



ZIURTAPEN PRAKTIKEN DEKLARAZIOA

Erreferentzia: IZENPE-ZPD
Bertsio zkia.: v 4.9.1
Data: 2011 uztailaren 8a.

© IZENPE 2011

Dokumentu hau IZENPErena da. Osotasunean soilik erreproduzi daiteke.

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

www.izenpe.com
info@izenpe.com
Tel.: 945 017 490



AURKIBIDEA

1 4

Sarrera 4

1.1	Aurkezpena	5
1.2	Identifikazioa	7
1.3	Komunitatea eta aplikagarritasuna	7
1.4	Harremanetarako xehetasunak	24

2 Xedapen orokorrak 26

2.1	Betebeharrak	26
2.2	Erantzukizun zibila	32
2.3	Finantza-ahalmena	35
2.4	Interpretatzea eta gauzatzea	36
2.5	Tarifak	37
2.6	IZENPEren Argitalpen Zerbitzua	38
2.7	Onespen-ikuskapena	39
2.8	Konfidentzialtasuna	40
2.9	Jabetza intelektualeko eskubideak	43

3 Identifikazioa eta kautotzea 44

3.1	Hasierako erregistroa	44
-----	-----------------------	----

4 Eskakizun operatiboak 47

4.1	Ziurtagiria eskatzea	47
4.2	Ziurtagiria jaulkitzea	48
4.3	Ziurtagiria onartzea	49
4.4	Ziurtagiriak eten eta ezeztatzea	49



4.5	Segurtasun-ikuskapeneko prozedurak	54
4.6	Informazioak artxibatzea	55
4.7	Gakoak berritzea	56
4.8	Gakoak arriskuan egotea eta hondamenditik suspertzea	56
4.9	Zerbitzua amaitzea	59
5	Segurtasun fisikoaren, prozeduren eta langileen kontrolak	60
5.1	Segurtasun fisikoaren kontrolak	60
5.2	Prozeduren kontrolak	62
5.3	Langileen kontrolak	63
6	Segurtasun teknikoaren kontrolak	65
6.1	Gako-parea sortu eta instalatzea	65
6.2	Gako pribatua babestea	67
6.3	Gako-parea kudeatzearen beste alderdi batzuk	69
6.4	Aktibatzeako datuak	69
6.5	Segurtasun informatikoaren kontrolak	70
6.6	Bizitza-zikloaren kontrol teknikoak	71
6.7	Sareko segurtasunaren kontrolak	72
6.8	Modulu kriptografikoen ingeniartzako kontrolak	72
7	Ziurtagirien profilak eta ezeztatutako ziurtagirien zerrendaren profilak	73
7.1	Ziurtagiriaren profila	73
7.2	Ezeztatutako ziurtagirien zerrendaren profila	79
8	Zehaztapenaren administrazioa	80
8.1	Aldaketa-prozedura	80
8.2	Argitalpen- eta jakinarazte-politika	80
8.3	Onespen-prozedura	81



9	Datu pertsonalak babestea	82
9.1	Sarrera	82
9.2	Aplikazio-esparrua	82
9.3	Datu pertsonalak babesteko segurtasun-antolamendua.	83
9.4	Datu pertsonalak dituzten fitxategien egitura	85
9.5	Segurtasuneko arauak eta prozedurak	86
10	Definizioak	89
11	Akronimoak	95
1		

Sarrera

Euskal botere publikoek informazioaren gizartea sustatu nahi izan dute, eta helburua herritarren jardura 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 informatikoen (aurrerantzean IZENPE deituko diogu).

Euskal administrazio publikoetako sozietate informatikoen 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 elektronikoa 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 atzeraezintasuneko 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 estandarraren arabera.

IZENPEk ETSI-Telekomunikazio Estandarren Europako Institutuaren ziurtapena du, TS zehaztapen teknikoen barnean, betiere onartutako ziurtapenak jaulkitzen dituzten ziurtapen-entitateek bete beharreko baldintzen politikari buruzko 101 456 arau teknikoari jarraiki. TS 101 456 arauan ezartzen diren TS zehaztapen teknikoek ziurtapenen kudeaketa eta praktikari buruzko oinarritzko baldintzak zehazten dituzte, eta baldintza horiek bete behar dituzte ziurtagiriak jaulkitzen dituzten entitateek, baldin eta jaulkitzen dituzten ziurtagiriak Europako Parlamentuko 1999/93/EE zuzentarauaren lege-esparruaren arabera badira –zuzentaru hori Espainiako erregimen juridikoan sinadura elektronikoari buruzko 59/2003 legearen bitartez sartu zen-.

Balidazio hedatuko SSL ziurtagiriak jaulkitzeko eta kudeatzeko jarraibideen arabera Webtrust for EVK egiaztatuta dago IZENPE (CA/Browser Forum guidelines for the issuance and management of extended validation certificates). CA/Browser Forum-ek definitutako jarraibide horiek ziurtapen-agintaritzek SSL-EV ziurtagiriak jaulkitzeko aplikatu beharreko gutxienezko eskakizunak zehazten dituzte, bisitatutako zerbitzuen identitatea identifikatzeko eta kontrolatzeko fidagarritasuna emateko helburuarekin.

1.1 Aurkezpena

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

- IZENPE Ziurtapen Digitalaren Zerbitzuak ziurtagiri onartuak nahiz lege onartuta ez dauden ziurtagiri arruntak jaulkitzen ditu, abenduaren 19ko sinadura elektronikoari buruzko 59/2003 Legeari jarraiki.



- Denbora Zigiluen Zerbitzuak entitate erabiltzaileari aukera ematen dio bermatzeko denbora-tarte jakin batean informazio jakin bat bazegoela.
- Egiztapen Aurreratuko Programak (aurrerantzean, EAP) zerbitzua erabiltzen duen entitateari aukera ematen dio IZENPEk jaulkitako ziurtagiriak erabiltzeko. Horretarako, ziurtagirien egoera begiratzan du, OCSP (Online Certificate Status Protocol) protokoloaren bidez.
- IZENPEk informatikako hainbat aplikazio ditu, baita sinadura elektronikoa erabiltzen duten aplikazioak garatzeko zehaztapen teknikoak ere. Aplikazio horiek lizentziapean eskaintzen dizkie entitate erabiltzaileei.

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

- Entitate publikoetako langileen ziurtagiria.
- Eusko Jaurlaritzaren langileen ziurtagiria.
- Administrazio Organoaren Ziurtagiria.
- Onartutako ziurtagiri korporatiboa.
- Onartu gabeko ziurtagiri korporatiboa.
- Onartutako ziurtagiri korporatibo pribatua.
- Onartu gabeko ziurtagiri korporatibo pribatua.
- Herritarraren Ziurtagiria.
- Entitate-ziurtagiria.
- Nortasun juridikorik gabeko entitatearen ziurtagiria.
- “Euskal Etxeak” Entitate Ziurtagiria.
- Osasun-identifikatzailea.
- Egoitza elektronikoko ziurtagiria.
- Zigilu elektronikoko ziurtagiria.
- Egoitza elektronikoko ziurtagiria.
- Balidazio zabaldua duen egoitza elektronikoko ziurtagiria.
- Gailu informatikoko ziurtagiria: SSL, SSL EV eta aplikazioa.
- Kode-sinaduraren ziurtagiria.

IZENPEk jaulkitako ziurtagiri 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 etorri jaulkitako ziurtagiri mota bakoitza berezita 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 Komunitatea eta aplikagarritasuna

1.3.3 Komunitatea

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

- Praktikak Onesteko Batzordeak.
- Ziurtapen-zerbitzuen egileak.
- Ziurtapen-agintaritzek.
- Erregistro-entitateak.
- Ziurtagirien erabiltzaileak.

1.3.3.1 Praktikak Onesteko Batzordeak

Praktikak Onesteko Batzordea IZENPEko Administrazio Kontseiluak osatzen du. Organo horri dagokio Ziurtapen Praktiken Deklarazio hau onesteko ardura, baita dokumentu honen 8. atalean deskribatutakoarekin bat etorri deklarazioan egin litezkeen aldaketak onesteko ardura ere.

1.3.3.2 Ziurtapen-entitatea

IZENPE (Mediterraneoaren hiribidea 14, Gasteiz, IFZ: 01337260) da ziurtapen-entitatea. Berak jaulkitzen ditu ziurtapen-praktiken deklarazio hau aplikagarri duten ziurtagiri publikoak.

1.3.3.3 Ziurtapen-agintaritzek.

IZENPEk honako ziurtapen-agintaritza hauek ditu:

1. Oinarrizko ziurtapen-agintaritza
2. Mendeko ziurtapen-agintaritza

1.3.3.3.1 Oinarrizko ziurtapen-agintaritza



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

IZENPEk honako oinarritzko ziurtapen-agintaritza hauek ditu:

Oinarritzko CA 2003

Subject	E = Info@izenpe.com CN = Izenpe.com 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 31/1/2003 until 31/1/2018
SHA1 thumbprint	4a 3f 8d 6b dc 0e 1e cf cd 72 e3 77 de f2 d7 ff 92 c1 9b c7

Oinarritzko 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

1.3.3.3.2 Mendeko ziurtagen-agintaritza

Azken entitateei ziurtagiri elektronikoak jaulkitzen dizkieten ziurtagen-agintaritzak dira.

1. Herritar eta Erakundeen onartutako CAk
2. Herritar eta Erakundeen onartu gabeko CAk
3. Herri Administrazioen onartu gabeko CAk
4. Herri Administrazioen onartutako CAk
5. Eusko Jaurlaritzako langileen CA
6. CA SSL EV
7. CA teknikoa



2003ko mendeko ziurtapen-agintaritzak.

CA horiek IZENPEren oinarritzko CA berrira migratu dira.

