

TECTRIL

Política de Retención y Eliminación de Documentos

Gobernanza del ciclo de vida de documentos y registros físicos y digitales

Esta política establece criterios para la creación, clasificación, conservación, acceso, preservación y eliminación segura de los registros de Tectril.

Código del documento	POL – Tectril – 03-ES
Revisión	Rev. 0
Clasificación	Uso institucional — publicación sujeta a aprobación
Responsable	Compliance, Privacidad y áreas propietarias de los registros
Aprobación	Dirección de Tectril
Vigencia	A partir de la aprobación formal

BORRADOR INSTITUCIONAL. La tabla de retención debe ser validada por especialistas jurídicos, contables, fiscales, laborales y de privacidad antes de su aprobación e implantación.

1. Objetivo

Establecer reglas uniformes para gestionar el ciclo de vida de los documentos y registros de Tectril, garantizando disponibilidad, integridad, autenticidad, confidencialidad, trazabilidad y eliminación segura, sin conservación excesiva de datos personales ni pérdida de evidencias necesarias.

2. Alcance

Se aplica a administradores, empleados, temporales, pasantes y terceros que creen, reciban, utilicen, almacenen o eliminen registros en nombre de Tectril Soluções em Logística e Comércio Ltda., independientemente del país, área, formato, sistema, dispositivo o lugar de almacenamiento.

- Documentos en papel, microfilm y otros soportes físicos.
- Archivos electrónicos, bases de datos, sistemas corporativos, nube, correos, mensajes y grabaciones.
- Registros de clientes, proveedores, socios, aduanas, finanzas, personas, compliance, privacidad, seguridad, SST y Canal de Integridad.
- Copias, backups, exportaciones de sistemas y registros conservados por encargados o proveedores contratados.

3. Principios

- Finalidad y necesidad: conservar solo lo necesario para fines legítimos y documentados.
- Cumplimiento: observar leyes, contratos, requisitos regulatorios y reglas de los países involucrados.
- Integridad y autenticidad: proteger contenido, contexto, autoría, fechas y trazabilidad.
- Acceso mínimo: restringir el acceso según función, sensibilidad y necesidad de conocer.
- Disponibilidad y recuperación: mantener los registros localizables y legibles durante todo el plazo.
- Eliminación defendible: eliminar de forma autorizada, coherente, registrada e irreversible.
- Plazo válido más largo: ante requisitos concurrentes, aplicar el plazo válido más extenso.

4. Definiciones

Documento o registro es la información creada o recibida como evidencia de una actividad, decisión, obligación, transacción o derecho. Registro oficial es la versión reconocida como fuente autorizada. Propietario del registro es el área responsable del contenido y del plazo. Repositorio oficial es el entorno aprobado de almacenamiento y recuperación. Plazo de retención es el período mínimo de conservación. Destinación es la destrucción segura, anonimización, devolución, transferencia o preservación permanente. Legal hold es la orden que suspende la alteración o eliminación.

5. Clasificación y fuente autorizada

Cada área deberá identificar sus registros, clasificarlos por proceso, sensibilidad y obligación, y almacenar la versión oficial en un repositorio aprobado. Las copias de conveniencia no sustituyen la fuente autorizada. La información confidencial, los datos sensibles, los secretos comerciales, las credenciales y las investigaciones requieren protección reforzada.

- Nombre y descripción de la categoría.
- Área propietaria y personas autorizadas.
- Evento que inicia el plazo.

- Plazo aplicable y fundamento.
- Sistema o ubicación oficial.
- Destinación final y necesidad de certificado de destrucción.

6. Cómputo y revisión de plazos

El plazo comienza en el evento definido en la tabla, como vencimiento contractual, terminación laboral, conclusión de la operación, pago, decisión definitiva o sustitución de versión. Las áreas propietarias revisarán al menos anualmente la necesidad de conservación e informarán a Compliance y Privacidad sobre cambios relevantes.

Regla de seguridad: ningún plazo de esta política autoriza la eliminación si existe investigación, auditoría, fiscalización, disputa, incidente, solicitud de autoridad, solicitud pendiente del titular u orden de preservación.

7. Suspensión de eliminación (legal hold)

Cuando un evento pueda exigir preservación, Jurídico, Compliance, Privacidad o la Dirección podrán emitir un legal hold que identifique alcance, custodios, sistemas, período y criterios de liberación.

- Suspender inmediatamente eliminaciones manuales y automáticas.
- Preservar documentos, metadatos, mensajes, adjuntos, logs y backups relevantes.
- Notificar a los custodios y obtener confirmación.
- Controlar el acceso y la cadena de custodia.
- Reanudar el plazo solo después de la liberación escrita del área emisora.

