

# training\_exercises\_plan

## NIS2 Formakuntza eta Simulakro Plana

### NIS2 Training & Exercises Plan

Dokumentu Kodea: NIS2-TRAIN-001

Bertsioa: 1.0

Data: 2026-02-06

Jabea: CISO + RRHH

NIS2 Artikulua: Art. 20.2 (Zuzendaritza), Art. 21.2.a (Ziber-higienea)

#### 1. HELBURUA

Plan honek definitzen du Zabala Gailetak-eko langileen zibersegurtasun formakuntza programa, NIS2 Direktibak eskatzen duen moduan. Helburu nagusiak:

- Art. 20.2:** Zuzendaritzak arriskuen kudeaketa neurrien formakuntza jaso behar du.
- Art. 21.2.a:** Langile guztiek oinarritzko ziber-higienea ikasi behar dute.
- CSIRT prestakuntza:** Intzidentzia erantzun taldeak simulakroak egin behar ditu.




#### 2. FORMAKUNTZA PROGRAMA

##### 2.1 Zuzendaritzarentzako Formakuntza (Art. 20.2 — Nahitaezkoa)





Ikastaroa	Edukia	Iraupena	Maiztasuna	Parte-hartzaileak	Egoera
NIS2 Executive Briefing	NIS2 betebeharrak, zigorak, gobernantza, erantzukizun pertsonala	4h	Urtekoa	CEO, CFO, COO, CISO	🕒 Q2 2026
Ziber-arrisku kudeaketa	Arrisku ebaluazioa, SoA, tratamendu plana, metrikak	4h	Urtekoa	Zuzendaritza + CISO	🕒 Q2 2026
Intzidentzia simulakro (TTX)	Tabletop exercise: ransomware eszenarioa	2h	Hiruhilekoa	Zuzendaritza + CSIRT	🕒 Q2 2026

##### 2.2 Langile Guztientzako Formakuntza (Art. 21.2.a)





Ikastaroa	Edukia	Iraupena	Maiztasuna	Parte-hartzaileak	Egoera
Ziber-higienea orokorra	Pasahitzak, phishing, gizarte ingeniarietza, BYOD, WiFi segurua	2h	Urtekoa	120 langile	🕒 Q2 2026

Ikastaroa	Edukia	Iraupena	Maiztasuna	Parte-hartzaileak	Egoera
Phishing simulazioa	Phishing email simulatuak + feedback	30min	Hilero	120 langile	 Hilero
GDPR & Datu Babesa	Datu pertsonalen kudeaketa, ihes jakinarazpena	1h	Urtekoa	120 langile	 Q2 2026
Clean Desk & Screen Lock	Segurtasun fisikoa eta digitala	30min	Urtekoa	120 langile	 Q2 2026


## 2.3 IKT/IT Taldearen Formakuntza


Ikastaroa	Edukia	Iraupena	Maiztasuna	Parte-hartzaileak	Egoera
SIEM kudeaketa (Wazuh)	Alerta triage, korrelazio arauak, dashboard-ak	8h	Urtekoa	IT taldea (5)	 Q2 2026
Intzidentzia erantzuna (IR)	NIST framework, forentse oinarriak, ebidentzia bilketa	16h	Urtekoa	IT + CSIRT	 Q2 2026
Secure Coding	OWASP Top 10, sarrera balioztatze, SQL injection prebentzioa	8h	Urtekoa	Garapentzaileak	 Q3 2026
Cloud segurtasuna	AWS/GCP segurtasuna, IAM, logging	4h	Urtekoa	IT taldea	 Q3 2026

## 2.4 CSIRT Taldearentzako Formakuntza

Ikastaroa	Edukia	Iraupena	Maiztasuna	Parte-hartzaileak	Egoera
NIS2 jakinarazpen drill	24h/72h workflow praktika txantiloiekin	2h	Hiruhilekoa	CSIRT osoa	 Q2 2026
Forensic workshop	RAM analisia (Volatility), disk analisia, malware triage	8h	Urtekoa	CSIRT teknikoak	 Q3 2026
Threat hunting	MITRE ATT&CK, SIEM hunting queries, IOC bilaketa	8h	Urtekoa	SOC + CSIRT	 Q3 2026
Ransomware response	Ransomware ezaugarriak, containment, recovery, No More Ransom	4h	Urtekoa	CSIRT osoa	 Q2 2026








## 2.5 OT Langileen Formakuntza

Ikastaroa	Edukia	Iraupena	Maiztasuna	Parte-hartzaileak	Egoera
OT zibersegurtasuna	IEC 62443, PLC segurtasuna, IT/OT	4h	Urtekoa	OT ingeniariak	 Q3

Ikastaroa	Edukia	Iraupena	Maiztasuna	Parte-hartzaileak	Egoera
	segmentazioa				2026
OT intzidentzia erantzuna	OT erasoak, manual mode, segurtasun protokoloak	4h	Urtekoa	OT + CSIRT	 Q3 2026

