Marco legal argentino y responsabilidad jurídica en Tecnologías de Información

1.1 Presentación del tema

Las organizaciones que operan en Argentina y utilizan sistemas de información para procesar datos, ejecutar transacciones, gestionar personal, administrar clientes, contratar proveedores o prestar servicios están sujetas a obligaciones legales. Estas obligaciones no son recomendaciones generales ni declaraciones de buenas intenciones. Son reglas cuyo incumplimiento puede generar responsabilidad administrativa, civil, penal, laboral o contractual, según el caso.

Desde la administración de Tecnologías de Información, el marco legal no debe verse como un elemento externo al negocio. Debe traducirse en controles, procedimientos, cláusulas contractuales, políticas internas, evidencias, registros y prácticas de gestión. Un sistema que procesa datos personales sin medidas de seguridad suficientes no representa solo un riesgo técnico. También puede representar un incumplimiento legal. Un incidente de seguridad mal gestionado no solo afecta la operación. También puede comprometer la responsabilidad jurídica de la organización.

Para estudiantes de administración de empresas, el tema resulta importante porque las decisiones sobre datos, sistemas, proveedores, accesos, contratos, confidencialidad, investigación de incidentes y conservación de evidencias tienen consecuencias legales. No se espera que el administrador actúe como abogado, pero sí que comprenda cuándo una decisión tecnológica requiere control jurídico, coordinación con el área legal y documentación adecuada.

Este material tiene finalidad académica. No constituye asesoramiento jurídico. Su objetivo es ordenar los principales aspectos del marco legal argentino aplicable a Tecnologías de Información y mostrar cómo se conectan con la gestión administrativa.

1.2 El marco legal como parte de la gestión de TI

El marco legal de TI debe analizarse como parte del gobierno organizacional. Una norma no se cumple solo porque se la conoce. Se cumple cuando la organización la convierte en procedimientos concretos y deja evidencia de su aplicación.

Norma o ámbito jurídico	Pregunta administrativa	Control esperado
Protección de datos personales	¿Qué datos se recolectan y con qué finalidad?	Registro, políticas de privacidad, seguridad y respuesta a derechos del titular
Delitos informáticos	¿Qué conductas digitales pueden generar responsabilidad penal?	Controles de acceso, logs, segregación y respuesta a incidentes
Responsabilidad civil	¿Qué daños puede causar una falla de seguridad?	Prevención, gestión de riesgos, seguros, contratos y evidencia
Derecho laboral	¿Qué obligaciones tienen los empleados al usar sistemas?	Política de uso aceptable, confidencialidad, sanciones y capacitación
Contratos tecnológicos	¿Qué exige la organización a sus proveedores?	Cláusulas de seguridad, SLA, auditoría, notificación de incidentes
Evidencia digital	¿Cómo se prueba un hecho ocurrido en sistemas?	Logs íntegros, cadena de custodia, preservación y trazabilidad

El criterio de gestión es simple: toda obligación legal debe traducirse en una práctica verificable. Si una organización afirma que protege datos personales, debe poder

demostrar qué datos trata, quién accede, qué medidas de seguridad aplica, cómo responde solicitudes y cómo conserva evidencia.

1.3 Protección de datos personales: Ley 25.326

La Ley 25.326 de Protección de Datos Personales es el marco normativo central en Argentina para el tratamiento de datos personales. Su finalidad es proteger integralmente los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento, públicos o privados destinados a dar informes.

Un dato personal es toda información referida a una persona física determinada o determinable. Puede identificarla de manera directa, como nombre, documento o correo electrónico, o de manera indirecta, mediante combinaciones de datos. Un dato sensible es aquel que revela aspectos especialmente protegidos, como origen racial o étnico, opiniones políticas, convicciones religiosas, afiliación sindical, información de salud o vida sexual.

Concepto	Explicación	Ejemplo
Dato personal	Información que identifica o permite identificar a una persona	Nombre, DNI, correo electrónico, número de cliente
Dato sensible	Información especialmente protegida	Salud, religión, afiliación sindical
Responsable de base de datos	Organización o persona que decide sobre el tratamiento	Empresa que administra una base de clientes
Titular del dato	Persona a quien corresponde la información	Cliente, empleado, proveedor persona humana

Concepto	Explicación	Ejemplo
Tratamiento	Operación sobre datos personales	Recolección, almacenamiento, consulta, cesión o eliminación

Desde TI, la Ley 25.326 obliga a pensar la protección de datos como un proceso completo. No se trata solo de guardar una base en un servidor. Debe definirse qué datos se recolectan, por qué se recolectan, quién accede, cuánto tiempo se conservan, cómo se protegen y cómo se eliminan.

