **5.3.4. Trebakuntza eguneratzeko baldintzak eta maiztasuna**

IZENPEren PKI eragiketan aldaketa garrantzitsu bat egiten den bakoitzean, trebakuntza-plana egingo da, eta plana gauzatzea dokumentatuko da.

#### **5.3.5. Lan-txandaketen segida eta maiztasuna**

Ez da aplikagarria.

#### **5.3.6. Baimendu gabeko konexioen zigorrak**

##### **Informazioaren segurtasuneko gertakariak**

IZENPEk segurtasun-larrialdiak kudeatzeko plana du.

##### **Zigor Prozesua**

Zigor-prozesua definitzen duen barne-erregimen diziplinarioa dago.

#### **5.3.7. Langileak kontratatzeke baldintzak**

IZENPEk langileak kontratatzeke eta eginkizunak eta erantzukizunak esleitzeko politika du.

#### **5.3.8. Langileei dokumentazioa ematea**

Konfiantzazko eginkizunekin lotutako langile guztiek honako hauek jasotzen dituzte:

- Ziurtapen Praktiken Deklarazioaren kopia bat.
- Eginkizun bakoitzaren betebeharrak eta prozedurak zehazten diren dokumentazioa.
- Sistemaren osagaietako bakoitzaren jardunari buruzko eskuliburuak.

### **5.4 Audit**

IZENPEren eta erregistro-entitateen softwareak sortutako gertaera aipagarriak berregiteko, log fitxategiak erabiliko dira, baita haiek eragin zituen erabiltzailea edo gertaera ere. Halaber, artekaritza-tresnatzat ere erabiliko dira gerta litezkeen auzietan, une jakin batean sinadura baten baliozkotasuna egiaztatuz.

#### **5.4.1. Erregistratutako gertaera motak**

Log-etan biltegitratzen dira:

- Gako kriptografikoen bizi-zikloari buruzko gertaera guztiak.
- Ziurtagirien bizi-zikloari buruzko gertaera guztiak.
- Gailu kriptografikoen jaulkipenari buruzko gertaera guztiak.
- IZENPEko administratzaileen eta operadoreen kontuen administrazioari buruzko gertaera guztiak.

Gertaera bakoitzaren data eta ordua grabatzen da, denbora-datu fidagarria erabiliz.



#### **5.4.2. Log fitxategien prozesamenduaren maiztasuna**

Aldiro begiratzen ditu log fitxategiak IZENPEko ikuskatzaileak.

#### **5.4.3. Audit logaren atxikipen-aldia**

Linean eduki behar da log fitxategian sortutako informazioa, artxibatzeke garaia iritsi arte. Artxibatu ondoren, 7 urtez gorde behar dira log fitxategiak.

#### **5.4.4. Audit logaren babesa**

Log erregistroa irakurtzeko eskubidea ematen zaie ikuskatzaileei.

Ez dago log erregistroak baimenik gabe ezabaterik edo aldatzerik log erregistroak euskarri ez-aldagarri batean ipiniz CD-ROM batean, adibidez.

#### **5.4.5. Audit-logaren backup prozedura**

Lineako logaren babeskopia egiten da, IZENPEko sistemaren gainerako elementuetarako erabiltzen diren planifikazio eta kontrol berekin.

#### **5.4.6. Log fitxategiak biltzea**

CAren, RAre eta LRAre log fitxategiak IZENPEren barne-sistemetan gordetzen dira.

#### **5.4.7. Log fitxategiak sortzea eragin duen ekintzaren jakinarazpena**

Ez dago aurreikusita log fitxategietako jardueraren berri gertaeraren eragileari jakinaraztea.

#### **5.4.8. Puntu ahulen azterketa**

Aldian behin puntu ahulen azterketa egiten da IZENPEko barne-sistemetan.

### **5.5 Erregistroak artxibatzea**

#### **5.5.1. Artxibatutako erregistroen mota**

Honako datu motak edo fitxategi motak artxibatzen dira, besteak beste:

- Erregistro-prozedurarekin eta ziurtagiriak eskatzearekin zerikusia duten datuak;
- Aurreko ataleko ikuskapen-erregistroak;
- Gakoen historikoa.

#### **5.5.2. Fitxategiaren atxikipen-aldia**

Ziurtagiri onartuei buruzko informazio eta dokumentazio guztia 15 urtez gordetzen da (jaulkitzen diren datatik), eta gainerako ziurtagiriei buruzkoa 7 urtez (ziurtagiria amaitzen den datatik).



### 5.5.3. Artxiboaren babesa

Artxiboa babesteko hartu beharreko neurriak hartuko dira, haren edukia inork ez manipulatzeko edo suntsitzeko.

### 5.5.4. Artxiboaren backup prozedurak

Segurtasun-kopien, kontingentzia-planen eta negozioaren jarraitasun-planen arloko politika finkatu da, eta gertakari baten aurrean jarduteko irizpideak eta estrategiak definitzen ditu politika horrek. Gertakarien aurrean jarduteko estrategia osoaren diseinua, beraz, aktiboan inbentarioan eta arriskuen azterketan oinarritzen da.

### 5.5.5. Erregistroen denbora zigilatze eskakizunak

IZENPEk erabiltzen dituen informazio-sistemek bermatu egiten dute haiek egiten diren denbora-uneak erregistratzea. Sistemetako denbora-uneak data- eta ordu-sistema seguru batek sortzen ditu. Sistema guztiek iturri horrekin sinkronizatzen dute beren denbora-unea.

### 5.5.6. Artxibatze sistema

IZENPEren instalazioetan dago artxibatze sistema, baita zerbitzuak egiten dituen entitateetan ere.

### 5.5.7. Artxiboaren informazioa lortzeko eta egiaztatze prozedurak

Horretarako baimena duten langileek bakarrik eskura dezakete informazio hori. Sarrera fisikoen eta logikoen aurkako babesak ditu informazioak, honako Ziurtapen Praktiken Deklarazio honen 5. eta 6. atalak agintzen dutenari jarraituz.

## 5.6 Gakoak aldatzea

Ziurtagiria berritzea, bai ezeztatu egin delako, bai indarraldia amaitu delako, ziurtagiri berria eskatu behar da, ziurtagiriak jaulkitzeko *Ziurtagiri bakoitzerako berariazko dokumentazioan* aurreikusitako prozesuari jarraituz.

Gakoak berritzeak berekin dakar ziurtagiria berritzea.

## 5.7 Larrialdietarako plana

### 5.7.1. Gertakariak kudeatzeko prozedurak

Larrialdietarako Planak zehazten du zer egin behar den, zer baliabide eta zenbat langile erabili behar diren, baldin eta k ematen dituen ziurtapen-zerbitzuak eta baliabideak ezin erabili uzten dituen edo hondatzen dituen gertakariren bat gertatzen bada (nahita eragindakoa edo halabeharrezkoa).

Larrialdietarako Planaren helburu nagusiak hauek dira:

- Berreskuratze-lanen eraginkortasuna areagotzea, hiru fase hauek erabiliz:



- Jakinarazteko/ebaluateko/aktibatze fasea, kalteak ebaluateko eta plana aktibatze.
- Berreskuratze fasea, behin-behingo eta partzialki zerbitzuak berriro martxan jartzeko, harik eta jatorrizko sisteman izandako kalteak konpondu arte.
- Konpontze fasea, sistema eta prozesuak bere ohiko martxara itzularazteko.
- Ohiko martxaren etenaldi luzeetan ordezko DPZ batean ziurtapen-zerbitzuak partzialki egiteko behar diren jarduerak, baliabideak eta prozedurak identifikatzea.
- Erantzukizunak esleitzea IZENPEk jarritako langileei eta gida bat prestatzea etenaldi luzeetan ohiko martxa berreskuratze.
- Planifikatu den larrialdirako estrategian esku hartzen duten eragile guztien koordinazioa bermatzea (entitateko sailak, kanpoko harremanak eta saltzaileak).

Ziurtapen-zerbitzuak egiteko beharrezko diren eginkizun, eragiketa eta baliabide guztiei aplikatu behar zaie IZENPEren Larrialdietarako Plana. Ziurtapen-zerbitzuetan diharduten IZENPEko langileei aplikatu behar zaie aipatu plana.

Larrialdietarako Planak talde jakin batzuen esku-hartzea aurreikusten du IZENPEren jardueren berreskuratze-lanetan.

Larrialdietarako Planak zehazten du kalteen ebaluazioa eta ekintza-plana nola egin behar diren.

Algoritmoa, erabilitako gako-tamainaren konbinazioa edota segurtasun teknikoak kaltetuko duen edozein ezbehar tekniko sortzen bada, aipatu Larrialdietarako Plana aplikatuko da. Jasotako inaktuaren azterketa egingo da. Azterketa horretan segurtasun-arazoaren larritasuna, arazoaren esparrua eta gertatutakoa konpontzeko estrategia aztertuko dira. Egondako inaktuaren azterketa-txostenean, gutxienez, honako puntu hauek zehaztuko dira:

- Kontingentziaren deskribapen zehatza, denbora-esparrua etab.
- Larritasuna, esparrua.
- Proposatutako irtenbidea edo irtenbideak.
- Hautatutako irtenbidea zabaltzeko plana. Plan horretan, gutxienez, honako puntu hauek hartuko dira kontuan:
  - Erabiltzaileei jakinaraztea, eraginkorra dela uste den bidea erabilia. Ziurtagirietako eskatzaileei nahiz harpidedunei eta egiaztatzaileei (fidagarriak diren hirugarrenak).
  - Sortutako kontingentziaren berri web-orrian ematea.
  - Kaltetutako ziurtagiriak ezeztatuko dira.
  - Berritze-estrategia.

### **5.7.2. Datu eta software ustelen aurrean jarduteko plana**

IZENPEren kontingentzia-planak egoera horien aurrean jarduteko estrategia jasotzen du.



### 5.7.3. Gako pribatuaren konpromisoaren aurreko prozedura

Oinarrizko CAk ezeztatu egingo du CA jaulkitzaile jakin baten ziurtagiria CA horren gako pribatua arriskupean badago.

Oinarrizko CAk CA jaulkitzailearen ziurtagiria ezeztatu beharra gertatuz gero, berehala jakinarazi behar die honako hauei:

- CA jaulkitzaileari.
- CA hori erregistratzeko baimena duten RA guztiei.
- CA horrek jaulkitako ziurtagirien sinatzaile titular guztiei.

Oinarrizko CAk ARLn ere (Ziurtapen Agintaritzak Ezeztatzeko Zerrenda) ere argitaratuko du ezeztatutako ziurtagiria.

Ezeztapena eragin zuten arazoak konpondu ondoren, Oinarrizko CAk honakoa egin behar du:

- Beste ziurtagiri bat sortu CA jaulkitzailerako.
- CAk jaulkitako ziurtagiri berri eta CRL guztiak gako berriarekin sinatzen direla ziurtatzea.

CA jaulkitzaileak kaltetutako azken entitate guztiei jaulki ahal dizkie ziurtagiriak.

Arriskupean dagoen gakoa oinarrizko CAren bada, kendu egingo da ziurtagiria aplikazio guztietatik eta beste bat banatuko da.

### 5.7.4. Hondamendi baten ondoren, negozioaren jarraipena

CAren jarduera eten egingo da harik eta hondamendia gainditzeko prozedura osatu eta zentro nagusian edo ordezkotan behar bezala funtzionatzen hasten den arte.

IZENPEren Larrialdietarako eta Negozioaren Jarraipenerako Plana aktibatuko da.

## 5.8 CAren edo RArekin amaiera

### 5.8.1. Ziurtapen-entitatea

IZENPEk CAren Amaiera Plana du, eta bertan horretarako gauzatuko den prozedura zehazten da.

Jarduera etetea erabakiz gero, harpidedunari jakinarazi behar dio IZENPEk ziurtapen-zerbitzuak egiteari uztekotan dela, jarduera eten baino bi hilabete lehenago, gutxienez. Harpidedunak jakinarazpena jasoko duela bermatzen duen bideren bat erabili behar du IZENPEk hura bidaltzeko.

Era berean, ZZEei, nabigatzaileen fabrikatzaileei eta IZENPErekin kontratu bidezko loturaren duten entitate guztiei emango zaie haien ziurtagirien erabileraren berri.

IZENPEren Zuzendaritza Nagusiak du jakinarazpen horren erantzukizuna, eta hark erabakiko du horretarako mekanismorik egokiena zein den.

IZENPEk jarduera beste ziurtapen-zerbitzuen egileren bati transferitzea erabakiz gero, ziurtagirien harpidedunari eta Industria, Energia eta Turismo Ministerioari emango die transferentzia-akordioen berri. Horretarako, IZENPEk transferentzia-baldintzak zehazten dituen agiria bidaliko dio harpidedunari, baita harpidedunaren eta ziurtagiriak transferitzen



zaizkion ZZEn arteko harremanak erregulatuko dituzten erabilera-arauak ere. Jakinarazpenak jasoko dela bermatzen duen bideren bat erabili behar da hura bidaltzeko, jarduera eten baino bi hilabete lehenago, gutxienez.

Harpidedunak espresuki onetsi behar du ziurtagirien transferentzia, eta onartu egin behar ditu ZZE berriaren baldintzak, transferentziaren hartzailearenak ere. Bi hilabete igaro eta ez badago transferentzia-hitzarmenik, edo harpidedunak ez badu hura espresuki onartzen, ezeztatu egingo dira ziurtagiriak.

Jakinarazpena 2 hilabete lehenago bidaltzeko epea amaitu eta beste ZZEn batzuekin akordiorik lortu ezean, automatikoki ezeztatuko dira ziurtagiri guztiak.

IZENPErekin zerbitzugintzako kontratua duten beste hirugarren batzuen edozein baimen (identifikatzeko, jaulkitzeko, gordetzeko, eta abar) amaitutzat emango da.

