

information_security_policy

Informazioaren Segurtasun Politika

Zabala Gailetak S.A

Dokumentuaren IDa: ISP-001

Bertsioa: 1.0

Data: 2026ko Urtarrilaren 8a

Sailkapena: Barne Erabilera

Jabea: Informazioaren Segurtasuneko Arduradun Nagusia (CISO)

Berrikuspen Maiztasuna: Urterokoa

Hurrengo Berrikuspen Data: 2027ko Urtarrilaren 8a

1. Dokumentuaren Kontrola

1.1 Bertsio Historia

Bertsioa	Data	Egilea	Aldaketak
1.0	2026-01-08	CISO	Hasierako politikaren sorrera

1.2 Onarpena

Rola	Izena	Sinadura	Data
Zuzendari Nagusia (CEO)	[Izena]		
Informazioaren Segurtasuneko Arduradun Nagusia (CISO)	[Izena]		
Aholtzulari Juridikoa	[Izena]		

1.3 Banaketa

Politika hau honako hauei banatzen zaie:

- Langile guztiak (egonkorra eta aldi baterakoak)
- Kontratistak eta aholtzulariak
- Sistemarako sarbidea duten hirugarrenen zerbitzu hornitzaleak
- Administrazio Kontseilua (laburpen exekutiboa)

2. Helburua eta Esparrua

2.1 Helburua

Informazioaren Segurtasun Politika honek Zabala Gailetak-en informazio-aktiboak babesteko esparrua

ezartzen du, IT sistemak, teknologia operatiboa (OT), negozio-datuak, bezeroen informazioa eta jabetza intelektuala barne. ISO/IEC 27001:2022, GDPR eta Spainiako legedi garrantzitsua (DBLO-GDD) betetzen dela ziurtatzen du.

2.2 Esparrua

Politika hau honako hauei aplikatzen zaie:

- Zabala Gaietak-en jabetzakoak edo kontrolpekoak diren informazio-aktibo guztiak
- Konpainiaren informazioa sartzen diren langile, kontratista, aholkulari eta hirugarren guztiak
- IT sistema guztiak (web aplikazioak, datu-baseak, hodeiko zerbitzuak)
- OT sistema guztiak (PLCak, SCADA, fabrikazio-ekipamendua)
- Instalazio fisikoak eta paperezko informazioa
- Urruneko lan-inguruneak eta BYOD (Bring Your Own Device) eszenatokiak

2.3 Salbuespenak

Politika honek ez ditu estaltzen:

- Negozio helburuetarako erabiltzen ez diren informazio pertsonaleko sistemak
- Hirugarrenen jabetzakoak diren informazio-sistemak, non Zabala Gaietak bezeroa den (akordio bereizien pean estalita)

3. Politika Adierazpena

Zabala Gaietak konprometituta dago bere informazio-aktiboen konfidentzialtasuna, osotasuna eta eskuragarritasuna babestera. Informazioaren segurtasuna negozioaren erraztailea da, ez oztopo bat, eta ezinbestekoa da bezeroen konfiantza, araudiaren betetzea eta galeta-fabrikazioaren industrian abantaila lehiakorra mantentzeko.

3.1 Zuzendaritzaren Konpromisoa

Zuzendaritza Exekutiboak honako konpromisoak hartzen ditu:

- Informazioaren segurtasunerako baliabide egokiak eskaintza
- Lege eta arauzko baldintzak betetzen direla ziurtatzea
- Erakunde osoan segurtasunaren inguruko kultura sustatzea
- Informazioaren Segurtasuna Kudeatzeko Sistema (ISMS) aldizka berrikusi eta hobetzea
- Segurtasun politika eta prozedurak jarraituz eredu ematea

3.2 Informazioaren Segurtasun Helburuak

1. **Konfidentzialtasuna:** Informazio sentikorra baimenik gabeko zabalkundetik babestea
2. **Osotasuna:** Informazioaren eta sistemen zehaztasuna eta osotasuna ziurtatzea
3. **Eskuragarritasuna:** Behar denean informaziorako baimendutako sarbidea ziurtatzea (%99.5eko uptime helburua)
4. **Betetzea:** Lege, arauzko eta kontratuzko betebehar guztiak betetzea
5. **Erresilientzia:** Negozio-eragiketak mantentzea segurtasun-intzidentzien bitartean eta ondoren
6. **Etengabeko Hobekuntza:** Segurtasun-jarrera aldizka ebaluatu eta hobetzea

