# Segurtasun Politika

| Bertsioa | Data | Honek berrikusia | Honek onartua | Aldaketa |
|---|---|---|---|---|
| 1 | 2026-09-04 | Segurtasun arduraduna | Segurtasun Batzordea | Hasierako edizioa |
| | | | | |

1. ONARTZEA ETA INDARREAN JARTZEA ..... 3
2. IRISMENA ..... 3
3. SARRERA ..... 3
4. MISIOA ..... 4
5. POLITIKAREN PRINTZIPIO GIDARIAK ..... 5
6. ARAU ESPARRUA ..... 6
7. INFORMAZIOAREN SEGURTASUNAREN ANTOLAMENDUA ..... 6
Funtzioak eta ardurak ..... 7
Gatazkak konpontzea ..... 10
Izendatzeko prozedura ..... 10
8. ERAKUNDEAREN DATU PERTSONALEN TRATAMENDUA ..... 10
9. ARRISKUEN KUDEAKETA ..... 11
10. INFORMAZIOAREN SEGURTASUN POLITIKAREN GARAPENA ..... 11
11. LANGILEEN BETEBEHARRAK ..... 11
12. HIRUGARREN ALDEAK / ZERBITZU EMAILEAK / SOLUZIOEN HORNITZAILEAK ..... 12
13. SEGURTASUN GERTAKARIEN KUDEAKETA ..... 13
14. ETENGABEKO HOBEKUNTZA ..... 13
15. POLITIKA ONARTZEA ETA INDARREAN JARTZEA / ERAGINKORTASUNA ..... 13
16. ALDAKETEN HISTORIKOA ..... 14

## 1. ONARTZEA ETA INDARREAN JARTZEA

Informazioaren Segurtasun Politika hau 2026ko irailaren 4an onartu zuen Informazioaren Segurtasun Batzordeak, eta egun horretatik aurrera da eraginkorra, Politika berri batekin ordezkatu arte.

## 2. IRISMENA

Sinplifikatze aldera, dokumentu honetan BOGAN izena erabiltzen da, besteak beste, Agintzari, Zabalduz eta Hirube kide diren erakunde taldea aipatzeko.

Hala ere, Informazioaren Segurtasuna Kudeatzeko Sistemaren eta Segurtasun Eskema Nazionalaren araberako ziurtapen prozesuaren irismena Agintzari, Zabalduz eta Hirube erakundeetara mugatzen da soilik, horien informazio sistemak baitira kategorizatu direnak eta auditoriaren xede direnak.

Ondorioz, politika hau Agintzari, Zabalduz eta Hirubeko informazio sistemei, erakunde horietako kide diren pertsonei eta sistema horietan esku hartzen duten zerbitzu emaileei edo IKT soluzioen hornitzaileei aplikatzen zaie. Gainerako dokumentuan BOGANi egiten zaion erreferentzia irismen horretara mugatuta dagoela ulertu beharko da, kontrakoa berariaz adierazten ez bada.

## 3. SARRERA

BOGANeko informazio sistemak arretaz administratu behar dira, arriskuaren arabera neurri egokiak hartuta, tratatutako informazioaren benetakotasunari, trazabilitateari, osotasunari edo konfidentzialtasunari edo emandako zerbitzuen erabilgarritasunari eragin diezaioketen ustekabeko edo nahita eragindako kalteen aurrean babesteko.

Informazioaren segurtasunaren azken helburua da erakundeak bere helburuak bete ahal izatea, bere funtzioak edo eskumenak garatu ahal izatea, eta informazioaren kalitatea eta zerbitzuak etengabe emateko eratu diren zerbitzuak eman ahal izatea, prebentzioz jokatuz, eguneroko jarduera gainbegiratuz eta gertakariei azkar erantzunez.

IKT sistemek babestuta egon behar dute informazioaren eta zerbitzuen konfidentzialtasun, osotasun, erabilgarritasun, aurreikusitako erabilera eta balioan eragiteko potentziala duten bilakaera azkarreko mehatxuen aurka. Mehatxu horietatik defendatzeko estrategia bat behar da, inguruneko baldintzen aldaketetara egokitzeko eta zerbitzuak etengabe ematen direla bermatzeko. Horrek esan nahi du departamentuek Segurtasun Eskema Nazionalak eskatzen dituen gutxieneko segurtasun neurriak aplikatu behar dituztela, zerbitzuak emateko mailen etengabeko jarraipena egin behar dutela, jakinarazitako ahultasunak kontrolatu eta aztertu behar dituztela, eta gertakariei erantzun eraginkorra eman behar zaiela, emandako zerbitzuen jarraitutasuna bermatzeko.

BOGANek ziurtatu behar du IKTen segurtasuna sistemaren bizi zikloaren etapa bakoitzaren zati integrala dela, sortzen denetik zerbitzua amaitzen den arte, kontuan hartuta baita ere garatzeko edo erosteko erabakiak eta ustiapen jarduerak. Segurtasun betekizunak eta finantzaketa beharrak identifikatu behar dira eta plangintzan, eskaintzen eskaeran eta lizitazio pleguetan sartu behar dira, datu pertsonalak tratatzen dituzten, IKT zerbitzuak eskuratzen dituzten edo informazio sistemei eragiten dieten zerbitzuak ematen dituzten proiektuetarako.