### **5.8.2. Erregistro-entitatea.**

Erregistro-entitateak, bereganatzen dituen eginkizunak bertan behera uzten dituenean, IZENPEri transferituko dizkio dauzkan erregistroak, informazioa artxibatuta edukitzeko obligazioa duen bitartean; bestela, baliogabetu eta deuseztatu egingo da.



## 6 Segurtasun teknikoaren kontrolak

---

### 6.1 Gako-parea sortu eta instalatzea

#### 6.1.1. Gako-parea sortzea

Hona hemen IZENPE osatzen edo harekin lankidetzan aritzen diren entitateetako gako-pareak zein elementutan sortzen diren:

- Oinarrizko CA: oinarrizko CA dagoen makinak oinarrizko CAren gakoak sortzeko berezia den gailu kriptografikoa du (HSM).
- CA jaulkitzaileak: CAk dituen makina bakoitzean modulu kriptografiko bat dago.
- Txartel kriptografikoan edo HSMan jaulkitako ziurtagiriak: gakoak gailu kriptografikoak sortzen ditu
- Software-euskarri kriptografikoan jaulkitako erabiltzaile-ziurtagiria: zerbitzua dagoen zerbitzariak sortzen ditu haren gakoak.
- Time Stamping-en Agintearen zerbitzaria (TSA) eta OCSP balidatze-zerbitzaria: bi zerbitzariak dauden sistemarekin lotutako moduluan sortutako gakoak.
- Edukitzaileak berak sortutako gakoak kasuan, gako horiek algoritmoko eta gakoak gutxienezko luzerako gomendioen arabera sortu beharko dira, ETSI TS 102 176an definitutako moduan.

#### 6.1.2. Gako pribatua harpidedunari banatzea

Gako pribatua IZENPE osatzen duten edo harekin lankidetzan jarduten duten entitateei emateko metodoa:

- Txartel kriptografikoan jaulkitako ziurtagiriak: kautotzeko eta sinadurako gako pribatuak gailu kriptografikoarekin batera ematen dira.
- HSMan jaulkitako ziurtagiriak: kautotzeko eta sinadurako gako pribatuak gailu kriptografikoan gordetzen dira.
- Software euskarrian jaulkitako ziurtagiriak: gako pribatua zerbitzarian bertan sortuko da. Ez da entregatu beharrik.

#### 6.1.3. Gako publikoa ziurtagiriaren jaulkitzaileari banatzea

Hona hemen gako publikoa IZENPE osatzen duten edo harekin lankidetzan jarduten duten entitateetatik dagokion ziurtagiri-jaulkitzaileari emateko metodoa:

- CA jaulkitzaileak: gako publikoa oinarrizko CAra bidaliko da X.509 edo PKCS#10 formatuaren bidez.
- Gailu kriptografikoan jaulkitako ziurtagiriak: gailu kriptografikotik irakurtzen dira.
- Software-euskarrian jaulkitako ziurtagiria: gako publikoa IZENPEren oinarrizko CAra bidaliko da X.509 edo PKCS#10 formatuaren bidez.



#### 6.1.4. Ziurtapen-entitatearen gako publikoa ziurtagirien erabiltzaileei banatzea

IZENPEren CAen gako publikoak hainbat bidetatik banatzen dira, besteak beste, IZENPEren web-orriaren bitartez. Gainera, Ziurtapen Praktiken Deklarazio honetako 1.3.1.1. eta 1.3.1.2. ataletan, oinarrizko CAen eta CA jaulkitzaileen arrastoak daude.

#### 6.1.5. Gakoen tamainak eta erabilitako algoritmoak

Kasu guztietan erabilitako algoritmoa RSA da, SHA-2 duena.

Gakoen tamaina kasuen arabera izango da:

- Gutxienez 2048 bit pertsona fisikoen, juridikoen eta gailuen gakoetarako, OCSP zerbitzarietarako, TSA zerbitzarietarako eta ziurtagiri teknikoetarako.
- Gutxienez 2048 bit 2006aren aurretik igorritako CAen gakoetarako, eta gutxienez 4096 bit Oinarrizko CA 2007 berrietan oinarrituta jaulkitakoetarako.

#### 6.1.6. Ziurtapen-sinaduretako algoritmoak

IZENPEk ziurtagiriak sinatzeko erabiltzen duen algoritmo-identifikatzailea (AlgorithmIdentifier) SHA-2 da (hash algoritmoa), RSArekin batera (sinadura-algoritmoa). Algoritmo-identifikatzaile hori "Identifier for SHA-2 checksum with RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc." da. Erabilitako padding-eskema emsa-pkcs1-v2.1 da (RFC 3447, 9.2 sekzioaren arabera).

Azken erabiltzaileen ziurtagiriak SHA-2 duen RSArekin daude sinatuta. Ziurtagiriarekin sinatzeko, SHA-2 duen RSA edo altuagoa erabiltzeko gomendatzen die azken erabiltzaileei IZENPEk.

IZENPEk industriak onartzen duen eta sinadura onartuko xederako egokia den algoritmo bat erabiltzen du. Horretarako, ziurtagiriaren indarraldia hartuko da aintzat, eta CA/B Forum-ek eta ETSIren estandarrek adierazitako gomendioei jarraituko zaie.

Algoritmoa, erabilitako gako-tamainaren konbinazioa edota segurtasun teknikoak kaltetuko duen edozein ezbehar tekniko sortzen bada, aipatu Larrialdietarako Plana aplikatuko da. Jasotako inpaktuaren azterketa egingo da. Azterketa horretan segurtasun-arazoaren larritasuna, arazoaren esparrua eta gertatutakoa konpontzeko estrategia aztertuko dira. Egonako inpaktuaren azterketa-txostenean, gutxienez, honako puntu hauek zehaztuko dira:

- Kontingentziaren deskribapen zehatza, denbora-esparrua etab.
- Larritasuna, esparrua.
- Proposatutako irtenbidea edo irtenbideak.
- Hautatutako irtenbidea zabaltzeko plana. Plan horretan, gutxienez, honako puntu hauek hartuko dira kontuan:
  - Erabiltzaileei jakinaraztea, eraginkorra dela uste den bidea erabilia. Ziurtagirietako eskatzaileei nahiz harpidedunei eta egiaztatzaileei (fidagarriak diren hirugarrenak).
  - Sortutako kontingentziaren berri web-orrian ematea.



- o Kaltetutako ziurtagiriak ezeztatuko dira.
- o Berritze-estrategia.

### **6.1.7. Gakoan erabilera baimenduak (KeyUsage field X.509v3)**

Key Usage eta Extended Key Usage luzapena barnean hartzen dute ziurtagiri guztiek, gakoan erabilera gaituak adierazita.

Lehenengoetarako, batik bat, sinadura digitala, gakoaren eta datuen zifratzea eta ukorik eza erabiltzen da, eta bigarrenetarako bezeroa edo zerbitzaria kautotzea, smartcard logon edo posta elektronikoaren babesa.

Oinarrizko CA gakoak mendeko CAetako eta ARLetako ziurtagiriak sinatzeko erabiliko dira soilik, eta mendeko CAen edo CA jaulkitzaileen gakoak azken erabiltzaileko eta CRLetako ziurtagiriak sinatzeko soilik erabiliko dira.

Ziurtagiri bakoitzerako gakoaren erabilera baimenduak *Ziurtagiri bakoitzerako berariazko dokumentazioan* zehazten dira.

## **6.2 Gako pribatua babestea**

### **6.2.1. Modulu kriptografikoen estandarrak**

Segurtasun kriptografikoaren modulua (HSM) gako kriptografikoak sortzen eta babesten dituen segurtasun-gailua da. Beharrezkoa da HSMek FIPS 140-2, 3. maila, gutxienez, edo baliokidea betetzea.

IZENPEK HSM bat garraiatzean eta biltegitratzean manipulatu ez dela egiaztatzeko protokoloak mantentzen ditu.

Sinadura elektronikoko kualifikatutako ziurtagiriak dituzten gailu kriptografikoei dagokienez, sinadura sortzeko gailu seguru gisa onartuak (DSCF), CC EAL4+ segurtasun-maila betetzen dute; baina ITSEC E3 edo FIPS 140-2 2. maila, gutxienez, ziurtagiri baliokideak ere onartzeko modukoak dira.

CEN CWA 14169 araua da harpidedun-gailuetarako Europako erreferentziatzeko araua.

IZENPEK, nolana ere, IZENPEK gakoak sortzeko erabiltzen dituen harpidedun-gailuak prestatzearen, biltegitratzearen eta banatzearen gaineko kontrola mantentzen du.

### **6.2.2. Gako pribatua pertsona batek baino gehiagok kontrolatzea (m-tik n)**

CAetako gako pribatuak erabiltzeko, bi lagunen onespina behar da gutxienez.

### **6.2.3. Gako pribatuaren zaintza**

Oinarrizko CAren gako pribatua FIPS 140-2, 3. maila, arauarekin eta/edo CC EAL4+ arauarekin ziurtatutako hardware-gailu kriptografiko batekin zainduta dago, eta, hala, bermatuta dago gako pribatua inoiz ez dagoela gailu kriptografikoaz kanpo. Gako pribatua aktibatzeke eta erabiltzeko, behar-beharrezkoa da lehentxeago aditzera emandako pertsona askotako kontrola.



Ziurtagiria hodeian” zerbitzuaren kasuan, ziurtagirien azken erabiltzaileko gako pribatuak gailu kriptografiko seguruetan gordeta daude –FIPS 140-2 3. maila arauarekin ziurtatuta daude gailu horiek–

Mendeko CAen gako pribatuak FIPS 140-2, 3. maila, arauarekin ziurtatutako gailu kriptografiko seguruetan daude zainduta.

Harpidedunak gako pribatua zaintzen duen kasuetan, hura arduratuko da bere kontrolpean soilik mantentzeaz..

#### **6.2.4. Gako pribatuaren babeskopia**

Bada CAren (jatorrizkoa edo mendekoa) modulu kriptografikoetako gakoak berreskuratzeko prozedura bat, eta larrialdietan aplika daiteke. 6.2.2. atalean adierazitako kontrol berberak egingo dira.

#### **6.2.5. Gako pribatua artxibatzea**

IZENPEK ez du ziurtagiriak sinatzeko gako pribatua artxibatuko, haren baliagarritasuneko aldia amaitu ostean.

CAren sistemaren osagaiek haien artean komunikatzeko, sinatzeko eta informazioa zifratzeko erabiltzen dituzten barne-ziurtagirien gako pribatuak artxibatuko dira, azken ziurtagiria jaulki ondoren.

Harpidedunen gako pribatuak harpidedunek beraiek artxiba ditzakete, sinadura sortzeko gailuaren bidez edo beste metodo batzuen bidez; izatez, beharrezkoak izan daitezke gako publikoarekin zifratutako informazio historikoa deszifratzeko, betiere zaintzako gailuak eragiketa ahalbidetzen badu.

#### **6.2.6. Gako pribatuaren transferentzia, modulu kriptografikora edo modulu kriptografikotik**

Gako pribatuak modulu kriptografikoetan berreskuratzeko larrialdietan soilik erabiliko da 6.2.4. atalean adierazitako prozedura.

#### **6.2.7. Gako pribatua modulu kriptografikoan biltegitratzea**

CAren gakoaren zeremonia-dokumentu bat dago, eta bertan deskribatzen dira gako pribatua sortzeko prozesuak eta hardware kriptografikoaren erabilera.

IZENPEK CAen gakoak sortzeko ETSI TS 102 042, 7.2.1 g) gomendioa eta Baseline Requirement Guidelines 17.7 gomendioa jarraitzen ditu.

IZENPEK, “hodeian” biltegitratutako azken erabiltzailearen ziurtagirien gakoak sortzeko, Europako Batzordearen gomendioak (eIDAS) eta CEN/TS 419241 gomendioak jarraitzen ditu.

Gako pribatuak modulu kriptografikoen kanpo biltegitratzen diren kasuan, gako pribatuak behar bezala babestuko dira, hau da, fisikoki modulu kriptografikoen barruan izango luketen babes-maila berarekin. IZENPEK ziurtapen-agintaritzen gako pribatuak biltegitratzeko erabilitako HSMs guztiek FIPS 140-2, 3. maila, ziurtapena dute.



### 6.2.8. Gako pribatua aktibatze metodoa

M-tik n gailu kriptografiko (txartel) aldi batera erabiltzea eskatzen duen prozesu baten bidez aktibatzen dira oinarrizko CAren eta mendeko CAen gakoak.

Harpidedunaren gako pribatura PIN baten bidez sartzen da. Gailuak bertara sartzearen aurkako babes-sistema bat du, blokeatu egiten da sarrera-kode okerra hirutan baino gehiagotan sartzen denean. Harpidedunak gailua desblokeatzeko kode bat du. Hiru aldiz oker sartzen bada, gailua behin betiko blokeatuko da, eta erabilezin geratuko da.

"Hodeian" dagoen ziurtagiriaren kasuan, harpidedunaren gako pribatura sartzeko bigarren kautotze-faktorea gaituko da, eta hori aldatu ahal izango da ziurtagiri motaren arabera

### 6.2.9. Gako pribatua desaktibatze metodoa

Txartel kriptografikoa irakurgailutik ateratzean, aribideko edozein eragiketa bukatzen da.

### 6.2.10. Gako pribatua deuseztatzeko metodoa

CAren gakoak suntsitzeko prozedura bat dago.

CAen gako probatuak dituen HSMA kentzen bada, suntsitu egingo dira horiek.

"Hodeian" dauden ziurtagiriaren gako pribatuen kasuan, IZENPErekiko erlazioa amaitzen denean edo iraungitzen direnean ezabatuko dira gakoak.

Prozedura hori ez zaie aplikatzen txartel kriptografikoan jaulkitako erabiltzailea kautotzeko gakoari edo sinadura-gakoari, gako berritzeko gailu kriptografiko bera berriro erabiltzen denean izan ezik. Horretan, aurreko gako suntsituko da eta euskarri berean beste gako batzuk sortuko dira.

### 6.2.11. Modulu kriptografikoaren kalifikazioa

Dokumentu honen 6.2.1 atalean aditzera ematen denaren arabera.