### 3. SIMULAKRO / EXERCISE PLANA

#### 3.1 2026 Egutegia

#	Data	Mota	Eszenarioa	Parte-hartzaileak	Iraupena	Egoera
EX-0 1	2026-Q2 (Apr)	Tabletop (TTX)	Ransomware — ekoizpen etendura	Zuzendaritza + CSIRT	3h	
EX-0 2	2026-Q2 (Mai)	NIS2 Notification Drill	24h/72h jakinarazpen praktika	CISO + DPO + Legal	2h	
EX-0 3	2026-Q3 (Jul)	Live Exercise	SIEM alerta → CSIRT aktibazio → containment	CSIRT + IT	4h	
EX-0 4	2026-Q3 (Sep)	OT Tabletop	PLC erasoak — manual mode, isolazioa	OT + CSIRT	3h	
EX-0 5	2026-Q3 (Sep)	BCP/DR Test	Failover + backup restore	IT + Operations	8h	
EX-0 6	2026-Q4 (Oct)	Full-chain Exercise	Phishing → ransomware → NIS2 notification	Guztiak	6h	
EX-0 7	2026-Q4 (Nov)	Data Breach TTX	Datu ihesa → GDPR + NIS2 dual notification	CSIRT + Legal + DPO	3h	

#### 3.2 Simulakro Txosten Txantiloia

Simulakro bakoitzaren ondoren txostena idatzi behar da honako egiturarekin:

1. Laburpen Exekutiboa
2. Eszenarioaren Deskribapena
3. Parte-hartzaileak
4. Kronologia
5. Emaizak:
  - Zer funtzionatu zuen ongi?
  - Zer ez zuen funtzionatu?
  - Detekzio denbora (TTD)
  - Erantzun denbora (TTR)
  - NIS2 timeline-ak bete dira?
6. Gap-ak Identifikatuak
7. Hobekuntza Ekintza Plana
8. Puntuazio Orokorra: /100

Txostenak gorde: evidence-pack/training/YYYY-QX\_exercise\_TYPE.md

---

## 4. PHISHING SIMULAZIO PROGRAMA

### 4.1 Hileko Kanpaina

Hilabetea	Gaia	Zailtasun Maila	Helburu Taldea
Martxoa	Pasahitz berrezartzea (IT txantiloia)	Erraza	Guztiak
Apirila	Faktura faltsua (finantza)	Ertaina	Admin + Kudeaketa
Maiatza	Office 365 login faltsua	Zaila	IT taldea
Ekaina	CEO fraud (whaling)	Oso zaila	Zuzendaritza
Uztaila	OT hornitzaile jakinarazpena	Ertaina	OT taldea
Abuztua	COVID/osasun lotutako	Erraza	Guztiak
Iraila	“Paketea ez da jaso” (kurier)	Ertaina	Guztiak
Urria	LinkedIn konexioa	Zaila	Guztiak
Azaroa	Black Friday eskaintza	Ertaina	Guztiak
Abendua	Gabon oparia	Erraza	Guztiak

### 4.2 KPIak

Metrika	Helburua	Hasierako Balioa
Click rate (hilekoa)	< 5%	Neurtu behar
Report rate (txostena egindakoak)	> 60%	Neurtu behar
Repeat clickers (errepikatutako klik-ak)	< 2%	—
Kontzientzia maila orokorra	> 85%	Neurtu behar

---

## 5. ERAGINKORTASUNAREN EBALUAZIOA

### 5.1 Formakuntza Ebaluazio Metodologia

Neurria	Tresna	Maiztasuna
Pre/Post test (galdetegi)	Google Forms	Ikastaro bakoitzean
Phishing simulazioen emaitzak	GoPhish / KnowBe4	Hilero

Neurria	Tresna	Maiztasuna
Simulakro puntuazioak	Txosten txantiloia	Hiruhilekoa
Intzidentzia metriken bilakaera	SIEM dashboard	Hilero
Langile satisfakzioa	Inkesta	Urtekoa

5.2 Compliance Metrikak (NIS2)

Metrika	Helburua	Egungo Balioa	Data
Zuzendaritza formakuntza (%100)	100%	0%	2026-02-06
Langile guztien formakuntza (urtekoa)	≥ 95%	0%	2026-02-06
CSIRT tabletop exercises (urtea)	≥ 4	0	2026-02-06
Phishing click rate	< 5%	N/A	—
BCP proba emaitza orokorra	> 80/100	N/A	—
NIS2 notification drill arrakasta	100%	N/A	—

6. AURREKONTUA (Training Budget)

Kontzeptua	Kostua (€)	Oharra
Kanpo formatzailea (IR + Forensic)	3.000	2 eguneko workshop
GoPhish / KnowBe4 lizentzia (urtekoa)	1.500	Phishing simulazioak
SIEM formakuntza (Wazuh)	500	Online ikastaroa
OT Security formakuntza (IEC 62443)	2.000	SANS edo parekidea
Material eta logistika	500	—
<b>GUZTIRA</b>	<b>7.500 €</b>	NIS2 planeko 5.000€ + 2.500€ gehigarri

7. ERREFERENTZIAK

- NIS2 (EU 2022/2555) Art. 20.2, Art. 21.2.a
- ISO 27001:2022 A.6.3 — Information security awareness, education and training
- ENISA: Cybersecurity Skills Framework

- NIST SP 800-50 — Building an IT Security Awareness and Training Program

---

**ONARPENA:**

- CISO: Mikel Etxebarria — Data: \_\_\_\_
- RRHH: \_\_\_\_\_ — Data: \_\_\_\_
- CEO: Jon Zabala — Data: \_\_\_\_

*Dokumentu hau: 2026-02-06 | Zabala Gailetak, S.L. — NIS2 Compliance*