Alineación normativa

Mapa control, capacidad y evidencia frente a ICN-POL-001, con los estados honestos de cumplimiento y de hoja de ruta, y punteros resumidos a los mapeos NORTIC, ISO 27001 y NIST.

Alcance y regla de lectura

Este documento resume la alineación pública de Abzu con la Política Criptográfica Nacional **ICN-POL-001** y apunta a los mapeos con los marcos NORTIC —solo para la República Dominicana— e ISO 27001 y NIST. Cada exigencia se clasifica como **Cumple**, **Cumple parcial**, **Hoja de ruta**, **Brecha declarada** o dependiente de un **instrumento** aún no emitido por el regulador. Ninguna partida de hoja de ruta se presenta como función existente.

La matriz formal de alineación lleva el folio `ABZU-ICN-2026-001`, con fecha 20 de octubre de 2026.

Mapa control, capacidad y evidencia frente a ICN-POL-001

Sección de la política	Capacidad de Abzu	Estado	Evidencia
§5.1 Protección de derechos fundamentales	Cifrado de respaldos en flujo y custodia sin acceso del proveedor en la forma gobierno: la institución controla las llaves	Cumple	Diseño del Protocolo de Custodia de Llaves
§5.2 Seguridad por diseño y por defecto	Controles que no actúan ante la duda, por defecto: admisión de recetas con escaneo, licenciamiento verificado y firma interna de informes	Cumple	Informes firmados de validación y de auditoría
§5.3 Adopción de estándares internacionales	Solo algoritmos estándar vigentes; ninguna criptografía propietaria	Cumple	Ficha de algoritmos y módulos
§5.4 Neutralidad tecnológica con soberanía estratégica	Forma gobierno perpetua y autocontenida; el proveedor no retiene fragmento alguno de las llaves institucionales	Cumple	Protocolo de Custodia de Llaves
§5.5 Proporcionalidad y enfoque basado en riesgo	Licenciamiento por agente con contenedores ilimitados; recuperación semi-automática con aprobación humana	Cumple	Informe de validación
	Agilidad construida y con criterio de no actuar ante la duda;		Ficha de algoritmos; compromiso de transición

Sección de la política	Capacidad de Abzu	Estado	Evidencia
§5.6 Agilidad criptográfica	sustitución de primitivas sin rediseño	Cumple parcial	post-cuántica en la hoja de ruta
§5.7 Defensa en profundidad	Autenticación mutua agente-consola, escaneo de imágenes, control de intrusiones, separación de funciones y antivirus en la verificación de respaldos	Cumple	Informes de validación y de auditoría
§5.8 Rendición de cuentas y trazabilidad	Bitácora de auditoría integral, actas de ceremonia firmadas, marca forense en documentos de custodia e informes firmados verificables	Cumple	Registro de firmas; ejercicio del protocolo
§6.2-I Criterios unificados	Clasificación del producto contra el Manual Criptográfico Nacional cuando el regulador lo emita	Instrumento del regulador	Pendiente del instrumento complementario
§6.2-II Protección e interoperabilidad segura	Respaldos cifrados e inmutables; consolas federadas con sobres firmados	Cumple	Informe de validación
§6.2-IV Transición a entornos ágiles y resistentes	Incorporación post-cuántica al madurar las bibliotecas estándar	**Hoja de ruta**	Hoja de ruta declarada
§7 Gobernanza criptográfica	Roles de instancia y de organización, solicitante disjunto de los custodios y visibilidad del centro de operaciones	Cumple	Manual de usuario; ejercicio del protocolo
§8.2 Ciclo de vida de la información	Respaldo cifrado en flujo, repositorio inmutable con bloqueo de objetos, retención por generaciones y recuperación a un punto en el tiempo verificada en tres motores	Cumple	Informe de validación; verificación de SQL Server
§8.2 Destrucción segura	Destrucción certificada de llaves con acta firmada	**Hoja de ruta**	Partida P2 de la hoja de ruta, prevista en la v2.3
§8.3 Identidad, autorización y registro	Inicio de sesión federado y por directorio, autenticación reforzada ante contexto anómalo y auditoría integral	Cumple	Informes de validación y de auditoría
§8.4 Datos personales	Cifrado en tránsito con autenticación mutua y cifrado en reposo de respaldos y del almacén de credenciales	Cumple	Ficha de algoritmos

