Delitos del Código Penal argentino aplicados a tecnologías y sistemas de información

1.1 Incidente informático no es sinónimo de delito

Un incidente informático puede producir pérdidas económicas, interrupción operativa, exposición de datos personales, daño reputacional y conflictos legales. Sin embargo, desde la mirada penal, **no alcanza con que exista un perjuicio**. Debe identificarse qué hizo una persona, qué norma describe esa conducta, si existió una causa que la justifique y si puede formularse un reproche penal.

La distinción entre error operativo, incumplimiento contractual, falta disciplinaria, infracción administrativa y **posible delito** es fundamental para la administración. Cada categoría exige una respuesta diferente, involucra a distintas áreas de la organización y tiene consecuencias distintas para las personas implicadas.

Para que una conducta pueda ser tratada penalmente debe reunir cuatro elementos:

Elemento	Qué significa
Conducta humana	El delito presupone una acción u omisión de una persona
Tipicidad	La conducta debe encuadrar en una descripción prevista por la ley penal
Antijuridicidad	La conducta debe resultar contraria al ordenamiento y no estar cubierta por una causa de justificación
Culpabilidad	Debe poder formularse reproche penal: la persona comprendía la ilicitud y pudo actuar de otro modo

En materia informática, la mayoría de las figuras penales relevantes exigen además **dolo**: conocimiento y voluntad de realizar la conducta tipificada.

1.2 Los cuatro elementos del delito en el entorno digital

1.2.1 Conducta humana — El punto de partida

El sistema, el servidor, la aplicación, el algoritmo o el programa malicioso no son sujetos penales. Funcionan como medios, instrumentos o entornos técnicos. La pregunta jurídica inicial es **quién ejecutó, ordenó, facilitó, toleró o participó** en la conducta.

En una organización, una acción penalmente relevante puede consistir en:

- Ingresar sin autorización a un sistema restringido.
- Alterar registros, copiar bases de datos o borrar archivos deliberadamente.
- Publicar comunicaciones privadas o interceptar comunicaciones ajenas.
- Modificar instrucciones de pago o inutilizar un sistema crítico.
- Utilizar credenciales ajenas o mantener acceso después de haber perdido autorización.

La conducta puede ser directa o mediada por tecnología. Si una persona configura un programa para intentar 10.000 combinaciones de contraseña, el hecho no deja de ser humano porque intervenga automatización. El *script* o programa es el medio técnico; la conducta relevante sigue siendo la decisión humana de ejecutarlo.

Implicancia para la administración: los *logs* (registros automáticos de actividad) permiten reconstruir accesos, horarios, direcciones de red, cambios en archivos y uso de credenciales. Un sistema sin registros adecuados dificulta diferenciar una falla técnica de una acción humana imputable. Las políticas internas deben definir qué eventos se registran, cuánto tiempo se conservan y quién puede consultarlos.

1.2.2 Tipicidad — No hay delito sin ley previa

Una conducta es típica cuando encuadra en una descripción prevista por la ley penal (*principio de legalidad*). En materia informática, esta regla es esencial: muchas conductas son técnicamente posibles, pero solo algunas fueron convertidas en delito por el legislador. La tipicidad exige comparar el hecho con el texto legal; no basta afirmar que alguien actuó mal o causó daño.

La tipicidad también exige **precisión técnica**:

Distinción	Por qué importa
Ver información en una carpeta abierta vs. superar una barrera de autenticación	El análisis de autorización y el grado de acción son distintos
Recibir un correo por error vs. interceptar comunicaciones ajenas	La conducta activa o pasiva cambia el análisis
Eliminar un archivo temporal vs. destruir una base de datos de facturación	El objeto afectado y la intención cambian la figura aplicable

En TI, la **autorización** es simultáneamente un concepto operativo y jurídico. Puede surgir de un contrato, una política interna, una orden de trabajo, un perfil asignado en el sistema o una función laboral. Cuando la autorización es verbal, ambigua o informal, aumenta el riesgo. El uso de IAM (*Identity and Access Management*), MFA (*Multi-Factor Authentication*) y revisión periódica de permisos no solo reduce incidentes: ayuda a probar quién podía hacer qué dentro del sistema.

