ZABALA GAILETAK, S.A.

AUZITEGI-ANALISI INFORMATIKOA

Ebidentzia Digitalen Bilketa Prozedura (SOP)

ISO/IEC 27037 eta RFC 3227 arabera

Dokumentu Kodea:	DFIR-ZG-002
Bertsioa:	1.0
Data:	2026-02-19
Ikasturtea:	2026
Sailkapena:	Heziketa — Barne Erabilera
Egilea:	Zabala Gailetak Zibersegurtasun Taldea

1. Helburua eta Esparrua

Prozedura honek ebidentzia digitalen bilketa, kudeaketa eta analisi metodologia ezartzen du Zabala Gailetak-en, ISO/IEC 27037:2012 eta RFC 3227 estandarren arabera.

2. Erantzukizun-matrizea

Rola	Erantzukizuna	Sailkapena
Auzitegi Analista	Bilketa, irudigintza, analisia	DFIR Taldea
CISO	Analisiaren onarpena eta komunikazioa	Kudeaketa
IT Arduraduna	Laguntzaile teknikoa	IT Taldea
Legal Aholkularia	Legez beteko erabileran gidaritza	Juridikoa
Zuzendari Nagusia	Beharrezko baliabideen onarpena	Zuzendaritza

3. Bilketa Protokoloa — Urrats Zehatza

Urratsa	Ekintza	Zehaztasuna
0	Deia jaso	CISO edo zerbitzu-mahaiak gertaera komunikatu eta DFIR analista aktibatu.
1	Eszena segurtatu	Gailua isolatu, argazkiak atera, inguruaren kontrola hartu.
2	Hegakorren bilketa	RAM, sare-konexioak, prozesuak USB-tik exekutatzen diren tresnekin.
3	Irudigintza	dc3dd edo Guymager erabiliz bit-mailako kopia egin idazketa-blokatzaileekin.
4	Hash egiaztapena	SHA-256 hash kalkuatu eta dokumentatu — jatorrizkoa eta kopian berdinak.
5	Etiketatze fisikoa	Ontziak, diskoak eta gailua ID unikoaz etiketatu.
6	Biltegi segurua	Ebidentzia gela itxian gorde sarbide-kontrolarekin.
7	Analisia hastea	Irudiaren gainean bakarrik lan egin, ez jatorrizkoan.

4. Debeku Absolutuak

■ DEBEKATUA: Sistemak INOIZ ez itzali ebidentziak bildu aurretik (RAM galdu egingo litzateke). Ez instalatu ezer sistema helburuan. Ez exekutatu antibirusik bertan.

5. Tresnen Inbentarioa (USB Forensea)

• LiME.ko — Linux kernel modulua RAM bilketarako
• WinPmem.exe — Windows RAM bilketarako
• dc3dd / Guymager — Irudigintza egiaztapenekin
• FTK Imager (Windows) — Disko irudigintza alternatiboa
• Volatility 3 — Memoria analisia
• Autopsy 4.x — Disko analisia GUI-rekin