4. Rolak eta Erantzukizunak

4.1 Zuzendari Nagusia (CEO)

- Informazioaren segurtasunaren azken erantzulea
- Informazioaren segurtasun politika eta aurrekontua onartzea
- Negoziaren jarraitutasuna eta hondamendien berreskuratze planak ziurtatzea
- Segurtasun gaien berri ematea Administrazio Kontseiluari

4.2 Informazioaren Segurtasuneko Arduradun Nagusia (CISO)

- ISMSa garatu, ezarri eta mantentzea
- Arriskuen ebaluazioak eta segurtasun-auditoriak egitea
- Segurtasun-intzidentziak kudeatu eta erantzuna koordinatzea
- Segurtasun-kontzientziajio prestakuntza ematea
- Segurtasun-metrikak zuzendaritza exekutiboari jakinaraztea
- Arau-agintariekin eta kanpo-auditroekin harremanetan jartzea

4.3 IT Arduraduna

- Segurtasun kontrol teknikoak ezartzea
- Sarbide-kontrol eta autentifikazio-sistemak kudeatzea
- Sistemaren adabakiak eta eguneraketak mantentzea
- Ohiko segurtasun-kopiak eta berreskuratze-probak egitea
- Sistema-erregistroak eta segurtasun-gertaerak monitorizatzea

4.4 OT/Produkzio Arduraduna

- Kontrol-sistema industrialak ziurtatzea (PLCak, SCADA)
- IT eta OT sareen arteko segmentazioa ezartzea
- Produkzio-eremuetako sarbide fisikoa kudeatzea
- OT segurtasuna IT segurtasun taldeekin koordinatzea
- Fabrikazio-prozesuetan segurtasuna eta babesa ziurtatzea

4.5 Datuen Babeserako Ordezkaria (DPO)

- GDPR betetzea ziurtatzea
- Datu-interesdunen eskubideen eskaerak kudeatzea
- Tratamendu-jardueren registroa mantentzea (ROPA)
- Datuen Babesaren gaineko Eraginaren Ebaluazioa (DPIA/EIPD) egitea
- Datu-urraketak Datuak Babesteko Espainiako Bulegoari (AEPD) jakinaraztea

4.6 Saitetako Kudeatzaileak

- Langileek segurtasun-politikak jarraitzen dituztela ziurtatzea
- Saileko informazio-aktiboak identifikatu eta sailkatzea
- Segurtasun-intzidentziak berehala jakinaraztea
- Negoziaren jarraitutasun plangintzan parte hartzea
- Bere taldekideen sarbide-eskaerak onartzea

4.7 Langile Guztiak

- Informazioaren segurtasun politika eta prozedura guztiak betetzea
- Derrigorrezko segurtasun-kontzientziajio prestakuntza osatzea
- Segurtasun-intzidentziak eta ahultasunak jakinaraztea
- Pasahitzak eta autentifikazio-kredentzialak babestea

- Informazio-aktiboak baimendutako negozio-helburuetarako soilik erabiltzea
- Erabilera Onargarriaren Politika sinatu eta atxikitzea

4.8 Hirugarrenak eta Kontratistak

- Konfidentzialtasun-hitzarmenak sinatzea (NDA)
- Zabala Gaietak-en segurtasun-politikak betetzea
- Sistemara sartu aurretik segurtasun-egiaztapena pasatzea
- Konpromisoan zehar edozein segurtasun-kezka jakinaraztea
- Kontratua amaitzean informazio-aktibo guztiak itzultzea

5. Informazioaren Segurtasun Esparrua

5.1 Informazioaren Segurtasuna Kudeatzeko Sistema (ISMS)

Zabala Gaietak-ek ISO/IEC 27001:2022 arauan oinarritutako ISMS bat darabil, PDCA (Plan-Do-Check-Act) zikloa ezarriz:

- **Plangintza (Plan):** Arriskuen ebaluazioa, segurtasun-helburuak, tratamendu-planak
- **Egitea (Do):** Kontrolak, politikak, prozedurak, prestakuntza ezartzeari buruzko lanak
- **Egiaztatzea (Check):** Barne-auditoria, monitorizazioa, metrikak, kudeaketa-berrikuspena
- **Jokatzea (Act):** Ekintza zuzentzaileak, etengabeko hobekuntza, ikasitako ikasgaiak

5.2 Arriskuen Kudeaketa

Arriskuen ebaluazioa urtero egiten da edo aldaketa garrantzitsuak gertatzen direnean:

1. **Aktiboen Identifikazioa:** Informazio-aktiboen inventarioa (ikus Aktiboen Erregistroa)
2. **Mehatxuen Ebaluazioa:** Mehatxu potentzialak identifikatu (zibererasoak, hondamendi naturalak, giza akatsak)
3. **Ahultasunen Analisia:** Sistemen eta prozesuen ahuleziak ebaluatu
4. **Arriskuen Ebaluazioa:** Arrisku maila kalkulatu ($\text{Probabilitatea} \times \text{Eragina}$)
5. **Arriskuen Tratamendua:** Arriskuak onartu, arindu, transferitu edo saihestu
6. **Hondar Arriskua:** Geratzen diren arriskuak dokumentatu eta onartu

Arriskuen Apetitoa: Zabala Gaietak-ek arrisku baxuak eta ertainak onartzen ditu kontrol egokiekin. Arrisku altuek exekutiboen onarpena eta arintze-planak behar dituzte.

5.3 Segurtasun Kontrolak

Segurtasun kontrolak ISO/IEC 27001:2022 Anexo A-tik hautatzen dira (ikus Aplikagarritasun Adierazpena). Kontrolak honela sailkatzen dira:

- **Prebentiboak:** Segurtasun-intzidentziak gertatu aurretik geldiaraztea (suebakiak, sarbide-kontrola)
- **Detektiboak:** Segurtasun-intzidentziak gertatzen direnean identifikatzea (SIEM, IDS, auditoriak)
- **Zuzentzaileak:** Intzidentzien eragina minimizatu eta berreskuratzea (segurtasun-kopiak, intzidentzien erantzuna)

6. Segurtasun Politika Gakoak

Informazioaren Segurtasun Politika orokor hau politika eta prozedura zehatzekin babesten da:

6.1 Sarbide Kontrolerako Politika

- Pribilegio Txikienaren Printzipioa:** Erabiltzaileek lan-funtzioetarako beharrezkoan den gutxieneko sarbidea jasotzen dute
- Eginkizunen Bereizketa:** Funtzio kritikoek pertsona bat baino gehiago behar dute
- Erabiltzaile Kontuen Kudeaketa:** Hornikuntza, aldaketa eta baja prozedurak
- Pasahitz Politika:** Ikus Pasahitz Politika dokumentu espezifikoa
- Faktore Anitzeko Autentifikazioa (MFA):** Derrigorrezko urruneko sarbiderako eta pribilegiatutako kontuetarako
- Sarbide Berrikuspena:** Erabiltzaileen sarbide-eskubideen hiruhileko berrikuspena

6.2 Erabilera Onargarriaren Politika

- Ikus Erabilera Onargarriaren Politika dokumentu espezifikoa
- IT baliabideen, posta elektronikoaren, interneten eta gailu mugikorren erabilera egokia estaltzen du
- Baimenik gabeko softwarea, legez kanpoko jarduerak eta arrazoizko mugatik gorako erabilera pertsonala debekatzen ditu

6.3 Datuen Sailkapena eta Kudeaketa

Informazioa lau mailatan sailkatzen da:

Sailkapena	Definizioa	Adibideak	Kudeaketa Baldintzak
Publikoa	Zabalkunde publikorako informazioa Marketing materialak,		
prentsa-oharrak	Ez dago murritzeta berezirik		
Barnekoa	Barne erabilerarako informazioa soilik	Barne oharrak,	
bilera-notak	Email enkriptatzea, barne sareak soilik		
Konfidentziala	Negoziointormazio sentikorra	Bezeroen datuak,	
finantza-txostenak, errezetak	Enkriptatzea geldirik eta trantsitoan,		
sarbide-kontrola			
Oso Konfidentziala	Zabaltzeak kalte larriak eragin ditzakeen informazio kritikoa		Merkataritza-sekretuak,
PII, ordainketa-txartelen datuak	Enkriptatze sendoa, MFA, auditoretza		

erregistroa, DLP

Kudeaketa Baldintzak:

- Dokumentu guztiak dagokien sailkapenarekin etiketatzea
- Konfidentziala eta Oso Konfidentziala den datua enkriptatzea
- Fitxategi-transferentzia segurua erabiltzea kanpoan partekatzeko
- Datu sentikorrik dituzten dokumentu fisikoak txikitzea
- Datu-urraketak aurkitu eta ordubeteko epean jakinaraztea