## 6.3 Gako-parea kudeatzearen beste alderdi batzuk

### 6.3.1. Gako publikoa artxibatzea

CAk sortutako ziurtagiriak, eta beraz, gako publikoak, CAk gordeko ditu indarrean dagoen legediak arautzen duen denboraldian.

### 6.3.2. Gako publikoa eta pribatua erabiltzekoaldiak

Ziurtagiri bakoitzaren balio-epea da.

## 6.4 Aktibatze datuak

### 6.4.1. Aktibatze datuak sortzea eta instalatzea

- Gailu kriptografikoan jaulkitako ziurtagiriak: ziurtagiri bakoitzarekin lotzen den gako pribatua erabiltzean, aktibatze datua (PIN) edo pasahitza behar da.



Aktibatze-datua (PINa) edo pasahitza:

- IZENPEren softwareak ausaz sortzen du PINa eta ziurtagiria eusten duen gailu kriptografikoan grabatzen da.
- PINa ziurtagiria jaulkitzeko unean sortzen eta inprimatzen da.
- Konfidentziasunari eusteko aukera ematen duen sistema baten bidez ematen zaio PINa erabiltzaileari.
- Harpidedunari PINa aldatzeko funtzio bat ematen dio IZENPEk txartelean.
- PINa ez da inoiz gordetzen.
- “Hodeian” jaulkitako ziurtagiriak: ziurtagiri bakoitzari lotzen zaion gako pribatuaren erabilerak kautotzeko bigarren faktorea eskatzen du.
- Software euskarrian jaulkitako ziurtagiriak: ziurtagiriekin lotutako gako pribatua instalatzeko eta abian jartzeko, erabiltzaileak berak definitutako segurtasun-sistema erabili beharko da.

IZENPEk ez du kontrolatzen eta ezin du definitu kasu horietan gako pribatura sartzeko modua.

#### **6.4.2. Aktibatze datuak babestea**

Sinadura aktibatze datuei dagokienez, ziurtagirien erabiltzaileei honako hau eskatzen zaie:

- Buruz gogora ditzatela.
- Zaindu ditzatela ahalik eta kontu gehienarekin.
- Ez ditzatela gailu kriptografikoarekin batera jaso, ezta beste jendeari erakutsi ere.
- PINa eta PUKa erabili aurretik alda ditzatela.

#### **6.4.3. Aktibatze datuen beste alderdi batzuk**

Aktibatze datuen gehieneko iraupena ez da arautuko. Bestalde, aldizka aldatu egingo dira zein diren aurkitzeko aukerak gutxitzeko.

### **6.5 Segurtasun informatikoaren kontrolak**

#### **6.5.1. Segurtasun informatikorako berariazko eskakizun teknikoak**

Badira hainbat kontrol IZENPEren ziurtagiri-zerbitzua egiteko sistemaren elementuen kokalekuan (CAk, IZENPEren datu-baseak, IZENPEren Internet zerbitzuak, CA eragiketa eta sarearen kudeaketa):

- Eragiketa-kontrolak.
  - Eragiketa-prozedura guztiak behar bezala dokumentatuta daude beren eragiketa-eskuliburuetan.

Larrialdietarako Plan bat dago.
  - Birusen eta kode kaltegarrien aurka babes-tresnak ezarrita daude.



- Ekipamendua etengabe mantentzen da, ekipamendua une oro erabilgarri eta osorik dagoela ziurtatzearen.
- Informazio-euskarriak, baliabide nahasgarriak eta ekipamendu zaharkituak ziurtasunez babesteko, ezabatzeko eta deuseztatzeko prozedura dago.
- Datu-trukeak. Datu-truke hauek zifratuta doaz dagokien konfidentzialtasuna ziurtatzeko.
  - RAen eta erregistroko datu-baseen arteko erregistro-datuen trukea.
  - Aurrerregistroko datuen trukea.
  - RAen eta CAen arteko komunikazioa.
- Ezeztapenen argitalpen-zerbitzuak behar bezalako funtzionalitateak ditu 24x7 funtzionatzea bermatzeko.
- Sarbide-kontrolak.
  - Erabiltzaile bakarreko IDak erabiliko dira; hartara, egiten dituzten ekintzekin lotuko dira erabiltzaileak eta ekintzen erantzukizuna eskatuko zaie.
  - “Pribilegioak ahalik eta gutxien ematea” printzipioa erabiliko da eskubideak esleitzeko.
  - Lanpostuz aldatzen duten edo erakundea uzten duten erabiltzaileen sarbide-eskubideak berehala ezabatuko dira.
  - Erabiltzaileei esleitutako sarbide-maila hiru hilean behin berrikusiko da.
  - Pribilegio bereziak “kasuak kasu” emango dira eta ezabatu egingo dira hura esleitzea eragin zuen kausa amaitzean.
  - Pasahitzen kalitateari dagozkion arteztarauak daude.

### **6.5.2. Segurtasun informatikoaren mailaren ebaluazioa**

Ziurtapen-zerbitzuak egiteko erabilitako produktuek "Common Criteria" nazioarteko ziurtagiria edo ISO/IEC 15408 estandarra dute.

## **6.6 Bizi-zikloaren kontrol teknikoak**

### **6.6.1. Sistemen garapen-kontrolak**

Softwarea produkzio-sistemetan ezartzea kontrolatzen da.

Sistema horietan sor daitezkeen arazoak saihesteko, kontrol hauek egiten dira:

- Baimen-prozedura formal bat bada ekoizten ari diren softwareko liburutegiak eguneratzeko (adabakiak barne). Baimena behar bezala funtzionatzen duela egiaztatu eta gero ematen da.
- Proba-sistema bat dago produkzio-sistemaz gain, produzitzen hasi baino lehen behar bezala funtzionatzen duen egiaztatzeke.
- Liburutegien eguneratze guztien log fitxategia dago.



- Softwarearen aurreko bertsioak gordetzen dira.
- Eskuratutako softwarea hornitzaileak kualifikatutako mailak mantentzen da.

### **6.6.2. Segurtasunaren kudeaketa-kontrolak**

Ziurtapen-zerbitzuak egiteko erabilitako produktuek "Common Criteria" nazioarteko ziurtagiria edo ISO/IEC 15408 estandarra dute.

### **6.6.3. Bizi-zikloaren segurtasun-kontrolak**

Probak egiteko datu kopuru handia behar da, produkzio-datuetatik ahalik eta hurbileneoak. Informazio pertsonala duten produkzioko datu-baseak erabiltzea saihesten da.

## **6.7 Sareko segurtasunaren kontrolak**

Sareko gailuei gainerako sistemei aplikatzen zaizkien segurtasun-neurri eta -kontrolak aplikatzen zaizkie.

Sareak eta sarearen zerbitzuak erabiltzeari buruzko politika zehaztu da –sareko segurtasun-politikan deskribatzen dena–.

Erabiltzaileak baimena duten zerbitzuetara bakarrik sar daitezke.

## **6.8 Denbora-iturria**

IZENPEk Armadaren Errege Behategirako konexio baten bidez lortzen du bere sistemen denbora, NTP protokoloari jarraituta, betiere Eusko Jaurlaritzarekin ezarritako konexioaren bitartez. NTP protokoloaren deskribapena IETF RFC 5905 estandarrean aurki daiteke.



## 7 Ziurtagirien profilak eta ezeztatutako ziurtagirien zerrendaren profilak

---

### 7.1 Ziurtagiriaren profila

IZENPEk jaulkitako ziurtagiriek honako arau hauei jarraitzen diete:

- Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 5280) 2002ko apirilekoa.
- Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension (RFC 4325), 2005eko abendukoa.
- Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 4630), 2006ko abuztukoak.
- ITU-T Recommendation X.509 (2005): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework.
- ETSI TS 101 867 Qualified Certificate Profile.
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile.

#### 7.1.1. Bertsio-zenbakia

Ziurtapen Praktiken Deklarazio honen arabera jaulkitako ziurtagiriek X509 3. bertsioa estandarra erabiltzen dute.

#### 7.1.2. Ziurtapenen luzapenak

Erabili diren luzapenak honako hauek dira:

- Authority Key Identifier
- subjectKeyIdentifier
- basicConstraints
- keyUsage
- certificatePolicies
- subjectAltName
- issuerAltName
- extKeyUsage
- cRLDistributionPoints
- NetscapeCertType
- Subject Directory Attributes



- Authority Information Access

Sinadura elektronikoko ziurtagirien, zifratze-ziurtagirien eta gailuko ziurtagirien profil generikoak zein diren jakiteko, ikusi *Ziurtagiri bakoitzerako berariazko dokumentazioan*.

Horietako bakoitzaren profilak indibidualizatuak IZENPERi eska dakizkioke.

### Sinadura elektronikoko ziurtagiriaren profil generikoa

Eremua	Edukia	Nahitaezk.	Kritikoa
1. X.509v1 Field			
1.1. Bertsioa	V3	Bai	
1.2. Serial Number	CA jaulkitzaileak automatikoki esleitutakoa	Bai	
1.3. Signature Algorithm	SHA-2 edo berriagoa, RSA sinadurarekin	Bai	
1.4. Signature Value	Sinadura kodetua bit-katearekin	Bai	
1.5. Issuer Distinguished Name	CA igorlearen subject-a	Bai	
1.6. Validity		Bai	
1.6.1. Not Before	Ziurtagiriaren indarraldiaren hasiera-data	Bai	
1.6.2. Not After	Ziurtagiriaren indarraldiaren amaiera-data	Bai	
1.7. Subject		Bai	
1.7.1. CountryName (C)	ES	Ez1	
1.7.2. Organization (O)	Harpidedunaren erakundearen izen osoa edo sozietatearen izena	Bai/Ez1	
1.7.3. Organizational Unit (OU)	Kargua edo/eta saila		
1.7.4. Organizational Unit (OU)	Ziurtagiria kualifikatua dela adieraztea, hala badagokio	Ez	
1.7.5. Organizational Unit (OU)	Ziurtagiri mota adieraztea	Bai	
1.7.6. Organizational Unit (OU)	Agintearen adierazlea	Bai/Ez	
1.7.7. Organizational Unit (OU)	"...n erabiltzeko baldintzak" + URL erreferentzia + lege-oharra	Bai	
1.7.8. dnQualifier	Pertsona fisikoa den harpidedunaren edo gakoaren edukitzailearen IFZ, AIZ; eta Osasun Txartelaren (OTI) zenbakia ere erabiltzeko aukera (*)  (* formatua: -nan nnnnnnnnL, edo aiz Xnnnnnnnnn eta, aukera dagoenean OTI nnnnnnnn	Bai/Ez1	
1.7.9. Common Name (CN)	Pertsona fisikoa den harpidedunaren edo gakoaren edukitzailearen izen-abizenak. Entitate-ziurtagirietan Sozietatearen izena.	Bai/Ez	

<sup>1</sup> Ez da ziurtagiri guztietan ageri.



1.7.10. GivenName	Pertsona fisikoa den harpidedunaren edo gakoaren edukitzailearen izena. Entitate-ziurtagirietan ordezkariaren izena.	Bai	
1.7.11. Surname	Pertsona fisikoa den harpidedunaren edo gakoaren edukitzailearen abizenak. Entitate-ziurtagirietan ordezkariaren abizenak.	Bai	
1.7.12. SerialNumber	Pertsona fisikoa den harpidedunaren edo gakoaren edukitzailearen IFZ, AIZ (*). Entitate-ziurtagirietan entitate juridikoaren IFK edo IFZ.	Bai	
1.7.13. 1.3.6.1.4.1.18838.1.1	Entitate-ziurtagirietan, arduradunaren IFZ edo AIZ. Gainerakoetan ez	Bai <sup>1</sup>	
1.8. Subject Public Key Info	2048-Bit gako publikoa, RFC5280 PKCS#1ren arabera kodetua	Bai	
2. X.509v3 Extensions			
2.1. Authority Key Identifier			
2.1.1. Key Identifier	Jaulkitzailearen gako publikoaren identifikatzailea.		
2.1.2. AuthorityCertIssuer	keyIdentifier-en identifikatutako gakoari dagokion CAren izena		
2.1.3. AuthorityCertSerialNumber	CAren ziurtagiriaren serie-zenbakia		
2.2. Subject Key Identifier			
2.2.1. Key Identifier	Harpidedunaren edo gakoaren edukitzailearen gako publikoaren identifikatzailea		
2.3. Key Usage		Bai	Bai
2.3.1. Digital Signature	Hautatua "1"	Bai	
2.3.2. Non Repudiation	Ez-hautatua "0"		
2.3.3. Key Encipherment	Hautatua/Ez-hautatua "1"/"0" <sup>2</sup>	Bai	
2.3.4. Data Encipherment	Ez-hautatua "0" 1		
2.3.5. Key Agreement	Ez-hautatua "0"		
2.3.6. Key Certificate Signature	Ez-hautatua "0"		
2.3.7. CRL Signature	Ez-hautatua "0"		
2.4. Qualified Certificate Statements		Bai	
2.4.1. qCStatement OID		Bai	
2.5. Certificate Policies		Bai	
2.5.1. Policy Identifier	Ziurtagiri-politikaren OID	Bai	
2.5.2. Policy Qualifier ID		Bai	
2.5.2.1. CPS Pointer	ZPDen URLa	Bai	
2.5.2.2. User Notice	explicitText eremua	Bai	
2.6. Subject Alternate Names			

<sup>2</sup> Ziurtagiri motaren arabera.