Sección de la política	Capacidad de Abzu	Estado	Evidencia
§9.1–9.2 Servicios de confianza	Firmas de informes y actas dentro de la plataforma, con comprobación de pruebas, y custodia por quórum de las llaves de la plataforma	Cumple parcial	Registro de firmas. La generalización a una infraestructura de llaves institucional es la partida P2, **hoja de ruta**
§9.4 Segregación de funciones y protección de llaves maestras	Protocolo de Custodia de Llaves: quórum configurable, solicitante que no aporta, llaves de acceso obligatorias, enfriamiento y aviso en la recuperación	Cumple	Diseño y ejercicio del protocolo
§10.1 Solo mecanismos aprobados	Algoritmos estándar vigentes únicamente y escaneo con criterio restrictivo en la admisión; la clasificación formal contra la lista oficial llega con el instrumento del regulador	Cumple parcial	Ficha de algoritmos
§10.2 Ciclo de vida de llaves y certificados	Ciclo completo para las llaves de la plataforma; el ciclo institucional completo es la partida P2	Cumple parcial / **Hoja de ruta**	Protocolo de Custodia de Llaves; hoja de ruta
§10.3 Protección en tránsito y en reposo	Autenticación mutua en el transporte y cifrado en flujo y en reposo	Cumple	Ficha de algoritmos
§10.4 Entornos críticos y continuidad	Recuperación con detección y preparación automáticas y ejecución solo con aprobación humana	Cumple	Informe de validación
§10.5 Excepciones documentadas y temporales	Registro formal de excepciones con justificación, aprobación, controles compensatorios y plan de remediación	**Hoja de ruta**	Partida P4 de la hoja de ruta, prevista en la v2.2
§11.2 Evaluación con esquemas reconocidos	Sin validación FIPS 140-3 ni Common Criteria; se propone la equivalencia que la propia política admite y el plan de modalidad FIPS	**Brecha declarada**	Ficha de algoritmos; hoja de ruta, modalidad FIPS prevista en la v2.4
§11.7 Valoración integral por el comprador	Declaración expresa de continuidad, soporte, dependencia tecnológica e integridad del proveedor	Cumple	Declaración conforme al §11.7 del expediente
	Detección en la verificación —el respaldo comprometido se marca	Cumple parcial	El flujo específico de incidente criptográfico es la

Sección de la política	Capacidad de Abzu	Estado	Evidencia
§12 Gestión de incidentes criptográficos	y se aísla, nunca se borra— y gestión de incidentes de la plataforma		partida P3, **hoja de ruta** prevista en la v2.2
§12.4 Vulnerabilidades en algoritmos y configuraciones	Inventario y postura criptográfica de la flota, clasificada contra la lista vigente	**Hoja de ruta**	Partida P1 de la hoja de ruta, prevista en la v2.1
§13.1 Fortalecimiento de capacidades	Manual de usuario en español e inglés, de 20 secciones, y documentación del producto	Cumple	Manual de usuario
§13.3 Cooperación e interoperabilidad	Interfaz pública, bibliotecas de integración y proveedor de infraestructura como código	Cumple	Informe de validación

El régimen de firma digital de la Ley 126-02 y la competencia del organismo regulador de telecomunicaciones quedan intactos: Abzu no presta servicios de confianza cualificados bajo ese régimen.

Marcos por mercado

Mercado	Marco aplicable	Documento de mapeo
República Dominicana	**NORTIC** — normas A5, A6, A8, A9, B1 y B2; la norma A4 se encuentra pendiente del texto oficial	Mapeo de cumplimiento NORTIC
Estados Unidos	**NIST** — SP 800-53 y CSF 2.0	Mapeo de cumplimiento internacional
Resto del mundo	**ISO/IEC 27001:2022**, Anexo A	Mapeo de cumplimiento internacional

NORTIC se aplica **solo** a la República Dominicana y no se comercializa fuera de ella.

Resumen de los mapeos NORTIC e internacionales

Bloque	Resultado público
NORTIC — activos, cambios, detección y continuidad	El diseño cubre el núcleo que le compete: inventario continuo, cambios versionados con reversión, registro de eventos protegido y planes de recuperación ejercitados con restauración real
NORTIC — identidad y acceso	Cubiertos la separación de funciones en la recuperación, la recertificación periódica de accesos y el escaneo de imágenes en la admisión. La obligatoriedad del segundo factor para administradores con cuentas locales se declara como partida de endurecimiento registrada, no como capacidad que deba darse por evidenciada sin comprobarla en la instalación

Bloque	Resultado público
NORTIC — continuidad	Respaldos cifrados, automatizados, fuera del sitio y verificados, con copia aislada frente a programas de secuestro de datos. Sin promesa de pérdida cero
ISO 27001 y NIST — bloques organizativos, de personas y físicos	Responsabilidad de la institución cliente; Abzu aporta la evidencia técnica que los alimenta —inventario, auditoría, recertificación e informes— y no los sustituye
ISO 27001 y NIST — bloques tecnológicos y de respuesta	Cumple el núcleo técnico del producto —inventario, mínimo privilegio, autenticación mutua, auditoría, respaldo cifrado y verificado y recuperación— y es parcial donde el proceso organizativo es del cliente

Hoja de ruta declarada

Estado: Hoja de ruta — no disponible.

- **v2.1:** inventario y postura criptográfica de la flota.
- **v2.2:** registro de excepciones criptográficas y flujo de incidentes criptográficos.
- **v2.3:** infraestructura de llaves institucional y destrucción certificada.
- **v2.4:** modalidad FIPS.