6.4 Datuen Babes eta Pribatasun Politika

- GDPR (EB 2016/679 Erregelamendua) eta DBLO-GDD (Espainiako 3/2018 Lege Organikoa) betetzea
- Tratamendurako oinarri juridikoa: baimena, kontratua, legezko betebeharra, interes legitimoa
- Datuen minimizazioa: beharrezkoak diren datuak soilik biltzea
- Helburuaren mugatzea: datuak adierazitako helburuetarako soilik erabiltzea
- Datu-interesdunen eskubideak: sarbidea, zuzenketa, ezabaketa, eramangarritasuna, aurkaritzza (ikus Datu-Interesdunen Eskubideen Prozedurak)
- Datuen atxikipena: ikus Datuen Atxikipen Egutegia
- Nazioarteko transferentziak: Klausula Kontratu Estandarrak (SCC) erabiltzea EBtik kanpoko transferentziatarako
- Datu-urraketaren jakinarazpena: AEPDri jakinaraztea 72 orduko epean pertsonentzat arriskua badago

6.5 Sare Segurtasun Politika

IT Sarea:

- Suebaki bidezko babes sareko perimetro guztieta
- Sare segmentazioa: produkzioa, bulegoa, gonbidatuen WiFi-a, DMZ
- Intrusioak Detektatzeko/Prebenitzeko Sistemak (IDS/IPS)
- VPN beharrezkoa urruneko sarbiderako (AES-256 enkriptatzea)
- Erabiltzen ez diren sare-zerbitzuak eta portuak desgaitzea
- Aldizkako ahultasun eskanearaztea (hilero)

OT Sarea:

- Air-gap edo suebaki arau zorrotzak IT eta OT sareen artean
- Interneteko sarbide zuzenik ez OT sistemetarako
- Zerrenda zurien ikuspegia OT komunikazioetarako
- Sarbide fisikoaren kontrola OT sareko ekipamendura
- Aldaketa-kudeaketa OT sareko aldaketa guztieta

WiFi Segurtasuna:

- WPA3 enkriptatzea WiFi korporatiborako
- Gonbidatuen WiFi bereizia atari gatibuarerek eta interneterako sarbidea soilik
- MAC helbideen iragazketa OT haririk gabeko gailuetarako
- Rogue access point eskanearaztea aldizka

6.6 Sistemen Garapen eta Mantentze Politika

- Software Seguruaren Garapen Bizi-zikloa (SSDLC)
- Garapena, probak eta produkzio inguruneak bereizita
- Kode berrikuspena eta segurtasun proba estatikoak/dinamikoak
- Dependentzien eskaneatzea ahultasunetarako (OWASP Dependency-Check)
- Aldaketa-kudeaketa prozesua sistema aldaketa guztieta rako
- Segurtasun probak produkzioan hedatu aurretik
- Hornitzaleen segurtasun ebaluazioa hirugarrenen softwarerako

6.7 Segurtasun-kopia eta Berreskuratze Politika

- **Segurtasun-kopien Maiztasuna:**
 - Sistema kritikoak: Eguneroko inkrementala, asteko osoa
 - Datu-baseak: Denbora errealeko erreplikazioa + egunerako kopiak
 - OT konfigurazioak: Aldaketan aurretik eta ondoren
- **Biltegiratzea:** Enkriptatuta, gunetik kanpoko biltegiratzea (3-2-1 araua: 3 kopia, 2 euskarri mota, 1 gunetik kanpo)
- **Atxikipena:** 30 egun linean, urtebeteko artxiboa
- **Berreskuratze Probak:** Hiruhileko berreskuratze simulazioak
- **Berreskuratze Denbora Helburua (RTO):** 4 ordu sistema kritikoetarako
- **Berreskuratze Puntu Helburua (RPO):** Ordu bateko datu-galera gehienez

6.8 Intzidentzien Kudeaketa Politika

- **Intzidentzia Definizioa:** Konfidentialitasuna, osotasuna edo eskuragarritasuna mehatxatzen duen edozein gertaera
- **Jakinarazpena:** Intzidentzia guztiak ordubeteko epean jakinaraztea security@zabalagailetak.com bidez edo intzidentzia telefono bidez
- **Sailkapena:** Kritikoa, Altua, Ertaina, Baxua eraginaren eta urgentziaren arabera
- **Erantzun Taldea:** CISO, IT Arduraduna, Lege Saila, DPO, PR (intzidentzia kritikoetarako)
- **Erantzun Prozesua:**
 - Detekzioa eta jakinarazpena
 - Hasierako ebaluazioa eta eustea
 - Ikerketa eta ebidentzia bilketa
 - Ezabapena eta berreskuratzea
 - Intzidentzia osteko berrikuspena eta ikasitako ikasgaiak
- **Komunikazioa:** Kaltetutako alderdiei, erregulatzaleei (beharrezkoan baino) eta zuzendaritzari jakinaraztea
- **Dokumentazioa:** Intzidentzia erregistroa eta auzitegi-ebidentzia mantentzea (ikus Audit Log)