Herritar eta Erakundeen onartutako CAk

Subject	E = Info@izenpe.com 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 = Info@izenpe.com 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

Herritar eta Erakundeen onartu gabeko CAk

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
Validity dates	from 30/01/2008 until 13/12/2037
SHA1 thumbprint	06 fb ac 35 ae 18 fc bf 22 29 78 8d d1 2d ac 89 8e 74 52 ae
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

Herri Administrazioen onartutako CAk

Subject	E = Info@izenpe.com 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 = Info@izenpe.com 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 Erakundeen onartutako CAk

Subject	E = Info@izenpe.com CN = Herritar eta Erakundeen 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 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
SHA1thumbprint	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

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 S
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
SHA1thumbprint	87 56 60 a3 5c b1 03 d7 e0 bb 00 44 24 f1 6d bf bf 21 e0 b4

Herri Administrazioen onartutako CAk



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
SHA1thumbprint	93 a1 44 6b 61 99 4b 5b 0e 99 d0 5b 14 cd bb 32 2e 6c 17 64

Herri Administrazioen onartu gabeko CAk

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
SHA1thumbprint	f7 9c da 11 e7 91 74 19 a0 41 8d b8 4b a7 43 c5 31 3a d7 f0

Eusko Jaurlaritzako langileen CA

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
SHA1thumbprint	25 e9 d1 6d f8 d6 4a 60 73 40 8c be 24 8e 52 9c 23 9e 32 92

CA SSL EV



Subject	CN = CA de Certificados SSL EV 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, 20 de noviembre de 2008 11:37:27 until lunes, 19 de noviembre de 2018 12:47:28
SHA1 thumbprint	d2 ad f8 38 5f e3 01 60 fc 51 69 ec 81 f8 cc 33 ab 88 ca 23

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 10:27:24 until martes, 20 de octubre de 2020 10:27:24
SHA1thumbprint	67 16 29 9c c4 c0 ca 25 52 ee 88 01 9a fc ee 49 b2 a1 63 34



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
SHA1thumbprint	6c 48 4d 0f 4d b2 95 ec 67 eb b3 e0 5e 3d c2 14 49 2a 9a b8

1.3.3.4 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 hitzarmena/kontratua sinatzen duen entitate erabiltzailea.

1.3.3.5 Ziurtagirien erabiltzaileak.

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

Honako entitate hauek izango dira ziurtapen-sistemaren azken entitateak:

1. Ziurtagirien eskatzaileak
2. Ziurtagiriaren sinatzailea
3. Ziurtagirien harpidedunak
4. Gakoen edukitzaileak
5. Ziurtagirietan konfiantza duten hirugarrenak

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

1.3.3.5.1 Ziurtagirien eskatzaileak

Ziurtagiri oro pertsona batek eskatu behar du, bere izenean edo erakunderen baten izenean.

1.3.3.5.2 Sinatzailea

Ziurtagirian identifikatzen den pertsona fisikoa edo juridikoa izango da sinatzailea.

1.3.3.5.3 Ziurtagirien harpidedunak

Harpidedunak ziurtagirian identifikatutako pertsona fisikoak edo juridikoak dira.

1.3.3.5.4 Gakoen edukitzaileak

Gakoen edukitzaileak sinadura digitaleko gakoak dituzten eta horiek zaintzeaz arduratzen diren pertsona fisikoak izango dira.

1.3.3.5.5 Ziurtagirietan konfiantza duten hirugarrenak

Ziurtapen Praktiken Deklarazio honen barruan, IZENPEk jaulkitako ziurtagiriak jasotzen dituzten pertsona fisiko edo juridikoak dira ziurtagirietan konfiantza duten hirugarrenak; beraz,



ziurtagiri horietan konfiantza izatea erabakitzen dutenean, ziurtapen-praktiken deklarazio honetan jasotakoa aplikatuko zaie.

Hirugarrenek ziurtagirietan jartzen duten konfiantza, beraz, harpidedunekiko harremanetan ziurtagiri horietaz egiten duten erabilera objektiboaren arabera izaten da.

Aipatutako erabilera egiten denean, honakoa 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 mota guztiak, eta fede onez eta leialtasunez jardun behar dute. Halaber, ez dute iruzur- edo zabarkeria-jarrerarik izan behar, ez dute ziurtagiriaren kategoriari dagokion konfiantza-esparruaren barruan bidalitako mezuei uko egitea helburu duen jarrerarik izan behar.

1.3.4 Zeri aplikatu

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

1.3.4.1 Ziurtagirien erabilera baimenduak

1.3.4.1.1 Ziurtagiri onartua

Ziurtagiri Onartuen erabilerari dagokionez:

- a. Sinadura elektronikoko ziurtagiri onartuek harpidedunaren identitatea eta sinaduraren gako pribatuaren edukizailearen identitatea bermatzen dituzte. Sinadura sortzeko gailu seguruekin erabiltzen direnean, ezin hobeak dira onartutako sinadura elektronikoa euskarria emateko, hau da, ziurtagiri onartuan oinarritzen den eta gailu seguruaren bidez sortu den sinadura elektronikoa aurreratuari euskarria emateko. Hori dela eta, sinadura elektronikoa buruzko abenduaren 19ko 59/2003 Legearen 3.4. artikularekin bat etorritik, lege-ondorioetarako eskuz idatzitako sinaduraren baliokidetzat jotzen da, beste eskakizunik bete behar izan gabe.
- b. Sinadura elektronikoko onartutako 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. Sinadura digital horrek sinadura-ziurtagiriaren harpidedunaren identitatea bermatzen du.

- c. Egoitza eta Egoitza EV ziurtagiriak webguneak modu fidagarrian identifikatzeko jaulkitzen dira.
- d. Egoitza eta ziurtagiri elektronikoko ziurtagiriak administrazio-egoitza eta dokumentuen zigilatze elektronikoa identifikatzeko jaulkitzen dira, betiere Zerbitzu Publikoetarako Hiritarren Sarrera Elektronikoari buruzko 11/2007 Legean aurreikusitakoaren arabera.

Onartutako ziurtagiriek Telekomunikazioko Arauen Europako Institutuaren TS 101 456 arau teknikoa betetzen dute.

1.3.4.1.2 Onartu gabeko ziurtagiria

Onartu gabeko ziurtagiriek harpidedunaren eta, hala badagokio, sinadura-gakoaren edukizaillearen 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 balio dute, baita kautotzeko hainbat modutarako ere, sinadura-gako pribatua modu fidagarrian babesten duten aplikazio informatikoekin batera erabiliz gero.

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

1.3.4.1.3 Gailu informatikoko ziurtagiria

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

1.3.4.1.4 Kode-sinaduraren ziurtagiria.

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

1.3.4.2 Ziurtagirien erabilera-esparrua

Erabilera-esparruari dagokionez bi kasu bereizten dira:



- a. 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.

- b. IZENPEk jaulkitako eta entitate erabiltzaileek eskatutako ziurtagiriak administrazio-organoaren 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.

1.3.4.3 Ziurtagiriak erabiltzeko mugak

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

Era berean, aplikagarri den legearekin bat etorritz bakarrik erabili behar dira ziurtagiriak, bereziki aldiari inportazio- eta esportazio-murrizketak kontuan hartuz.

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

Ziurtagiriak ez dira diseinatu egoera arriskutsuetan kontrol-ekipo gisara edo huts-egitean 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.

1.4 Harremanetarako xehetasunak

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	info@izenpe.com
Telefonoa	945 06 77 23

2 Xedapen orokorrak

2.1 Betebeharrak

2.1.1 Ziurtapen-entitatearen betebeharrak

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

2.1.2 Zerbitzua egiteko betebeharrak

IZENPEk 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 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 gordetzea eta 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.

2.1.2.1 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 iraungi edo bertan behera

utziko 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 indargabetzen den 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 teknikoa 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 onartutako ziurtagiriak biltegitzeko. 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.

2.1.2.2 Identifikazio-betebeharrak

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

2.1.2.3 Erabiltzaileei eman beharreko informazioa: betebeharrak

Harpidedunari ziurtagiria jaulki eta eman aurretik, honako honen berri ematen dio hari IZENPEk: ziurtagiria erabiltzeko bete behar diren baldintzen berri, prezioaren berri –finkatuta badago–, erabilera-mugen berri 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.

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 jardura 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.

2.1.2.4 Egiaptapen-programak: betebeharrak

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

2.1.2.5 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 gakoaren 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 eragiketarak baliozko ziurtagiriak 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.
- Aplikagarriak 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 aitortu duten.
- IZENPEren ondare-erantzukizuna bermatzeko era.

2.1.3 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 ematea ziurtagiriak azkar eta modu fidagarrian ezeztatzeako eskaeren berri.
- IZENPEri artxiboak erabiltzen uztea, baita jardueretarako erabiltzen diren prozeduren eta horretarako behar den informazioaren mantentze-lanen ikuskapena egiten ere.
- IZENPEri ematea ziurtagiriak jaulki, berritu edo berraktibatzeako eskaeren berri, baita hark jaulkitzen dituen ziurtagiriei buruzko beste zeinahi alderdiren berri ere.
- Garaiz begiratzea ziurtagirien iraunaldian eragina izan dezaketen ezeztatzeako zergatiak.
- IZENPEri eskatzea behar den denboraz etetea ziurtagiriaren balioa, hori ezeztatzea eragin duen zergatia egiaztatzen duen dokumentazioa begiratzeko.
- Ziurtagiriak jaulki, berritu, ezeztatu eta berraktibatzeako IZENPEk ezarritako prozedurak eta gai horretaz indarrean dagoen legeriak agindutakoa betetzea.

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

2.1.4 Ziurtagiri-eskatzailearen betebeharrak

Honako betebeharrak dituzte ziurtagiri-eskatzaileak:

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

2.1.5 Ziurtagiri-harpidedunaren betebeharrak

- a. Informazio osoa eta egokia ematea IZENPEri, Ziurtagiri Praktiken Deklarazioko eskakizunen arabera, erregistro-prozedurari dagokionez batez ere.
- b. Ziurtagirietan jarri beharreko informazioaren egiazkotasuna, osotasuna eta gaurkotasuna bermatzea.
- c. Ziurtagiriak erabiltzeko baldintzak jakitea eta onartzea, baita haiei egiten zaizkien aldaketak ere.
- d. Ziurtagiriren bat jaulki eta eman aurretik, horretarako onespena ematea.
- e. Ziurtagirien euskarriak ongi erabili eta gordeko direla bermatzea.

- f. Ziurtagiria egokiro erabiltzea, eta, zehazki, ziurtagirien erabilera-mugak aintzat hartzea.
- g. Arretaz zaintzea gako pribatua, baimendu gabeko erabilerak saihestearren, Ziurtapen Praktiken Deklarazioko 6.1, 6.2 eta 6.4 sailek agintzen dutenaren arabera.
- h. IZENPERi eta harpidedunaren ustez ziurtagirian konfiantza duen edonori honakoa jakinaraztea, justifikatzerik ez dagoen atzerapenik gabe:
 - 1. Gako pribatua galdu izana, 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.
- i. Gako pribatua erabiltzeari uztea ziurtagiriaren balio-epea amaitu ondoren.
- j. Gakoen edukitzaileei jakinaraztea zein betebeharrak dagozkien.
- k. Ziurtagiri-zerbitzuen ezartze teknika ez kontrolatzea, manipulatzeko edo atzeranzko ingeniartzeko ekintzarik ez egitea, aurrez Ziurtapen Entitatearen idatzizko baimenik eduki gabe.
- l. Ziurtagiri-zerbitzuen segurtasuna arriskuan nahita ez jartzea.
- m. 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 kriptografikoa erabiltzen denean, betiere sinadura elektronikoko buruzko abenduaren 19ko 59/2003 Legearen 3.4. artikulua agintzen duenaren arabera.