## 4. MISIOA

BOGANen xede soziala da bere barnean biltzen dituen kooperatiben misioaren garapena bultzatu, sustatu, koordinatu, osatu eta bermatzea, eta, horretarako, zerbitzu teknikoak, aholkularitzakoak, kudeaketakoak, administraziokoak, kontabilitatekoak, juridikoak, komertzialak eta ordezkaritza instituzionalekoak eskaintzen ditu, bai bigarren mailako kooperatibarentzat, bai kooperatiba bazkideentzat.

BOGANen xede soziala osatzen duten jarduerak, gutxienez konpromiso kooperatiboaren oinarrizko alderdiei dagokienez, berak eta bere kooperatiba bazkideek garatu beharko dituzte zuzenean; horri kalterik egin gabe, jarduera horiek berak parte hartzen duen edo lankidetza akordioak lortzen dituen beste erakunde batzuen bidez erraztu, osatu eta koordinatu ahal izango dira.

Kooperatiba bazkideei dagokienez, bigarren mailako kooperatiba honen azken helburua da ahalik eta enpresa efizientziarik handiena lortzea eta sozietatearentzako interes komuneko zerbitzuak ematea, baita bere entitate zerbitzu guztientzat ere, zerbitzu osagarri batzuk eskainiz, jarduerak koordinatuz eta horien ordezkaritza instituzionalaren bidez.

Zerbitzu horiek hainbat erakunde eta eredu operatiboren bidez egiten dira, horien artean egonik Zabalduz, Agintzari eta Hiruberi lotutako sistemak, baita funtzionatzeko beharrezkoak diren laguntza zerbitzuak ere.

Bere jardueraren izaeraren ondorioz, BOGANek informazio pertsonala tratatzen du, kasu askotan sentsibilitate berezikoa, esku hartze sozialeko prozesuei lotua, eta horrek informazioa behar bezala babesten dela eta aplikatu beharreko araudia betetzen dela bermatzea eskatzen du.

Erakundeak ziurtatzen du bere zerbitzuen euskarri diren informazio sistema guztiak arriskuan oinarritutako segurtasun irizpideen arabera kudeatzen direla, zerbitzuen erabilgarritasuna, informazioaren konfidentzialtasuna eta osotasuna eta garatutako jardueren jarraitutasuna bermatzeko, Segurtasun Eskema Nazionalarekin bat eginda.

Segurtasun arloan, BOGANek Politika honekin helburu hauek bermatu nahi ditu:

- Zerbitzuen prestazioan informazioaren konfidentzialtasuna, osotasuna, egiazkotasuna eta jarraitutasuna bermatzea.
- Arriskuaren araberako segurtasun neurriak ezartzea.
- BOGANeko kideak informazioaren segurtasunari buruz prestatzea eta kontzientziatzea. Sarbideen trazabilitatea ahalbidetuko duten segurtasun neurriak ezartzea eta, besteak beste, pribilegio minimoaren printzipioa errespetatzea, erabiltzaileen konfidentzialtasun betebeharra ere indartuz, beren funtzioak betetzean ezagutzen duten informazioari dagokionez.
- Segurtasun fisikoa hedatzea eta kontrolatzea, informazioaren aktiboak sarbideen kontrolek babestutako eremu seguruetan egon daitezen, antzemandako arriskuak kontuan hartuta.
- Beharrezko prozeduren bidez komunikazioen kudeaketan segurtasuna ezartzea, komunikazio sareen bidez transmititzen den informazioa behar bezala babestuta egon dadin.
- Informazio sistemen erosketa, garapena eta mantentze lana kontrolatzea informazio sistemen bizi zikloaren fase guztietan, segurtasuna bermatzea lehenetsiz.
- Zerbitzuak ematean segurtasun neurriak betetzen direla kontrolatzea, eta sistemaren osagai berriak eskuratzean eta txertatzean kontrola mantentzea.

- Segurtasun gertakariak kudeatzea, horiek behar bezala detektatu, geldiarazi, arindu eta konpontzeko, eta horiek berriro gerta ez daitezen beharrezkoak diren neurriak hartzea.
- Informazio pertsonala babestea, tratamenduaren ondoriozko arriskuei erantzuteko neurri teknikoak eta antolamendukoak hartuta, datuak babesteari buruzko legeriaren arabera.
- Segurtasuna kudeatzeko sistema etengabe gainbegiratzea, detektatutako eraginkortasunik ezak hobetzeko eta zuzentzeko.