2.6.1. rfc822Name	Harpidedunaren edo gakoaren edukitzailearen posta elektronikoko helbidea		
2.7. Issuer Alternative Name			
2.7.1. dnsName	Ziurtagiriaren jaulkitzailearen DNS helbidea		
2.8. Extended Key Usage			
2.8.1. emailProtection	OID emailProtection		
2.8.2. clientAuth	OID clientAuth		
2.9. cRLDistributionPoint			
2.9.1. distributionPoint	CRLren helbidea		
2.10. NetscapeCertType	SSL client, SMIME client		
2.11. Subject Directory Attributes		Bai	
2.11.1. Date of Birth	Pertsona fisikoa den harpidedunaren edo gakoaren edukitzailearen jaiotze-data <sup>3</sup>		
2.12. Authority Information Access		Bai	
2.12.1. Access Description		Bai	
2.12.1.1. Access Method	On-line Certificate Status Protocol-en OID	Bai	
2.12.1.2. accessLocation	On-line Certificate Status Protocol-en URL	Bai	

### 7.1.3. Algoritmo-objektuen identifikatzailea

IZENPEk ziurtagiria sinatzeko erabiltzen duen algoritmo-identifikatzailea (AlgorithmIdentifier) SHA-2/RSA da; "Identifier for SHA-2 checksum with RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc."-en identifikatzailearekin bat dator.

### 7.1.4. Izenen formatuak

Ziurtapen Praktiken Deklarazio honetako 3.1. eta 3.2. ataletan zehaztutakoaren arabera.

### 7.1.5. Izenen murrizpenak

Ez da izenik murrizten.

### 7.1.6. Ziurtagiriaren politikaren objektu-identifikatzailea

Ziurtapen Praktiken Deklarazio honetako 1.2. atalean zehaztutakoaren arabera.

### 7.1.7. "Politika-murrizpenak" luzapenaren erabilera

Ez da politika-murrizpenik erabiltzen.

---

<sup>3</sup> Entitatearen ziurtagirietan izan ezik, horietan ez dago gakoaren edukitzailea.



### 7.1.8. Politika kalifikatzaileen sintaxia eta semantika

Certificate Policies luzapenak politika-kalifikatzaile hauek ditu:

CPS Pointer: IZENPEren Ziurtapen Praktiken Deklaraziorako erakuslea du, <http://www.lzenpe.com/cps>.

User notice: hirugarren batek ziurtagiria egiaztatzen duenean, aplikazio bat eskatuta edo erabiltzaile batek eskatuta, pantailan bistaratzeko den testu-oharra.

Policy Identifier: ziurtagiriaren OID adierazten du

Ziurtagiri guztietarako User Notice komuna:

<b>USER NOTICE</b>	Bermeen mugak ezagutzeko <a href="http://www.lzenpe.com">www.lzenpe.com</a> Ziurtagirian konfiantza izan aurretik kontratua irakurri. Limitaciones de garantías en <a href="http://www.lzenpe.com">www.lzenpe.com</a> Consulte el contrato antes de confiar en el certificado
--------------------	---

### 7.1.9. “certificate policy” luzapenerako tratamendu semantikoa

Certificate Policy luzapenari esker, IZENPEk ziurtagiriarekin zer politika lotzen duen eta politika horiek non aurki daitezkeen identifika daiteke.

## 7.2 Ezeztatutako ziurtagirien zerrendaren profila

IZENPEk jaulkitako ziurtagiriek honako arau hauei jarraitzen diete:

Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 5280) 2002ko apirilekoa.

Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension (RFC 4325), 2005eko abendukoa.

Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 4630), 2006ko abuztukoak.

### 7.2.1. Bertsio-zenbakia

2. bertsioa.

### 7.2.2. Zerrendako elementuen ezeztatutako ziurtagirien eta luzapenen zerrenda

Erabili diren luzapenak honako hauek dira:

Eremua	Nahitaezk.	Kritikoa
X.509v2 Extensions		
1. Authority Key Identifier	Ez	Ez
2. CRL Number	Bai	Ez



Eremua	Nahitaezk.	Kritikoa
<b>3. Issuing Distribution Point</b>	Bai	Ez
<b>4. Reason Code</b>	Bai	Ez
<b>5. Invalidation Date</b>	Bai	Ez

### 7.3 OCSP profila

IZENPEk jaulkitako ziurtagiriek honako arau hauei jarraitzen diete:

Internet X.509 Public Key Infrastructure Online Certificate Status Protocol-OCSP (RFC 6960)  
June 2013

#### 7.3.1. Bertsio-zenbakia

3. bertsioa.

#### 7.3.2. OCSParen luzapenak

Eremua	Nahitaezk.	Kritikoa
<b>1. Issuer Alternative Name</b>	Ez	Ez
<b>2. Subject Key Identifier</b>	Ez	Ez
<b>3. CRL Distribution Points</b>	Ez	Ez
<b>4. Key Usage</b>	Bai	Bai
<b>5. Enhanced Key usage</b>	Bai	Bai



## 8 Denbora Zigilatzeko Zerbitzuaren Praktiken Deklarazioa (TSA)

---

Denbora zigilatzeko zerbitzuaren praktiken deklarazioak (TSA) definitzen ditu IZENPEk eskaintzen duen zerbitzuaren eskakizunak. Kanpo-entitate batek ikuskatuko ditu definitutako prozedurak eta horien ezarpen zuzena, betiere ETSIk TS 102 023 v1.2.2 arauaren bidez definitutako zuzentarauen arabera.

### 8.1 TSAren dibulgazio-deklarazioa

Dokumentu honetan ezartzen diren baldintzak lotesleak izango dira harpidedun guztientzat eta IZENPEren denbora zigilatzeko zerbitzuen erabileran konfiantza duten aldeentzat.

- Harremanetarako informazioa nahi izanez gero, kontsultatu dokumentu honen 1.5.2. puntua.
- IZENPEk jaulkitako denbora zigilatzeko token guztiek barnean hartzen dute politika identifikatzeko objektua: (OID) 1.3.6.1.4.1.14777.3.3
- Sinatzeko erabiltzen den ziurtagiria sortzean sha256WithRSAEncryption erabili da, betiere 4096 bit-eko gako luzerarekin.
- Tokenaren hash algoritmoa SHA-1 da.
- TSAk UTC denbora-doitasuneko arauekin bateragarria den denbora-doitasuna ziurtatzen du, betiere +/- 1 segundoko doitasun minimoarekin. IZENPEren TSAk ez ditu denbora-zigiluko tokenak jaulkiko, baldin eta ez bada denbora-doitasuna ziurtatzen.
- Denbora-zigiluak jaulkitzen dituen entitatearen betebeharrak dokumentu honen 10.6.11. puntuan definituta daude.
- Harpidedunaren betebeharrak dokumentu honen 10.6.12. puntuan definituta daude.
- Hirugarren batzuen betebeharrak dokumentu honen 10.6.13. puntuan definituta daude.
- Denbora zigilatzeko agintaritzaren erantzukizunak dokumentu honen 10.7.2. puntuan definituta daude.
- Zerbitzuak IZENPEren prezio-katalogoko tarifen arabera kostua du.
- IZENPEk TSAren eragiketa guztien erregistroa gordetzen du, dokumentu honen 5.4. puntuan aditzera ematen denaren arabera.
- IZENPEren erantzukizuna dokumentu honen 10.7.1. puntuan eta harpidedun-kontratuan dago definituta.
- Balizko erreklamazioak eta auziak ebazteko kontsultatu dokumentu honen 10.12. puntua.

Harpidedunek eta hirugarren aldeek onartu egiten dituzte IZENPEk definitutako erabilera-baldintzak.



## 9 Bete beharreko ikuskapenak

---

Segurtasun-baldintzak betetzen diren egiaztatzea –segurtasun-ikuskapena edo segurtasun-azterketa ere deitzen zaio– honetarako egiten da: IZENPEren ziurtapen-zerbitzuko sistemaren segurtasun-plana betetzen dela bermatzeko eta hari egokitzeko. Ikuskapen Plan batean dago zehaztuta jarduera hori.

Egiaztapenak in situ egiten dira, IZENPEko langileek prozedurak eta berariazko babes-neurriak aintzat hartzen dituzten jakiteko.

### 9.1 Ikuskapenaren maiztasuna

Aldiro begiraten da ziurtapen-sistema bat datorren segurtasun-baldintzekin. Aurreikusitako beste jarduera batzuekin batera planifikatzen eta gauzatzen da zeregin hori.

### 9.2 Ikuskatzailearen kualifikazioa

Ikuskatzaileak badu gaitasuna eta eskarmentua –aski frogatuak biak– ekoizpen-sistema seguruen ikuskaritzak egiten, egiaztapen digitaleko sistemena bereziki.

### 9.3 Ikuskatzailearen eta ikuskatutako enpresaren arteko harremana

Erakundearen barruko edo kanpoko ikuskatzaileak erabiltzen dira; nolana ere, ikuskatu behar den ekoizpen-zerbitzuarekin funtzionamendu-loturarik ez dutenak behar dute izan.

### 9.4 Ikuskapenaren mende dauden elementuak

Hauek dira ikuskatu beharreko elementuak:

- PKI prozesuak.
- Informazio-sistemak.
- Datuak prozesatzeko zentroaren babes-sistema.
- Dokumentuak.

IZENPEren Ikuskapen Planean dago zehaztuta elementu horietako bakoitzaren ikuskapena nola egin behar den.

### 9.5 Urritasunen ondoriozko erabakiak hartzea

Babes-sistemak baldintzek agintzen dutenarekin bat ez datozela antzemanaz gero, zuzentze-jarduerak jarri behar dira martxan, baita emaitzak begiratu ere.

### 9.6 Emaitzen berri ematea

Segurtasun Batzordeari eman behar zaizkio ikuskapen-txostenak, hark azter ditzan.

Ikuskapena dela-eta ziurtagiriren bat ezeztatu behar izanez gero, IZENPEren Argitalpen Zerbitzuan argitaratu behar da txostena, ezeztapenaren egiazttagiri gisara.



## 10 Beste lege eta jarduera gai batzuk

---

### 10.1 Tarifak

IZENPEk dagozkion ordain ekonomikoak jasoko ditu, Administrazio Kontseiluak kualifikatutako tarifen arabera.

#### 10.1.1. Ziurtagiriak jaulkitzeko edo berritzeko tarifak

Erabiltzaileek ziurtagiriak jaulkitzearen edo berritzearen ordain gisa ordaindu beharreko tarifak 9.1. atalean jaso dira.

#### 10.1.2. Ziurtagirien egoerari buruzko informazioa eskuratzeko tarifa

IZENPEk ziurtagirien egoerari buruzko doako informazio-zerbitzuak eskaintzen ditu CRLen edo OCSPren bidez.

#### 10.1.3. Beste zenbait zerbitzutarako tarifak

Beste zerbitzu batzuetarako tarifak IZENPEren eta eskainitako zerbitzu horien bezeroen artean finkatuko dira.

#### 10.1.4. Itzultze-politika

IZENPEk ez du itzultze-politikarik.

### 10.2 Finantza-erantzukizunak

IZENPEk, erregistro-entitateek eta entitate erabiltzaileek behar adina baliabide daukate dagozkien eragiketak eta jarduerak gauzatzeko.

IZENPEk erantzukizun zibileko aseguruia du, ziurtagiriak sortzeko unean izan daitezkeen eta zehazki egiten den jarduerara zabal daitezkeen hutsuneak eta/edo hutsegiteak berdintzeko. IZENPEk eta erregistro-entitateek esku hartzen badute, harpidedunekin eta ziurtagirien erabiltzaileekin duten harremana ez da mandatuzkoa, ezta mandatu-hartzailearen eta mandatu-emailearen artekoa ere. Harpidedunek eta ziurtagirien erabiltzaileek ez dute IZENPE eta erregistro-entitateak inongo prestazio ematera behartzeko eskubiderik, ez kontratu bidez, ez antzeko beste inongo bitartekoz baliatuz.

### 10.3 Informazioaren konfidentzialtasuna

#### 10.3.1. Informazio konfidentzialaren irismena

Zerbitzuak egiteko, IZENPEk eta erregistro-entitateek hainbat informazio bildu eta biltegiratu beharra daukate, zenbait datu pertsonal ere tarteko direla. Interesatuei eurei eskatzen zaie informazio hori, haien onespren esplizituaz. Interesatuaren onesprenik gabe ere jaso daiteke informazioa, datuak babesteko legeriak horretarako baimena ematen duen kasuetan.



IZENPEk eta erregistro-entitateek ziurtagiriak jaulkitzeko, horiek mantentzeko eta sinadura elektronikoki dagozkion beste zerbitzu batzuk egiteko behar dituzten datuak bakarrik biltzen dituzte, eta ezin dira bestelako xedeetarako erabili sinatzailearen baimen zehatzik gabe.

IZENPEk zaindu egiten du datu-emaileen intimitatea, datu pertsonalak babesteko indarrean dagoen legeriak agintzen duen legez.

IZENPEk eta erregistro-entitateek ez dute datu pertsonalik plazaratzen eta inori uzten, Ziurtapen Praktiken Deklarazio honetako dagozkien atalek eta IZENPEren eta erregistro-entitateen jardura-amaiera kasurako dagozkion atalak aurreikusitako egoeretan izan ezik.

IZENPEk eta erregistro-entitateek konfidentzialtzat gordetzen dituzte honako informazio hauek:

- Ziurtagiri-eskaerak –kualifikatuak zein onartu gabeak–, baita ziurtagiriak jaulkitzeko eta mantentzeko eskuratutako gainerako informazio guztia ere, dagozkion atalean zehaztutako informazioa izan ezik.
- IZENPEk sortutako edo biltegitratutako gako pribatuak.
- Transakzioen erregistroak, erregistro osoak eta transakzioen ikuskapen-erregistroak ere barne direla.
- IZENPEk edo erregistro-entitateek eta horien ikuskatzaileek sortutako eta/edo mantendutako barne- eta kanpo-ikuskapenen erregistroak.
- Negozioen jarraitutasun-planak eta larrialdietarako planak.
- Segurtasun-politika eta -planak.
- Eragiketen eta gainerako eragiketa-planen dokumentazioa, hala nola artxibatzea, kontrolatzea eta antzeko beste zenbait.

