1. OBJETIVO

Establecer los límites y las responsabilidades específicas entre **ADATEC S.A.S.** (en adelante "El Proveedor") y **EL CLIENTE** respecto a la seguridad de la información, la protección de datos personales y la operación de los servicios tecnológicos por suscripción (SaaS). Este acuerdo busca garantizar la confidencialidad, integridad y disponibilidad de la información procesada, diferenciando las obligaciones de seguridad "de la nube" (responsabilidad de ADATEC) y seguridad "en la nube" (responsabilidad del Cliente).

2. ALCANCE

Este modelo aplica a todos los servicios SaaS B2B provistos por ADATEC y regula la interacción entre los procesos internos de ADATEC y las operaciones del Cliente que hacen uso de la plataforma

3. RESPONSABILIDADES

3.1. RESPONSABILIDADES DE ADATEC (El Proveedor)

ADATEC actúa como Encargado del Tratamiento de los datos y proveedor de la infraestructura tecnológica. Sus responsabilidades incluyen:

A. Seguridad de la Infraestructura y Plataforma

- **Seguridad de infraestructura y Ambiental**: ADATEC es responsable de proteger los centros de datos, servidores y equipos donde se procesa la información, asegurando controles de acceso físico y protección contra amenazas ambientales.
- **Seguridad de la Red y Perímetro**: Implementación de firewalls, sistemas de detección de intrusos y segmentación de redes para proteger los servicios contra accesos no autorizados dentro de la infraestructura de ADATEC..
- **Desarrollo Seguro**: Garantizar que el software entregado como servicio ha sido diseñado siguiendo principios de seguridad por diseño y por defecto, incluyendo análisis de vulnerabilidades y pruebas de penetración antes del despliegue en producción.

B. Protección y Disponibilidad de Datos

- **Copias de Respaldo**: Realizar copias de seguridad (backups) periódicas de la información, bases de datos y configuraciones críticas, asegurando su integridad y disponibilidad para recuperación ante desastres de los recursos de ADATEC.
- **Cifrado**: Implementar cifrado fuerte para la información clasificada como "Restringida" o "Confidencial" tanto en reposo como en tránsito.
- **Gestión de Logs**: Generar y proteger los registros de auditoría (logs) de la infraestructura para permitir la trazabilidad forense.

C. Privacidad (Rol de Encargado)

- Procesar los datos personales administrados por los clientes únicamente bajo sus instrucciones y no utilizarlos para fines propios ni compartirlos sin autorización, salvo obligación legal.

3.2. RESPONSABILIDADES DEL CLIENTE (El Usuario)

El Cliente actúa como Responsable del Tratamiento de los datos y administrador de sus accesos. Sus responsabilidades incluyen:

A. Gestión de Accesos y Usuarios

- **Autorización**: Definir qué usuarios de su organización tienen acceso a la plataforma y qué privilegios se les asignan, bajo el principio de "necesidad de saber".
- **Credenciales**: Asegurar que sus usuarios utilicen contraseñas robustas, no compartan sus cuentas y, cuando esté disponible, utilicen autenticación multifactor (MFA).
- **Revocación**: Gestionar la baja de cuentas de usuarios que han dejado de laborar en su organización.

B. Seguridad de los Dispositivos del Cliente

- **Seguridad del Endpoint**: Asegurar que los computadores o dispositivos móviles desde los cuales sus empleados acceden a los servicios de ADATEC cuenten con antivirus actualizado, sistema operativo parcheado y bloqueo automático por inactividad.
- **Entorno de Trabajo**: Garantizar que sus empleados, especialmente en teletrabajo, operen en entornos que prevengan la visualización no autorizada de información (política de escritorio limpio).

C. Privacidad y Datos (Rol de Responsable)

- **Consentimiento**: Obtener la autorización expresa e informada de los titulares (sus propios clientes, empleados o beneficiarios) para recolectar y tratar sus datos personales en la plataforma de ADATEC.
- **Calidad del Dato**: Responder ante los titulares por la exactitud, actualización y rectificación de los datos ingresados en el sistema.

MATRIZ DE RESPONSABILIDADES:

Actividad / Proceso	Responsabilidad de ADATEC (ISO 27001: Controles A.5 a A.8)	Responsabilidad del CLIENTE (ISO 27001: Controles A.6.2 y A.7)
Infraestructura y Red	Seguridad de centros de datos, servidores, energía y protección	Seguridad de la red local del cliente, dispositivos finales (laptops/móviles) y

	perimetral (Firewalls/WAF).	conexión a internet segura.
Gestión de Identidades	Proveer mecanismos de autenticación robustos y cifrado TLS para el transporte.	Gestión del ciclo de vida del usuario (alta/baja), custodia de credenciales y uso de MFA.
Datos y Privacidad	Ejecución de backups, cifrado de datos en reposo/tránsito y rol de Encargado del Tratamiento de la infraestructura de ADATEC.	Clasificación de la información, obtención de consentimiento de los titulares y rol de Responsable del Tratamiento. Backups de sus equipos de computo.
Ciclo de Vida del Software	Desarrollo seguro (Secure SDLC), pruebas de penetración y corrección de bugs.	Configuración de reglas de negocio específicas y parámetros de usuario dentro de la aplicación.
Gestión de Incidentes	Detección, contención y recuperación ante fallos de plataforma o ataques externos.	Reporte inmediato de sospechas de compromiso de cuentas o errores de operación interna.