## 5. POLITIKAREN PRINTZIPIO GIDARIAK

- Irismen estrategikoa: informazioaren segurtasunak erakundeko maila guztien konpromisoa eta laguntza izan behar du, eta gainerako ekimen estrategikoekin modu koherentean koordinatu eta integratu behar da.
- Segurtasun integrala: segurtasuna prozesu integral gisa ulertuko da, informazio sistemei lotutako elementu tekniko, humano, material eta antolamenduko guztiak kontuan hartuta, edozein jarduera puntual edo tratamendu koiuntural saihesten saiatuz. Informazioaren segurtasuna ohiko jardunaren zatitzat hartu behar da, eta IKT sistemen hasierako diseinutik egon behar da presente eta aplikatu behar da.
- Arriskuan oinarritutako segurtasunaren kudeaketa: identifikatutako arriskuetan oinarritutako segurtasunaren kudeaketak ingurune kontrolatu bat mantentzea ahalbidetuko du, arriskuak maila onargarrietaraino minimizatzeko. Segurtasun neurriak informazioak dituen arriskuen eta sistemen arabera ezarriko dira, eta tratatzen duten arriskuarekiko proportzionalak izango dira, eta justifikatuta egon beharko dira. Datu pertsonalen tratamenduan identifikatutako arriskuak ere kontuan hartuko dira.
- Prebentzioa, detekzioa, erantzuna eta kontserbazioa, gertakariak prebenitzeko ekintzak inplementatuz, detektatutako ahultasunak minimizatuz, mehatxuak gauzatzea galaraziz eta, mehatxuak gertatzen direnean, bizkor erantzunez, emandako informazioa edo zerbitzuak lehengoratzeko eta informazioaren kontserbazio segurua bermatzeko.
- Defentsa lerroak egotea: erakundearen segurtasun estrategia segurtasun geruzetan diseinatu eta inplementatzen da.
- Etengabeko zaintza eta aldizkako berrebaluazioa: erakundeak ezohiko jarduerak edo portaerak detektatzeko eta horiei erantzuteko bitartekoak ezartzen ditu. Gainera, aktiboen segurtasun egoeraren ebaluazio jarraitua ahalbidetzen duten beste batzuez gain, etengabeko hobekuntza prozesu bat ere egongo da, segurtasun neurriak aldizka berrikusteko eta eguneratzeko, haien eraginkortasunaren eta arrisku eta babes sistemen bilakaeraren arabera.
- Segurtasuna lehenestea diseinutik bertatik: sistemek segurtasun lehenesten dela bermatzeko diseinatuta eta konfiguratuta egon behar dute. Sistemek diseinatu ziren zerbitzua emateko beharrezkoa den gutxieneko funtzionaltasuna emango dute.
- Ardurak bereiztea: printzipio hau aplikatuz, segurtasun arduradunaren eta sistemaren arduradunaren eginkizunak bereizita egongo dira.

BOGANeko langile guztiek, baita BOGANekin lankidetzan aritzen diren kanpoko langileek ere, Informazioaren Segurtasun Politika hau eta Baliabide Teknologikoak Erabiltzeko Politika ezagutzeko eta betetzeko betebeharra dute, eta Informazioaren Segurtasun Batzordearen ardura da informazioa eragindako langileengana iristeko beharrezkoak diren bitartekoak edukitzea.

## 6. ARAU ESPARRUA

Politika honi eragiten dioten arau nagusiak hauek dira:

- 311/2022 Errege Dekretua, maiatzaren 3koa, Segurtasun Eskema Nazionala arautzen duena.
- Ebazpena, 2016ko urriaren 13koa, Administrazio Publikoen Estatu Idazkaritzarena, Segurtasun Jarraibide Teknikoa onartzen duena, Segurtasun Eskema Nazionalaren arabera.
- Ebazpena, 2016ko urriaren 7koa, Administrazio Publikoen Estatu Idazkaritzarena, Segurtasunaren Egoerari buruzko Txostenaren Segurtasun Jarraibide Teknikoa onartzen duena.
- Ebazpena, 2018ko martxoaren 27koa, Funtzio Publikoaren Estatu Idazkaritzarena, Informazio Sistemen Segurtasuna Ikuskatzeko Segurtasun Jarraibide Teknikoa onartzen duena.
- Ebazpena, 2018ko apirilaren 13koa, Funtzioa Publikoen Estatu Idazkaritzarena, Segurtasun Gertakariak Jakinarazteko Segurtasun Jarraibide Teknikoa onartzen duena.
- 3/2018 Lege Organikoa, abenduaren 5ekoa, Datu Pertsonalak Babestekoa eta eskubide digitalak bermatzekoa.
- 2016/679 (EB) Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2016ko apirilaren 27koa, datu pertsonalen tratamenduari eta datu horien zirkulazio askeari dagokienez pertsona fisikoak babesteari buruzkoa, eta 95/46/EE Zuzentaraua (Datuak Babesteko Erregelamendu Orokorra) indargabetzen duena.
- 34/2002 Legea, uztailaren 11koa, Informazioaren gizartearen zerbitzuei eta merkataritza elektronikoari buruzkoa
- 11/2022 Legea, ekainaren 28koa, Komunikazioen Orokorra.
- 25/2007 Legea, urriaren 18koa, Komunikazio elektronikoei eta komunikazio sare publikoei buruzko datuak gordetzeari buruzkoa.
- 6/2020 Legea, azaroaren 11koa, Konfiantzazko zerbitzu elektronikoen zenbait alderdi arautzen dituena.