1.4 Derechos de los titulares de datos

Los titulares de datos tienen derechos reconocidos legalmente. Entre ellos se encuentran el derecho de acceso, rectificación, actualización, supresión y, en ciertos casos, oposición al tratamiento.

El derecho de acceso permite que una persona solicite información sobre los datos personales que una organización conserva sobre ella. La Ley 25.326 prevé que el responsable debe proporcionar la información solicitada dentro del plazo legal aplicable. La rectificación, actualización o supresión procede cuando los datos sean incorrectos, estén desactualizados o corresponda eliminarlos.

Derecho	Qué permite solicitar	Implicancia para TI
Acceso	Conocer qué datos se tienen sobre la persona	Capacidad de búsqueda y respuesta documentada
Rectificación	Corregir datos incorrectos	Procedimiento de modificación y evidencia
Actualización	Poner datos al día	Control de versión y fecha de cambio

Derecho	Qué permite solicitar	Implicancia para TI
Supresión	Eliminar datos cuando corresponda	Borrado seguro y trazabilidad
Oposición	Oponerse a ciertos tratamientos cuando sea procedente	Gestión de preferencias o restricciones

Para cumplir estos derechos, los sistemas deben permitir localizar datos, identificar su origen, verificar quién los modificó, corregirlos, eliminarlos cuando corresponda y dejar registro de la acción realizada.

Ejemplo: una empresa de comercio electrónico almacena nombre, domicilio, historial de compras y datos de contacto de sus clientes. Si un cliente solicita acceso o rectificación, la organización debe tener un procedimiento para recibir la solicitud, verificar identidad, consultar los sistemas involucrados, responder dentro del plazo legal y documentar la respuesta.

1.5 Medidas de seguridad sobre datos personales

La protección de datos personales requiere medidas técnicas y organizacionales. Las medidas técnicas pueden incluir control de accesos, autenticación multifactor, cifrado, backups, registros de actividad, monitoreo, segmentación y eliminación segura. Las medidas organizacionales incluyen políticas, capacitación, responsabilidades, contratos, auditorías y procedimientos de respuesta.

Riesgo sobre datos personales	Control técnico	Control organizacional
Acceso no autorizado	Perfiles, MFA, mínimo privilegio	Aprobación de accesos y revisión periódica
Fuga de datos	Cifrado, DLP, monitoreo de descargas	Clasificación de información y capacitación

Riesgo sobre datos personales	Control técnico	Control organizacional
Datos incorrectos	Validaciones y pistas de auditoría	Procedimiento de rectificación
Pérdida de datos	Backup y restauración probada	Plan de continuidad y responsables
Conservación innecesaria	Retención y eliminación segura	Política de conservación documental
Uso indebido por terceros	Registros y control de accesos externos	Contratos y auditoría a proveedores

La seguridad debe adecuarse al tipo de dato tratado. No requiere el mismo nivel de protección una base pública de información institucional que una base con datos salariales, cuentas bancarias o información de salud.

Desde administración, la pregunta central no es solo "qué dice la ley", sino qué evidencia permite demostrar que la organización adoptó medidas razonables. Sin evidencia, la defensa ante un reclamo o incidente se debilita.

1.6 Delitos informáticos: Ley 26.388 y Código Penal

La Ley 26.388 modificó el Código Penal argentino para incorporar figuras vinculadas con sistemas informáticos, datos, comunicaciones digitales y documentos electrónicos. No creó un código penal informático separado. Adaptó figuras penales existentes para contemplar conductas realizadas mediante medios digitales.

Conducta	Descripción general	Riesgo organizacional
Acceso ilegítimo	Ingreso sin autorización o excediendo permisos	Intrusión, abuso de credenciales o acceso de ex empleados

Conducta	Descripción general	Riesgo organizacional
Daño informático	Destrucción, inutilización o alteración de datos o sistemas	Borrado de bases, sabotaje, interrupción
Fraude informático	Manipulación informática para obtener beneficio indebido	Desvío de pagos, alteración de registros
Violación de secretos	Acceso, revelación o difusión indebida de comunicaciones o información privada	Exposición de correos, bases de clientes o información confidencial
Interceptación o divulgación	Captura o difusión de comunicaciones electrónicas	Riesgo en correo, mensajería y redes

Ejemplo: un empleado desvinculado accede con credenciales aún activas al servidor de la empresa y elimina bases de datos de clientes. La conducta puede involucrar acceso ilegítimo y daño informático. La organización, a su vez, queda expuesta a una pregunta administrativa: por qué esas credenciales seguían activas luego de la desvinculación.

La prevención penal se conecta con controles de TI. La organización debe administrar accesos, revocar permisos, registrar operaciones, conservar logs y preservar evidencia. Sin estos elementos, resulta más difícil demostrar qué ocurrió, quién intervino y qué daño se produjo.