4. DEFINICIONES

- **Software como Servicio (SaaS):** Modelo de entrega de software donde ADATEC aloja la aplicación y los datos en la nube, y el Cliente accede a ellos a través de internet.
- **Responsabilidad Compartida**: Modelo operativo que delimita las obligaciones de seguridad; ADATEC es responsable de la seguridad "de" la nube (infraestructura), mientras que el Cliente es responsable de la seguridad "en" la nube (datos y accesos).
- **Responsable del Tratamiento**: Actor que decide sobre la finalidad y el tratamiento de los datos personales; en este acuerdo, es el rol que desempeña el Cliente.
- **Encargado del Tratamiento**: Actor que realiza el tratamiento de datos personales por cuenta del responsable; en este acuerdo, es el rol que desempeña ADATEC.
- **Confidencialidad**: Propiedad de la información de no estar disponible ni ser revelada a individuos, entidades o procesos no autorizados.
- **Integridad**: Propiedad de salvaguardar la exactitud y completitud de los activos de información y los datos procesados.
- **Disponibilidad**: Propiedad de que la información y los servicios sean accesibles y utilizables cuando lo requiera el Cliente.
- **Activos de Información**: Elementos como bases de datos, archivos, configuraciones y

credenciales que tienen valor para la organización y deben ser protegidos.

- **Incidente de Seguridad:** Suceso inesperado o no deseado que tiene una probabilidad significativa de comprometer las operaciones del negocio o amenazar la seguridad de la información.
- **Autenticación Multifactor (MFA):** Método de control de acceso que requiere más de una evidencia de identidad para permitir el ingreso a la plataforma.
- **Endpoint (Punto Final):** Dispositivos físicos (computadores, tabletas, móviles) utilizados por los empleados del Cliente para conectarse a los servicios de ADATEC.

5. ACUERDO DE RESPONSABILIDAD COMPARTIDA DE SEGURIDAD DE LA INFORMACIÓN

5.1 GESTIÓN DE INCIDENTES Y COMUNICACIÓN

- **Reporte**: El Cliente se compromete a notificar a ADATEC de manera inmediata sobre cualquier sospecha de compromiso de credenciales o incidente de seguridad a través de los canales de soporte establecidos (Ticket de soporte).
- **Respuesta**: ADATEC ejecutará su procedimiento de gestión de incidentes para contener, erradicar y recuperar el servicio, notificando al Cliente si sus datos se vieron afectados.

5.2 Continuidad del Negocio (ISO 27001: A.5.29 / ISO 22301):

- **ADATEC***:* Se compromete a mantener un Plan de Recuperación ante Desastres (DRP) que garantice el RTO y RPO pactados.
- **CLIENTE***:* Debe tener procedimientos de contingencia manuales en caso de indisponibilidad temporal del servicio.

5.3 Gestión de Cambios (ISO 9001: 8.5.6):

ADATEC notificará con antelación cambios significativos en la plataforma que puedan afectar la operación del Cliente. El Cliente es responsable de validar el impacto en sus procesos internos.

5.4 Auditoría y Monitoreo (ISO 27001: A.5.35):

ADATEC garantiza la trazabilidad mediante logs de auditoría. El Cliente tiene derecho a solicitar reportes de cumplimiento o resúmenes de pruebas de seguridad anuales.

5.5 Cese del Servicio (ISO 27001: A.5.10):

En caso de terminación del contrato, ADATEC garantiza la devolución de la información del cliente en un formato estándar y la eliminación segura de los datos en sus infraestructuras tras el periodo de gracia establecido.

5.6 ACEPTACIÓN DE NORMAS

Al hacer uso de los servicios, el Cliente acepta que su personal debe cumplir con las directrices éticas y de uso aceptable de los activos, prohibiendo el uso del servicio para fines ilegales, envío de spam o almacenamiento de contenido malicioso.

El uso del servicio implica la aceptación de este acuerdo, así como de los Términos y Condiciones del software R-SALES®. TÉRMINOS Y CONDICIONES DE USO DEL SOFTWARE COMO SERVICIO (SaaS) R-SALES® "VENTAS REMOTAS"