Informazio gehiago nahi izanez gero, berrikusi SGSI.PR11.01 dokumentua: Lege eta kontratu baldintzak betetzea.

## 7. INFORMAZIOAREN SEGURTASUNAREN ANTOLAMENDUA

### Informazioaren Segurtasun Batzordea

Segurtasun Batzordea da informazioaren eta zerbitzuen segurtasunaren arduradun nagusia. Batzordeak osaera hau izango du:

- Zerbitzuen arduraduna
- Informazioaren arduraduna
- Informazioaren segurtasunaren arduraduna
- Sistemaren arduraduna
- Datuak babesteko ordezkaria

Nahi izanez gero, BOGANeko beste kide batzuk ere sartu ahal izango dira Batzordearen zereginetan, lantalde espezializatuak barne, barnekoak, kanpokoak edo mistoak.

Segurtasun Batzordeko idazkaria izango da sistemaren arduraduna, eta Batzordearen bilerak deitzeaz eta horietako akta egiteaz arduratuko da.

Segurtasun Batzordeak eginkizun hauek izango ditu:

- Erakundeko Zuzendaritzak eta departamentuek segurtasunaren arloan planteatzen dituzten kezkei erantzutea.
- Zuzendaritzari aldian-aldian informazioaren segurtasunaren berri ematea.
- Informazioaren segurtasuna kudeatzeko sistema etengabe hobetzea sustatzea, plan espezifikoak onartuz.
- Informazioaren segurtasunari dagokionez, erakundearen bilakaeraren estrategia prestatzea.
- Informazioaren segurtasunaren arloan arlo guztiek egiten dituzten ahaleginak koordinatzea, ahaleginak sendoak direla eta arlo horretan erabakitako estrategiarekin lerrokatuta daudela ziurtatzeko, eta bikoiztasunak saihesteko.
- Hondarreko arriskua murrizteko proposatutako neurrien betetze maila aldizka kontrolatzea (hobetzeko ekintzak proposa ditzake), baita kudeaketa eta gertakarien prozedurak behar bezala funtzionatzen duela ere, gertakari horien kudeaketan segurtasun arlo guztiak koordinatzen direla zainduz.
- Informazioaren Segurtasun Politika lantzea (eta aldian-aldian berrikustea), Zuzendaritzak (edo organo eskudunak) onar dezan, eta Informazioaren Segurtasun Araudia onartzea
- Erakundeak segurtasun arloan dituen betebeharrak betetzen direla egiaztatzea ahalbidetzen duten aldizkako auditoriak egitea sustatzea.
- Erakundeak bere gain hartutako hondarreko arrisku nagusiak monitorizatzea eta jarduera posibleak gomendatzea.
- Erakundeak segurtasun arloan dituen betebeharrak betetzen direla egiaztatzea ahalbidetuko duten aldizkako auditoriak egitea sustatzea.
- Segurtasun arloko jarduerei lehentasuna ematea baliabideak mugatuak direnean.
- Segurtasun printzipioa diseinutik bertatik errespetatzen dela zaintzea, eta segurtasunaren arduradunak aholkularitza eskatu ahal izango du informazioaren edo sistemen segurtasunari eragiten dioten erakundearen ekimen guztietan. Bereziki, bikoiztasunak murriztuko dituzten eta sistema guztien funtzionamendu homogeneoa bultzatuko duten zerbitzu horizontalak sortzen eta erabiltzen direla zaindu beharko du.
- Arduradunen artean eta/edo erakundeko arloen artean ager daitezkeen erantzukizun gatazkak konpontzea, eta, erabakitzeko autoritate nahikorik ez duenean, kasuak gora jasotzea.

## Funtzioak eta ardurak

### Informazioaren arduraduna

Informazioaren arduradunaren eginkizunak hauek izango dira:

- Sistemetan tratatutako informazioaren sailkapena zehaztea eta eguneratuta mantentzea, haren sentsibilitate maila kontuan hartuta.

- Informaziorako beharrezkoak diren segurtasun betekizunak definitzea, sailkapenaren arabera, eta dagozkien sistemetan inplementatzen direla ziurtatzea.
- Sisteman kudeatutako informazioaren segurtasuna gainbegiratzea, sistemaren arduradunarekin eta segurtasunaren arduradunarekin lankidetzan.
- Informazioaren kudeaketa aplikatu beharreko lege, erregelamendu eta antolamenduko xedapenetara egokitzen dela bermatzea.
- Informazioari lotutako segurtasun gorabeherak identifikatzen, kudeatzen eta konpontzen parte hartzea.