1.7 Acceso ilegítimo, abuso de privilegios y bajas de usuarios

El acceso ilegítimo no se limita al ingreso de un atacante externo. También puede producirse cuando una persona excede los permisos que tiene o cuando conserva accesos que debieron haber sido revocados.

La baja de accesos es un control legal, laboral y de seguridad. Cuando una persona deja la organización o cambia de puesto, sus permisos deben revisarse de inmediato. Si la organización demora la baja, aumenta el riesgo de acceso indebido, manipulación de datos y conflicto probatorio.

Situación	Riesgo	Control
Usuario desvinculado sigue activo	Acceso posterior no autorizado	Baja inmediata de accesos
Cambio de puesto sin revisión	Acumulación de permisos	Revisión por transferencia interna
Cuentas compartidas	Imposibilidad de atribuir acciones	Usuarios individuales
Cuenta administrativa permanente	Abuso de privilegios	PAM, aprobación temporal y logs
Proveedor conserva acceso	Riesgo de tercero	Acceso con vencimiento y monitoreo

Ejemplo: una persona pasa del área de proveedores al área de auditoría interna. Si conserva permisos para modificar cuentas bancarias y además recibe permisos de revisión, puede quedar en una posición incompatible. La transferencia debe activar una revisión completa de accesos.

1.8 Evidencia digital

La evidencia digital incluye registros electrónicos que pueden servir para reconstruir hechos, probar operaciones, demostrar accesos, verificar modificaciones o documentar incidentes. Puede utilizarse en investigaciones internas, auditorías, reclamos civiles, causas penales, conflictos laborales o procedimientos administrativos.

Tipo de evidencia digital	Ejemplo
Logs de sistema	Ingresos, intentos fallidos, cambios de permisos
Correos electrónicos	Comunicaciones internas o externas
Archivos	Documentos, bases, planillas, reportes
Registros transaccionales	Pagos, facturas, aprobaciones, anulaciones
Capturas con metadatos	Evidencia visual acompañada de fecha y origen
Imágenes forenses	Copias técnicas de discos o dispositivos
Registros de red	Conexiones, tráfico, direcciones IP
Tickets o solicitudes	Pedidos de soporte, aprobaciones o incidentes

La evidencia digital debe preservar integridad, autenticidad y trazabilidad. No basta con tener una captura de pantalla o un archivo exportado. Debe poder demostrarse de dónde salió, quién lo obtuvo, cuándo, con qué método, si fue alterado y quién tuvo acceso.

1.9 Valor probatorio de logs

Los logs son registros automáticos de actividad. Permiten reconstruir accesos, cambios, errores, operaciones, intentos fallidos y acciones administrativas. Para que tengan valor probatorio, deben cumplir condiciones técnicas y procedimentales.

Requisito	Finalidad
Hora sincronizada	Ordenar cronológicamente los hechos
Integridad de registros	Evitar alteraciones o eliminaciones

Requisito	Finalidad
Identificación de usuario	Atribuir acciones a una cuenta individual
Retención suficiente	Conservar evidencia durante el período necesario
Acceso restringido	Evitar manipulación por usuarios no autorizados
Procedimiento de extracción	Documentar cómo se obtuvieron los registros
Registro de acceso a logs	Saber quién consultó o extrajo evidencia
Correlación entre sistemas	Comparar eventos de distintas fuentes

La sincronización horaria mediante NTP es relevante porque permite que los eventos registrados por distintos sistemas sean comparables. Si el servidor de pagos, el servidor de correo y el servidor de logs tienen horarios diferentes, reconstruir una secuencia de hechos puede volverse difícil.

Ejemplo: una empresa presenta logs que muestran que un usuario aprobó transferencias no autorizadas. Si los registros tienen hora consistente, no muestran alteraciones, identifican al usuario y fueron preservados con cadena de custodia, su valor probatorio aumenta. Si los logs pueden ser modificados por cualquier administrador o si la hora del sistema es inconsistente, la evidencia se debilita.

1.10 Cadena de custodia

La cadena de custodia es el registro documentado de todas las personas que tuvieron contacto con la evidencia desde su identificación hasta su presentación en un proceso interno, administrativo o judicial.

Debe indicar quién identificó la evidencia, cuándo se recolectó, cómo se preservó, dónde se almacenó, quién accedió, cuándo se trasladó y qué acciones se realizaron sobre ella.