2.1.6 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, Ziurtapen Praktiken Deklarazioan eta egiaztatzailearen eta IZENPERen arteko ziurtapen-zerbitzuak egiteko kontratuan aurreikusten denaren 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 ezeztatzeko arrazoia izan daitezkeenak.
- 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 elektronikoa horiek eskuz idatzitako sinaduren baliokideak direla, sinadura elektronikoari buruzko abenduaren 19ko 59/2003 Legearen 3.4. artikulua arabera.

2.1.7 Argitalpen Zerbitzuen betebeharrak

Ez da aplikagarria, Argitalpen Zerbitzua ez baita entitate independentea.

2.2 Erantzukizun zibila

2.2.1 Ziurtapen-entitatearen erantzukizun zibila

IZENPEk arduragabekeriarengatik edo behar adinako ardurarik izan ez delako erantzungo du, Ziurtapen Praktiken Deklarazio honetan deskribatutako zerbitzuetan, baita sinadura elektronikoa 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 ziurtagirien 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 ziurtagirien, 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 (ikus 2.1.2.).
- 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 kontsulta-zerbitzuan edota ziurtagirien indarraldia iraungitzeari edo eteteari buruzko kontsulta-zerbitzuan ez sartzeak edo berandu sartzeak kalterik edo hondamenik eragiten badio inori bere lanean, betiere sinadura elektronikoa buruzko abenduaren 19ko 59/2003 Legearen 22. artikulua agintzen duenez. Era berean, ziurtapen-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.

2.2.2 Erregistro-entitatearen erantzukizun zibila

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

Identifikazio-funtzioak ziurtagirien harpidedun diren Administrazio Publikoek egiten dituztenean, Administrazio Publikoen ondare-erantzukizuna izango da aplikagarria, Administrazio Publikoen Erregimen Juridikoko Legearen 139. artikulua eta hurrengoek eta Administrazio Prozedura Erkideak agintzen dutenez.

2.2.3 Ziurtagiri-harpidedunaren erantzukizun zibila

Bere gako pribatuarekin sortutako sinadura digital baten bidez kautotutako komunikazio elektronikoa guztien erantzule izango da harpideduna, baldin eta IZENPEren egiaztapen-zerbitzuek ziurtagiria baliozkoa dela egiaztatzen badute.

Ziurtagiria galdu egin dela edo lapurtu egin dutela jakinarazten ez den bitartean –2.1.4 atalak agintzen duen legez–, harpidedunari dagokio ziurtagiriak baimenik gabe eta/edo era desegokian erabiltzearen erantzukizuna.

Ziurtagiriak onartzearekin batera, honako erantzukizuna 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 zehazki 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:

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

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

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

2.2.4 Ziurtagirietan konfiantza duten hirugarrenen erantzukizun zibila

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:

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

2.2.5 IZENPEren Argitalpen Zerbitzuaren erantzukizun zibila

Ez da aplikagarria, Argitalpen Zerbitzua ez baita entitate independentea.

2.3 Finantza-ahalmena

2.3.1 Kalte-gabetasuneko klausulak

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

2.3.2 Harreman fiduziarioak

Ez da aplikagarria.

2.3.3 Prozesu administratiboak

IZENPEK, erregistro-entitateek eta entitate erabiltzaileek behar hainbat baliabide daukate dagozkien eragiketak eta jarduerak gauzatzeko. Halaber, entitate horiek badaukate behar hainbateko ahalmena harpidedunenganako eta ziurtagirien erabiltzaileenganako erantzukizun zibila bereganatzeko.

IZENPEK erantzukizun zibileko aseguruua du, ziurtagiriak sortzean izan daitezkeen hutsuneak eta/edo hutsegiteak estaltzeko. IZENPEren jarduera eskusiboak ere estaltzen ditu aseguruak.

IZENPEK eta erregistro-entitateek –esku hartzen badute– harpidedunekin eta ziurtagirien erabiltzaileekin duten harremana ez da mandatuakoa, 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.



2.4 Interpretatzea eta gauzatzea

2.4.1 Aplikatu behar den legeria

Ziurtapen Praktiken Deklarazio hau gauzatzeari, egiteari, interpretatzeari eta baliozkotzeari dagozkien alor guztietan aplikatu behar da Espainiako legeria.

2.4.2 Banatzeko, bizirauteko, osoko hitzarmeneko eta jakinarazteko klausulak

Berez da baliozkoa Ziurtapen Praktiken Deklarazio honetako klausula bakoitza, eta ez ditu gainerakoak baliogabetzen. Klausula baliogabearen edo osatu gabearen ordez beste bat jar daiteke –haren baliokidea eta baliozkoa–, alde guztiek hala adosten badute.

2.1 eta 2.2 ataletako (Betebeharrak eta Erantzukizun Zibila), 2.7 ataleko (Onespen-ikuskapena) eta 2.8 ataleko (Konfidentzialtasuna) arauak indarrean jarraituko dute Ziurtapen Praktiken Deklarazio honen balio-epea amaitu eta gero ere.

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 idatzizko 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.

Posta ziurtatuz eta hartu izana adieraziz, edo zerbitzu baliokidez, bidali behar zaizkio idatzizko komunikazioak IZENPEri, honako helbide honetara:

IZENPE, SA

Tomas Zumarraga Dohatsuaren kalea, 71-1.

01008 Vitoria-Gasteiz

Erregistro-entitateei ere aplikatu behar zaie atal hori. Jakinarazpenak, ordea, horiek harpidedunei ematen dizkieten helbideetara bidali behar dira.

2.4.3 Eskumena duen jurisdikzioaren klausula.

Espainiako legeria prozesalak agintzen duen jurisdikzioak dauka eskumena.

2.4.4 Auziak konpontzea

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 herritarren ziurtagirien esparruan, eskatzaileengandik edo harpidedunengandik sor daitekeen beste edozein auzi dagokion jurisdikzioaren esku geratuko da.

2.5 Tarifak

Indarrean dauden tarifak kobratzen dizkie IZENPEk ziurtagirien harpidedunei, Ziurtapen Praktiken Deklarazio honetan araututako ziurtapen-zerbitzuak erabiltzeagatik betiere. IZENPEk entitate erabiltzaileekin izenpetzen dituen hitzarmenen arabera izango dira tarifak.

Ziurtapen-zerbitzuak lehenagoko produktuen edo zerbitzuen barruan badaude, ziurtapen-zerbitzuen prezioa produktu edo zerbitzu horien barruan dagoela joko da –produktu edo zerbitzu horren kontratuan edo bestelako tresna arautzailean finkatutako mugak kontuan hartuta–, baldin eta ez bada finkatzen ziurtapen-zerbitzurako berariazko unitateko tarifarik (adibidez: ziurtagiria jaulkitzeagatik, ziurtagiria balio gabetzeagatik...).

2.5.1 Ziurtagiriak jaulkitzea edo berritzea: tarifak

Ziurtagiriak jaulkitzeagatik edo berritzeagatik erabiltzaileek ordaindu beharreko tarifak entitate erabiltzaileek eta IZENPEk elkarrekin adostutako ziurtapen-zerbitzuak emateko hitzarmenetan daude finkatuta.

2.5.2 Ziurtagiriak jasotzeko tarifa

Ez da aplikagarria.

2.5.3 Ziurtagiriaren egoerari buruzko informazioa jasotzeko tarifa

Ziurtagirien egoerari buruzko informazioa jasotzeagatik (OCSP, ordu eta data batetik aurrera ezeztatutako egiaztagiria argitaratzeko zerbitzua erabiltzeagatik) erabiltzaileek ordaindu beharreko tarifak entitate erabiltzaileek eta IZENPEk elkarrekin adostutako ziurtapen-zerbitzuak egiteko hitzarmenetan daude finkatuta.

2.5.4 Beste zenbait zerbitzuren tarifak

Ez da aplikagarria.



2.5.5 Itzultze-politika

Ez da aplikagarria.

2.6 IZENPEren Argitalpen Zerbitzua

2.6.1 Ziurtapen-entitatearen informazioaren argitalpena

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

Informazio hori <http://www.izenpe.com> web orrian dago eskuragarri, 24 orduetan, asteko 7 egunetan.

Zerbitzu horren bitartez, IZENPEk on-line informazioaren osotasuna bermatzen du. Dena den, dokumentu horren bertsio osoa, paperezko euskarrian, eman ahal da ikuskapenak, inspeizioak edo ziurtapen-zerbitzuen beste egile batzuekin ziurtapen gurutzatuak egin behar direnean, edo gakoan edukitzaileak edo hirugarren batek hala eskatzen dutenean.

Jaulkitako ziurtagirien erregistroa azkar eta modu seguruan kontsultatzeko aukera eskaintzen du IZENPEk. 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). 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, 4.4.10 atalak dioenaren arabera.

2.6.2 Argitalpen-maiztasuna

Onartu bezain pronto argitaratzen da Ziurtapen Praktiken Deklarazioa.

Ziurtapen Praktiken Deklarazioan egin beharreko aldaketak dokumentu honetako 8. atalak dioenaren arabera egin behar dira.

Ziurtagirien ezeztatze-egoerari buruzko informazioa dokumentu honetako 4.4.10 eta 4.4.11 atalek diotenaren arabera argitaratu behar da.



2.6.3 Sarbide-kontrola

IZENPEk bere Argitalpen Zerbitzuan 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 honakoa eskatzen die erabiltzaileei: egiaztatze-tresna juridikoren baten edo CRLren erabiltze-kontratuaren bidez eskuratzea sarbidea ziurtagirietara, ziurtagirien egoerari buruzko informazioa edo CRLetara.

IZENPEk eta, hala dagokienean, erregistro-entitateek Argitalpen Zerbitzurako sistema fidagarriak erabiltzen dituzte. Ondorioz:

- Baimendutako jendeak bakarrik erants dezake informazioa edo egin ditzake aldaketak.
- Informazioaren egiazkotasuna egiaztatzeko aukera badago.
- Harpidedunak horretarako baimena eman badu kontsulta daitezke ziurtagiriak; bestela, ez.
- Segurtasun-baldintzei eragiten dien aldaketa oro antzeman egiten da.

2.7 Onespen-ikuskapena

IZENPEren ziurtapen-zerbitzuko sistemaren segurtasun-plana betetzen dela bermatzeko, eta hari egokitzeke, egiaztatzen da segurtasun-baldintzak betetzen diren egiaztatzea –segurtasun-ikuskapena edo segurtasun-azterketa ere deitzen zaio–. Ikuskapen Plan batean dago zehaztuta jarduera hori.