### **10.3.2. Irismenaren barruan ez dagoen informazioa**

Honako informazio hau ez-konfidentzialtzat jotzen da, eta halakotzat onartzen dute interesatuek eurek ere IZENPErekin daukaten tresna juridiko loteslean:

- Jaulkitako ziurtagiriak, edo jaulkitze-bidean direnak.
- Pertsona fisikoa den harpidedun batek IZENPEk jaulkitako ziurtagiri batekin duen lotura.
- Ziurtagiriaren harpidedunaren izen-abizenak/ziurtagiriaren harpideduna eta sinatzailea pertsona fisikoa bada, edo gakoaren edukitzailearenak ziurtagiriaren harpideduna pertsona juridikoa edo administrazio-organoa bada, baita titularraren beste edozein zirkunstantzia edo datu pertsonal ere, ziurtagiriaren xedeetarako garrantzizkoa bada.
- Hala agertzen bada, ziurtagiriaren harpidedunaren helbide elektronikoa – ziurtagiriaren harpideduna eta sinatzailea pertsona fisikoa bada–, gakoaren edukitzailearen helbide elektronikoa –ziurtagiriaren harpideduna pertsona juridikoa edo administrazio-organoa bada–, edo harpidedunak esleitutako helbide elektronikoa –gailuetarako ziurtagiriak bada–.



- Ziurtagiriak finkatzen dituen muga eta erabilera ekonomikoak.
- Ziurtagiriaren balio-epaia, baita ziurtagiriaren jaulkitze- eta iraungitze-datak ere.
- Ziurtagiriaren serie-zenbakia.
- Ziurtagiriaren egoera guztiak, baita horietako bakoitzaren hasiera-data ere. Zehazki: sortzeko eta/edo entregatzeko zain, balidatua, ezeztatua, etena edo iraungia, baita egoera-aldaketa eragin zuen zergatia ere.
- Ezeztatutako Ziurtagirien Zerrendak (CRLak), baita ezeztatze-egoerei dagozkien gainerako informazioak ere.
- IZENPEren Argitalpen Zerbitzuan dagoen informazioa.
- Ziurtapen Praktiken Deklarazioko informazio konfidentzialen atalean ageri ez den gainerako informazio guztia.

### **10.3.3. Informazio konfidentziala babesteko erantzukizuna**

Legeak horretarako aurreikusten dituen kasuetan bakarrik argitaratuko dute informazio konfidentziala IZENPEk edo erregistro-entitateek.

Ziurtagiriko datuen fidagarritasuna bermatzen duten erregistroak, zehazki, prozedura judizial batean ziurtapena egiaztatzeko eskatzen badituzte argitaratuko dira, baita ziurtagiriaren harpidedunaren baimenik gabe ere.

Ziurtagiriak argitaratzean sinadura elektronikoa buruzko abenduaren 19ko 59/2003 Legearen 18.c) artikulua agintzen duenari jarraituko zaio.

## **10.4 Datu pertsonalak babestea**

### **10.4.1. Sarrera**

IZENPEk, ziurtapen-zerbitzuen emaile den heinean, datu pertsonalen fitxategiak babestu egiten ditu, datu pertsonalak babesteari buruzko abenduaren 13ko 15/1999 Legean aurreikusitakoari jarraiki, baita datu pertsonalak babesteari buruzko 15/1999 Lege Organikoa garatzeko Erregelamendua onartzen duen 1720/2007 Errege Dekretuan aurreikusten denari, eta gainerako garapeneko araudiari jarraiki ere.

Sinadura elektronikoa buruzko Legean ezarritakoa kontuan izanik, Ziurtapen Praktiken Deklarazio hau segurtasun-dokumentutzat hartzen da, betiere datu pertsonalak babesteari buruzko legedian aurreikusten den helburuetarako. Gisa horretako dokumentu batek bete behar dituen baldintzak betetzen ditu.

### **10.4.2. Aplikazio-esparrua**

Datu pertsonalak dituzten fitxategiak babesteko segurtasun-dokumentuan, IZENPEk bere fitxategietan dauden datu pertsonalen babesa bermatzeko beharrezko segurtasun-neurriak ezartzen ditu, betiere datu pertsonalak tratatzen dituzten instalazioetan, euskarri-plataformetan eta informazio-sistemetan oinarrituta –automatizatueta, automatizatu gabeetan zein mistoetan–.



Horrela, segurtasun-dokumentuan honako alderdiak jorratuko dira:

- Datu pertsonalak babesteko segurtasun-antolamendua.
- Datu pertsonalak dituzten fitxategien egitura eta segurtasun-mailak.
- Segurtasuneko arauak eta prozedurak.

Bestalde, datu pertsonalak tratamendu, sarrera, aldaketa edo galera baimendu gabeen aurrean eraginkortasunez babestuko badira, informazio hori eskuratzeko erabil daitezkeen bide guztiak kontrolatuko dira.

Horrela, hauek dira datu pertsonalak dituzten IZENPEren fitxategietara sartu ahal izateko zuzeneko edo zeharkako bide izan daitezkeen baliabideak –ondorio horretarako araudiak kontrolatu behar dituenak–:

- Fitxategiak kokatuta dauden eta horien euskarriak edo dokumentuak biltegitzen diren tratamendu-zentroak edo -instalazioak eta lokalak.
- Fitxategiak kokatuta dauden eta fitxategi automatizatuekin lan egiten den sistema eragilearen eta komunikazio-sistemaren ingurunea eta zerbitzariak.
- Baimendu gabeko dokumentazio eta informazioko fitxategiak.
- Datuetara sartzeko ezarritako sistemak (automatizatuak, eskuzkoak edo mistoak).

#### **10.4.3. Datu pertsonalak babesteko segurtasun-antolamendua.**

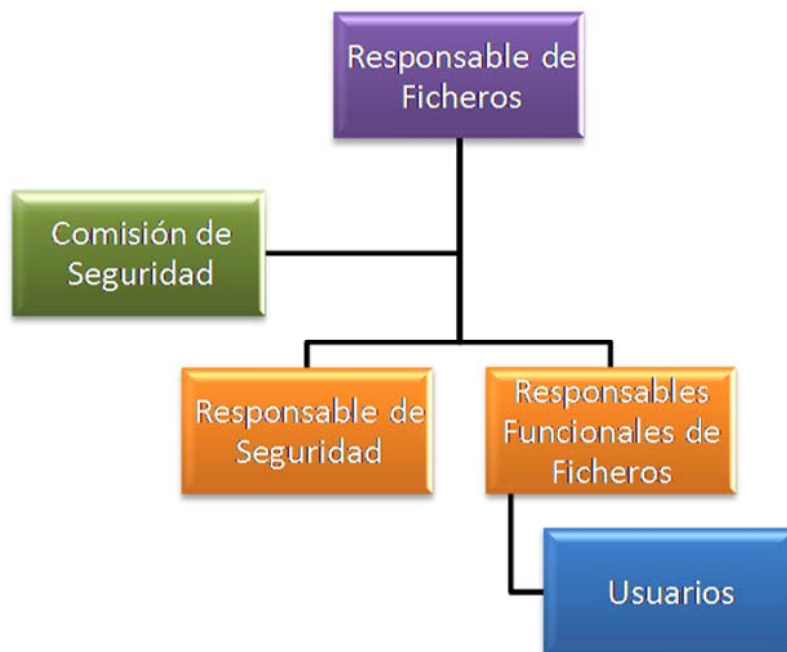
Atal honetan deskribatzen da IZENPEk datu pertsonalen segurtasuna bermatzeko ezarritako segurtasun-antolamendua.

Segurtasun-antolamenduaren eredia aurkezten da. Tartean dauden unitateak ez ezik, horien arteko mendetasun hierarkikoa eta funtzionala ere identifikatzen eta aurkezten da.

IZENPEren segurtasun-dokumentuan, segurtasun-antolamenduko unitateetako bakoitzak garatu beharreko funtzioak zehazten dira.

#### **10.4.4. Segurtasun-antolamenduaren eredia**

Organigrama honetan jasotzen da IZENPEren datu pertsonalen segurtasuna kudeatzeko eta kontrolatzeko segurtasun-egituraren irudikapen grafiko sinplifikatua. Segurtasunaren antolamenduan inplikaturako unitateak irudikatzen dira, baita horien arteko lotura hierarkikoak edo funtzionalak ere (zehazki, fitxategien arduraduna, segurtasun-batzordea, segurtasuneko arduraduna, IZENPEren fitxategien arduradun funtzionalak eta erabiltzaileak).



Fitxategien arduraduna / Segurtasun-batzordea / Segurtasun-arduraduna / Fitxategien arduradun funtzionalak / Erabiltzaileak

#### 10.4.5. Segurtasuna antolatzeko unitateen sailkapena

Aurretik deskribatutakoaren arabera, segurtasunaren antolamendurako segurtasun-dokumentuan zerrendatutako unitateak eta langileak honako kategoria hauetan sailkatzen dira:

- Fitxategiaren arduraduna, fitxategiaren xedeari, edukiari eta erabilerari buruzko erabakiak hartzen dituen pertsona fisikoa edo juridikoa.

Fitxategiaren segurtasunaz arduratzen da, eta beharrezko segurtasun-neurriak hartzen eta ezartzen ditu, dokumentu hau bete behar duten langileek dagozkien funtzioen garapenean eragina duten arauak ezagut ditzaten.

Dokumentua eguneratuta mantentzen du, eta datuen segurtasunaren arloan indarrean dauden xedapenetara egokitu beharko du beti dokumentu honen edukia.

- Segurtasun-arduraduna, fitxategiko arduradunak izendatzen duen pertsona honek fitxategiko datuei aplikatu dakizkiekeen segurtasun-neurriak koordinatzeko eta kontrolatzeko funtzioak bete behar ditu.

Fitxategiko arduradunarekin elkarlanean, segurtasun-dokumentuaren hedapena bultzatzen du, eta berau betetzen dela zaintzeko lanetan ere laguntzen du.

- Segurtasun-batzordea, informazioaren segurtasunari eta datuen babesari dagozkion erabakiak hartzean, antolakundeko unitateen kontsulta eta laguntzarako organo gorenena da. Bere eskumenak baliatzean, Batzordeak eskuordetze bidez jarduten du, IZENPERen ordezkaritza gorenena den Zuzendaritza-Gerentziaren babes osoarekin –datu pertsonalak dituzten fitxategien arduraduna den aldetik– eta fitxategi horiek atxikitzen



diren zuzendaritza-organoen babes osoarekin –horien ardura duten barne-organo diren aldetik–.

- Fitxategien arduradun funtzionala, zerbitzuen ikuspuntu funtzionaletik Informazio Sistemen alderdi operatiboetan erabakiak hartzeaz arduratzen den pertsonari dagokion irudia da. Irudi horiek fitxategien arduradun den IZENPEren ordezkartzan jardungo dute. Tartean den zerbitzuaren kudeaketaren arduradunak, hau da, arloetako bakoitzeko arduradunak izango dira funtzio hori beteko duten IZENPEren pertsonak.
- Fitxategiaren erabiltzailea, bere funtzioak betetzean datu pertsonalak tratatzen dituen edo datu horiek eskura dituen pertsona da. Erabiltzaile horiek, datu pertsonalen alorrean, Segurtasun Dokumentuan biltzen diren arauak eta prozedurak errespetatu beharko dituzte, baita indarrean dagoen eta aplikatzekoa den legeriaren ondoriozkoak ere.

#### **10.4.6. Datu pertsonalak dituzten fitxategien egitura**

Ziurtapen Praktiken Deklarazio honen ondorioetarako, IZENPE da Datuak Babesteko Espainiako Agentziak datu pertsonalak dituzten honako fitxategi hauen (aurrerantzean FITXATEGIEN) arduraduna:

- Erabiltzaileak: oinarrizko segurtasun-maila.
- Administrazio-kudeaketa: oinarrizko segurtasun-maila.
- Giza baliabideak: oinarrizko segurtasun-maila.
- Curriculum Vitaea: oinarrizko segurtasun-maila.
- Dokumentazioaren sarrera eta irteerako erregistro-fitxategia: oinarrizko segurtasun-maila.
- Transakzioak: oinarrizko segurtasun-maila.
- Hirugarren batzuekiko harremanak: oinarrizko segurtasun-maila.

Fitxategiek datu pertsonalak dituztenez gero, 1720/2007 Errege Dekretuaren 81. artikuluan ezartzen denez, dagozkien segurtasun-neurri guztiak izango zaizkie aplikatzekoak.

Fitxategien egituraren deskribapena Antolamenduaren Segurtasun Dokumentuan zehazten da.

#### **10.4.7. Segurtasuneko arauak eta prozedurak**

Datu pertsonalen segurtasuna bermatuko duten neurri, arau eta prozedura zehatzak daude.

Horretarako, segurtasun-dokumentuak arreta berezia eskaintzen dio sistema eragilearen inguruneari, baita segurtasun-dokumentuaren babespeko fitxategiaz baliatzen diren ordenagailuak kokatzen diren lokalei eta lanpostuei ere.

##### **Arauak**

IZENPEk, bere funtzioen jardunean, tratatzen dituen datu pertsonalen babesa bermatzeko beharrezko arauak ditu, eta, horrela, mota horretako datuei aplikatzekoa zaien legeria betetzen du.



Arau horiek IZENPEren zerbitzu, dependentzia eta informazio-sistema guztiei aplikatzen zaizkie; edozein formatutan (paperean, informatikoan, bideoan, ...) biltzen diren datu pertsonal guztiei aplikatzen zaie, elementu horiek erabiltzen dituen pertsona edozein izanik ere (barnekoa zein kanpoko).