Etapa	Acción esperada
Identificación	Determinar qué evidencia es relevante
Preservación	Evitar alteración o pérdida
Recolección	Obtener evidencia con método documentado
Registro	Documentar fecha, responsable y procedimiento
Almacenamiento	Guardar en entorno seguro y controlado
Acceso	Limitar consulta a personas autorizadas
Análisis	Trabajar sobre copias, no sobre originales
Presentación	Mantener trazabilidad hasta el uso formal

Ejemplo: ante un incidente, el área de TI no debería modificar el equipo afectado ni trabajar directamente sobre el disco original si el caso puede derivar en acciones legales. Debe preservarse la evidencia, generar una copia forense cuando corresponda, calcular hash, documentar cada paso e involucrar al área legal.

Una cadena de custodia incompleta puede debilitar o invalidar evidencia, aunque el contenido parezca verdadero.

1.11 Informática forense e investigaciones internas

La informática forense es la disciplina que establece procedimientos para recolectar, preservar, analizar y presentar evidencia digital de forma técnicamente confiable. Su finalidad no es solo “encontrar información”. Busca que la evidencia pueda sostenerse en una investigación formal.

Una organización debería definir cuándo activar un procedimiento forense. No todos los incidentes requieren ese nivel de formalidad, pero sí aquellos que pueden implicar delitos, daños a terceros, conflictos laborales, fraude, sabotaje, exposición de datos personales o reclamos contractuales.

Situación	Conveniencia de activar protocolo forense
Sospecha de fraude interno	Alta
Acceso no autorizado a datos personales	Alta
Eliminación deliberada de información	Alta
Ransomware con impacto crítico	Alta
Error operativo menor sin daño	Baja o media, según contexto
Fallo técnico común	Baja, salvo recurrencia o impacto

La investigación interna debe coordinarse con el área legal. Si se actúa sin preservar evidencia, la organización puede perder capacidad de reclamar, defenderse o sancionar correctamente.

1.12 Responsabilidad civil por incidentes de seguridad

La responsabilidad civil puede surgir cuando un incidente de seguridad causa daño a terceros. No requiere necesariamente intención de causar daño. Puede basarse en negligencia, impericia, incumplimiento contractual o falta de medidas razonables de prevención.

El Código Civil y Comercial de la Nación incorpora el deber de prevención del daño. En términos de TI, esto significa que la organización debe adoptar medidas razonables para evitar daños previsibles o reducirlos si ya comenzaron.

Daño posible	Ejemplo
Económico directo	Fondos sustraídos por uso de datos filtrados
Daño moral	Afectación por exposición de datos sensibles
Daño reputacional	Pérdida de confianza por brecha de seguridad

Daño posible	Ejemplo
Costos de recuperación	Reposición de documentos, monitoreo o asistencia
Interrupción de servicios	Pérdida por caída prolongada de sistemas

Ejemplo: una plataforma tercerizada de recursos humanos sufre una brecha que expone datos de nómina, documentos y cuentas bancarias de empleados. Los afectados pueden reclamar daños a la empresa que contrató la plataforma y al proveedor, según el caso. La empresa contratante puede repetir contra el proveedor si el contrato contiene cláusulas adecuadas.

Desde administración, la prevención civil exige gestión de riesgos, contratos claros, controles de seguridad, auditoría de proveedores, políticas internas y evidencia de cumplimiento.

1.13 Responsabilidad contractual con proveedores tecnológicos

Cuando una organización contrata un servicio tecnológico, puede delegar parte de la operación, pero no desaparece su responsabilidad sobre los datos y procesos involucrados. Por eso, los contratos con proveedores deben incorporar cláusulas de seguridad.

Cláusula recomendada	Contenido esperado
Medidas de seguridad	Controles técnicos y organizacionales exigidos
Confidencialidad	Obligación de reserva sobre datos e información
Notificación de incidentes	Plazo y forma de informar brechas o fallas
Accesos del proveedor	Usuarios autorizados, permisos y registros

Cláusula recomendada	Contenido esperado
Derecho de auditoría	Posibilidad de revisar controles o evidencias
Ubicación de datos	País o región donde se almacenan o procesan
Subcontratación	Reglas para terceros del proveedor
Borrado o devolución	Tratamiento de datos al finalizar el contrato
SLA	Disponibilidad, soporte y tiempos de respuesta
Responsabilidad	Consecuencias por incumplimiento

Ejemplo: una empresa contrata un proveedor de nube para alojar su sistema de gestión de clientes. Si el contrato no contiene cláusulas de seguridad, notificación de incidentes, acceso a logs, responsabilidad y salida ordenada, la empresa puede quedar en una posición débil ante una brecha.

La contratación tecnológica debe verse como una decisión de riesgo. No alcanza con evaluar precio y funcionalidad. Deben evaluarse seguridad, continuidad, cumplimiento legal, soporte, ubicación de datos y evidencia disponible.

1.14 Acuerdos de nivel de servicio

Los SLA son acuerdos de nivel de servicio. Definen compromisos del proveedor sobre disponibilidad, rendimiento, soporte, tiempos de respuesta, recuperación, notificación de incidentes y, cuando corresponde, seguridad.