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

2.7.1 Onespen-ikuskapenaren maiztasuna

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

2.7.2 Ikuskatzailearen nortasuna eta gaitasuna

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



2.7.3 Ikuskatzailearen eta ikuskatutako erakundearen arteko harremana

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

2.7.4 Ikuskatu beharreko objektuen zerrenda

Hauek dira ikuskatu beharreko elementuak:

- PKI prozesuak.
- Informazio-sistemak.
- Prozesatzeko zentroaren babes-sistema.
- Dokumentuak.

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

2.7.5 Onespenez delata hartu beharreko neurriak

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

2.7.6 Ikuskapen-txostenen tratamendua

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

Ikuskapena delata ziurtagiriren bat ezeztatu behar izanez gero, IZENPEren Argitalpen Zerbitzuan argitaratu behar da txostena, ezeztapenaren egiaztagiri gisara.

2.8 Konfidentziasuna

2.8.1 Informazio konfidentzialak

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

IZENPEk eta erregistro-entitateek ziurtagiriak jaulkitzeko, horiek mantentzeko eta sinadura elektronikoa 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-emaielen intimitatea, datu pertsonalak babesteko indarrean dagoen legeriak agintzen duen legez.

IZENPEk eta erregistro-entitateek ez dute datu pertsonalik plazaratzen eta inori uzten, salbu Ziurtapen Praktiken Deklarazio honetako dagozkien atalek aurreikusitako egoeretan eta IZENPEren eta erregistro-entitateen jarduera-amaiera kasurako dagokion atalak aurreikusitako egoeretan.

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

- Ziurtagiri-eskaerak –onartuak zein onartu gabeak–, baita ziurtagiriak jaulkitzeko eta mantentzeko eskuratutako gainerako informazio guztia ere, dagokion atalean zehaztutako informazioa izan ezik.
- IZENPEk sortutako edo biltegitutako 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 planak artxibatzea, kontrolatzea eta antzeko beste zenbait.

2.8.2 Informazio ez-konfidentzialak

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 gakoan 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–, gakoan edukitzailearen helbide elektronikoa –ziurtagiriaren harpideduna pertsona juridikoa edo administrazio-organoa bada–, edo harpidedunak esleitutako helbide elektronikoa –gailuetarako ziurtagiriak badira–.

- 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.

2.8.3 Ziurtagiriak eteteari eta ezeztatzeari buruzko informazioaren hedapena

IZENPEk Ezeztatutako Ziurtagirien Zerrendak (CRLak) jaulkitzen ditu eta, eskuragarri egonez gero, ziurtagiriak denbora errealean egiaztatzeko zerbitzuak eskaintzen ditu, Online Certificate Status Protocol-aren bidez (OCSP). 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, 4.4.10 atalak dioenaren arabera.

2.8.4 Informazioa legez argitaratzea

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

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

2.8.5 Informazioa argitaratzea, haren titularrak hala eskatuta

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

2.8.6 Informazioa argitaratzeko beste egoera batzuk

Ez da aplikagarria.



2.9 Jabetza intelektualeko eskubideak

2.9.1 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 ezeztatzeko informazio-sistemari.

2.9.2 Ziurtapen Praktikaren jabetza

IZENPE da honako Ziurtapen Praktiken Deklarazio honen jabea.

2.9.3 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 Praktikaren Deklarazioko 3. atalean zehaztutako informazioek osatzen dute aipatutako izena.

2.9.4 Gakoan eta horiei dagokien materialaren jabetza

Ziurtagirien harpidedunak dira gako-pareen jabeak.



3 Identifikazioa eta kautotzea

3.1 Hasierako erregistroa

3.1.1 Izen motak

Azken entitateko ziurtagiri guztiek X.500 izen bereizgarri bat daukate *Subject Name* eremuan.

Bestalde, *Ziurtagiri bakoitzerako berariazko dokumentazioak* IZENPEk jaulkitako ziurtagiri bakoitzari dagozkion xehetasunak aurreikusten ditu.

Common Name eremuaren balio kautotua gakoaren edukitzailearen izena da.

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

3.1.1.1 Issuer (2003ko abenduaren 19ko 59/2003 Legearen 11.2. artikuluko c) letraren baldintza)

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

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

3.1.1.2 Subject (2003ko abenduaren 19ko 59/2003 Legearen 11.2. artikuluko e) letraren baldintza)

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 IZENPEk jaulkitako ziurtagiri bakoitzaren profil zehatza.

3.1.2 Izenen esanahia

Ikusi *Ziurtagiri bakoitzerako berariazko dokumentazioan*.



3.1.3 Izen-formatuen interpretazioa

Erabaki gabe.

3.1.4 Izen-bakartasuna

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

3.1.5 Izenen gaineko auziak konpontzea

Ziurtagiri-eskatzaileek ez dute eskaeretan etorkizuneko harpidedunak hirugarrenen eskubideak urratzeko moduko izenik jarri behar.

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.

Izenen inguruko auziei dagokienez, jarraitu *Ziurtagiri bakoitzerako berariazko dokumentazioan* ezarritakoari.

3.1.6 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.

3.1.7 Gako pribatuaren jabetza-froga

Gako-parea erregistro-entitate batek sortua bada, honela frogatzen da gako pribatuaren jabetza: gailu kriptografikoa entregatzeko eta onartzeko prozedura fidagarriaren indarrez, horri dagokion ziurtagiriaren bitartez, eta barruan duen gako-pareari esker.

Gako-parea ziurtagiriaren gakoan edukitzaileak sortua bada, honela frogatzen da gako pribatuaren jabetza: ziurtagiria behar bezala erabiliz.



3.1.8 Erakunde baten nortasuna kautotzea

Erakunde baten identitatea kautotzeko baldintzak *Ziurtagiri bakoitzerako berariazko dokumentazioan* zehazten dira.

Pertsona fisiko baten nortasuna kautotzea

Pertsona fisiko baten identitatea kautotzeko baldintzak *Ziurtagiri bakoitzerako berariazko dokumentazioan* zehazten dira.

Gako eta ziurtagirien ohiko berritzerako erregistroa

Ziurtagiri bat berritzeko, beste bat eskatu behar da, horretarako *Ziurtagiri bakoitzerako berariazko dokumentazioan* finkatutako ziurtagirien jaulkipen-prozesuari jarraituko zaio.

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.

Gako eta ziurtagiriak ezeztatu ondoren berritzeko erregistroa.

Ziurtagiria ezeztatu eta beste bat jaulki ondoren, gakoak berritu egin behar dira beti.

Ezeztatzeko, eteteko edo berraktibatze eskaera kautotzea

Ezeztatzeko, eteteko edo berraktibatze eskaera baten kautotzeko baldintzak *Ziurtagiri bakoitzerako berariazko dokumentazioan* garatzen dira.



4 Eskakizun operatiboak

Atal honetan IZENPEk jaulkitako ziurtagirientzako komunak diren eskakizun operatiboak ezartzen dira

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

4.1 Ziurtagiria eskatzea

Erregistro-entitatean eskatzailearen identitatea egiaztatu ostean, erakundeak ziurtagiria jaulkitzeko eskaera sinatu beharko du eta, horrela, [Harpidedun kontratua](#) onartuko da.

Ziurtagiria –edo harekin lotzen den dokumentazioa– jaulkitzean eta/edo banatzean akats teknikoak gertatzeagatik egiten den ezeztapenaren ondoriozko jaulkipenen kasuan, ez da beharrezkoa izango ziurtagiria berriro jaulki dadin eskatzea.

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.

Ziurtagirian eta eskaeran gakoan edukitzailea identifikatzen duten datuak dira eskatzen diren identifikazio-dokumentuetan azaltzen direnak.

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

Ziurtagiria egin ondoren ziurtagirian edo identifikazio-dokumentuetan agertzen den egoeraren bat aldatzen bada, erregistro-entitateari jakinarazi beharko zaio, ziurtagiria ezeztatzea ekar baitezake horrek.

4.1.1 Eskaeraren egiaztapena

Erregistro-entitateko langileek sistema informatikoan sartzen dituzte eskatzailearen datuak eta, horrenbestez, gauzatu egiten dute ziurtagiri-eskaera.

Eskaera telematika bidez egin bada, erregistro-entitateko langileek aurrerregistrora jotzen dute eta zuzendu egiten dituzte oker dauden datuak.



Eskaera balidatu ondoren, eskatzaileari ematen zaio, sina dezan; jarraian, berriz, artxibatu egiten dute erregistro-entitateko langileek.

Eskatutako ziurtagiriaren araberako dokumentazio kautotua ere eraman behar du eskatzaileak, erregistro-entitaterako ziurtagiri-eskaerarekin batera artxiba dezaten.

4.2 Ziurtagiria jaulkitzea

Ziurtagiria egiteak berarekin dakar eskaeraren azken onarpena, eta onarpen osoa.

Ziurtagiriaren arabera, gailu kriptografikoan edota software-euskarrian jaulki daiteke.

I. Gailu kriptografikoan jaulkitzerakoan jarraitu beharreko prozedura:

1. Erregistro Entitateak egiaztatu egiten du eskatzaileek aurkeztutako dokumentuaren baliozkotasuna.
2. Kautotze-lana amaitu ondoren, ziurtagiri bat jaulkitzeko eskatzen dio IZENPERi erregistro-entitateak.
3. Eskaera erregistro-entitate baimendu batek bidali duela egiaztatu ondoren, IZENPEk ziurtagiria jaulkitzen du –ezarritako prozedurari jarraiki– eta erregistro-entitateari igortzen dio.
4. Eskaera IZENPEk bidali duela egiaztatu ondoren, erregistro-entitateak sinadura sortzeko gailuan kargatzen du ziurtagiria, gailu kriptografikoak kudeatzeko prozesu seguru bat erabiliz.
5. 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).
6. Ziurtagiria eta gutunak (barruan PINa eta PUKa dituztenak) modu seguruan emango zaizkio ziurtagiriaren harpidedunari edo gakoaren edukitzaileari.
7. Arrazoiren batengatik IZENPEk ziurtagiria ez jaulkitzea erabakitzen badu (nahiz eta kautotze-prozedurak egokiak izan), erabaki horren arrazoiak jakinarazi egin behar zaizkio eskatzaileari.

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



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

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

4.3 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 gakoen 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.

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

4.4 Ziurtagiriak eten eta ezeztatzea

4.4.1 Ziurtagiriak ezeztatzeko arrazoiak

Honako egoera hauetan ezeztatuko ditu ziurtagiriak IZENPEk:

- a. Ziurtagiriak ezeztatzea sinatzaileak, edo hori ordezkatzan duen pertsona fisikoak edo juridikoak eskatuta edota hirugarren baimendu batek edo pertsona juridikoko ziurtagiri elektronikoa eskatu duen pertsona fisiko batek eskatuta.
- b. Sinatzailearen edo ziurtapen-zerbitzuen egilearen sinadura sortzeko datuak urratzea edo arriskuan jartzea, edo sinatzaileak edo hirugarren batek datu horiek bidegabe erabiltzea.
- c. Ebazpen judizial edo administratiboren batek hala agintzea.