6.9 Negozioaren Jarraitutasuna eta Hondamendien Berreskuratze Politika

- Ikus Negozioaren Jarraitutasun Plana dokumentu espezifikoa
- Negozioaren Eraginaren Analisia (BIA) urtero egina
- Etenaldi Jasangarriaren Gehieneko Epea (MTPD): 24 ordu prozesu kritikoetarako
- Hondamendien berreskuratze prozedurak IT eta OT sistematarako
- Lan-antolamendu alternatiboak (urruneko lana, babeskopia instalazioak)
- Urteroko mahai-gaineko ariketak eta bi urtean behingo simulazio osoak

6.10 Segurtasun Fisiko eta Ingurumenekoa

Datu Zentroa eta Zerbitzari Gela:

- Sarbide kontrola (txartela + biometrikoak)
- 24/7 bideo zaintza (90 eguneko atxikipena)

- Ingurumenaren monitorizazioa (temperatura, hezetasuna)
- Suteak itzaltzeko sistema (FM-200 edo baliokidea)
- Etenik Gabeko Elikatze Sistema (UPS) eta sorgailu laguntzailea

Produkzio Instalazioak:

- Permetroko segurtasuna (hesia, argiztapena, kamerak)
- Bisitarien kudeaketa (sinadura, laguntzaileak)
- Informazio sentikorra duten hondakinen deuseztapen segurua
- Mahai garbia eta pantaila garbia politika

Gailu Mugikorrak eta Ordenagailu Eramangarriak:

- Disko osoaren enkriptatzea (BitLocker, FileVault)
- Gailu Mugikorren Kudeaketa (MDM) konpainiako gailuetarako
- Galdutako/lapurtutako gailuak urrunetik garbitzeko gaitasuna
- Pantaila blokeo automatikoa 5 minuturen ondoren

6.11 Hirugarren eta Hornitzairen Segurtasun Politika

- Segurtasun ebaluaziona kontratatu aurretik
- Kontratu-segurtasun baldintzak akordio guztietai
- Konfidentzialtasun Hitzarmenak (NDA) datu Konfidentzialetarako sarbidea izateko
- Segurtasun berrikuspen erregularrak hornitzairen kritikoentzat
- Hornitzairen segurtasun kontrolak auditatzeko eskubidea
- Sarbidea eta datuak itzultzeko amaiera-prozedurak

6.12 Kontrol Kriptografikoen Politika

- **Enkriptatze Estandarrak:**
 - Datuak geldirik: AES-256
 - Datuak trantsitoan: TLS 1.3 edo altuagoa
 - VPN: AES-256 IKEv2/IPsec-ekin
- **Gakoen Kudeaketa:**
 - Gakoen kudeaketa sistema zentralizatua
 - Gakoen txandakatzea 12 hilabetero
 - Gako biltegiratze segurua (HSM gako kritikoetarako)
 - Negozioaren jarraitutasunerako gako fidantza (key escrow)
- **Sinadura Digitalak:** RSA 2048-bit edo ECDSA P-256
- **Hashing:** SHA-256 edo altuagoa (ez MD5 edo SHA-1)
- **Pasahitz Biltegiratzea:** bcrypt 12+ errondarekin edo Argon2

6.13 Segurtasun Monitorizazio eta Erregistro Politika

- **Erregistro Baldintzak:** Autentifikazioa, sarbide-kontrola, sistema aldaketak, segurtasun gertaerak
- **Erregistro Atxikipena:** Gutxienez urtebetetik (legezko betekizuna), 3 urte sistema kritikoetarako
- **SIEM (Security Information and Event Management):** Denbora errealeko erregistro korrelazioa eta alertak
- **Erregistro Babesa:** Manipulazioen aukakoa, enkriptatua, sarbide-kontrolatua
- **Berrikuspen Maiztasuna:** Denbora errealeko analisi automatizatua, asteko eskuzko berrikuspena
- **Alertak:** Alerta kritikoak segurtasun taldeari 24/7

7. Betetzea eta Lege Baldintzak

7.1 Araudi Betetzea

Zabala Gaietak-ek honako hauek betetzen ditu:

- **GDPR (EB 2016/679):** Datuen Babeserako Erregelamendu Orokorra
- **DBLO-GDD (Espainiako 3/2018 Lege Organikoa):** Espainiako datuen babeserako legea
- **ePrivacy Zuzentaraua (2002/58/EE):** Komunikazio elektronikoen pribatutasuna
- **PCI DSS:** Ordaintza Txartelen Industriaren Datuen Segurtasun Estandarra (txartel bidezko ordainketak prozesatzen badira)
- **ISO/IEC 27001:2022:** Informazioaren Segurtasuna Kudeatzeko ziurtagiri helburua
- **Espainiako Zigor Kodea (197. artikulua):** Datu pertsonalen legez kanpoko zabalkundea
- **Langileen Estatutua:** Langileen pribatutasuna eta monitorizazioa
- **Elikagaien Segurtasun Araudiak:** GMP, HACCP (zeharka datuen osotasunari eragiten dio)

7.2 Kontratuzko Betebeharra

- Bezeroen datuak babesteko klausulak salmenta-akordioetan
- Hornitzaleen segurtasun baldintzak kontratacio-kontratuetaan
- Aseguru-polizen betetzea (ziber-aseguru baldintzak)
- Banku eta ordainketa-prozesadoreen segurtasun estandarrak

7.3 Jabetza Intelektualaren Babesa

- Merkataritza-sekretuen babesia gaitza errezeptetarako eta fabrikazio-prozesuetarako
- Copyright babesia softwarerako, dokumentaziorako, marketing materialetarako
- Zabala Gaietak markaren babesia
- Patenteen babesia fabrikazio-teknika berritzaleetarako (badaagokio)

8. Segurtasun Kontzientzia eta Prestakuntza

8.1 Prestakuntza Programa

Langile guztiekin jasotzen dute:

- **Kontratacio Berrien Prestakuntza:** Segurtasun oinarriak lehen astean
- **Urteroko Freskatze Prestakuntza:** Derrigorrezkoa langile guztientzat (2 ordu)
- **Rol Espezifikoko Prestakuntza:**
 - Garatzaileak: Kodeketa segura, OWASP Top 10 (8 ordu urtero)
 - Sistema Administratzialeak: Hardening, monitorizazioa, intzidentziaren erantzuna (16 ordu urtero)
 - Zuzendaritza: Arriskuen kudeaketa, legezko betebeharra (4 ordu urtero)
 - Produkzio Langileak: OT segurtasuna, segurtasun fisikoa (4 ordu urtero)
- **Phishing Simulazioak:** Hiruhileko phishing kanpaina simulatuak
- **Segurtasun Buletina:** Hilera segurtasun aholkuak eta mehatxuen eguneraketak

8.2 Prestakuntza Gaiak

- Pasahitz segurtasuna eta MFA
- Phishing eta gizarte-ingeniaritza
- Datuen sailkapena eta kudeaketa
- IT baliabideen erabilera onargarria
- Intzidentziak jakinarazteko prozedurak

- GDPR eta datuen babesia
- Segurtasun fisikoa eta mahai garbia
- Urruneko lan-praktika seguruak

8.3 Prestakuntza Metrikak

- Prestakuntza osatze-tasa: %100 helburua
 - Phishing simulazioan klik tasa: <%10 helburua
 - Intzidentziak jakinarazteko erantzun-denbora: <1 ordu helburua
 - Prestakuntzaren eraginkortasunaren ebaluazioa galdetegi eta ariketa praktikoen bidez
-

9. Monitorizazioa eta Berrikuspena

9.1 Errendimendu Neurketa

Funtsezko Errendimendu Adierazleak (KPIak):

KPI	Helburua	Neurketa Maiztasuna
Sistema eskuragarritasuna	%99.5	Hilero
Segurtasun intzidentziak	<10 ertain/urtean	Hiruhilero
Adabaki betetzea	%95 adabaki kritiko 7 egunetan	Hilero
Sarbide berrikuspen osatzea	%100 hiruhilero	Hiruhilero
Prestakuntza osatzea	%100 urtero	Urtero
Segurtasun-kopia arrakasta tasa	%99	Egunero
Phishing simulazio klik tasa	<%10	Hiruhilero
Detektatzeko Batezbesteko Denbora (MTTD)	<2 ordu	Intzidentziako
Erantzuteko Batezbesteko Denbora (MTTR)	<4 ordu	Intzidentziako

9.2 Barne Auditoriak

- Urteroko ISMS barne-auditoria ISO 27001 arauaren aurka
- Hiruhileko ahultasun teknikoen ebaluazioak
- Kanpo-auditoreek egindako urtean bitan penetrazio-probak
- Auditoria-aurkikuntzak jarraitu eta adostutako epeetan konpondu