8. Almacenamiento, acceso y seguridad

- Utilizar únicamente repositorios, cuentas y dispositivos aprobados.
- Aplicar acceso por función, autenticación, registro de actividad y cifrado cuando corresponda.
- Mantener backups y pruebas de restauración proporcionales a la criticidad.
- No conservar registros oficiales únicamente en buzones personales, mensajería, computadoras locales o medios removibles no gestionados.
- Exigir a los proveedores obligaciones de retención, devolución, portabilidad y supresión al terminar el contrato.
- Preservar la legibilidad y migrar medios o formatos obsoletos cuando sea necesario.

9. Datos personales

Los datos personales se conservarán únicamente durante el tiempo necesario para la finalidad o sobre una base legal de conservación. Al finalizar, serán eliminados, anonimizados o bloqueados, salvo conservación autorizada. Tectril documentará base, finalidad, plazo y controles de acceso y atenderá las solicitudes de titulares sin eliminar evidencia exigida por ley o para el ejercicio regular de derechos.

10. Eliminación segura y evidencia

La eliminación exige confirmar el vencimiento del plazo, la inexistencia de legal hold y la autorización del propietario. El método deberá impedir la reconstrucción o el acceso no autorizado.

- Papel: trituración segura o destrucción certificada.
- Medios: saneamiento, sobrescritura o destrucción física según el riesgo.
- Sistemas y nube: eliminación lógica y, cuando corresponda, expiración de backups según el ciclo técnico.
- Datos estructurados: supresión, anonimización irreversible o agregación validada.
- Terceros: certificado de destrucción o evidencia equivalente.
- Registro de eliminación: categoría, período, volumen, método, fecha, autorizaciones, ejecutor y excepciones.

11. Responsabilidades

11.1 Dirección

Aprobar esta política, asignar recursos y decidir excepciones relevantes.

11.2 Compliance, Jurídico y Privacidad

Orientar requisitos, coordinar legal holds, evaluar riesgos, monitorear el cumplimiento y promover actualizaciones.

11.3 Áreas propietarias

Inventariar registros, identificar la fuente autorizada, aplicar plazos, autorizar la eliminación y conservar evidencias.

11.4 Tecnología de la Información y Seguridad

Implantar controles técnicos, backups, logs, preservación, recuperación y eliminación segura.

11.5 Usuarios y terceros

Archivar correctamente, proteger los registros, cumplir las suspensiones y no eliminar, alterar o retirar documentos sin autorización.

12. Excepciones, incidentes y consecuencias

Las excepciones requieren justificación documentada y aprobación de Compliance, Privacidad, Jurídico o Dirección según el riesgo. La pérdida, alteración, eliminación o acceso no autorizado deberá comunicarse inmediatamente a compliance@tectril.com.br y, si involucra datos personales, a privacidade@tectril.com.br. Las infracciones podrán dar lugar a medidas disciplinarias, contractuales y legales.

13. Tabla corporativa mínima de retención

La tabla siguiente es una referencia corporativa inicial. Cada área deberá confirmar el plazo legal o contractual específico y el evento correcto de inicio. “Fin + plazo” significa desde el cierre definitivo, salvo regla distinta.

Categoría	Ejemplos de registros	Plazo mínimo	Observaciones
-----------	-----------------------	--------------	---------------