Elemento del SLA	Pregunta de gestión
Disponibilidad	¿Qué porcentaje de tiempo debe estar operativo el servicio?
Soporte	¿En qué horarios se atienden incidentes?
Tiempo de respuesta	¿Cuánto tarda el proveedor en atender un reporte?
Tiempo de resolución	¿Cuánto tarda en resolver o escalar?
RTO	¿En cuánto tiempo debe recuperarse el servicio?
RPO	¿Cuánta información puede perderse como máximo?
Penalidades	¿Qué ocurre si no se cumple el servicio?
Reportes	¿Qué evidencia entrega el proveedor?

Ejemplo: una empresa de logística depende de un sistema de seguimiento de envíos administrado por un proveedor. Si el contrato no define RTO, RPO ni penalidades, una caída de cuarenta y ocho horas puede generar daños operativos sin herramientas contractuales suficientes para reclamar.

1.15 Responsabilidad laboral por uso indebido de sistemas

Los empleados que utilizan sistemas de información tienen obligaciones derivadas del contrato de trabajo, reglamentos internos y políticas de uso aceptable. El uso indebido de sistemas puede generar consecuencias laborales, según la gravedad de la conducta y la evidencia disponible.

La Ley de Contrato de Trabajo prevé que el empleador puede extinguir el vínculo con justa causa cuando exista injuria que impida la continuidad de la relación laboral. En el contexto de TI, ciertas conductas pueden ser graves: acceso no autorizado a información

confidencial, extracción de bases de datos, instalación de software prohibido, manipulación de registros, divulgación de información o daño deliberado.

Conducta	Riesgo laboral y organizacional
Exportar base de clientes sin autorización	Violación de confidencialidad y posible daño comercial
Compartir contraseñas	Pérdida de trazabilidad y acceso indebido
Instalar software no autorizado	Riesgo de malware y violación de licencias
Acceder a datos fuera de función	Abuso de privilegios
Borrar registros deliberadamente	Daño informático y afectación operativa
Usar sistemas para fines personales indebidos	Incumplimiento de políticas internas

Para aplicar consecuencias laborales, la organización debe haber comunicado formalmente sus políticas, prohibiciones y consecuencias. Una política desconocida o no documentada resulta más difícil de exigir.

1.16 Política de uso aceptable

La política de uso aceptable de TI establece qué se permite y qué se prohíbe en el uso de sistemas, redes, correo, dispositivos, aplicaciones y datos de la organización. Tiene importancia técnica, administrativa y legal.

Contenido de una política de uso aceptable	Finalidad
Uso permitido de sistemas	Definir actividades autorizadas
Prohibición de compartir claves	Preservar trazabilidad
Instalación de software	Evitar programas no autorizados

Contenido de una política de uso aceptable	Finalidad
Uso de correo y mensajería	Controlar comunicaciones laborales
Tratamiento de información confidencial	Proteger datos sensibles
Monitoreo permitido	Informar controles de la organización
Consecuencias del incumplimiento	Establecer marco disciplinario
Reporte de incidentes	Indicar cómo actuar ante eventos de seguridad

Ejemplo: un empleado exporta la base completa de contactos del CRM antes de renunciar. Si existen logs, clasificación de datos, política firmada y prohibición expresa de extracción, la organización cuenta con mejor base para iniciar acciones internas, civiles o penales.

1.17 Obligaciones de confidencialidad

Las obligaciones de confidencialidad pueden surgir de la ley, el contrato o la política interna. En TI, se aplican a empleados, proveedores, consultores, auditores, técnicos externos y cualquier persona que acceda a información no pública.

Fuente de confidencialidad	Ejemplo
Ley	Deber de reserva sobre datos personales
Contrato	NDA con proveedor o consultor
Política interna	Reglas de tratamiento de información confidencial
Relación laboral	Deber de fidelidad y reserva
Normas sectoriales	Reglas especiales para salud, finanzas u otras actividades

Un NDA debe definir qué información es confidencial, quiénes están obligados, qué usos se permiten, por cuánto tiempo se mantiene la obligación, cómo se devuelve o elimina la información y qué consecuencias existen ante incumplimiento.

Ejemplo: un consultor externo accede a logs financieros, bases de clientes y configuraciones de red. Si el contrato no incluye un NDA adecuado, la organización tiene menos herramientas contractuales para exigir reserva, devolución o sanción ante un uso indebido.

1.18 Proveedores, terceros y cadena de suministro

La seguridad de la información no termina en los sistemas propios. Cuando una organización permite que proveedores, socios, consultores o empresas de outsourcing procesen datos o accedan a sistemas, extiende su superficie de riesgo.