9.3 Kudeaketa Berrikuspena

- Hiruhileko segurtasun metrikak zuzendaritza exekutiboari aurkeztu
- Urteroko ISMS berrikuspena CEO eta goi-zuzendaritzaren eskutik
- Berrikuspen agenda:
 - Auditoria emaitzak eta ekintza zuzentzaileak
 - Segurtasun intzidentziak eta joerak

- KPIen aurkako errendimendua
 - Arriskuen ebaluazio eguneraketak
 - Lege/arau baldintzen aldaketak
 - Baliabide beharrak eta aurrekontua
 - Etengabeko hobekuntza aukerak
-

10. Politikaren Betearazpena

10.1 Betetze Monitorizazioa

- Segurtasun taldeak politikaren betetzea monitorizatzen du honako bidez:
 - Segurtasun tresna automatizatuak (SIEM, DLP, endpoint babesia)
 - Sarbide kontrol erregistroak eta auditoria arrastoak
 - Ohiko sarbide berrikuspenak
 - Ausazko egiaztapenak eta ikuskapenak
 - Langileen jakinarazpenak eta salaketa mekanismoak

10.2 Urratsak eta Diziplina Neurriak

Politika hau urratzeak honakoak ekar ditzake:

1. **Lehen Urraketa (Arina):** Ahozko ohartarazpena eta berriro prestatzea
2. **Bigarren Urraketa edo Urraketa Larria:** Idatzizko ohartarazpena eta errendimendua hobetzeko plana
3. **Urraketa Oso Larriak edo Errepikatuak:** Etenaldia, kaleratzea edo legezko ekintzak

Urraketa Adibideak:

- Arina: Pasahitz ahula, desblokeatutako lan-estazioa zaintzarik gabe
- Larria: Pasahitzak partekatzea, baimenik gabeko software instalazioa, politika ez betetzea ohartarazpenaren ondoren
- Oso Larria: Nahita egindako datu-urraketa, jarduera maltzurra, iruzurra, informazio lapurreta

Diziplina-ekintza guztiak Espainiako lan-legearekin eta lan-kontratuekin bat dator.

10.3 Salbuespenak eta Uko Egiteak

- Politika salbuespenek CISOren eta dagokion departamentuko arduradunaren idatzizko onarpena behar dute
 - Salbuespenak denbora mugatukoak dira (gehienez 6 hilabete) eta dokumentatuak
 - Konpentsazio-kontrolak ezarri behar dira
 - Salbuespenak hiruhilero berrikusten dira
-

11. Politikaren Mantentzea

11.1 Berrikuspena eta Eguneraketak

- **Urteroko Berrikuspena:** Politika Urtarrilero berrikusten da
- **Ad-hoc Eguneraketak:** Aldaketa garrantzitsuak gertatzen direnean:
 - Lege baldintza berriak
 - Segurtasun intzidentzia nagusiak

- Erakunde aldaketak
- Teknologia aldaketak
- Politika eguneratzea eskatzen duten auditoria aurkikuntzak

11.2 Aldaketa Kudeaketa

Politika aldaketek prozesu hau jarraitzen dute:

1. Eguneraketa zirriborroa CISO edo politika jabearen aldetik
2. Lege, DPO, IT Arduradunaren berrikuspena
3. CEOren onarpena
4. Langile guztiei jakinaraztea
5. Prestakuntza eguneraketak beharrezkoa bada
6. Bertsio kontrola eta artxibatzea

11.3 Dokumentu Biltegiratzea

- Kopia maisua ISMS dokumentu biltegian gordeta
- Bertsio-kontrolatua eta sarbide-mugatua
- Artxibatutako bertsioak 10 urtez gordeta (legezko betekizuna)

12. Lotutako Dokumentuak

- Aplikagarritasun Adierazpena (SOA) - Dokumentuaren IDa: SOA-001
- Erabilera Onargarriaren Politika - Dokumentuaren IDa: AUP-001
- Pasahitz Politika - Dokumentuaren IDa: PWD-001
- Negozioaren Jarraitutasun Plana - Dokumentuaren IDa: BCP-001
- Aktiboen Erregistroa - Dokumentuaren IDa: ASR-001
- Arriskuen Ebaluazio Txostena - Dokumentuaren IDa: RAR-001
- Intzidentzien Erantzun Procedura - Dokumentuaren IDa: IRP-001
- Datuen Babesaren gaineko Eraginaren Ebaluazio Txantiloia - Dokumentuaren IDa: DPIA-001
- Datu Urraketa Jakinarazpen Txantiloia - Dokumentuaren IDa: DBN-001
- Datu Interesdunen Eskubideen Prozedurak - Dokumentuaren IDa: DSR-001