Zehazki, honako hauek dira ezarritako arauak:

- Segurtasun-arduradunari fitxategien komunikazioari buruzko araudia.
- Erabiltzaileen administrazioari buruzko araudia.
- Maila handiko fitxategien sarrera-erregistroari buruzko araudia.
- Datu pertsonalak dituzten euskarriak eta/edo dokumentuak sartzea eta irtetea baimentzeari buruzko araudia.
- Datu pertsonalak dituzten eskarien eta dokumentuen erregistroari buruzko araudia.
- Euskarriak eta/edo dokumentuak identifikatzeari eta inbentariatzeari buruzko araudia.
- Datu pertsonalak dituzten euskarriak eta/edo dokumentuak berrerabiltzeari eta suntsitzeari buruzko araudia.
- Aldi baterako fitxategien tratamenduari buruzko araudia.
- Segurtasun-dokumentuan xedatutakoa egiaztatzeako kontrolari buruzko araudia.
- Aldian behin ikuskapenak egiteari buruzko araudia.
- Probetan benetako datu pertsonalak erabiltzeari buruzko araudia.
- IZENPEren lokaletara eta dependentzietara eta datu pertsonaletara fisikoki sartzeko kontrolari buruzko araudia.
- Datu pertsonalak dituzten fitxategiak sortzeari, aldatzeari eta ezabatzeari buruzko araudia.
- Fitxategiak garatzeko eta ezartzeko segurtasun-neurriei buruzko araudia.
- Babes-kopiak egiteari buruzko araudia.
- Datu pertsonalak babesteari buruzko araudia.
- Automatizatu gabeko euskarriak eta/edo dokumentuak kudeatzeari eta zaintzeari buruzko araudia.
- Automatizatu gabeko fitxategiak artxibatzeari buruzko araudia.
- Automatizatu gabeko fitxategietan biltegitratzeko gailuei buruzko araudia.
- Automatizatu gabeko fitxategietako dokumentuak kopiatzeari eta erreproduzitzeari buruzko araudia.
- Automatizatu gabeko dokumentazioa eskuratzeari buruzko araudia.
- Komunikazioetako segurtasun-neurriei buruzko araudia.

## Prozedurak

Bestalde, IZENPEk datu pertsonalen babesa bermatzeko beharrezko prozedurak ditu.

Prozedura horiek IZENPEren zerbitzu, dependentzia eta informazio-sistema guztiei aplikatzen dira; edozein formatutan (paperean, informatikoan, bideoan, ...) biltzen diren datu pertsonal guztiei aplikatzen zaie, elementu horiek erabiltzen dituen pertsona edozein izanik ere (barnekoa zein kanpoko).

Zehazki, honako hauek dira ezarritako prozedurak:

- Erabiltzaileak administratzeko prozedura.



- Gertakariak jakinarazteko eta kudeatzeko prozedura.
- Babes-kopiak egiteko prozedura.
- Datuak berreskuratzekeo prozedura.
- Datu pertsonaletara sartzeko eskubideaz baliatzeko prozedura.
- Datu pertsonalak zuzentzeko eta ezabatzeko eskubideaz baliatzeko prozedura.
- Datu pertsonaletarako oposizio-eskubideaz baliatzeko prozedura.

## **10.5 Jabetza intelektualeko eskubideak**

### **10.5.1. Ziurtagirien jabetza**

IZENPE da jaulkitzen dituen ziurtagirien gaineko jabetza intelektualeko eskubideak dituen erakunde bakarra.

Ez dira eskubide horietan sartzen ziurtapen digitaleko sistemaren aplikaziotik eratorritako eta hirugarren baten jabetzapeko jabetza intelektualeko eskubideak.

Arau berberak aplikatu behar zaizkio ziurtagiriak ezeztatzekeo informazio-sistemari.

### **10.5.2. Ziurtapen Praktikaren jabetza**

IZENPE da honako Ziurtapen Praktiken Deklarazio honen jabea.

### **10.5.3. Izenen gaineko informazioaren jabetza**

Harpidedunak eta, hala badagokio, gakoan edukitzaileak, gorde egiten ditu ziurtagiriko markaren, produktuaren edo deitura komertzialaren gaineko eskubide guztiak (baldin eta eskubiderik badauka).

Harpideduna eta, hala badagokio, gakoan edukitzailea da ziurtagiriaren izen bereizgarriaren jabea. Ziurtapen Praktiken Deklarazioko 3. atalean zehaztutako informazioek osatzen dute aipatutako izena.

### **10.5.4. Gakoan eta horiei dagokien materialaren jabetza**

Ziurtagirien harpidedunak dira gako-pareen jabeak.

## **10.6 Betebeharrak eta bermeak**

IZENPEk, ziurtagiriak ziurtapen-praktiken deklarazio honen arabera jaulkitzen dituen ziurtapen-entitatea den aldetik, bere gain hartzen ditu betebeharrak hauek.

### **10.6.1. Zerbitzua egitekeo betebeharrak**

Izenpe, SAK Ziurtapen Praktiken Deklarazio honen arabera ematen ditu ziurtapen-zerbitzuak, horrek zehazten baititu bere zereginak, jarduteko prozedurak eta segurtasun-neurriak.



Bereziki, dagozkion betebeharrak guztiak betetzeko ardura bere gain hartzen du, erregistro-entitateak praktika hauetan berariaz egiten dituenak izan ezik, baldin eta erregistro-entitate gisa jarduten ez badu. Ziurtapen-entitatearen betebeharrak honako hauek dira:

- Zerbitzuak egin zaizkion pertsonaren sinadura sortzeko datuak ez kopiatzea.
- Egindako ziurtagiriak adieraziko dituen eta ziurtagiri horiek indarrean dauden edo indarraldia eten edo iraungi den adieraziko duen sistema mantentzea.
- Ziurtagiri onartuei eta unean une indarrean dauden ziurtapen-praktiketako deklarazioei buruzko informazio eta dokumentazio guztia edozein baliabide seguru bidez erregistratzea, gutxienez 15 urtez egiten diren unetik bertatik kontatzen hasita. Hortaz, egiten diren sinadurak eta gainerako ziurtagiriei dagozkienak 7 urtez egiaztatu ahal izango dira.
- Sinatzaileak sinadura sortzeko datuak dituela ziurtatzea –ziurtagirian jasoarazten diren egiaztatzeari dagozkion datuak–.
- Sinadura sortzeko eta egiaztatzeko datuen osagarritasuna bermatzea, betiere biak ziurtapen-zerbitzuen egileak sortu baditu.
- Segurtasuneko araudia eta estandarrak betetzea (datu pertsonalak babesteari buruzko Lege Organikoa, ISO, ETSI eta IZENPEren segurtasun-politika).
- Gordetzeko zerbitzuaren hornitzaileei segurtasuneko araudia eta estandarrak (datu pertsonalak babesteari buruzko Lege Organikoa, ISO, ETSI eta IZENPEren segurtasun-politika) bete ditzaten eskatzea.

#### **10.6.2. Jardun fidagarriko betebeharrak**

IZENPEK honako hau bermatzen du:

- Ziurtagirian agertzen den identitatea ziurtagirian agertzen den gako publikoari dagokiola, era unibokoan.
- Zerbitzua bizkor eta modu seguruan eskaintzea. Bereziki, ziurtagirien baliozkotasuna kontsultatzeko zerbitzu bizkorra eta segurua erabiltzeko aukera ematen du, eta ziurtagirien eraginkortasuna modu seguruan eta berehala iraungiko bada, horren berri emango duela bermatzen du, Ziurtapen Praktiken Deklarazio honek aurreikusten duenarekin bat etorritik. Zerbitzua eguneko 24 orduetan erabili daiteke, asteko 7 egunetan.
- Sinadura elektronikoen arloan indarrean dagoen legeriak finkatzen dituen eskakizun teknikoak eta langileei buruzkoak betetzea:
  1. Ziurtatze-zerbitzuak egiteko beharrezko fidagarritasuna frogatzea.
  2. Ziurtagiri bat jaulki edo bere indarraldia amaitu den eguna eta ordua zehaztasunez adierazi ahal izan dadin bermatzea.
  3. Eskaintzen diren ziurtatze-zerbitzuak egiteko behar adinako kualifikazioa, ezagutzak eta esperientzia duten langileak erabiltzea, baita sinadura elektronikoen esparruko segurtasuneko eta kudeaketako prozedura egokiak ere.
  4. Erabiltzen diren sistemak eta produktuak fidagarriak izatea, aldaketa ororen aurka babestuta daudenak eta jasaten dituzten ziurtatze-prozesuen



- segurtasun tekniko eta –hala badagokio– kriptografikoa bermatzen dutenak, betiere Segurtasun Politikari jarraituz.
5. Ziurtagirien faltsifikazioaren aurkako neurriak hartzea eta konfidentzialtasuna bermatzea sinadura (gako pribatua) sortzeko datuen eratze-prozesuan, 6. atalak diotenaren arabera. Gainera, sinatzaileari prozedura seguru baten bidez ematea.
  6. Sistema fidagarriak erabiltzea kualifikatutako ziurtagiriak biltegitratzeko. Sistema horiek ziurtagiriak kautotzeko aukera eman behar dute, eta baimendurik gabeko pertsonak datuak aldatu ahal izatea saihestu beharko dute. Sinatzaileak aditzera eman dituen pertsonak eta kasu jakin batzuetan, soilik, sartu ahal izango dira datu horietara, eta hala bermatu behar du sistema horrek. Gainera, segurtasun-baldintzetan eragina izan dezakeen edozein aldaketa antzeman beharko dute sistema horiek.
- Segurtasunaren kudeaketa egokia, Informazioaren Segurtasuna Kudeatzeko Sistema ezartzeari esker, betiere ISO/IEC 27001 arauak ezarritako printzipioen arabera. Honako neurri hauek, besteak beste, hartu dira aintzat:
1. Segurtasuna aldi behin egiaztatzea, ezarritako estandarrekiko adostasuna ziurtatzearen.
  2. Segurtasun-gertakarien kudeaketa osoa gauzatzea, gertakari horiek hauteman, ebatzi eta optimizatu direla bermatzearen.
  3. Segurtasunaren arloan interes berezia duten taldeekin harreman egokiak izatea, hala nola adituekin, segurtasun-foroekin, eta informazioaren segurtasunaren arloko elkargo profesionalekin.
  4. Sistemen mantentze-lana eta bilakaera behar bezala planifikatzea, erabiltzaileen eta bezeroen iguripenak berme osoz beteko dituen zerbitzua eta etekin egokia ziurtatzearen.

### 10.6.3. Identifikazio-betebeharrak

Kualifikatutako ziurtagirien kasuan, IZENPEk identifikatu egiten du ziurtagiriaren harpideduna, sinadura elektronikoari buruzko abenduaren 19ko 59/2003 Legearen 12. eta 13. artikuluen arabera, eta Ziurtapen Praktiken Deklarazio honen arabera.

### 10.6.4. Erabiltzaileei eman beharreko informazioa: betebeharrak

- Harpidedunari ziurtagiria jaulki eta eman aurretik, honako honen berri jakinarazten dio hari IZENPEk: ziurtagiria erabiltzeko bete behar diren baldintzen, prezioaren –finkatuta badago–, erabilera-mugen eta Ziurtapen Praktiken Deklarazio honen 2.1.1.6. atalean dauden tresna juridiko lotesleen berri.

“Ziurtagiria erabiltzeko baldintzak” izeneko testuaren bidez egiten da hori. Posta elektronikoz nahiz komunikabide iraunkorren baten bidez transmititu behar da testua, ongi ulertzeko moduan idatzita betiere.



- IZENPEk gakoan edukitzaileari haren ziurtagiriaren indarraldia iraungitzearen berri eman beharko dio, ziurtagiri elektronikoaren indarraldia amaitu edo eten aurretik edo aldi berean, eta ziurtagiria indarrik gabe geratzearen arrazoiak zehaztuko dizkio, baita data eta ordua ere.
- Bi hilabete lehenago jakinaraziko die IZENPEk sinatzaileei ziurtapen-zerbitzuak egiteari utzi egingo diola, eta, hala badagokio, ziurtagirien kudeaketa eskualdatzen zaion emailearen ezaugarrien berri emango die. Dokumentu honek aurreikusitakoaren arabera egin behar dira sinatzaileekiko komunikazioak.
- IZENPEk badu jarduera eteteko amaiera-plan bat eta, bertan, etete hori zein baldintzatan egingo litzatekeen zehazten da.
- Ziurtagiriei buruzko informazio publiko guztia IZENPEren Argitalpen Zerbitzuan jaso da, Ziurtapen Praktiken Deklarazio honen 2.6. atalean.

#### **10.6.5. Egiatzapen-programak: betebeharrak**

IZENPEk edonork erabiltzeko ziurtagirien baliozkotasuna egiaztatzeko bitarteko publikoak eskaintzen ditu Ziurtapen Praktiken Deklarazio honetan deskribatzen diren sistemen bidez.

#### **10.6.6. Ziurtapen-zerbitzuaren arautze juridikoa: betebeharrak**

IZENPEk bere gain hartzen ditu ziurtagirian ageri diren betebeharrak guztiak, baita beste batzuen erreferentzia gisara hartutakoak ere. Erreferentzia bidez jasotzeko, objektu-identifikatzailea edo dokumentuari lotzeko beste bideren bat erantsi behar zaio ziurtagiriari.

Idatzizko hizkuntza ulergarria da IZENPE eta eskatzailea, harpideduna edo gakoan edukitzailea lotesten dituen tresna juridikoa, baita ziurtagirian konfiantza duen hirugarrena ere. Honako eduki hauek izan behar ditu, gutxienik, aipatu tresnak:

- Ziurtapen Praktiken Deklarazio honetako 2.1.4., 2.1.5., 2.1.6., 2.2., 2.3. eta 2.4. atalek diotena betetzeko aginduak.
- Zein Ziurtapen Praktiken Deklarazio den aplikagarri adierazi behar du, eta, hala badagokio, zehaztu egin behar du ziurtagiriak salgai daudela eta sinadura sortzeko nahiz mezuak deszifratzeko gailu segurua erabili behar dela.
- Gako pribatuak jaulki, eten, ezeztatu eta, hala badagokio, berreskuratzeko bete beharreko klausulak.
- Ziurtagirian dagoen informazioa zuzena dela adierazi behar du, harpidedunak kontrakoa jakinarazten ez badu behintzat.
- Sinadura sortzeko gailu segurua hornitzeko erabilitako informazioa biltegitratzeko baimena, betiere harpideduna erregistratzeko, gailu kriptografikoa hornitzeko eta informazio hori beste batzuei uzteko, baldin eta IZENPEren eragiketarako ziurtagiri baliozkoak ezeztatu gabe amaitzen badira.
- Ziurtagiria erabiltzeko mugak, 1.3.2. atalekoak barne.
- Ziurtagiriak nola balidatu jakiteko informazioa, ziurtagiriaren egoera egiaztatzea barne dela, baita ziurtagirian dezenteko konfiantza izateko baldintzei buruzkoa ere.