La seguridad de la cadena de suministro implica evaluar, contratar, controlar y cerrar relaciones con terceros de manera segura.

Etapa	Control esperado
Evaluación previa	Revisar antecedentes, certificaciones, controles y riesgos
Contratación	Incluir cláusulas de seguridad, confidencialidad y auditoría
Alta del proveedor	Asignar accesos mínimos y con vigencia definida
Operación	Monitorear actividad, incidentes y cumplimiento
Revisión periódica	Verificar permisos y controles del proveedor

Etapa	Control esperado
Finalización	Revocar accesos, devolver activos y borrar datos
Evidencia	Conservar registros de cumplimiento y comunicaciones

Ejemplo: un proveedor de soporte técnico conserva acceso remoto permanente a servidores críticos. Si no hay MFA, registro de actividad, vencimiento, justificación ni revisión periódica, existe un riesgo relevante. La comodidad operativa no justifica accesos indefinidos sin control.

1.19 Neutralidad de red y seguridad organizacional

La neutralidad de red es el principio según el cual los proveedores de acceso a Internet deben tratar el tráfico de manera no discriminatoria, sin restricciones arbitrarias por origen, destino, contenido, aplicación o servicio. En Argentina, la Ley 27.078 reconoce este principio. El artículo 56 garantiza la neutralidad de red y el artículo 57 establece prohibiciones para los prestadores de servicios de TIC.

Desde la seguridad de TI, este tema debe distinguirse correctamente. La neutralidad de red se aplica a los prestadores de acceso a Internet, no a las redes privadas internas de una organización. Una empresa puede aplicar controles de seguridad sobre su propia red, como filtros, firewalls, bloqueo de sitios maliciosos o restricciones de navegación, siempre que respete el marco legal laboral, contractual y de privacidad aplicable.

Situación	Relación con neutralidad de red
Proveedor de Internet bloquea tráfico arbitrariamente	Puede involucrar neutralidad de red
Empresa bloquea malware en su red interna	Medida de seguridad corporativa

Situación	Relación con neutralidad de red
Empresa filtra sitios no laborales desde equipos corporativos	Política interna, no neutralidad de red
Organización prioriza tráfico crítico interno	Gestión de red privada
ISP degrada un servicio específico sin causa válida	Puede afectar principio de neutralidad

Ejemplo: una organización implementa filtrado de contenido para bloquear sitios maliciosos desde su red interna. Esa medida no viola la neutralidad de red, porque no actúa como proveedor de acceso a Internet frente al público. Es un control de seguridad dentro de una red corporativa.

1.20 Relación entre norma, control y evidencia

El cumplimiento legal en TI debe expresarse en tres niveles: norma, control y evidencia. La norma indica la obligación. El control muestra cómo la organización intenta cumplirla. La evidencia demuestra que el control se aplicó.

Norma u obligación	Control	Evidencia
Proteger datos personales	Perfiles de acceso y cifrado	Listado de permisos, logs y configuración
Responder derechos del titular	Procedimiento de solicitudes	Registro de pedidos y respuestas
Evitar accesos indebidos	Baja inmediata de usuarios	Fecha de desvinculación y bloqueo
Preservar evidencia digital	Cadena de custodia	Actas, hashes y registro de acceso

Norma u obligación	Control	Evidencia
Exigir seguridad al proveedor	Cláusulas contractuales	Contrato, SLA y reportes
Comunicar políticas internas	Política de uso aceptable	Firma, capacitación y acuse de recibo

Este esquema permite convertir el marco legal en una práctica administrativa. Sin controles, la norma queda como declaración. Sin evidencia, el control queda como afirmación no verificable.

1.21 Ejemplo integrador: incidente con datos de clientes

Una empresa detecta que se descargó una base de clientes desde una cuenta interna fuera del horario habitual. El incidente permite observar cómo se relacionan los conceptos legales y administrativos.

Aspecto	Acción esperada
Seguridad	Bloquear la cuenta y preservar logs
Evidencia	Documentar extracción, hora, usuario y origen
Cadena de custodia	Registrar quién accede a la evidencia
Datos personales	Evaluar si hubo exposición de datos personales
Laboral	Verificar si el usuario era empleado y si violó políticas
Penal	Analizar posible acceso ilegítimo o violación de secretos

Aspecto	Acción esperada
Civil	Evaluar daños potenciales a clientes
Contractual	Revisar si intervino un proveedor o sistema externo
Comunicación	Coordinar con legal, TI y dirección
Acción correctiva	Revisar permisos, alertas y controles de descarga

El análisis no debe comenzar con una conclusión jurídica apresurada. Primero deben preservarse los hechos: qué ocurrió, cuándo, qué datos se afectaron, quién intervino, qué evidencia existe y qué controles fallaron.