### Zerbitzuaren arduraduna

Zerbitzuaren arduradunaren eginkizunak hauek izango dira:

- Zerbitzuei aplikatu beharreko segurtasun betekizunak ezartzea eta Informazioaren Segurtasun Batzordeari aurkeztea, onar ditzan.
- Zerbitzuaren garapena, mantentzea eta jarduna gainbegiratzea, eta adostutako segurtasun mailetara egokitzen dela egiaztatzea.
- Segurtasunaren arduradunarekin, sistemaren arduradunarekin eta informazioaren arduradunarekin koordinatzea, zerbitzuan segurtasunaren kudeaketa integrala bermatzeko.
- Zerbitzuari eragiten dioten segurtasun gertakariak identifikatzen eta konpontzen parte hartzea, eta gertakari horien berri ematea, ezarritako prozeduren arabera.
- Zerbitzuak aplikatu beharreko barne eta kanpo araudiak betetzen dituela ziurtatzea.
- Zerbitzuari eragin diezaioketen arriskuak identifikatzen, aztertzen eta kudeatzen laguntzea, eta eragin nabarmena izan dezaketenei buruzko informazio egokia ematea.

### Segurtasunaren arduraduna

Segurtasunaren arduradunaren eginkizunak hauek izango dira:

- Aplikatu beharreko segurtasun neurriak zehaztea, informazioaren eta zerbitzuen arduradunek egindako balorazioen arabera.
- Aplikagarritasun Adierazpena egitea eta onartzea, informazioaren eta zerbitzuaren arduradunen eskakizunak kontuan hartuta
- Sistemaren kategoria zehaztea, informazioaren eta zerbitzuaren arduradunen balorazioak kontuan hartuta.
- Informazioaren segurtasun neurriak sistemaren arduradunak behar bezala ezarri dituela egiaztatzea.
- Informazioaren Segurtasun Politika eta Segurtasunaren Eskema Nazionala aplikatzeko prozedurak, araudiak eta jarraibideak lantzen eta proposatzen parte hartzea.
- Arauen mapa osatzen duten segurtasun prozedurak onartzea (Batzordearen eskumenekoak ez direnak) eta Batzordeari aldi bakoitzean egin diren aldaketen berri ematea.
- BOGANen aktiboen arriskuen analisia eta ebaluazioa egitea, horien arduradunekin batera.
- Entitatean adimen artifizialeko sistemak hedatu aurretik arriskuak aztertzea, informazioaren eta zerbitzuaren arduradunaren eta, hala badagokio, datuak babesteko ordezkariaren balorazioak kontuan hartuta, eta haien hedapena gainbegiratzea.
- Informazioaren segurtasunaren arloko prestakuntza eta kontzientziazioa sustatzea, bere erantzukizun eremuaren barruan.

- IKT zerbitzuen hornitzaileek segurtasun neurriak eta arauak eta zerbitzu mailako akordioak betetzen dituzten zaintzea.
- Segurtasuna hobetzeko planak egiten eta ezartzen parte hartzea eta, hala badagokio, jarraitutasun planetan parte hartzea eta baliozkotzea.
- Segurtasun Batzordeari aldaketen onarpena eta sistemaren beste betekizun batzuk helaraztea.
- Bere eskumen eremuko sistemei buruzko lehen, bigarren edo hirugarren alderdi baten auditoria txostenak aztertzea, eta horien ondorioak sistemaren arduradunari eta, hala badagokio, Informazioaren Segurtasun Batzordeari aurkeztea.
- Zibergertakarien kudeaketan, erakundearen, informazioaren eta zerbitzuen arduradunak kontuan hartuta, haien arriskugarritasuna kalifikatuko du CCN-STIC 817 Gidaren arabera, segurtasunaren arloan eskumena duten agintariekin harremanetan jartzeko kontaktu puntu gisa jardunez, eta, Politikan esleitutako rolen arabera, CCN-CERTi jakinarazi ahal izango dizkio gertakariak, hala badagokio. Erreferentziazko CSIRT taldeari jakinaraztea beharrezkoa denean, bidegabeko atzerapenik gabe eta berehala egin beharko da, pixkanaka informazio zabalagoa bidaltzearen kalterik gabe.

### Sistemaren arduraduna

Sistemaren arduradunaren eginkizunak hauek izango dira:

- Sistema garatzea, erabiltzea eta mantentzea bere bizi ziklo osoan, baita haren zehaztapenak, instalazioa eta funtzionamendu egokia egiaztatzea ere.
- Segurtasun auditorien ondoriozko neurri zuzentzaileak hartzea
- Sistemaren topologia eta kudeaketa definitzea, erabiltzeko irizpideak eta eskuragarri dauden zerbitzuak zehaztuz.
- Beharrezko prozedura operatiboak prestatzea.
- Segurtasun neurri espezifikoak segurtasun esparru orokorraren barruan behar bezala integratzen direla ziurtatzea.
- Segurtasuna hobetzeko planak egiten eta ezartzen parte hartzea eta, hala badagokio, jarraitutasun planetan parte hartzea.
- Sistemaren kategoria zehazteko aholkularitza ematea, segurtasunaren arduradunarekin eta/edo IKT Segurtasun Batzordearekin lankidetzan.
- Sistemari eragiten dioten segurtasun gertakariak ikertzea, eta, hala badagokio, segurtasunaren arduradunari edo hark zehazten duenari jakinaraztea.
- Zerbitzuaren jarraitutasun planak ezartzea, segurtasunaren arduradunak aholkatuta.
- Segurtasun gertakarien (zibergertakarien) kudeaketan, segurtasunaren arduradunarekin adostuta, informazioaren tratamendua eta zerbitzuen prestazioa kautelaz eta premiaz eten ahal izango ditu, kontrolerako neurri gisa. Etenaldi hori erakundearen titularrari eta informazioaren eta zerbitzuaren arduradunei jakinarazi beharko zaie, eta, datu pertsonalei eragiten badie, Datuak Babesteko ordezkariari, eta administrazio izapideei eragiten badie, erakundearen zerbitzu juridikoei, epeak eteteko, hala badagokio.