- Aplikagarri diren erantzukizun-mugak, barne direla IZENPEk bere erantzukizuna onartzen edo baztertzen duen erabilerak.
- Ziurtagiri-eskaerei buruzko informazioa zenbat denboraz eduki behar den artxibatuta.
- Ikuskaritza-erregistroak zenbat denboraz eduki behar diren artxibatuta.
- Auziak konpontzeko aplikagarri diren prozedurak.
- Aplikagarri den legea eta eskumena duen jurisdikzioa.
- IZENPE entitate publikoren baten edo batzuen ziurtapen-politikekiko bateragarri aitortu duten, eta, hala badagokio, zein sistemaren arabera.
- IZENPEren ondare-erantzukizuna bermatzeko era.

#### **10.6.7. Erregistro-entitatearen betebeharrak**

Honako betebeharrak hartzen ditu bere gain erregistro-entitateak:

- Eskatzailearen, harpidedunaren eta gakoaren edukitzailearen nortasuna eta beste zenbait datu pertsonal egiaztatzea –ziurtagirien xedeetarako garrantzizkoak direnak edo ziurtagirietan daudenak–, prozedura hauen arabera.
- Kudeatzen dituen ziurtagirien jaulkipenari, berritzeari, ezeztatzeari edo berraktibatzeari buruzko dokumentazio eta informazio guztia gordetzea.
- IZENPEri garaiz jakinaraztea ziurtagiriak azkar eta modu fidagarrian ezeztatzeko eskaeren berri.
- IZENPEri artxiiboak erabiltzen uztea, baita jardueretarako erabiltzen diren prozeduren eta horretarako behar den informazioaren mantentze-lanen ikuskapena egiten ere.
- IZENPEri jakinaraztea ziurtagiriak jaulki, berritu edo berraktibatzeko eskaeren berri, baita hark jaulkitzen dituen ziurtagiriei buruzko beste zeinahi alderdiren berri ere.
- Garaiz begiratzea ziurtagirien iraunaldian eragina izan dezaketen ezeztatzeko zergatiak.
- Ziurtagiriak jaulki, berritu eta ezeztatzeko IZENPEk ezarritako prozedurak eta gai horretaz indarrean dagoen legeriak agindutakoa betetzea.
- Segurtasuneko araudia eta estandarrak betetzea (datu pertsonalak babesteari buruzko Lege Organikoa, ISO, ETSI eta IZENPEren segurtasun-politika).

Hala dagokionean, bere gain hartu ahal du eginkizun hau ere: gakoaren edukitzailearen esku jartzea sinadura (gako pribatua) sortzeko eta sinadura elektronikoa (gako publikoa) egiaztatzeko prozedura teknikoak.

#### **10.6.8. Ziurtagiri-eskatzailearen betebeharrak**

Honako betebeharrak ditu ziurtagiri-eskatzaileak:



- Ziurtagiri-eskaerak egiteko eman duen informazioaren egiazkotasuna, osotasuna eta gaurkotasuna bermatzea, baita haietan jarri beharreko informazioarena ere.
- Berariazko dokumentazioan finkatutako eskaera-prozedura betetzea.

#### 10.6.9. Ziurtagiri-harpidedunaren betebeharrak

- Informazio osoa eta egokia ematea IZENPERi, Ziurtapen Praktiken Deklarazioko eskakizunen arabera, erregistro-prozedurari dagokionez batez ere.
- Ziurtagirietan jarri beharreko informazioaren egiazkotasuna, osotasuna eta gaurkotasuna bermatzea.
- Ziurtagiriak erabiltzeko baldintzak jakitea eta onartzea, baita haiei egiten zaizkien aldaketak ere.
- Ziurtagiriren bat jaulki eta eman aurretik, horretarako onespina ematea.
- Ziurtagirien euskarriak ongi erabili eta gordeko direla bermatzea.
- Ziurtagiria egokiro erabiltzea, eta, zehazki, ziurtagirien erabilera-mugak aintzat hartzea.
- Arretaz zaintzea gako pribatua, baimendu gabeko erabilerak saihestearren, Ziurtapen Praktiken Deklarazioko 6.1, 6.2 eta 6.4 sailek agintzen dutenaren arabera.
- IZENPERi eta harpidedunaren ustez ziurtagirian konfiantza duen edonori honakoa jakinaraztea, justifikatzerik ez dagoen atzerapenik gabe:
  1. Gako pribatua galdu, norbaitek ostu edo arriskuan jarri izana.
  2. Gako pribatuaren kontrola galdu izana, aktibatze-datuak (gailu kriptografikoaren PIN kodea, adibidez) arriskuan jartzeagatik edo beste edozein arrazoiengatik.
  3. Ziurtagiriaren edukian dauden okerrak edo izandako aldaketak (harpidedunak dakizkienak edo jakin litzakeenak). Aldaketak ziurtagiria ezeztatzea badakar, horretarako eskaera egin behar du harpidedunak.

Gako pribatua erabiltzeari uztea ziurtagiriaren balio-epea amaitu ondoren.

Gakoen edukitzaileei jakinaraztea zein betebeharrak dagozkien.

Ziurtagiri-zerbitzuen ezartze teknikoak ez kontrolatzea, manipulatzeko edo atzeranzko ingeniartzeko ekintzarik ez egitea, aurrez Ziurtapen Entitatearen idatzizko baimenik eduki gabe.

Ziurtagiri-zerbitzuen segurtasuna arriskuan nahita ez jartzea.

Ziurtagirietako gako publikoei dagozkien gako pribatuak ez erabiltzea inongo ziurtagiri izenpetzeko, ziurtapen-entitatea balitz bezala.

Ziurtagirian zerrendatutako gako publikoari dagokion gako pribatua erabiliz sinadura digitalak sortzen dituen ziurtagiri onartuen harpidedunak aitortu egin behar du, dagokion bitarteko juridikoaz, sinadura elektronikoko horiek eskuz idatzitako sinaduren baliokide direla, gailu kriptografikoak erabiltzen denean, betiere sinadura elektronikoa



buruzko abenduaren 19ko 59/2003 Legearen 3.4. artikulua agintzen duenaren arabera.

#### **10.6.10. Ziurtagirien erabiltzaile egiaztatzailearen betebeharrak**

Ziurtagirien erabiltzaile egiaztatzaileak honako betebeharrak ditu:

- Eman nahi zaion erabilerarako ziurtagiria egokia den ala ez jakiteko, informazioa iturri independenteetatik jasotzea.
- Ziurtagiriak erabiltzeko baldintzak zein diren jakitea, Ziurtagiri Praktiken Deklarazioak eta egiaztatzailearen eta IZENPEren arteko ziurtagiri-zerbitzuak egiteko kontratuak aurreikusten dutenaren arabera.
- Emandako ziurtagirien baliozkotasuna edo ezeztapena egiaztatzea. Horretarako, ziurtagirien egoerari buruzko informazioa erabiliko da.
- Ziurtagirien hierarkiako ziurtagiri guztiak egiaztatzea, sinadura digitalean edo hierarkiako ziurtagiriaren bategan konfiantza jarri baino lehen.
- Kontuan izatea ziurtagiria erabiltzeko dauden mugak, nonahi daudelarik ere: ziurtagirian bertan nahiz egiaztatzailearen kontratuan.
- Kontuan izatea kontratuan edo beste nonbait finkatutako badaezpadako neurri guztiak, edozein delarik ere haren izaera juridikoa.
- Jakinaraztea ziurtagiriari buruzko gertaera edo egoera irregular guztiak, ziurtagiria ezeztatzeko arrazoia izan daitekeenak.
- Ziurtagiri-zerbitzuen ezartze teknika ez kontrolatzea, manipulatzeko edo atzeranzko ingeniartzeko ekintzarik ez egitea, aurrez IZENPEren idatzizko baimenik gabe.
- Ziurtagiri-zerbitzuen segurtasuna arriskuan nahita ez jartzea.

Ziurtagiri onartuen erabiltzailea behartuta dago aitortzera dagokion tresna juridikoan sinadura elektronikoko horiek eskuz idatzitako sinaduren baliokideak direla, sinadura elektronikoko buruzko abenduaren 19ko 59/2003 Legearen 3.4. artikulua arabera.

#### **10.6.11. Denbora-zigiluak jaulkitzen dituen entitatearen betebeharrak**

IZENPEren denbora zigilatzeko agintaritzak denbora-zigiluko token seguruak (TST) jaulkitzen ditu denbora zigilatzeko zerbitzuen erabiltzaileentzat (harpidedunentzat zein hirugarren aldeentzat).

IZENPEren denbora zigilatzeko agintaritzak bere gain hartzen du denbora zigilatzeko zerbitzuak egiteko erantzukizuna. IZENPEren denbora zigilatzeko agintaritzak denbora zigilatzeko hainbat unitate identifikagarriekin (TSU) lan egin dezake, eta horietako bakoitzak bere sinadura-gakoa izan dezake.

IZENPEren denbora zigilatzeko agintaritzak identifikatuta dago denbora zigilatzeko zerbitzuetarako erabiltzen den ziurtagiri digitalean.



#### **10.6.12. Denbora-zigiluen harpidedunaren betebeharrak**

Denbora-zigiluen harpidedunak ETSI TS 101 861 “Requirements of a TSP client” arauaren 4. atala betetzeko soilik erabil dezake denbora zigilatzeke zerbitzua.

Harpidedunak egiaztatu beharko du denbora zigilatzeke agintaritzak behar bezala sinatu duela denbora-zigiluko tokena, baita denbora-zigiluko tokena sinatzeko erabilitako gako pribatua ez dela ezeztatu.

#### **10.6.13. Denbora-zigiluak egiaztatzen dituzten hirugarren aldean betebeharrak**

Denbora zigilatzeke token bat jasotzen denean, hirugarren aldeak egiaztatu beharko du behar bezala sinatuta dagoela eta denbora-zigilua sinatzeko erabilitako gako pribatua ez dela ezeztatu.

Denbora-zigilua sortzeko erabilitako ziurtagiriaren balio-aldian, dagokion CRLan bertan egiaztatu ahal izango da sinadura-gakoaren baliozkotasuna.

Egiaztapena ziurtagiriaren balio-aldiaren ondoren egiten bada, hirugarren aldeak egiaztatu beharko du erabilitako hash funtzioa, algoritmoak eta gako kriptografikoen luzera oraindik ere segurutzat jo daitezkeen.

#### **10.6.14. Argitalpen Zerbitzuaren betebeharrak**

Ez da aplikagarria, Argitalpen Zerbitzua ez baita entitate independentea.

### **10.7 Erantzukizunak**

#### **10.7.1. Ziurtapen-agintaritzaren erantzukizunak**

IZENPEk arduragabekeriarengatik edo behar adinako ardurarik izan ez delako erantzungo du, Ziurtapen Praktiken Deklarazio honetan deskribatutako zerbitzuetan, baita sinadura elektronikoari buruzko legerian ezartzen diren betebeharrak betetzen ez direnean. Honako kasu hauetan izan ezik:

- IZENPE ez da ziurtagirietako informazioek eragindako kalteen erantzule izango, betiere, haien edukiak Ziurtapen Praktiken Deklarazioa betetzen badu.
- IZENPE ez da ziurtagiriaren eraginkortasuna agortzearen erantzule izango, betiere, Ziurtapen Praktiken Deklarazioan aurreikusitako argitalpen-betebeharrak betetzen baditu.
- IZENPE ez da sor daitezkeen kalte zuzen edo zeharkako, berezi, intzidentziazko eta emergenteen erantzule izango, ezta eskuratu gabeko irabazien, datu-galeren eta zigor-kalteen erantzule ere –aurreikusteko modukoak izan edo ez–, baldin eta horiek ziurtagiriaren, sinadura digitalen edo Ziurtapen Praktiken Deklarazioan eskaintzen edo aurreikusten den bestelako edozein transakzio edo zerbitzuren erabilera, entrega, baimen, funtzionamendu edo funtzionamendu ezarekin lotuta badaude eta behar ez bezalako erabilerak eragin baditu.



- IZENPE ez da ziurtagirian ageri diren datuen zehaztapen-ezagatik harpidedunari edo fede oneko hirugarren pertsoneri eragindako kalte eta galeren erantzule izango, baldin eta datu horiek dokumentu publiko baten bidez (notaritzakoa, judiziala edo administratiboa) ziurtatu badira, Erregistro Entitateak eman duen dokumentu bidez denean izan ezik.
- IZENPE ez da ziurtagiriaz fidatzen diren harpidedunek edo hirugarren pertsonen dituzten betebeharrak ez betetzeagatik harpidedunari edo fede oneko hirugarren pertsoneri eragindako kalteen erantzule izango.

IZENPE erantzule izango da, dena den, ziurtagirien indarraldiari buruzko edota ziurtagirien indarraldia iraungitzeari edo etetei buruzko kontsulta-zerbitzuan ez sartzeak edo berandu sartzeak kalterik edo hondamenik eragiten badio inori bere lanean, betiere Sinadura Elektronikoari buruzko Legearen 22. artikulua agintzen duenez.

Era berean, ziurtagiri-zerbitzuak egiteko beharrezko funtzioak hirugarren batzuen esku uzten dituztenean, bere gain hartuko du pertsona horien jardunaren ondorioz hirugarren pertsonen aurrean sor daitekeen edozein erantzukizun. Ildo horretan, 3.500.000 euroko zenbatekoa duen erantzukizun zibileko aseguruia eratu da, ziurtagirien erabilerak eragin ditzakeen kalteen eta galeren erantzukizun-arriskuari aurre egiteko.