Categoría	Ejemplos de registros	Plazo mínimo	Observaciones
Societarios y gobierno	Estatutos, modificaciones, actas, poderes estratégicos y registros de gobierno.	Permanente	Preservar versiones firmadas y el historial societario.
Políticas y gobierno	Políticas aprobadas, códigos, aprobaciones e historial de revisiones.	Vigencia + 10 años	Las versiones de valor histórico pueden ser permanentes.
Contables, fiscales y tributarios	Libros, declaraciones, facturas, guías, cálculos y soporte.	10 años	Base conservadora; ampliar por créditos, cuotas, activos o controversias.
Aduanas y comercio exterior	DI/DUIMP, DU-E, LI/LPCO, invoices, packing lists, documentos de transporte, regímenes especiales y prueba de cierre.	10 años después del cierre	En regímenes suspendidos o asuntos pendientes, contar después de la extinción o decisión final.
Contratos y terceros	Contratos, propuestas aceptadas, adendas, due diligence y evidencia de ejecución.	Fin + 10 años	Garantías, indemnizaciones o investigaciones pueden ampliar el plazo.
Clientes y operaciones	Órdenes, instrucciones, aprobaciones, evidencia operativa, facturación y comunicaciones materiales.	Cierre + 10 años	Evitar duplicados sin valor probatorio.
Finanzas y bancos	Extractos, pagos, conciliaciones, funding, cambio y comprobantes.	10 años	Observar requisitos bancarios, fiscales y contractuales.
Laborales y personal	Expediente, jornada, vacaciones, beneficios, nómina y terminación.	Fin + 5 años; nómina: 10 años	Seguridad social, FGTS y prueba del vínculo pueden exigir más tiempo.
SST y salud ocupacional	PGR, PCMSO, ASO, registros médicos ocupacionales, exposiciones y accidentes.	20 años o plazo legal mayor	Acceso restringido; aplicar reglas específicas a registros médicos y exposiciones.
Selección no contratada	CV, evaluaciones y comunicaciones con candidatos.	6 meses	Plazo mayor solo con consentimiento u otra base documentada.
Privacidad y seguridad	Inventarios, evaluaciones, consentimientos, solicitudes, incidentes, logs y evidencia.	5 años después del cierre	Los logs técnicos pueden ser más breves; preservar evidencia de cumplimiento.
Acceso a aplicaciones	Registros de acceso a aplicaciones cuando Tectril sea proveedor legalmente obligado.	6 meses	Aplicar el Marco Civil de Internet y controles de seguridad.
Canal de Integridad e investigaciones	Reportes, triage, investigación, medidas y evidencias.	Cierre + 10 años	Segregación, confidencialidad y acceso estrictamente restringido.
Jurídico y litigios	Dictámenes, notificaciones, procesos, acuerdos y pruebas.	Cierre definitivo + 10 años	Prevalece el legal hold; registros estructurales pueden ser permanentes.
Marketing y sitio web	Aprobaciones, campañas, licencias de imagen, versiones publicadas y métricas.	Cierre + 5 años	Licencias y cesiones siguen el contrato o plazo permanente.
CCTV y acceso físico	Imágenes y registros de entrada/salida.	30 a 90 días	Salvo incidente, investigación o exigencia contractual.
Correos y mensajes	Comunicaciones con valor decisorio, contractual, fiscal, operativo o probatorio.	Según la categoría del contenido	Archivar en el repositorio oficial; el buzón no es un archivo permanente.
Copias y borradores	Duplicados, versiones intermedias y notas sin valor legal u operativo.	Hasta 90 días	Eliminar al perder utilidad, sujeto a cualquier suspensión.
Backups	Copias de seguridad de sistemas y repositorios.	Ciclo técnico de 30 a 180 días	El backup no sustituye el archivo oficial; aplicar rotación segura.

14. Procedimiento de implantación

- Asignar propietarios por categoría y completar el inventario de repositorios.
- Validar plazos con Jurídico, Contabilidad, Fiscal, RR. HH., SST, Privacidad y Comercio Exterior.
- Configurar automatizaciones solo después de validación y prueba.
- Crear formulario de legal hold y registro central de eliminación.
- Capacitar a usuarios e incluir obligaciones en contratos con terceros.
- Realizar revisión anual y auditorías por muestreo.

15. Monitoreo y revisión

Compliance coordinará la revisión al menos anualmente o ante cambios legales, tecnológicos, contractuales u operativos relevantes. Los indicadores podrán incluir categorías inventariadas, legal holds activos, eliminaciones certificadas, excepciones, incidentes y repositorios fuera del estándar.

16. Disposiciones finales

Esta política entra en vigor tras su aprobación formal. En caso de duda, prevalecerán la preservación temporal y la consulta a Compliance, Jurídico o Privacidad. Un plazo mínimo no autoriza conservación indefinida sin finalidad o fundamento.

17. Principales referencias normativas

- Ley brasileña n.º 13.709/2018 — Ley General de Protección de Datos (LGPD), especialmente arts. 15 y 16.
- Ley brasileña n.º 12.965/2014 — Marco Civil de Internet, cuando corresponda a registros de acceso.
- Ley brasileña n.º 5.172/1966 — Código Tributario Nacional, incluidas reglas de decadencia y prescripción.
- Código Civil y normas laborales, previsionales, de SST, fiscales y aduaneras aplicables.
- Contratos, licencias, órdenes de autoridades y requisitos de los países donde opere Tectril.

18. Control de aprobación y revisión

Etapas	Responsable	Fecha	Registro/firma
Elaboración / revisión	Compliance y Privacidad	____/____/____	_____