Sistemaren konplexutasunak hala justifikatzen duenean, sistemaren arduradunak beharrezkotzat jotzen dituen sistemaren arduradun ordezkariak izendatu ahal izango ditu. Era berean, esleitzen zaizkion arduren beste eginkizun zehatz batzuk ere eskuordetu ahal izango ditu.

### Datuak babesteko ordezkaria:

Hauek dira datuak babesteko ordezkariaren eginkizunak:

- BOGANi eta tratamenduaz arduratzen diren erabiltzaileei dagozkien betebeharren berri ematea eta aholkuak ematea, Datuen Babesaren arloan indarrean dagoen araudiaren arabera.
- BOGANen segurtasun araudian eta barne politiketan datuen babesaren arloan xedatutakoa betetzen dela gainbegiratzea, horren barruan egonik erantzukizunak esleitzea, tratamendu eragiketetan parte hartzen duten langileen kontzientziazioa eta prestakuntza, eta dagozkion auditoriak.
- Datuen babesaren inguruko inpaktuaren ebaluazioari buruz eskatzen zaion aholkularitza eskaintzea, eta horren aplikazioa gainbegiratzea.
- Datuak Babesteko Espainiako Bulegoarekin lankidetzan aritzea, hark hala eskatzen duenean, eta harekin harremanetan jartzeko kontaktu puntu gisa jardutea datuen tratamenduari buruzko gaietarako.
- Datuak babesteko ordezkariak tratamenduko eragiketei lotutako arriskuei arreta emanez beteko ditu bere funtzioak. Horretarako, hau egiteko gai izan behar du:
    - Tratamendu jarduerak zehazteko informazioa biltzea.
    - Tratamendu jardueren egokitasuna aztertu eta egiaztatzea.
    - Tratamenduaren arduradunari edo eragileari informazioa, aholkuak eta gomendioak ematea. Tratamendu eragiketen erregistroa gainbegiratzeko informazioa biltzea.
    - Diseinuzko eta lehenetsitako datuen babesaren printzipioari buruz aholkatzea.
    - Aholkularitza ematea inpaktuaren ebaluazioak egiten diren ala ez jakiteko, metodologiari buruz, aplikatu beharreko babesei buruz, etab.
    - Arriskuen arabera, jarduerak lehenestea.
    - Tratamenduaren arduradunari aholkularitza ematea auditorietan egin beharreko arloei, prestakuntza jarduerei, tratamendu eragiketei eta denbora eta baliabide gehiago emateari buruz.

### Gatazkak konpontzea

Arduradunen arteko gatazkak badaude, Informazioaren Segurtasun Batzordeak ebatzi ahal izango ditu desadostasunak.

### Izendatzeko prozedura

- BOGANeko Kontseilu Errektoreko lehendakariak sortuko du Informazioaren Segurtasunerako Batzordea, kideak izendatuko ditu eta politika honetan identifikatutako arduradunak izendatuko ditu.
- Izendapenak bi urtean behin berrikusi ahal izango dira, eta lehenago egin ahal izango dira postua hutsik geratzen denean edo, aldez aurretik ohartarazita, funtzioak behin eta berriz betetzen ez direnean.

## 8. ERAKUNDEAREN DATU PERTSONALEN TRATAMENDUA

BOGANek datu pertsonalak tratatzen ditu, Tratamenduko Jardueren Erregistroan deskribatzen denaren arabera. BOGANek tratatutako datu pertsonalei lotutako arriskuak ebaluatu beharko ditu, eta jarduera plan bat proposatu beharko du baimendutako atalasea gainditzen duten arriskuak zuzentzeko.

Arriskuen analisia aldizka berrebaluatuko da, Datuak Babesteko Ordezkariaren aholkularitzarekin eta gainbegiratzearekin, eta, nolanahi ere, arrisku handiko tratamendu bat detektatzen denean, eta, hala badagokio, inpaktuaren ebaluazioa egin beharko da. Arriskua tratatzeko planaren inplementazioa SENen planarekin koordinatuko da, baita datuak babesteko betebeharretatik eratorritako gainerako segurtasun prozedurak edo

arauak ere, batez ere zerbitzu emaileen kontrolean edo datu pertsonalen gertakariei eta/edo arrakalei erantzutean.

## 9. ARRISKUEN KUDEAKETA

Politika honi lotutako sistema guztiek arriskuen analisia egin beharko dute, arriskuak eta mehatxuak ebaluatuz. Analisi hori errepikatu egingo da:

- erregularki, urtean behin gutxienez.
- erabilitako informazioan aldaketak gertatzen direnean.
- emandako zerbitzuetan aldaketak gertatzen direnean.
- segurtasun gertakari larri bat gertatzen denean.
- ahultasun larrien berri ematen denean.
- datuak babesteko arriskuen analisian edo inpaktuaren ebaluazioetan aldaketak egiten direnean.