- d. 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.
- e. IZENPEk jarduera etetea, baldin eta, sinatzailearen aurretiko onespena dela medio, hark jaulkitako ziurtagiri elektronikoen kudeaketa ez bazaio transferitzen beste ziurtapen-zerbitzuen egileren bati.
- f. Ziurtagiria lortzeko emandako datuak aldatzea edo ziurtagiria emateko egiaztatutako zirkunstantziak aldatzea.
- g. Ziurtagiria galtzen bada edo lapurtzea, edo erabiltzeko ez dela geratzea, bai ziurtagiriaren euskarria hondatu delako, bai Ziurtapen Politikak aurreikusten ez duen beste euskarri batera aldatu delako.
- h. Aldeetakoren batek dagozkion betebeharrak ez betetzea.
- i. Ziurtagiria jaulkitzean akatsen bat gertatzea, ezarritako prozedurari ez egokitzeagatik edo jaulkitze-prozesuan arazo teknikoak sortzeagatik.
- j. Sinadura sortzeko datuen hitzarmenetik kanpoko gorabeherak direla medio, IZENPEk jaulkitako ziurtagirien fidagarritasuna eta sistemen segurtasuna arriskuan jartzea.
- k. Ziurtagiria edo harekin lotzen den dokumentazioa jaulkitzean eta/edo banatzean akats teknikoak gertatzea.
- l. Ziurtagiria eskatu zen egunetik hiru hilabete pasatzea eskatzaileak jaso duen arte.
- m. IZENPEk ziurtagiria jaulkitzeko eskaera bat jasotzea, eta politika bereko eta bakartasun-irizpide bereko beste ziurtagiri bat egotea, eta, horrenbestez, ezeztatzea indarrean dagoen ziurtagiria, baina eskatzaileak ezeztatzeko eskaera egin ondoren.

4.4.2 Ezeztatzeko eskaera zein entitatek egin dezakeen

Ikusi *Ziurtagiri bakoitzerako berariazko dokumentazioan*.

4.4.3 Ezeztatzeko eskaera egiteko prozedurak

Ziurtagiri bat ezeztatu nahi duenak IZENPEri edo, hala badagokio, erregistro-entitateari eskatu behar dio, ziurtagiri mota bakoitzeko *berariazko dokumentazioan* biltzen denari jarraiki. Honako informazio hau eduki behar du ezeztatzeko eskaerak:

- Ziurtagiriaren harpidedunaren edo gakoaren edukitzailearen identitatea.
- Ezeztatzeko eskaera egiteko arrazoia, ongi zehaztua.



- Ezeztatzea eskatzen duenaren izena.
- Ezeztatzea eskatzen duenarekin harremanetan jartzeko informazioa.

Eskaerarekin batera, eta hala behar izanez gero, ziurtagiriaren balio-epea amaitu dela egiaztatzen duen dokumentazioa ere aurkeztu behar du ezeztatzeko eskaera egiten duenak.

Ziurtagiri mota bakoitzeko *berariazko dokumentazioan* biltzen denari jarraiki kautotu behar da eskaera.

Ziurtagiria ezeztatzeko arrazoirik badagoela eta arrazoa zuzena dela egiaztatu behar dute erregistro-entitateko langileek; ondoren, IZENPERi eman beharko diote arrazoiaren berri, erakunde horrek ezeztapena gauza dezan.

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

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

IZENPEk ez dauka baimenik ezeztatutako ziurtagiririk berraktibatzeke.

4.4.4 Ezeztatzeko eskaera egiteko denbora-epea

Ezeztatzeko eskaerak berehala bidali behar dira, ezeztatzeko zergatiaren berri jaso bezain pronto.

4.4.5 Ziurtagiriak eteteko arrazoiak

Honako egoera hauetan etengo ditu ziurtagiriak IZENPEk:

- Edozein unetan, gakoan edukitzaileak eskatzen badu eta ziurtagiria galdu egin bada, edo lapurtu egin badute.
- Erregistro-entitateak eskatu ahal dio IZENPERi ziurtagiria eteteko, harik eta ziurtagiriaren balio-epearen galera eragin duen gertakaria frogatzeko aurkeztutako dokumentazioa begiratu arte.
- Ebazpen judizial edo administratiboren batek hala agintzen badu.

4.4.6 Eteteko eskaera zein entitatek egin dezakeen

Ikusi *Ziurtagiri bakoitzerako berariazko dokumentazioan*.



4.4.7 Eteteko eskaera egiteko prozedurak

Ikusi Ziurtagiri bakoitzerako berariazko dokumentazioan.

Ziurtagiriaren baliogabetzea eragin duen zergatia egiaztatzen duen dokumentazioa begiratzeko denbora gehiago behar badu erregistro-entitateak, IZENPEri eskatu behar dio beti.

4.4.8 Etenaren gehieneko epea

Etenak gehienez hamabost egun naturaleko iraupena izango du, ziurtagiriaren harpidedunak edo gakoan edukitzaileak baliogabetzea eskatu duen egunetik kontatzen hasita.

Epe horretan, harpidedunak edo gakoan edukitzaileak ziurtagiria berraktibatzea berretsi egin behar du.

Epe hori igaro bada eta harpidedunak edo gakoan edukitzaileak berraktibatzea berretsi ez badu, ziurtagiria ezeztatu egingo da.

Etenaren gehieneko iraupena hamabost egun naturalekoa da, eskaera-egunetik zenbatzen hasita, baldin eta eskaera erregistro-entitateak egin badu. Epe hori igarotakoan, eteteko agindua kendu egingo da.

4.4.9 Berraktibatze eskaera egiteko prozedurak.

Ikusi Ziurtagiri bakoitzerako berariazko dokumentazioan.

4.4.10 Ezeztatutako ziurtagirien zerrendak jaulkitzeko 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. Ezeztatzerik gertatzen ez bada, egunero sortzen da berrito ezeztatutako ziurtagirien zerrenda.

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

4.4.11 Ezeztatutako ziurtagirien zerrendak kontsultatzeko obligazioa

Egiaztatzaileek begiratu egin behar dute zein egoeratan dauden haien konfidantza izango duten ziurtagiriak.

Ziurtagirien egoera begiratzeko metodo bat honakoa da: IZENPEK jaulki duen azken CRLa kontsultatzea.



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

CRLak asteko 7 egunetan, eguneko 24 orduetan daude erabilgarri, eta publikoak eta anonimoak dira.

Sistemak edo zerbitzuak huts egiten badu, edo IZENPEren kontrolpean ez dagoen beste faktore batek huts egiten badu, IZENPEk ahalegin guztiak egingo ditu zerbitzua 24 ordutan, gehienez, erabilgarri egoteko.

4.4.12 Ziurtagiriak ezeztatzeko eta eteteko dauden zerbitzuak

IZENPEk ziurtagiriak ezeztatzeko eta eteteko 24x7 zerbitzua eskaintzen die entitate erabiltzaileei (24 ordukoa asteko 7 egunetan). Zerbitzuok 24x7 daude erabilgarri.

Sistemak edo zerbitzuak huts egiten badu, edo IZENPEren kontrolpean ez dagoen beste faktore batek huts egiten badu, IZENPEk ahalegin guztiak egingo ditu zerbitzua 24 ordutan, gehienez, erabilgarri egoteko.

4.4.13 Ziurtagirien egoera zein den jakiteko dauden zerbitzuak

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

Bada beste web-zerbitzu iraunkor bat ere, IZENPEk ezeztatutako ziurtagirien eguneratze inkremental telematikoa kontsultatzeko aukera eskaintzen duena.

Bi zerbitzu horiek 24x7 daude erabilgarri.

Sistemak edo zerbitzuak huts egiten badu, edo IZENPEren kontrolpean ez dagoen beste faktore batek huts egiten badu, IZENPEk ahalegin guztiak egingo ditu zerbitzua 24 ordutan, gehienez, erabilgarri egoteko.

4.4.14 Ziurtagirien egoera zein den jakiteko dauden zerbitzuak kontsultatzeko obligazioa

IZENPErekin horretarako izenpetzen duten hitzarmenean finkatuko da entitate erabiltzaileek OCSP (Online Certificate Status Protocol) protokoloaren bidez kontsultak egiteko obligazioa.

4.4.15 Ziurtagirien ezeztapenari buruzko beste informazio-bide batzuk

Ez da aplikagarria.



4.4.16 Ziurtagirien ezeztapenari buruzko beste informazio-bide batzuk kontsultatzeko obligazioa

Ez da aplikagarria.

4.4.17 Gako pribatua arriskupean: betekizun bereziak

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

IZENPEren CAREN gako pribatua arriskupean badago, dokumentu honen 4.8.3 atalak dioena egin behar da.

4.5 Segurtasun-ikuskapeneko prozedurak

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.

4.5.1 Erregistratutako gertaera motak

Segurtasun logean gorde behar 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.

4.5.2 Ikuskaritza-erregistroen tratamendu-maiztasuna

Aldiro begiratzen ditu log fitxategiak IZENPEko ikuskatzaileak.

4.5.3 Ikuskaritza-erregistroak zenbat denboraz eduki behar diren artxibatuta

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



4.5.4 Ikuskaritza-erregistroen babesa

Log erregistroa irakurtzeko eskubidea ematen zaie ikuskatzaileei.

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

4.5.5 Babeskopiak egiteko prozedurak

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

4.5.6 Ikuskaritza-erregistroen metatze-sistema aurkitzeko

CAREN, RAREN eta LRAREN log artxiboak IZENPEren barne-sistemetan gordetzen dira.

4.5.7 Ikuskatu beharreko gertaeraren berri ematea gertaera-eragileari

Ez dago aurreikusita log fitxategietako jardueraren berri gertaeraren eragileari jakinaraztea.

4.5.8 Puntu ahulen azterketa

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

4.6 Informazioak artxibatzea

4.6.1 Erregistratutako gertaera motak

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

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

4.6.2 Erregistroak zenbat denboraz eduki behar diren artxibatuta

Ziurtagiri onartuei buruzko informazio eta dokumentazio guztia 15 urtez gorde behar da; gainerako ziurtagiriei buruzkoak, 7 urtez.

4.6.3 Artxiboaren babesa

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



4.6.4 Babeskopiak egiteko prozedurak

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

4.6.5 Data eta ordua zigitatzeko baldintzak

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

4.6.6 Artxibatzeko sistema nola aurkitu

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

4.6.7 Artxiboko informazioa eskuratzeko 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.

4.7 Gakoak berritzea

Ziurtagiria ezeztatu egin delako edo indarraldia amaitu delako, ziurtagiri berria eskatu behar da, ziurtagiriak jaulkitzeko *Ziurtagiri bakoitzerako berariazko dokumentazioan* aurreikusitako prozesuari jarraituko zaio.