1.22 Ejemplo integrador: proveedor tecnológico sin cláusulas de seguridad

Una organización contrata una plataforma externa para gestionar datos de empleados. El contrato solo define precio y funcionalidades, pero no regula seguridad, incidentes, auditoría, ubicación de datos ni devolución al finalizar.

Debilidad contractual	Riesgo
Sin obligación de notificar incidentes	La empresa puede enterarse tarde de una brecha
Sin acceso a logs	Dificultad para investigar
Sin SLA	Falta de compromiso ante caída del servicio
Sin cláusula de confidencialidad	Menor protección contractual de la información

Debilidad contractual	Riesgo
Sin obligación de borrado	Datos retenidos después de finalizar el contrato
Sin derecho de auditoría	Imposibilidad de verificar controles
Sin ubicación de datos	Riesgo en transferencias internacionales

La decisión de contratar tecnología requiere evaluación legal y administrativa. El proveedor puede ejecutar el servicio, pero la organización sigue teniendo responsabilidades frente a empleados, clientes o terceros afectados.

1.23 Ideas clave

- El marco legal de TI debe traducirse en controles, procedimientos y evidencia.
- La Ley 25.326 regula el tratamiento de datos personales en Argentina.
- Los datos sensibles requieren especial protección.
- Los titulares de datos tienen derechos de acceso, rectificación, actualización, supresión y, cuando corresponda, oposición.
- La Ley 26.388 incorporó figuras vinculadas con delitos informáticos al Código Penal.
- La baja oportuna de accesos reduce riesgos legales, laborales y de seguridad.
- Los logs tienen valor probatorio si son íntegros, trazables y técnicamente confiables.
- La cadena de custodia permite preservar evidencia digital para investigaciones o procesos.
- La responsabilidad civil puede surgir por falta de medidas razonables de prevención.

- Los contratos tecnológicos deben incluir cláusulas de seguridad, confidencialidad, incidentes, auditoría y salida.
- Las políticas de uso aceptable tienen valor como control de seguridad y como instrumento legal.
- La confidencialidad puede surgir de la ley, el contrato y las políticas internas.
- La gestión de proveedores forma parte de la seguridad organizacional.
- La neutralidad de red se aplica a prestadores de Internet, no a controles internos de redes corporativas.
- El cumplimiento se demuestra mediante la relación entre norma, control y evidencia.

1.24 Conclusión

El marco legal argentino aplicable a Tecnologías de Información no es un conjunto de normas aisladas. Es un sistema de obligaciones que se relacionan con protección de datos personales, delitos informáticos, responsabilidad civil, relaciones laborales, contratos tecnológicos, confidencialidad, proveedores, evidencia digital y neutralidad de red.

Para la administración de empresas, el aprendizaje central consiste en comprender que el cumplimiento legal en TI requiere gestión. No alcanza con conocer la ley. Deben existir políticas, controles, procedimientos, contratos, registros, responsables y evidencia. La norma establece la obligación; la gestión la convierte en una práctica verificable.

La protección de datos personales exige controlar qué datos se recolectan, quién accede, cómo se conservan, cómo se corrigen y cómo se eliminan. Los delitos informáticos muestran que ciertas conductas digitales pueden tener consecuencias penales. La evidencia digital demuestra que los registros técnicos solo son útiles si se preservan con integridad y cadena de custodia. La responsabilidad civil recuerda que la organización debe prevenir daños razonablemente previsibles. Los contratos con proveedores muestran que tercerizar tecnología no elimina la responsabilidad. El derecho laboral exige políticas

claras para el uso de sistemas. La confidencialidad protege información crítica más allá de la relación contractual.

Una organización que documenta sus decisiones, implementa controles razonables, capacita a su personal, audita proveedores y preserva evidencia se encuentra en una posición mucho más sólida ante incidentes, reclamos o investigaciones. La responsabilidad en TI no es solo técnica ni solo jurídica. Es una responsabilidad de gobierno organizacional.

1.25 Preguntas de evaluación

1. ¿Por qué el marco legal de TI debe entenderse como parte de la gestión organizacional?
2. ¿Qué regula la Ley 25.326 de Protección de Datos Personales?
3. ¿Cuál es la diferencia entre dato personal y dato sensible?
4. ¿Qué derechos tienen los titulares de datos personales?
5. ¿Qué controles debe implementar una organización que trata datos personales?
6. ¿Qué conductas pueden quedar alcanzadas por la Ley 26.388 de delitos informáticos?
7. ¿Por qué la baja inmediata de usuarios desvinculados tiene relevancia legal?
8. ¿Qué es la evidencia digital?
9. ¿Qué condiciones deben cumplir los logs para tener mayor valor probatorio?
10. ¿Por qué la sincronización horaria mediante NTP puede ser relevante en una investigación?
11. ¿Qué es la cadena de custodia?
12. ¿Por qué se recomienda trabajar sobre copias forenses y no sobre evidencia original?