Arriskuen analisiak harmonizatzeko, Informazioaren Segurtasun Batzordeak erreferentziazko balorazio bat ezarriko du erabilitako informazio motetarako eta emandako zerbitzuetarako. Segurtasun Batzordeak sistemen segurtasun beharrei erantzuteko baliabideen erabilgarritasuna dinamizatuko du, inbertsio horizontalak sustatuz.

Datuak babesteko arriskuak kontuan hartuko dira, Datuak Babesteko ordezkariaren iritzia kontuan hartuta, eta, gainera, arriskua tratatzeko planak koordinatuko dira.

## 10. INFORMAZIOAREN SEGURTASUN POLITIKAREN GARAPENA

Informazioaren Segurtasun Politika hau hainbat segurtasun araudi eta gomendioren bidez osatuko da (segurtasun araudiak eta prozedurak, segurtasun prozedura teknikoak, txostenak, erregistroak eta ebidentzia elektronikoak). Informazioaren Segurtasun Batzordeari dagokio hau urtero berrikustea eta/edo mantentzea, eta, beharrezkoa bada, hobekuntzak proposatzea. Informazioaren segurtasunari buruzko araudia hiru mailatan garatuko da, aplikazio eremuaren, xehetasun teknikoaren eta nahitaez bete beharraren arabera; horrela, garapen maila jakin bateko arau bakoitza goragoko mailako arauetan oinarrituko da. Arauen garapen maila horiek hauek dira:

a) Lehen arau maila: Informazioaren Segurtasun Politika hau eta Informazioaren Segurtasuna Kudeatzeko Sistemaren Eskuliburua.

b) Bigarren arau maila: Baliabide Teknologikoak Erabiltzeko Politika, informazio sistemak behar bezala erabiltzeko.

c) Hirugarren arau maila: prozedurak, gidak eta jarraibide teknikoak. Dokumentu horiek, Informazioaren Segurtasun Politikan azaldutakoa betez, prozesu bat gauzatzean egin beharreko ekintzak edo zereginak zehazten dituzte.

Segurtasun Batzordeari dagokio Informazioaren Segurtasun Politika, Baliabide Teknologikoak Erabiltzeko Politika eta gainerako dokumentuak onartzea, eta hura zabaltzeaz ere arduratuko da, eragindako alderdiek ezagut dezaten.

## 11. LANGILEEN BETEBEHARRAK

BOGANeko informazio sistemak erabiltzen dituzten pertsona guztiek, baita BOGANekin lankidetzan aritzen diren kanpokoek ere, Informazioaren Segurtasun Politika hau eta Baliabide Teknologikoak Erabiltzeko Politika ezagutzeko eta betetzeko betebeharra dute, eta Informazioaren Segurtasun Batzordearen ardura da informazioa eragindako langileengana iristeko beharrezkoak diren bitartekoak edukitzea.

Etengabeko kontzientziazio programa bat ezarriko da informazio sistemen erabiltzaile guztiei arreta emateko, bereziki sartu berri direnei.

IKT sistemen erabileran, eragiketan edo administrazioan erantzukizuna duten pertsonek prestakuntza jasoko dute sistemak modu seguruan erabiltzeko, beren lana egiteko behar duten neurrian. Prestakuntza nahitaezkoa izango da ardura bat hartu aurretik, bai lehenengoz izendatzen denean, bai lanpostuz edo arduraz aldatzen denean.

Informazioaren Segurtasun Politika edo araudia eta horietatik eratorritako prozedurak nabarmen ez betetzeak dagozkion diziplina neurriak abiaraztea ekar dezake, eta, kasua bada, aplikatu beharreko beste lege neurri batzuk ere bai.

## 12. HIRUGARREN ALDEAK / ZERBITZU EMAILEAK / SOLUZIOEN HORNITZAILEAK

BOGANek beste erakunde batzuei zerbitzuak ematen dizkienean edo beste erakunde batzuei buruzko informazioa erabiltzen duenean, Informazioaren Segurtasun Politika honen berri emango zaie, alde batera utzi gabe datuak babesteko araudiaren betebeharrak errespetatzea, aipatutako zerbitzuak ematean tratamenduaren arduradun gisa jarduten badu, eta jarduteko prozedurak ezarriko dira dagozkien Segurtasun Batzordeen berri emateko eta koordinatzeko kanalak eta segurtasun gorabeheren aurrean erreakzionatzeko. Gainera, segurtasunaren arduraduna (edo hark eskuordetutako pertsona) Kontaktu Puntua izango da (POC).

BOGANek hirugarrenen zerbitzuak erabiltzen dituenean edo hirugarrenei informazioa lagatzen dienean, Segurtasun Politika honen eta zerbitzu edo informazio horiei eragiten dien Segurtasun Araudiaren berri emango die, datuak babesteko beste betebehar batzuk betetzearen kalterik gabe.

