POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (PSI)

Documento: Política de Seguridad de la Información (PSI)
Plataforma: NUNGU Smart Business System
Empresa: NOVELOSTECH
Versión: 1.0
Fecha de Emisión: 2026-04-24

1. Propósito y Alcance

La presente Política de Seguridad de la Información (PSI) establece los lineamientos técnicos, operativos y administrativos diseñados para garantizar la confidencialidad, integridad y disponibilidad de la información procesada a través de la plataforma NUNGU. Este documento da cumplimiento a las exigencias técnicas de la Dirección General de Impuestos Internos (DGII) para Proveedores de Servicios de Facturación Electrónica en la República Dominicana.

2. Arquitectura de Seguridad y Cifrado

NUNGU opera sobre una arquitectura de nube corporativa de alta seguridad (Google Cloud Platform - GCP).

- **Datos en Tránsito:** Toda comunicación entre los nodos locales (clientes) y el servidor central (Master Server), así como las transmisiones hacia la DGII, están protegidas mediante protocolos criptográficos robustos (TLS 1.2 y TLS 1.3), previniendo ataques de intermediario (Man-in-the-Middle).
- **Datos en Reposo:** Las bases de datos transaccionales utilizan cifrado nativo en reposo (AES-256), asegurando que los registros de los Comprobantes Fiscales Electrónicos (e-CF) permanezcan protegidos a nivel de disco.

3. Custodia Segura de Certificados Digitales

Cumpliendo con los mandatos de la DGII respecto a la firma delegada y gestión de certificados:

- Los Certificados Digitales (archivos .p12 o .pfx) de los contribuyentes son custodiados exclusivamente en el Master Server en un entorno aislado (Vault).
- Bajo ninguna circunstancia los certificados digitales son almacenados en las terminales locales o de facturación física.
- Las contraseñas asociadas a los certificados son protegidas mediante algoritmos de derivación de claves (hashing robusto), garantizando que ni el personal de NOVELOSTECH tenga acceso en texto plano a las credenciales de firma.

4. Control de Acceso y Gestión de Identidades (IAM)

- El acceso a la infraestructura de producción está estrictamente limitado al personal técnico autorizado mediante políticas de menor privilegio (Principio de Zero Trust).
- El acceso administrativo requiere autenticación multifactor (MFA) y conexiones a través de redes privadas virtuales (VPN) seguras o túneles cifrados (SSH con llaves asimétricas).
- El sistema mantiene bitácoras (logs) inalterables que registran la trazabilidad de accesos, creación de documentos fiscales y cambios en la configuración del sistema.