13. ¿En qué casos conviene activar un protocolo de informática forense?
14. ¿Cómo puede surgir responsabilidad civil por un incidente de seguridad?
15. ¿Qué cláusulas deberían incluir los contratos con proveedores tecnológicos?
16. ¿Qué función cumple un SLA?
17. ¿Qué consecuencias laborales puede generar el uso indebido de sistemas?
18. ¿Por qué una política de uso aceptable tiene valor legal y administrativo?
19. ¿Qué es un NDA y qué debería incluir?
20. ¿Qué controles deberían aplicarse sobre proveedores con acceso a datos o sistemas?
21. ¿Cómo se relaciona la neutralidad de red con la seguridad de una red corporativa?
22. ¿Qué significa vincular norma, control y evidencia?
23. ¿Por qué tercerizar un servicio tecnológico no elimina la responsabilidad de la organización?
24. ¿Qué acciones deberían tomarse ante una descarga sospechosa de una base de clientes?
25. ¿Por qué el marco legal de TI requiere coordinación entre dirección, área legal y área técnica?

1.26 Referencias normativas orientativas

- Ley 25.326 de Protección de Datos Personales.
- Decreto 1558/2001, reglamentario de la Ley 25.326.
- Ley 26.388, modificatoria del Código Penal en materia de delitos informáticos.
- Código Penal de la Nación Argentina.

- Código Civil y Comercial de la Nación, especialmente deber de prevención del daño.
- Ley 20.744 de Contrato de Trabajo.
- Ley 27.078 Argentina Digital, especialmente artículos sobre neutralidad de red.
- Normas y criterios de la Agencia de Acceso a la Información Pública aplicables al tratamiento de datos personales.

1.27 Glosario de términos y siglas

Término o sigla	Explicación
AAIP	Agencia de Acceso a la Información Pública. Autoridad de aplicación en materia de protección de datos personales en Argentina.
AUP (*Acceptable Use Policy*)	Política de uso aceptable. Documento interno que regula el uso permitido y prohibido de sistemas, redes, correo, dispositivos y datos.
Chain of custody	Cadena de custodia. Registro documentado de identificación, recolección, preservación, acceso y traslado de evidencia.
CRM (*Customer Relationship Management*)	Sistema de gestión de relaciones con clientes.
Dato personal	Información referida a una persona física determinada o determinable.
Dato sensible	Dato personal especialmente protegido, como salud, religión, origen racial o afiliación sindical.

Término o sigla	Explicación
Digital forensics	Informática forense. Disciplina que recolecta, preserva, analiza y presenta evidencia digital con método técnico.
DLP (*Data Loss Prevention*)	Prevención de pérdida de datos. Controles para evitar salidas no autorizadas de información.
Hash	Huella digital criptográfica que permite verificar si un archivo o registro fue alterado.
Log	Registro automático de eventos de un sistema.
MFA (*Multi-Factor Authentication*)	Autenticación multifactor. Método que exige más de un factor para validar identidad.
NDA (*Non-Disclosure Agreement*)	Acuerdo de no divulgación. Contrato o cláusula que obliga a mantener confidencialidad sobre determinada información.
Net neutrality	Neutralidad de red. Principio de tratamiento no discriminatorio del tráfico de Internet por parte de prestadores de acceso.
NTP (*Network Time Protocol*)	Protocolo de tiempo de red. Permite sincronizar la hora de sistemas y servidores.
PAM (*Privileged Access Management*)	Gestión de accesos privilegiados. Control específico sobre cuentas con permisos elevados.
Phishing	Técnica de engaño para obtener credenciales o información confidencial.
Ransomware	Software malicioso que cifra o bloquea datos y exige una condición o pago para recuperarlos.

Término o sigla	Explicación
RPO (*Recovery Point Objective*)	Objetivo de punto de recuperación. Indica cuánta información puede perderse medida en tiempo.
RTO (*Recovery Time Objective*)	Objetivo de tiempo de recuperación. Indica cuánto tiempo puede estar caído un servicio.
SLA (*Service Level Agreement*)	Acuerdo de nivel de servicio. Define compromisos de disponibilidad, soporte, respuesta, recuperación y penalidades.
Supply chain security	Seguridad de la cadena de suministro. Gestión de riesgos asociados a proveedores y terceros.
TI / IT (*Information Technology*)	Tecnologías de Información. Recursos tecnológicos utilizados para procesar, almacenar, transmitir y proteger información.
VPN (*Virtual Private Network*)	Red privada virtual. Canal seguro para acceso remoto a recursos internos.