Hodeian aktiboak erabiltzeko eskubideak eskuratzean, 311/2022 Errege Dekretuaren II. eranskineko segurtasun neurrietan eta hura garatzeko gidan ezarritako baldintzak hartuko ditu kontuan.

Hirugarren alderdi hori araudian ezarritako betebeharren mende geratuko da, eta araudi hori betetzeko bere prozedura operatibo propioak garatu ahal izango ditu, BOGANek horiek gainbegiratu edo horiek betetzen direla erakusten duten ebidentziak eskatu ahal izateko moduan, baita bigarren edo hirugarren alderdi baten auditoriak ere. Gertakarien berri emateko eta konpontzeko prozedura espezifikoak ezarriko dira, eta inplikatutako hirugarrenen POCak bideratu beharko ditu, eta, gainera, datu pertsonalei eragiten dienean, Datuak Babesteko ordezkariak. Hirugarrenek bermatuko dute beren langileak segurtasun arloan behar bezala kontzientziatuta daudela, gutxienez politika honetan ezarritakoaren edo kontratuan berariaz eska daitekeenaren maila berean.

Hirugarren batek Politikaren alderdiren bat bete ezin duenean, aurreko paragrafoetan eskatzen denaren arabera, Segurtasunaren arduradunak txosten bat egingo du, gertatzen diren arriskuak eta horiek tratatzeko modua zehazteko. Informazioaren arduradunek eta ukitutako zerbitzuek onartu beharko dute txosten hori, kontratazioa

hasi aurretik. Txostena erakundearen ordezkariari helaraziko zaio, eta hark hirugarrenaren kontratazioa izapidetzen jarraitzeko baimena eman beharko du, hautemandako arriskuak bere gain hartuta.

Erakundeak Adimen Artifizialeko sistema bat eskuratzen, garatzen edo ezartzen duenean, arlo horretan indarrean dagoen araudian ezarritakoa betetzeaz gain, Segurtasunaren arduradunaren txostena izan beharko du, eta hark Informazioaren eta Zerbitzuaren arduradunei eta, beharrezkoa denean, Sistemaren arduradunari kontsulta egingo die, eta Datuak Babesteko ordezkariak ere bere iritzia eman beharko du.

## 13. SEGURTASUN GERTAKARIEN KUDEAKETA

BOGANek prozedura bat izango du informaziorako eta zerbitzuetarako mehatxua diren segurtasun gertakariak eta jazoerak arin kudeatzeko.
Prozedura hori beste arau sektorial batzuetako segurtasun gertakariekin zerikusia duten beste batzuekin integratuko da, hala nola datu pertsonalak babestearekin edo erakundeari eragiten dion beste batekin, erantzuna ikuspegi desberdinetatik koordinatzeko eta kontrol erakundeei bidegabeko atzerapenik gabe jakinarazteko, eta, beharrezkoa denean, Estatuko Segurtasun Indar eta Kidegoei edo epaitegiei.

## 14. ETENGABEKO HOBEKUNTZA

Informazioaren segurtasunaren kudeaketa etengabe eguneratu beharreko prozesu bat da. Adibidez, antolaketan, mehatxuetan, teknologietan edota legedian aldaketak gertatzen direnean, sistemak etengabe hobetu behar dira.

Horregatik, beharrezkoa da prozesu iraunkor bat ezartzea, besteak beste ekintza hauek ekarriko dituena:

a) Informazioaren Segurtasun Politika berrikustea.
b) Zerbitzuak eta informazioa berrikustea eta kategorizatzea.
c) Arriskuen analisia urtero egitea.
d) Barne auditoriak edo, hala dagokionean, kanpo auditoretzak egitea.
e) Segurtasun neurriak berrikustea.
f) Arauak eta prozedurak berrikustea eta eguneratzea.

## 15. POLITIKA ONARTZEA ETA INDARREAN JARTZEA / ERAGINKORTASUNA

Politika honetan aldaketak egiten badira eta horrek aldaketak edo eraginkortasun ezari aurre egiteko egokitzapenak egin behar badira, aldaketok Informazioaren Segurtasun Batzordeak egingo ditu, eta urtero berrikusi beharko ditu.

Aldaketek funtsezko moldaketa bat badakarte edo izendatutako printzipioak edo ardurak aldatzen badira, Segurtasun Batzordeak aldaketak proposatuko ditu, eta, hala badagokio, behar diren eskumenak dituen pertsonak edo organoak onartu beharko ditu.

Informazioaren Segurtasun Batzordeak eskatuko du Politika ordeztea, eta behar diren eskumenak dituen pertsonak edo organoak berretsiko du; horren berri behar bezala emango zaie interesdunei, zabaltzeko erabilitako kanal berberen bidez.

## 16. ALDAKETEN HISTORIKOA

| Bertsioa | Data | Honek berrikusia | Honek onartua | Aldaketa |
|---|---|---|---|---|
| 1 | 2026-09-04 | Segurtasun arduraduna | Segurtasun Batzordea | Hasierako edizioa |
| | | | | |