

INSTITUTO DOMINICANO DE METEOROLOGÍA (INDOMET)

DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

SISTEMA DE RESERVAS DE SALÓN V2.1.0

Código: POL-SEG-003 Clasificación: CONFIDENCIAL Revisión: 2026

1. OBJETIVO

Definir las directrices de seguridad técnica y administrativa para proteger la confidencialidad, integridad y disponibilidad de la información procesada por el Sistema de Reservas, en cumplimiento con la Normativa **NORTIC A6:2016**.

2. CONTROL DE ACCESO (AUTENTICACIÓN Y AUTORIZACIÓN)

2.1 Gestión de Contraseñas

- **Encriptación:** Todas las contraseñas de usuario deben ser almacenadas utilizando algoritmos de hashing robustos (Bcrypt).
- **Prohibición:** Se prohíbe terminantemente el almacenamiento de credenciales en texto plano.
- **Robustez:** Las contraseñas deben tener una longitud mínima de 8 caracteres.

2.2 Roles y Privilegios

El sistema implementa el principio de menor privilegio a través de la siguiente matriz de roles:

Rol	Ver Calendario	Gestionar Propia	Gestionar Global	Administración
Usuario				

Rol	Ver Calendario	Gestionar Propia	Gestionar Global	Administración
Manejador Admin				

2.3 Gestión de Sesiones

- **Tiempo de Vida:** Las sesiones inactivas deben cerrarse automáticamente después de **60 minutos** (`SESSION_LIFETIME`).
- **Anti-Fijación:** El identificador de sesión será regenerado en cada inicio de sesión exitoso.

3. SEGURIDAD EN LAS COMUNICACIONES

3.1 Cifrado de Tránsito

- De acuerdo con **NORTIC A6:2016 (4.02)**, todo el tráfico entre cliente y servidor debe estar cifrado.
- Es obligatorio el uso del protocolo **HTTPS (TLS 1.2+)** en producción.
- La redirección de HTTP a HTTPS debe ser forzosa.

4. SEGURIDAD DE BASE DE DATOS

4.1 Protección de Archivos

- Los archivos SQLite (`usuarios.db`, `reservas.db`) deben residir fuera del directorio público web (`public/`).
- El acceso directo a estos archivos vía navegador debe estar bloqueado.

4.2 Sanitización

- Todas las consultas deben utilizar **Sentencias Preparadas (PDO)** para mitigar Inyección SQL.
- Se validarán estrictamente los datos de entrada en todos los formularios.

5. AUDITORÍA Y TRAZABILIDAD

El sistema registrará eventos críticos para auditoría forense, incluyendo: 1. Intentos de inicio de sesión fallidos. 2. Creación o elevación de privilegios de usuarios. 3. Errores críticos del aplicativo.

Dirección de Seguridad de la Información INDOMET