### **10.7.2. Denbora zigilatze agintaritzaren erantzukizuna**

IZENPEk bere TSA politikaren eta bere ZPDren arabera jarduten du, baita IZENPEren eta denbora zigilatze zerbitzuaren erabilzaileen arteko bestelako akordio lotesle baten baldintzen arabera ere. IZENPEk ahalegin berezia egiten du bere zerbitzuetan prestasun handia eskaintzeko, baina ez du prestasunaren arloko erabateko bermerik eskaintzen, ezta denbora-zigiluetan doitasuna ere. IZENPE ez da inola ere onura-galeraren, zeharkako edo ondoriozko kalteen edo datu-galeraren erantzule izango, betiere indarrean dagoen legeriak hala ahalbidetzen duen heinean. IZENPE ez da harpidedunak edo hirugarren aldeek egindako arau-hausteen ondoriozko kalteen erantzule izango, aplikatzekoak diren baldintzetan. IZENPE ez da inola ere ezinbesteko gorabeheren ondoriozko kalteen erantzule izango, hala nola hondamendi naturalen, elektrizitatea edo telekomunikazioak erortzearen, suteen, kanpo-eraso ez aurreikusgarrien –birusen edo hacker-en erasoen–, gobernu ekintzen, edo greben ondoriozko kalteen erantzule. Edonola ere, IZENPEk gorabehera horien ondorioak arintzeko zentzuzko neurri guztiak hartuko ditu. IZENPEk ez ditu estaliko ezinbesteko gorabehera batek eragindako atzerapenaren ondoriozko kalteak.

### **10.7.3. Erregistro-agintaritzaren erantzukizunak**

IZENPE ez den eta erregistro-entitate gisara aritzen den erakunde oro bere gain hartutako eginkizunek eragiten dituzten kalteen erantzule izango da IZENPEren aurrean, dagokion legetresnak finkatzen duenaren arabera.

Identifikazio-funtzioak ziurtagirien harpidedun diren Administrazio Publikoek egiten dituztenean, Administrazio Publikoen ondare-erantzukizuna izango da aplikagarria, Administrazio Publikoen Erregimen Juridikoko Legeak eta Administrazio Prozedura Erkideak agintzen dutenez.



#### 10.7.4. Harpidedunen betebeharrak

Bere gako pribatuarekin sortutako sinadura digital baten bidez kautotutako komunikazio elektronikoz guztien erantzule izango da harpideduna, baldin eta IZENPERen egiaztapenez zerbitzuek ziurtagiria baliozkoa dela egiaztatzen badute.

Ziurtagiria galdu egin dela edo lapurtu egin dutela jakinarazten ez den bitartean –Ziurtapen Praktiken Deklarazio honetan agintzen duen legez–, harpidedunari dagokio ziurtagiriak baimenik gabe eta/edo era desegokian erabiltzearen erantzukizuna.

Ziurtagiriak onartzearekin batera, erantzukizun hau hartzen du bere gain harpidedunak: kalte guztietatik salbu uztekoa eta, hala badagokio, kalte-ordainak ordaintzekoa IZENPERi, erregistro-entitateei, eta entitate erabiltzaileei kalteak, galerak, zorrak, gastu prozesalak edo zeinahi bestelakoak eragiten dituzten ekintzengatik edo ez-egiteengatik, barne direla IZENPERi, erregistro-entitateei, edo entitate erabiltzaileei ziurtagiriak erabiltzeagatik edo argitaratzeagatik dagozkien ordainsariak. Honako arrazoi hauek eragin dezakete aipatu erantzukizuna:

- ziurtapen-entitatearekin lotzen duen tresna juridikoaren aginduak ez betetzeak;
- baimendu gabeko jendearekiko komunikazio elektronikoz ziurtagiri digitalak erabiltzeak;
- harpidedunak datuak faltsutzeak edo akats faktikoak egiteak;
- zabarkeriagatik edo IZENPE entitate publiko erabiltzaileak edo harpidedunaren ziurtagirian konfiantza eduki dezaketen hirugarrenak engainatzeko asmoz ziurtagirietan funtsezko datuak ez jartzeak;
- gako pribatuak gordetzeko eta horiek ez galtzeko, inork ez jakiteko, ez aldatzeko edo baimenik gabe ez erabiltzeko agindua ez betetzeak.

IZENPE ez da ziurtagiriez fidatzen diren harpidedunei edo fede oneko hirugarren pertsonen harpidedunari dagozkion honako betekizun hauek ez betetzeak eragindako kalteen erantzule izango:

- IZENPERi edo erregistro-entitateari informazio egiazkoa, osoa eta zehatza ematea ziurtagirian jarri beharreko edo hura jaulki, ezeztatu edo eteteko behar diren datuei buruz, baldin eta zerbitzu-egileak ezin izan badu datuen zehaztasun-eza antzeman.
- Ahalik eta azkarren jakinaraztea IZENPERi edo erregistro-entitateari ziurtagirian dauden zirkunstantzien aldaketa ororen berri.
- Arretaz gordetzea sinadura sortzeko datuak, horien konfidentzialtasuna bermatzeko eta horietara inor ez sartzeko edo inork ez datuak ezagutarazteko.
- Ziurtagiria eteteko edo ezeztatze eskatzea zalantzarik egonez gero sinadura sortzeko datuen konfidentzialtasunaz.
- Sinadura sortzeko datuak ez erabiltzea ziurtagiriaren balio-epea agortu edo zerbitzu-egileak balio gabetzearen berri eman ondoren.
- Ziurtagirian jasotzen diren erabilpen-mugak aintzat hartzea, eta ziurtapen-zerbitzuen sinatzaileari jakinarazitako eta finkatutako baldintzen arabera erabiltzea.



### **10.7.5. Ziurtagirietan konfiantza duten hirugarrenen erantzukizunak**

Ziurtagiri baliogabeaz edo egiaztatu gabeko sinadura digitalaz fidatzen den hirugarrenak bere gain hartzen ditu horri loturiko arrisku guztiak eta ez dauka inongo erantzukizunik eskatzerik IZENPEri, erregistro-entitateei, entitate erabiltzaileei edo harpidedunei ziurtagiri eta sinadura horietaz fidatzeak eragindako gorabeherengatik.

IZENPEk ez du erantzukizunik izango harpidedunari edo fede oneko hirugarrenei eragindako kalteengatik, baldin eta elektronikoki sinatutako dokumentuen hartzaileak ez badu betetzen honako arreta-betekizun hauetakoren bat:

- Egiaztatzea eta kontuan hartzea ziurtagiria erabiltzeko eta harekin egin daitezkeen transakzioen banakako zenbatekoari buruzko murriztapenak.
- Ziurtagiriaren baliozkotasuna egiaztatzea.

## **10.8 Kalte-ordainak**

IZENPEk kalte-gabetasun klausulak ezartzen ditu harpidedunarekin edo egiaztatzailearekin lotzen duten tresna juridikoetan, haiek beren betebeharrak edo aplikagarri den legeria urratzen dituzten kasuetarako.

## **10.9 Baliozkotze-aldia**

### **10.9.1. Epea**

ZPD argitaratzen den unean sartzen da indarrean.

### **10.9.2. Amaiera**

Gaur egungo ZPDa dokumentuaren beste bertsio bat argitaratzen den unean indargabetuko da.

Bertsio berriak oso-osorik ordeztuko du aurreko dokumentua.

### **10.9.3. Amaieraren ondorioak**

Aurreko ZPD baten mende jaulki diren eta indarrean dauden ziurtagirietarako, bertsio berria nagusituko zaio aurreko bertsioari, honen aurkakoa ez den guztian.

## **10.10 Banako jakinarazpenak eta komunikazioa parte-hartzaileekin**

IZENPEk, harpidedunarekiko tresna juridiko loteslean, jakinarazpenetarako bitartekoak eta epeak ezarriko ditu.

Oro har, IZENPEren web-orria, [www.izenpe.com](http://www.izenpe.com), erabiliko da edozein jakinarazpen eta komunikazio egiteko.



## 10.11 Zuzenketak

### 10.11.1. Aldaketetarako prozedura

Dokumentu honetan egiten diren aldaketak IZENPEren Administrazio Kontseiluak onetsiko ditu. Aldaketa horiek Ziurtapen Praktiken Deklarazioaren dokumentuan jasoko dira. IZENPEk bermatzen ditu dokumentu horren mantentze-lanak.

Ziurtapen Praktiken Deklarazioaren bertsio eguneratuak eta egindako aldaketak gordailuan kontsulta daitezke, helbide honetan: <http://www.izenpe.com>.

IZENPE Ziurtapen Praktiken Deklarazioa alda dezake, berak bakarrik, baldin eta prozedura honi jarraitzen badio:

- Aldaketa teknikoki, legalki eta komertzialki justifikatuko da eta IZENPEren zuzendaritzak abala eman beharko du.
- Zehaztapenen bertsio berriaren alde tekniko eta legal guztiak hartuko dira kontuan.
- Aldaketa-kontrola ezarriko da, ondoriozko zehaztapenek bete nahi ziren baldintzak eta aldaketa eragin zutenak betetzen dituztela bermatzeko.
- Zehaztapenak aldatzeak erabiltzailearengan dituen eraginak ezarriko dira, eta aldaketa horiek hari jakinarazteko beharra aztertuko da.

### 10.11.2. Jakinarazteko aldia eta mekanismoa

IZENPEren Segurtasun Batzordeak urtero berraztertuko du ZPDa, eta bertan aldaketa bat egin behar den guztietan. Berrazterketa hori batera egingo dute dokumentua lantzeaz eta mantentzeaz arduratzen diren eta zeregin horretan parte hartzen duten arloek.

IZENPEk aldaketak egin ahal izango ditu dokumentu horretan, aurrez erabiltzaileei horien berri eman beharrik gabe, esate baterako:

- Akats tipografikoak zuzentzea dokumentuan
- Harremanetako informazioa aldatzea.

Beste aldaketa batzuk berriz erabiltzaileei jakinarazi beharko zaizkie, esate baterako:

- Aldaketak zehaztapenetan edo zerbitzu-baldintzetan.
- URLak aldatzea

### 10.11.3. OIDA zer zirkunstantzietan aldatu behar den

Dokumentu honetan deskribatutako prozeduretakoren bat aldatzen den zirkunstantzietan aldatu beharko da OIDA.

## 10.12 Erreklamazioak eta auzien ebazpena

IZENPEk kontsumoko artekaritza-sistemaren kontrolpean dihardu, aplikagarri zaion legeriak aurreikusten duenaren arabera. Hala, eskatzaileen edo harpidedunen kexuak edo erreklamazioak artatu eta ebatziko ditu, eta hartzen duen erabakia loteslea eta betearazlea izango da alde bientzat, herritarren ziurtagiriei dagokienez betiere.



Xede horretarako, eskatzaileak edo harpidedunak sistema hori onartzen duela joko da dagokion Kontsumoko Artekaritza Batzordean artekaritza-eskaera formalizatzen duen une beretik.

Kontsumoko artekaritza-sistematik at dauden herritarraren ziurtagirien esparruan eskatzaileengandik edo harpidedunengandik sor daitekeen beste edozein auzi dagokion jurisdikzioaren esku geratuko da.

### 10.13 Aplikatzeko den araudia

Ziurtapen Praktiken Deklarazio hau gauzatzeari, egiteari, interpretatzeari eta baliozkotasunari dagozkien alor guztietan aplikatu behar da sinadura elektronikoari buruzko Espainiako legeria.

Honako hau da dokumentu honi eta ondoriozko eragiketei aplika dakiekeen araudia:

- 1999/93/EE zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 1999ko abenduaren 13koa, sinadura elektronikoari buruzko erkidegoko esparrua ezartzen duena.
- 59/2003 Legea, abenduaren 19koa, sinadura elektronikoari buruzkoa.
- 11/2007 Legea, ekainaren 22koa, Zerbitzu Publikoetarako Hiritarren Sarrera Elektronikoari buruzkoa.
- Abenduaren 13ko 15/1999 Lege Organikoa, datu pertsonalak babesteari buruzkoa.
- 1720/2007 Errege Dekretua, abenduaren 21ekoa, datu pertsonalak babesteari buruzko abenduaren 13ko 15/1999 Lege Organikoa garatzeko Araudia onartzen duena.
- Identifikazio elektronikoari eta barne-merkatuko transakzio elektronikoetarako konfiantzako zerbitzuei buruzko 910/2104 Europako araudia (eIDAS)

### 10.14 Aplikatzekoa den araudia betetzea

Jurisdikzio eskuduna une bakoitzean legeria prozesal espainiarrak agintzen duena izango da.

Edonola ere, IZENPEk jakinarazi du 9.13. atalean adierazten diren araudiak betetzen dituela.

### 10.15 Askotariko estipulazioak

Berez da baliozkoa Ziurtapen Praktiken Deklarazio honetako klausula bakoitza eta ez ditu gainerakoak baliogabetzen. Baliorik gabeko edo osatu gabeko klausula baliokidea den beste batekin ordeztuko da.

8. eta 9. sailetan biltzen diren arauak indarrean egongo dira Ziurtapen Praktiken Deklarazio honen balio-epea amaitu ondoren ere bai.

IZENPEren eskubideei eta betebeharrei zuzenean eragiten dien eta gainerako aldeei eragiten ez dien Ziurtapen Praktiken Deklarazio honetako agindu bakar bat ere ez da zuzendu, ukatu, gehitu, aldatu edo ezabatu behar, IZENPEren idatziko eta kautotutako dokumentu bidez ez bada. Aldaketa hori ez da, inondik ere, berritze iraungitzailea, aldatzaile hutsa baizik, eta ez die eragiten gainerako aldeen bestelako eskubideei eta betebeharrei.



IZENPEri zuzentzen zaizkion komunikazio idatziak helbide honetara bidali beharko dira:

IZENPE, SA

Tomas Zumarraga Dohatsuaren kalea, 71-1.

01008 Vitoria-Gasteiz