13. Harremanetarako Informazioa

13.1 Segurtasun Taldearen Kontaktuak

Informazioaren Segurtasuneko Arduradun Nagusia (CISO)

Email: ciso@zabalagaietak.com

Telefonoa: +34 XXX XXX XXX

Bulegoa: A Eraikina, 201 Gela

IT Segurtasun Taldea

Email: security@zabalagaietak.com

Telefonoa: +34 XXX XXX XXX (24/7 Segurtasun Telefonoa)

Datuen Babeserako Ordezkaria (DPO)

Email: dpo@zabalagaietak.com

Telefonoa: +34 XXX XXX XXX

Intzidentzia Jakinarazpena

Email: incident@zabalagaitak.com

Telefonoa: +34 XXX XXX XXX (24/7)

Barne Luzapena: 911

13.2 Kanpo Kontaktuak

Datuak Babesteko Espainiako Bulegoa (AEPD)

Webgunea: <www.aepd.es>

Telefonoa: +34 901 100 099

Helbidea: C/ Jorge Juan, 6, 28001 Madrid

INCIBE (Zibersegurtasuneko Institutu Nazionala)

Telefonoa: +34 017 (24/7 zibersegurtasun intzidentziak)

Webgunea: <www.incibe.es>

14. Aitorta

Langile guztiak politika hau jaso eta ulertu dutela aitortu behar dute:

Aitortzen dut Zabala Gaietak-en Informazioaren Segurtasun Politika jaso, irakurri eta ulertu dudala. Baldintza guztiak betetzea onartzen dut eta ulertzen dut urraketek diziplina-ekintzak ekar ditzaketela, enplegu edo kontratuaren amaiera barne.

Langilearen Izena: _____

Langilearen IDa: _____

Sinadura: _____

Data: _____

Eranskina A: Definizioak eta Akronimoak

Informazio Aktiboa: Erakundearrentzat balioa duen edozein datu, sistema edo baliabide

Informazioaren Segurtasuna: Informazioa baimenik gabeko sarbide, erabilera, zabalkunde, eten, aldaketa edo suntsipenetik babestea

Konfidentialtasuna: Informazioa baimendutako pertsonek soilik eskura dezaketela ziurtatzea

Osotasuna: Informazioaren zehaztasuna eta osotasuna ziurtatzea

Eskuragarritasuna: Behar denean informaziorako baimendutako sarbidea ziurtatzea

CIA Hirukotea: Konfidentialtasuna, Osotasuna, Eskuragarritasuna - informazioaren segurtasunaren hiru zutabeak

ISMS: Information Security Management System - informazioaren segurtasuna kudeatzeko sistema sistematikoa

Arriskua: Mehatxu batek ahultasun bat ustiatzen duenean galera edo kaltea izateko potentziala

Mehatxua: Nahi ez den intzidentzia baten kausa potentziala

Ahultasuna: Mehatxu batek ustiatu dezakeen ahulezia

Kontrola: Arriskua aldatzen duen neurria

PII: Personally Identifiable Information (Informazio Pertsonal Identifikagarria)

GDPR: General Data Protection Regulation (Datuen Babeserako Erregelamendu Orokorra)

AEPD: Datuak Babesteko Espainiako Bulegoa

DPO: Data Protection Officer (Datuen Babeserako Ordezkaria)

SIEM: Security Information and Event Management

IDS/IPS: Intrusion Detection/Prevention System

MFA: Multi-Factor Authentication (Faktore Anitzeko Autentifikazioa)

VPN: Virtual Private Network (Sare Pribatu Birtuala)

DMZ: Demilitarized Zone (sare segmentua)

OT: Operational Technology (teknologia operatiboa / kontrol sistema industrialak)

PLC: Programmable Logic Controller (Kontrolatzaile Logiko Programagarria)

SCADA: Supervisory Control and Data Acquisition

RTO: Recovery Time Objective (Berreskuratze Denbora Helburua)

RPO: Recovery Point Objective (Berreskuratze Puntu Helburua)

MTPD: Maximum Tolerable Period of Disruption (Etenaldi Jasangariaren Gehieneko Epea)

BIA: Business Impact Analysis (Negoziaren Eraginaren Analisia)

DLP: Data Loss Prevention (Datu Galeraren Prebentzioa)

MDM: Mobile Device Management (Gailu Mugikorren Kudeaketa)

HSM: Hardware Security Module

OWASP: Open Web Application Security Project

PCI DSS: Payment Card Industry Data Security Standard

DOKUMENTUAREN AMAIERA