Regulatory alignment

Control, capability and evidence map against ICN-POL-001, with honest compliance and roadmap statuses, and summarised pointers to the NORTIC, ISO 27001 and NIST mappings.

Scope and how to read this document

This document summarises Abzu's public alignment with the National Cryptographic Policy **ICN-POL-001** and points to the mappings with the NORTIC frameworks — for the Dominican Republic only — and ISO 27001 and NIST. Each requirement is classified as **Compliant**, **Partially compliant**, **Roadmap**, **Declared gap**, or dependent on an **instrument** not yet issued by the regulator. No roadmap item is presented as an existing function.

The formal alignment matrix carries reference `ABZU-ICN-2026-001`, dated 20 October 2026.

Control, capability and evidence map against ICN-POL-001

Policy section	Abzu capability	Status	Evidence
§5.1 Protection of fundamental rights	Backup encryption in stream and custody without vendor access in the government form: the institution controls the keys	Compliant	Key Custody Protocol design
§5.2 Security by design and by default	Fail-closed controls by default: recipe admission with scanning, verified licensing and internal report signing	Compliant	Signed validation and audit reports
§5.3 Adoption of international standards	Only current standard algorithms; no proprietary cryptography	Compliant	Algorithms and modules sheet
§5.4 Technological neutrality with strategic sovereignty	Perpetual, self-contained government form; the vendor retains no share of institutional keys	Compliant	Key Custody Protocol
§5.5 Proportionality and risk-based approach	Per-agent licensing with unlimited containers; semi-automatic recovery with human approval	Compliant	Validation report
§5.6 Cryptographic agility	Agility built in with a fail-closed criterion; replacement of primitives without redesign	Partially compliant	Algorithms sheet; post-quantum transition commitment on the roadmap

Policy section	Abzu capability	Status	Evidence
§5.7 Defence in depth	Agent–console mutual authentication, image scanning, intrusion control, separation of duties and antivirus in backup verification	Compliant	Validation and audit reports
§5.8 Accountability and traceability	Comprehensive audit log, signed ceremony minutes, forensic marking on custody documents and verifiable signed reports	Compliant	Signature registry; protocol exercise
§6.2-I Unified criteria	Product classification against the National Cryptographic Manual when the regulator issues it	Regulator instrument	Pending the complementary instrument
§6.2-II Secure protection and interoperability	Encrypted and immutable backups; federated consoles with signed envelopes	Compliant	Validation report
§6.2-IV Transition to agile and resilient environments	Post-quantum incorporation as standard libraries mature	**Roadmap**	Declared roadmap
§7 Cryptographic governance	Instance and organisation roles, requester disjoint from custodians and operations centre visibility	Compliant	User manual; protocol exercise
§8.2 Information lifecycle	Backup encrypted in stream, immutable repository with object lock, generational retention and point-in-time recovery verified on three engines	Compliant	Validation report; SQL Server verification
§8.2 Secure destruction	Certified destruction of keys with signed minutes	**Roadmap**	Roadmap item P2, planned for v2.3
§8.3 Identity, authorisation and logging	Federated and directory sign-in, step-up authentication on anomalous context and comprehensive audit	Compliant	Validation and audit reports
§8.4 Personal data	Encryption in transit with mutual authentication and encryption at rest of backups and the credential store	Compliant	Algorithms sheet
§9.1–9.2 Trust services	Report and minutes signatures within the platform, with proof verification, and quorum custody of platform keys	Partially compliant	Signature registry. The generalisation to an institutional key infrastructure is item P2, **roadmap**

Policy section	Abzu capability	Status	Evidence
§9.4 Segregation of duties and master key protection	Key Custody Protocol: configurable quorum, requester who does not contribute, mandatory access keys, cooldown and notice on recovery	Compliant	Protocol design and exercise
§10.1 Only approved mechanisms	Only current standard algorithms and restrictive-criterion scanning on admission; formal classification against the official list arrives with the regulator's instrument	Partially compliant	Algorithms sheet
§10.2 Key and certificate lifecycle	Full lifecycle for platform keys; the full institutional lifecycle is item P2	Partially compliant / **Roadmap**	Key Custody Protocol; roadmap
§10.3 Protection in transit and at rest	Mutual authentication in transport and encryption in stream and at rest	Compliant	Algorithms sheet
§10.4 Critical environments and continuity	Recovery with automatic detection and preparation and execution only with human approval	Compliant	Validation report
§10.5 Documented and temporary exceptions	Formal register of exceptions with justification, approval, compensating controls and remediation plan	**Roadmap**	Roadmap item P4, planned for v2.2
§11.2 Evaluation under recognised schemes	No FIPS 140-3 validation or Common Criteria evaluation; the equivalence admitted by the policy itself and the FIPS mode plan are proposed	**Declared gap**	Algorithms sheet; roadmap, FIPS mode planned for v2.4
§11.7 Comprehensive assessment by the purchaser	Express declaration of continuity, support, technological dependence and vendor integrity	Compliant	Declaration under §11.7 of the dossier
§12 Cryptographic incident management	Detection in verification — a compromised backup is marked and isolated, never deleted — and platform incident management	Partially compliant	The specific cryptographic incident flow is item P3, **roadmap** planned for v2.2
§12.4 Vulnerabilities in algorithms and configurations	Fleet cryptographic inventory and posture, classified against the current list	**Roadmap**	Roadmap item P1, planned for v2.1
§13.1 Capacity building	User manual in Spanish and English, in 20 sections, and product documentation	Compliant	User manual
§13.3 Cooperation and interoperability	Public interface, integration libraries and infrastructure-as-code provider	Compliant	Validation report

The digital signature regime of Law 126-02 and the competence of the telecommunications regulator remain intact: Abzu does not provide qualified trust services under that regime.

Frameworks by market

Market	Applicable framework	Mapping document
Dominican Republic	**NORTIC** — standards A5, A6, A8, A9, B1 and B2; standard A4 is pending the official text	NORTIC compliance mapping
United States	**NIST** — SP 800-53 and CSF 2.0	International compliance mapping
Rest of the world	**ISO/IEC 27001:2022**, Annex A	International compliance mapping

NORTIC applies **only** to the Dominican Republic and is not marketed outside it.

Summary of the NORTIC and international mappings

Block	Public result
NORTIC — assets, changes, detection and continuity	The design covers the core within its scope: continuous inventory, versioned changes with rollback, protected event logging and recovery plans exercised with real restoration
NORTIC — identity and access	Covered: separation of duties in recovery, periodic access recertification and image scanning on admission. Mandatory second factor for administrators with local accounts is declared as a registered hardening item, not as a capability to be taken as evidenced without verifying it in the installation
NORTIC — continuity	Encrypted, automated, off-site and verified backups, with an isolated copy against ransomware. No promise of zero loss
ISO 27001 and NIST — organisational, people and physical blocks	Responsibility of the client institution; Abzu provides the technical evidence that feeds them — inventory, audit, recertification and reports — and does not replace them
ISO 27001 and NIST — technological and response blocks	Meets the product's technical core — inventory, least privilege, mutual authentication, audit, encrypted and verified backup and recovery — and is partial where the organisational process belongs to the client

Declared roadmap

Status: Roadmap — not available.

- **v2.1:** fleet cryptographic inventory and posture.
- **v2.2:** cryptographic exceptions register and cryptographic incident flow.
- **v2.3:** institutional key infrastructure and certified destruction.
- **v2.4:** FIPS mode.