SISTEMA TEMIS

app.sistematemis.com

ANEXO DE SEGURIDAD

Medidas técnicas y organizativas de seguridad de la información en Temis

Responsable de la plataforma:

Ing. Franklin Yamali Castillo

C.I. V-09554554

RIF V-09554554-4

Barquisimeto, estado Lara, República Bolivariana de Venezuela

Versión 1.1

Última actualización: 4 de julio de 2026

Este Anexo complementa los Términos y Condiciones, la Política de Privacidad, el Acuerdo de Tratamiento de Datos y el SLA de Temis. Describe medidas razonables de seguridad aplicables a la Plataforma conforme a su capacidad operativa actual.

1. Principios de Seguridad

Temis aplica medidas razonables orientadas a proteger la confidencialidad, integridad y disponibilidad de la información. Las medidas podrán evolucionar conforme crezca la infraestructura, base de clientes, criticidad operativa y madurez técnica de la Plataforma.

2. Control de Acceso

- Uso de cuentas individuales para usuarios autorizados.
- Credenciales personales e intransferibles.
- Roles y permisos según funcionalidades disponibles.
- Restricción de acceso a módulos conforme al Plan contratado y permisos asignados.
- Revocación o modificación de accesos por parte del Cliente cuando corresponda.

3. Separación Lógica de Datos

Temis procura mantener separación lógica de información por Cliente, organización o empresa, conforme al diseño multiempresa de la Plataforma. Esta separación busca evitar accesos cruzados o visualización de datos entre Clientes no relacionados.

4. Cifrado y Comunicaciones

La Plataforma utiliza cifrado en tránsito mediante HTTPS/TLS para proteger las comunicaciones entre el navegador del Usuario y los servicios de Temis. El cifrado en reposo dependerá de las capacidades y configuración del proveedor de infraestructura utilizado.

5. Registros de Auditoría y Trazabilidad

Temis podrá registrar eventos relevantes de acceso, autenticación, creación, modificación, eliminación, errores, actividad administrativa y acciones críticas para fines de seguridad, soporte, diagnóstico, auditoría y defensa de derechos.

La disponibilidad de reportes de auditoría para el Cliente podrá depender del Plan contratado, configuración de la Plataforma o acuerdo particular.

6. Backups y Continuidad

Temis realizará respaldos periódicos conforme al SLA vigente. Los respaldos se orientan a continuidad del Servicio y recuperación ante incidentes graves. El Cliente conserva la responsabilidad de exportar y resguardar copias propias de información crítica cuando su operación lo requiera.

7. Acceso Administrativo

El acceso administrativo a datos del Cliente estará limitado a fines de soporte, mantenimiento, seguridad, diagnóstico, cumplimiento contractual, recuperación, investigación de incidentes o requerimiento legal válido. Temis procurará aplicar el principio de mínimo privilegio y limitar el acceso a personal o colaboradores que lo requieran para prestar el Servicio.

8. Ambientes de Desarrollo y Prueba

Temis evitará utilizar datos reales del Cliente en ambientes de desarrollo o prueba, salvo que sea necesario para soporte técnico, diagnóstico, validación o corrección de errores. Cuando resulte posible, se aplicarán medidas de minimización, anonimización, restricción de acceso o uso de datos ficticios.

9. Gestión de Incidentes

- Identificación preliminar del evento.
- Evaluación de alcance, severidad e impacto potencial.
- Contención o mitigación técnica cuando sea posible.
- Comunicación al Cliente afectado cuando el incidente pueda comprometer datos personales o continuidad del Servicio.
- Documentación interna de acciones correctivas o preventivas razonables.

10. Responsabilidades del Cliente

- Asignar usuarios solo a personas autorizadas.
- Configurar permisos conforme a funciones reales de cada usuario.
- Proteger contraseñas, correos, dispositivos y redes internas.
- Revocar accesos cuando un usuario deje de trabajar para el Cliente o cambie de funciones.
- Evitar compartir credenciales o utilizar cuentas genéricas sin control.
- Exportar y conservar copias propias de información crítica cuando sea necesario para su operación.

11. Evolución de las Medidas de Seguridad

Las medidas descritas en este Anexo reflejan la capacidad operativa actual de Temis. El Proveedor podrá incorporar progresivamente nuevas medidas, tales como autenticación multifactor, controles avanzados de auditoría, monitoreo externo, cifrado reforzado, alertas de actividad sospechosa, políticas de contraseñas más estrictas o controles específicos para planes Enterprise.

12. Contacto de Seguridad

- Correo de soporte: soporte@sistematemis.com
- Correo de privacidad: privacidad@sistematemis.com
- Correo legal: legal@sistematemis.com