Gakoak berritzeak berekin dakar ziurtagiria berritzea.

4.8 Gakoak arriskuan egotea eta hondamenditik suspertzea

Larrialdietarako Planak zehazten du zer egin behar den, zer baliabide eta zenbat langile erabili behar diren, baldin eta gertakariren baten ondorioz (nahita eragindakoa edo halabeharrezkoa), IZENPEk ematen dituen ziurtapen-zerbitzuak eta baliabideak ezin erabili geratzen badira edo hondatzen badira. Larrialdietarako Planaren helburu nagusiak hauek dira:

- Berreskuratze-lanen eraginkortasuna areagotzea, hiru fase hauek erabiliz:
 - Jakinarazteko/ebaluatze/aktibatze fasea, kalteak ebaluatze eta plana aktibatze.

- Berreskuratzeko fasea, behin-behingo eta partzialki zerbitzuak berriro martxan jartzeko, harik eta jatorrizko sistemari izandako kalteak konpondu arte.
- Konpontzeko fasea, sistema eta prozesuak bere ohiko martxara itzularazteko.
- Ohiko martxaren etenaldi luzeetan DPZ alternatibo 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 berreskuratzeko.
- Planifikatu den larrialdiarako 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 berreskuratzeko lanetan.

Larrialdietarako Planean deskribatzen da kalteen ebaluazioa eta ekintza-plana.

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. Egondako 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 eskatzaileak nahiz harpidedunak eta egiaztatzaileak (fidagarriak diren hirugarrenak) barnean hartuko dira.
 - Sortutako kontingentziaren berri web orrian emango da.
 - Kaltetutako ziurtagiriak ezeztatuko dira.
 - Berritze-estrategia.

4.8.1 Baliabideak, aplikazioak edo datuak hondatzea

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



4.8.2 Entitatearen gako publikoa ezeztatzea

CAREN gako publikoa ezeztatzen denean, haren PKI azpiegitura berreskuratu egin behar da. Horretarako, berriro martxan jarri behar dira CAREN gakoak eta ziurtagiriak eta harpidedun guztien ziurtagiriak. CAREN ziurtagiri berria hartaz fidatu behar duten aplikazioei emango zaie. Horrez gain, argitaratu egingo da, harpidedunek jaitsi ahal izan dezaten.

4.8.3 Entitatearen gakoa arriskupean

Oinarrizko CAk ezeztatu egingo du CA jaulkitzaile jakin baten ziurtagiria, baldin eta 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 sortzea 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.

4.8.4 Hondamendia instalazioetan

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

IZENPEren Larrialdietarako Plana aktibatuko da.



4.9 Zerbitzua amaitzea

4.9.1 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.

Ziurtapen-zerbitzuen egileei, nabigatzaileen fabrikatzaileei, eta, ziurtagirien erabileraren arloan, IZENPErekin kontratu-loturaren bat duen entitate orori ere jakinaraziko zaie.

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

IZENPEk jarduera beste ziurtapen-zerbitzuen egileren bati transferitzea erabakiz gero, ziurtagirien harpidedunari eta Industria, Turismo eta Merkataritza Ministerioari emango die transferentzia-akordioen berri. Horretarako, IZENPEk transferentzia-baldintzak zehazten dituen agiria bidaliko dio harpidedunari, baita harpidedunaren eta ziurtagiriak transferitzen zaizkion ZZEren arteko harremanak erregulatuko dituzten erabilera-arauak ere. Jakinarazpenak jasoko direla 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 ZZEren batzuekin akordiorik lortu ezean, automatikoki ezeztatuko dira ziurtagiri guztiak.

4.9.2 Erregistro-entitatea.

Erregistro-entitateak, bereganatzen dituen eginkizunak bertan behera uzten dituenean, IZENPEri transferituko dizkio dauzkan erregistroak, informazioa artxibatuta edukitzeko obligazioa duen bitartean (4.6.2 atala); bestela, baliogabetu eta deuseztatu egingo da.

5 Segurtasun fisikoaren, prozeduren eta langileen kontrolak

5.1 Segurtasun fisikoaren 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:

- a. 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.
- b. Ate eta leiho guztiak itxita eta babestuta daude, baimenik ez duen inor sartu ez dadin.

5.1.2 Sarbide fisikoa

5.1.2.1 IZENPEren instalazioak

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

- a. Segurtasun-perimetro bat, lur errealetik sabai errealeraino, baimenik gabeko inor sar ez dadin.
- b. 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. Ez daramanari langileek eurek eskatzea bultzatzen du enpresak.
 - Gainbegiratu egiten dira IZENPEren jarduerarekin zerikusirik ez duten eta haren instalazioetan lanean aritzen diren langileak.
- c. Sarbideen log fitxategi bat, leku seguruan gordeta.
- d. IZENPEra sartzeko ateen sarbide-mekanismoak.
- e. IZENPEk ziurtapen-zerbitzua egiteko erabiltzen dituen elementuak monitorizatzen dituen telebista-zirkuitu itxi bat.



5.1.2.2 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 daitezzen.

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.
- Aireztatze-sistema deskonektatzea, suteen aurkako atea ixtea, elektrizitate-hornidura etetea eta itzaltze-sistema automatikoa abiaraztea.

5.1.6 Euskarrien biltegiatzea

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 ditzaketen 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 konfiguratzea da.
- Bigarrena funtzioak hainbat lagunen artean banatzea da, asmo txarreko jarduera gauzatzeko hainbat lagunekin adostea beharrezkoa izateko.

IZENPEk antolakundean 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 eslei daitezke.

5.2.3 Eginkizun bakoitzean identifikatzea eta kautotzea

Konfiantzazko rolak behar bezain segurua den bitarteko batez kautotu beharko dira, eta beti erabiltzaile pertsonalekin.

IZENPEk badu Eginkizun eta Erantzukizun Politika bat.



5.3 Langileen kontrolak

5.3.1 Historialei, kalifikazioei, esperientziari eta kautotzei buruzko baldintzak

Burutu behar dituen zerbitzuetan esperientzia eta kalifikazioak dituen langileak enplegatzeko dituzten baldintzak IZENPEk.

Konfiantzazko eginkizunak dituzten langileek ez dute IZENPEko eragiketen inpartzialtasunari kalte egin diezaizkieten interesik.

5.3.2 Historiala ikertzeko prozedurak

Ez da Espainiako araudiari jarraiki aplikatzen.

5.3.3 Trebakuntza-baldintzak

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

1. Ziurtapen Praktiken Deklarazioaren kopia bat ematea.
2. Segurtasunaren arloan kontzientziatzea.
3. Softwarearen eta hardwarearen funtzionamendua eginkizun jakin bakoitzerako.
4. Segurtasun-prozedurak eginkizun jakin bakoitzerako.
5. Funtzionamendu eta administrazioko prozedurak eginkizun jakin bakoitzerako.
6. Hondamenak konpontzeko prozedurak.

5.3.4 Trebakuntza eguneratzeko baldintzak eta maiztasuna

IZENPEren funtzionamenduan aldaketa garrantzitsu bat egiten den bakoitzean, trebakuntza-plana egingo da, eta planaren gauzatzeaz dokumentatuko da.

5.3.5 Lan-txandaketen segida eta maiztasuna

Ez da aplikagarria.



5.3.6 Baimendu gabeko konexioen zigorrak

5.3.6.1 Informazioaren segurtasuneko gertakariak

IZENPEk segurtasun-larrialdiak kudeatzeko plana du.

5.3.6.2 Zigor Prozesua

Zigor-prozesua definitzen duen barne-erregimen diziplinarioa dago.

5.3.7 Langileak kontratatzeko baldintzak

IZENPEk langileak kontratatzeko 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.

Gainera, langileek sistemaren osagaien funtzionamenduari buruzko eskuliburuak eskuratzeko aukera dute.

6 Segurtasun teknikoaren kontrolak

6.1 Gako-parea sortu eta instalatzea

6.1.1 Gako-parea sortzea

Hona hemen IZENPE osatzen duten 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.
- Gailu kriptografikoan jaulkitako ziurtagiriak: gakoak gailu kriptografikoak sortzen ditu.
- Software-euskarrian 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.

6.1.2 Gako pribatua harpidedunari banatzea

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

- Gailu kriptografikoan jaulkitako ziurtagiriak: kautotze eta sinadura elektronikoa aurreratuko gako pribatuak gailu kriptografikoarekin batera ematen 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 IZENPE osatzen duten edo harekin lankidetzan jarduten duten entitateek ziurtagiri-jaulkitzaileari gako publikoa emateko metodoa:

- CA jaulkitzaileak: gako publikoa oinarrizko CAra bidaliko da X.509 edo PKCS#10 formatuaren bidez.
- Gailu kriptografikoan jaulkitako ziurtagiriaren kasuan: 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. atalean SHA1 arrastoak daude.

6.1.5 Gakoen tamainak eta erabilitako algoritmoak

Kasu guztietan erabilitako algoritmoa SHA-1 duen RSA da, Oinarrizko CA 2007-n eta mendeko CAetan izan ezik. Kasu horretarako SHA-256 ziurtapena jaulki da.

Gakoen tamaina kasuen arabera izango da:

- Gutxienez 1024 bit pertsona fisikoen gakoetarako, OCSP zerbitzarietarako eta TSA zerbitzarietarako.
- 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-1 da (hash algoritmoa), RSArekin batera (sinadura-algoritmoa). Algoritmo-identifikatzaile hori "Identifier for SHA-1 checksum with RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc." da. 2007. urtetik aurrera SHA-256 algoritmoa ezartzen hasi zen urratsez urrats, inguru teknologiko bakoitzaren arabera.

Azken erabiltzaileen ziurtagiriak SHA-1 duen RSArekin daude sinatuta. Ziurtagiriarekin sinatzeko, SHA-1 duen RSA edo altuagoa erabiltzeko gomendatzen die azken erabiltzaileei Izenpek (SHA-224 edo SHA-256).

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. Egondako 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, eraginkorrena dela uste den bidea erabilia. Ziurtagirietako eskatzaileei nahiz harpidedunei eta egiaztatzaileei (fidagarriak diren hirugarrenak).
- Sortutako kontingentziaren berri web orrian ematea.
- Kaltetutako ziurtagiriak ezeztatzea.
- Berritze-estrategia.

6.1.7 Gako publikoko parametroak sortzea

- HSM euskarrian sortutako gakoak: FIPS 140-2 3. mailako gomendioei jarraitzen zaie. HSM gailuetan gakoak sortzeko, gutxienez bi pertsonen onespena behar da.
- Gailu kriptografikoan sortutako gako kriptografikoak: FIPS 140-2 2. maila estandarren edo baliokideen gomendioei jarraitzen zaie.

6.1.8 Gako publikoaren parametroen kalitatea egiaztatzea

6.1.6. ataleko gomendioak aplikatzen dira.

6.1.9 Gakoak sortzea

Gakoak, kasuaren arabera, honela sortzen dira:

- CA: HSM gailuan bertan.
- Gailu kriptografikoetan.
- Gailuak: haiek dituzten gailuetan edo sistemetan.

6.1.10 Gakoak erabiltzeko helburuak

Gakoak kautotzeko eta zifratzeko erabiltzen dira, baita sinadura elektronikoa aurreraturako ere. Gako jakin baten erabilera *KeyUsage* luzapenaren bidez zehazten da. Luzapen hori ziurtagiri guztietan dago, eta kritiko gisa markatuta dago, ziurtagiria jaulki den helbururako erabilia izan dadin mugatzeko.

6.2 Gako pribatua babestea

6.2.1 Modulu kriptografikoaren estandarrak

Segurtasun kriptografikoaren modulua (HSM) gako kriptografikoak sortzen eta babesten dituen segurtasun-gailua da. Beharrezkoa da HSMek FIPS 140-1 3. maila edo baliokidea betetzea.



Sinadura elektroniko aurreraturako 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 ziurtagiri baliokideak ere onartzeko modukoak dira.

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

CAetako gako pribatuak erabiltzeko, bi lagun onespena behar da gutxienez.

6.2.3 Gako pribatuaren gordailua

Ez dago gakoak berreskuratzeko mekanismorik.

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 modulu kriptografikoan sartzea

Gako pribatuak modulu kriptografikoetan sartzekoan, larrialdietan bakarrik erabiliko da 6.2.4. atalean adierazitako prozedura.

6.2.6 Gako pribatua aktibatze metodoa

- Gailu kriptografikoan jaulkitako ziurtagirien kasuan: PINak erabiltzen dira gailu kriptografikoetako gako pribatuak erabiltzeko.
- Beharrezko konfidentzialtasunari eusteko eta inprimakiak manipulatu ez direla ziurtatzeko aukera ematen duen sistema batean ematen da.
- CAen kasuan, txartela duen administrari batek erabiltzen ditu gako pribatuak.

6.2.7 Gako pribatua desaktibatze metodoa

Gailu kriptografikoa irakurgailutik ateratzean, aribideko edozein eragiketa bukatzen da.

6.2.8 Gako pribatua deuseztatze metodoa

CAren gakoak suntsitzeko prozedura bat dago.

Prozedura hori ez zaie aplikatzen erabiltzaile-gakoei, ez baitira CAk eraturakoak, gakoa berritzeko gailu kriptografiko bera berriro erabiltzen denean izan ezik. Horretan, aurreko gakoa suntsituko da eta euskarri berean beste gako batzuk sortuko dira.



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 ziurtagirien kasuan: 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.
- Konfidentzialtasunari 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.
- Software euskarrian jaulkitako ziurtagiriak: ziurtagiriarekin 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.

6.4.3 Aktibatzekeo datuen beste alderdi batzuk

Aktibatzekeo datuen gehienezko iraupena ez da arautuko. Bestalde, aldizka aldatu egingo dira, zein diren aurkitzekeo aukerak gutxitzekeo.

6.5 Segurtasun informatikoaren kontrolak

6.5.1 Segurtasun informatikorako berariazko eskakizun teknikoak

Badira hainbat kontrol IZENPEren ziurtagiri-zerbitzua egitekeo sistemaren elementuen kokalekuetan (CAk, IZENPEren datu-baseak, IZENPEren Interneteko 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 ziurtatzearren.
 - Informazio-euskarriak, baliabide nahasgarriak eta ekipamendu zaharkituak ziurtasunez babesteko, ezabatzekeo eta deuseztatzekeo prozedura dago.
- Datu-trukeak. Datu-truke hauek zifratuta doaz dagokien konfidentzialtasuna ziurtatzekeo.
 - Datuen trukea identifikazio-puntuen eta RAen artean.
 - RAen eta erregistroko datu-baseen artekeo erregistro-datuen trukea.
 - Aurrerregistroko datuen trukea.
 - RAen eta CAen artekeo komunikazioa.
- Ezeztapenen argitalpen-zerbitzuak behar bezalako funtzionalitateak ditu, 24x7 funtzionatzea bermatzekeo.
- Sarbide-kontrolak.
 - Erabiltzaile bakarrekeo IDak erabiliko dira; hartara, egiten dituzten ekintzekeo 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 banaka 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 15408:1999 estandarra dute.

6.6 Bizitza-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:

- Ekoizten ari diren softwareko liburutegiak eguneratzeko (adabakiak barne) baimen-prozedura formal bat dago. 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 onartutako mailan mantentzen da.

6.6.2 Bizitza-zikloaren segurtasun-mailaren ebaluazioa

Ziurtapen-zerbitzuak egiteko erabilitako produktuek "Common Criteria" nazioarteko ziurtagiria edo ISO/IEC 15408:1999 estandarra dute.

6.6.3 Proba-datuak babestea

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



6.6.4 Aldaketak kontrolatzeko prozedurak

Softwarean egiten diren aldaketen kontrol zorrotza egiten da, informazio-sistemetan gerta daitezkeen arazoak saihesteko. Aldaketak kontrolatzeko prozedura formalak betetzen dira. Honako neurri hauek hartzen dira, besteak beste:

- Adostutako baimen-mailen erregistroa edukitzea.
- Aldaketak baimendutako erabiltzaileek egiten dituztela ziurtatzea.
- Segurtasun-kontrolak gainbegiratzea aldaketek ez dietela eragiten egiaztatzeko.
- Aldatu behar den softwarea, informazioa, datu-baseak eta hardwarea identifikatzea.
- Lana egiten hasi aurretik onespena izatea.
- Aldaketa amaitzean, sistemaren dokumentazioa eguneratu dela eta dokumentazio zaharra artxibatu edo suntsitu dela ziurtatzea.
- Aldaketa guztien erregistro bat edukitzea onespeneren eta ezartze-daten xehetasunekin.

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 Modulu kriptografikoen ingeniartzako kontrolak

Modulu kriptografikoek FIPS 140-1 3. maila edo FIPS 140-2 3. maila estandarrari jarraitzen diote.

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:

1. Authority Key Identifier
2. subjectKeyIdentifier
3. basicConstraints
4. keyUsage
5. certificatePolicies
6. subjectAltName
7. issuerAltName
8. extKeyUsage



9. cRLDistributionPoints
10. NetscapeCertType
11. Subject Directory Attributes
12. Authority Information Access

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

Horietako bakoitzaren profil 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-1 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. LS		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 Ez da ziurtagiri guztietan ageri.



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 onartua 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 nnnnnnnL, edo aiz Xnnnnnnn 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	
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	Bai1	
1.8.	Subject Public Key Info	1024-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" ²	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 Ziurtagiri motaren arabera.

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			
2.6.1.	rfc822Name	Harpidedunaren edo gakoan 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 gakoan edukitzailearen jaiotze-data ³		
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	

³ Entitatearen ziurtagirietan izan ezik, horietan ez dago gakoan edukitzailea.



2.12.1.2.	accessLocation	On-line Certificate Status Protocol-en URL	Bai	
-----------	----------------	--	-----	--

Algoritmo-objektuen identifikatzailea

IZENPEK ziurtagiria sinatzeko erabiltzen duen algoritmo-identifikatzailea (AlgorithmIdentifier) SHA-1/RSA da; "Identifier for SHA-1 checksum with RSA encryption for use with Public Key Cryptosystem One defined by RSA Inc."-en identifikatzailearekin bat dator.

IZENPEK SHA-256/RSA algoritmoa ezarriko du urratsez urrats, inguru teknologikoaren arabera.

7.1.3 Izenen formatuak

Ziurtagen Praktiken Deklarazio honetako 3.1. atalean zehaztutakoaren arabera.

7.1.4 Izenen murrizpenak

Ez da izenik murrizten.

7.1.5 Ziurtagiriaren politikaren objektu-identifikatzailea

Ziurtagen Praktiken Deklarazio honetako 1.2. atalean zehaztutakoaren arabera.

7.1.6 "Politika-murrizpenak" luzapenaren erabilera

Ez da politika-murrizpenik erabiltzen.

7.1.7 Politika kalifikatzaileen sintaxia eta semantika

Certificate Policies luzapenak politika-kalifikatzaile hauek ditu:

CPS Pointer: IZENPEren Ziurtagen Praktiken Deklaraziorako erakuslea du.

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

Policy Qualifier ID: URL bat adierazten du, eta horretan eskura dago IZENPEren Ziurtagen Praktiken Deklarazioa.

Ziurtagiri guztietarako User Notice komuna:

USER NOTICE	Bermeen mugak ezagutzeko www.izenpe.com helbidean. Ziurtagirian konfiantza izan aurretik kontratua irakurri. Limitaciones de garantías en www.izenpe.com Consulte el contrato antes de confiar en el certificado
--------------------	--

7.2 Ezeztatutako ziurtagirien zerrendaren profila

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
3. Issuing Distribution Point	Bai	Ez
4. Reason Code	Bai	Ez
5. Invalidity Date	Bai	Ez

8 Zehaztapenaren administrazioa

8.1 Aldaketa-prozedura

Dokumentu honetan egiten diren aldaketak Praktikak Onesteko Batzordeak 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 ziurtapen-zerbitzuen arduradunaren sinadurak abalatuko du.
- Zehaztapenen bertsio berriaren alde tekniko eta legal guztiak hartuko dira kontuan.
- Aldaketa-kontrola ezarriko da, ondoriozko zehaztapenek bete nahi ziren baldintzak betetzen dituztela bermatzeko, baita aldaketa eragin zutenak ere.
- Zehaztapenak aldatzeak erabiltzailearengan dituen eraginak ezarriko dira, eta aldaketa horiek hari jakinarazteko beharra aztertuko da.

8.1.1 Erabiltzaileei jakinarazi beharrik ez dauden aldaketak

IZENPEk dokumentu honetan aldaketak egin ditzake erabiltzaileei jakinarazteko beharrik gabe, betiere, aldaketa materialak ez badira, adibidez:

- Akats tipografikoak zuzentzea dokumentuan.
- URLak aldatzea.
- Harremanetako informazioa aldatzea.

Erabiltzaileei jakinarazi beharreko aldaketak

IZENPEk erabiltzaileei jakinarazi behar dizkie zerbitzuaren zehaztapenetan edo baldintzetan egindako aldaketa guztiak.

8.2 Argitalpen- eta jakinarazte-politika

Zerbitzuaren zehaztapenetan edo baldintzetan egindako aldaketak IZENPEren web-orri nagusiaren (<http://www.izenpe.com>) bidez jakinaraziko zaizkie erabiltzaileei.

IZENPEren web-orri nagusian 30 egunez emango aldaketen berri, eta bertan egongo dira aldatu den agiria, eguneratzeko agiria eta bertsio berria.



30 egunera, egindako aldaketen aipamena kenduko da orri nagusitik, baita bertsio zaharra dokumentaziotik ere. Azken hori IZENPEk gordeko du gutxienez 15 urtez, eta kontsultatu ahal izango dira interesatuek zergatia arrazoitzen badute.

8.2.1 Ziurtapen Praktiken Deklarazioan argitaratzen ez diren elementuak

Ziurtapen Praktiken Deklarazio honetako 2.8.1. atalean lehendik dauden osagaiei, azpiosagaiei eta elementuei, baina horien konfidentziasuna gordetzeko publikoarentzat erabilgarri ez daudenei, egiten zaie erreferentzia.

8.3 Onespen-prozedura

Dokumentu honetan egindako azken aldaketak Praktikak Onesteko Batzordeak onetsiko ditu, 8.1. atalean ezarritako baldintzak betetzen direla egiaztatu eta gero.



9 Datu pertsonalak babestea

9.1 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 abenduaren 13ko 15/1999 Lege Organikoa garatzeko Erregelamendua onartzen duen, abenduaren 21eko, 1720/2007 Errege Dekretuan aurreikusten denari, eta gainerako garapeneko araudiari jarraiki ere.

Sinadura elektronikoari buruzko abenduaren 19ko 59/2003 Legearen 19.3. artikuluan 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.

9.2 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 eskura dagoen bide guztien kontrolaren bidez egin beharko da babesa.

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 artxiboak.
- Datuetara sartzeko ezarritako sistemak (automatizatuak, eskuzkoak edo mistoak).

9.3 Datu pertsonalak babesteko segurtasun-antolamendua.

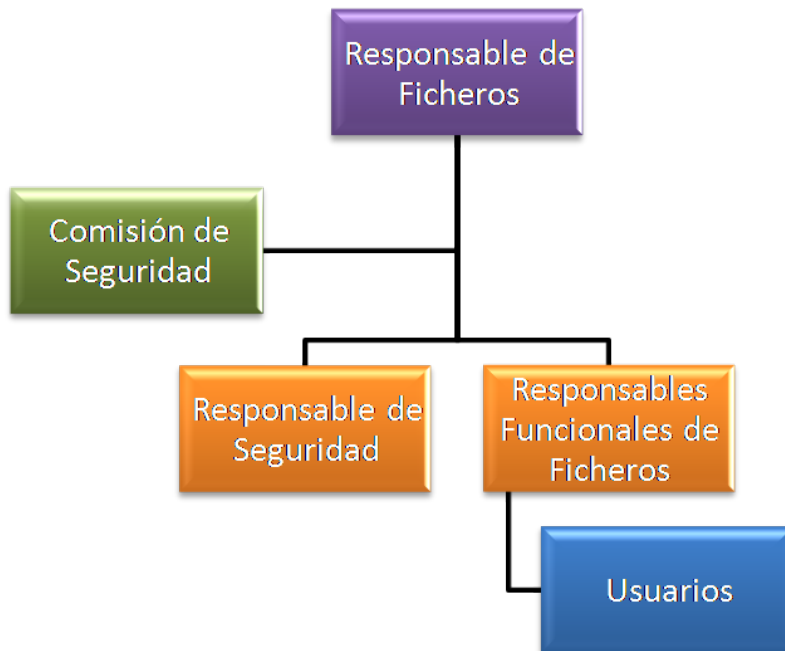
Atal honetan deskribatzen da IZENPEk datu pertsonalen segurtasuna bermatzeko ezarritako segurtasun-antolamendua.

Segurtasun-antolamenduaren eredua 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.

9.3.1 Segurtasun-antolamenduaren eredua

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, segurtasun-arduraduna, IZENPEren fitxategien arduradun funtzionalak eta erabiltzaileak).



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

9.3.2 Segurtasuna antolatzeko unitateen sailkapena

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

- a. Fitxategiko 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.

- b. Segurtasuneko 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.

- c. Segurtasun-batzordea: informazioaren segurtasunari eta datuen babesari dagozkion erabakiak hartzean, antolakundeko unitateen kontsultarako eta laguntzarako organo gorenena da. Haien eskumenen jardunean, Batzordeak ordezkari izan dira, eta Zuzendaritzaren/Gerentziaren, hau da, IZENPEren ordezkari gorenaren ageriko babesarekin dihardu, datu pertsonalak dituzten fitxategien arduradun den aldetik, baita fitxategi horiekin lotzen diren zuzendaritza-organoen babesarekin ere, fitxategien barne-organo arduradunak diren aldetik.
- d. Fitxategiaren arduradun funtzionala: zerbitzuen ikuspuntu funtzionaltik, Informazio Sistemen alderdi operatiboetan erabakiak hartzeaz arduratzen den pertsonari dagokion irudia da. Irudi horiek fitxategien arduradun den IZENPEren ordezkari izan dira jardungo dute. Tartean den zerbitzuaren kudeaketaren arduradunak, hau da, arloetako bakoitzeko arduradunak izango dira funtzio hori beteko duten IZENPEren pertsonak.
- e. Fitxategiaren erabiltzailea: beren funtzioak betetzean, datu pertsonalak tratatzen dituzten edo datu horiek eskura dituzten pertsonak dira. Erabiltzaile horiek, datu pertsonalen alorrean, Segurtasun Dokumentuan biltzen diren arauak eta prozedurak errespetatu beharko dituzte, baita indarrean dagoen eta aplikatzekoa den legeriaren ondoriozkoak ere.

9.4 Datu pertsonalak dituzten fitxategien egitura

Ziurtapen Praktiken Deklarazio honen ondorioetarako, Datuak Babesteko Espainiako Agentzian inskribatuta dauden datu pertsonalen honako fitxategien (aurrerantzean FITXATEGIEN) arduraduna da IZENPE:

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

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

Fitxategien egituraren deskribapena Antolamenduaren Segurtasun Dokumentuan zehazten da.



9.5 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 kokatutako lokalei eta lanpostuei ere.

9.5.1 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 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 egiaztatzeko kontrolari buruzko araudia.
- Aldian behin ikuskapenak egiteari buruzko araudia.



- Probetan benetako datu pertsonalak erabiltzeari buruzko araudia.
- IZENPEren lokaletara eta dependenzietara 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 biltegitzeko gailuei buruzko araudia.
- Automatizatu gabeko fitxategietako dokumentuak kopiatzeari eta erreproduzitzeari buruzko araudia.
- Automatizatu gabeko dokumentazioa eskuratzeari buruzko araudia.
- Komunikazioetako segurtasun-neurriei buruzko araudia.

9.5.2 Prozedurak

Bestalde, IZENPEk maneiatzen dituen datu pertsonalen babesa bermatzeko beharrezko prozedurak ditu.

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

Zehazki, honakoak dira ezarritako prozedurak:

- Erabiltzaileak administratzeko prozedura.
- Gertakariak jakinarazteko eta kudeatzeko prozedura.
- Babes-kopiak egiteko prozedura.



- Datuak berreskuratzeko prozedura.
- Datu pertsonaletara sartzeko eskubideaz baliatzeko prozedura.
- Datu pertsonalak zuzentzeko eta ezabatzeko eskubideaz baliatzeko prozedura.
- Datu pertsonaletarako oposizio-eskubideaz baliatzeko prozedura.

10 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.

Azken finean, ziurtagirien gakoan eskatzaileak, harpidedunak eta edukitzaileak identifikatuko dituzten entitateak dira; horrez gain, ziurtagirietan jasotzen diren zirkunstantziak egiaztatzen dituen dokumentazioa ziurtatzen dute, eta ziurtagiriak jaulkitzeko, ezeztatzeko 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 da. 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 onartua:** 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.
- **Konfidentzialtasuna:** konfidentzialtasuna dokumentu elektroniko bat pertsona-zerrenda jakin bati izan ezik gainerako erabiltzaile guztiei eskuraezin egiteko gaitasuna da. Horrela, komunikazioak beste batzuek entzun ezin izateko moduan egitea eta dokumentuak adierazitako hartzaileak soilik irakurri ahal izateko moduan igortzea lor dezakegu.
- **Kriptografia:** kriptografia matematikaren adar bat da, eta aztertzen 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 egiazta eta deszifra 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 lor 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, etetean 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 estandarraren araberako 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 ezarritakoari 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 ezagut dezakeen moduan sortzen da.
- **Sinadura elektronikoa onartua:** sinadura elektronikoa onartua 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 ordezkatzeko 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 ziurtapen-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 Organiko honen helburua da datu pertsonalak baliatzerakoan pertsona fisikoen askatasun publikoak eta oinarrizko eskubideak bermatu eta babestea, batez ere, pertsona horien ohorea eta intimitate pertsonala eta familiakoa.
- **Ezeztatutako Ziurtagirien Zerrenda (CRLak):** IZENPEk jaulkitzen dituen ziurtagiri ezeztatuek edo etendakoek osatzen duten zerrenda da, eta berehalako ezeztatze 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 negatiboek –puntu batez banatuta– osatzen duten sekuentzia. Erregistratutako objektuei egokitu dakieke, eta bakarrak 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, baita karaktere teknikoak, ziurtapen-zerbitzuak ematerakoan jarraitutako prozeduretarako arauak, eta ziurtagirien erabilpen-baldintzak ere.
- **Gakoen edukitzaileak:** sinadura digitaleko gakoen eta deszifratze-gakoen zaintzaz arduratzen den 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.
- **Egiaztatze Aurreratuko Programa (EAP):** programa 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-sistemarekin 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 denbora-tarte jakin batean informazio jakin bat bazegoela bermatzeko.
- **Zerbitzari segurua:** web-zerbitzari bat da eta, bertan, komunikazioa zifratuta doa batetik bestera, modu seguruan. Eragiketa hori egiteko, 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 internet-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 deszifratzeko erabiltzen diren gako pribatuak biltzeko, sinadura elektronikoak sortzeko eta datu-mezuak deszifratzeko erabil dezake.
- **Hirugarrengoen 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.



11 Akronimoak

ARL: Ziurtapen Agintaritzak Ezeztatzeko Zerrenda.

CA: Ziurtapen Agintaritza.

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.

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).

EAP: egiaztatze aurreratuko programa.

RA: Erregistro-agintaritza.

SSL: Secure Socket Layer

TSA: Time Stamping agintaritza-zerbitzua