1.2.3 Antijuridicidad — La justificación como límite

Una conducta típica no siempre es antijurídica. Puede estar cubierta por una **causa de justificación**:

Situación	Análisis
Un auditor de seguridad ingresa a un sistema con herramientas de prueba bajo autorización expresa, alcance definido, fecha, responsable y reglas de reporte	La conducta es típica externamente, pero puede estar justificada por consentimiento y finalidad legítima
Un administrador restaura un *backup* y reemplaza archivos dañados siguiendo un procedimiento aprobado	Modifica datos, pero responde a una función autorizada y documentada
Un empleado de soporte consulta información privada de un usuario sin caso asignado ni necesidad funcional	Sin justificación: hay autorización técnica pero no autorización funcional
Un colaborador usa credenciales activas después de finalizar su relación contractual	El acceso original era legítimo; el acceso posterior no tiene amparo

Para las organizaciones, la prevención de conductas antijurídicas exige: - Políticas de uso aceptable documentadas. - Clasificación de información. - Gestión de accesos y baja oportuna de usuarios. - **Segregación de funciones** (*Separation of Duties*): una misma persona no debería poder crear proveedores, modificar cuentas bancarias, aprobar pagos y ejecutar transferencias sin controles compensatorios.

1.2.4 Culpabilidad, dolo y culpa — El reproche penal

Concepto	Definición	Relevancia en el entorno digital
Culpabilidad	Capacidad de comprender la ilicitud y haber podido actuar de otro modo	Categoría general que habilita el reproche penal

Concepto	Definición	Relevancia en el entorno digital
Dolo	Conocimiento y voluntad de realizar la conducta típica	La mayoría de las figuras informáticas relevantes lo requieren
Culpa	Imprudencia, negligencia o impericia	Solo es penalmente relevante cuando la ley prevé esa modalidad

En la práctica organizacional, esta diferencia evita errores frecuentes:

- Una mala configuración de permisos puede permitir que usuarios comunes vean carpetas internas. Eso puede generar responsabilidad administrativa, civil o contractual, pero no necesariamente un delito por parte del usuario que accedió, salvo que se demuestre que sabía que no debía ingresar.
- Un empleado que borra por error una planilla puede causar un incidente operativo. Si no hay voluntad de dañar ni figura culposa aplicable, el tratamiento penal puede no corresponder.

Clave para la administración: el análisis técnico responde *qué pasó, cuándo, desde qué cuenta, sobre qué activo y con qué impacto*. El análisis jurídico evalúa si esos hechos encuadran en una figura penal y si puede atribuirse culpabilidad. Ambos análisis son necesarios y deben mantenerse separados.

1.3 Cómo organiza el Código Penal argentino los delitos informáticos

Los delitos informáticos en la Argentina no se encuentran en una sección autónoma del Código Penal. El sistema los distribuye según el **bien jurídico afectado**. El medio digital no define por sí solo el delito: lo define la conducta tipificada y el bien que protege.

Sector del Código Penal	Bien jurídico protegido	Aplicación informática frecuente	Ejemplo organizacional
Delitos contra la integridad sexual	Protección de menores y libertad sexual	Material de explotación sexual, contacto con menores por medios electrónicos	Uso de plataformas de mensajería para captar o distribuir contenido prohibido
Delitos contra la libertad, secretos y privacidad	Privacidad, confidencialidad y reserva de comunicaciones	Acceso ilegítimo, interceptación, publicación de comunicaciones, bases de datos personales	Ingreso no autorizado al sistema de RR.HH. para consultar legajos
Delitos contra la propiedad	Patrimonio y disponibilidad de bienes digitales	Fraude informático, daño sobre datos, programas o sistemas	Alteración de una orden de pago mediante manipulación de datos
Delitos contra la seguridad de comunicaciones	Continuidad de comunicaciones y servicios	Interrupción o entorpecimiento de comunicaciones	Ataque que impide operar un canal de comunicación esencial
Delitos contra la administración pública y la prueba	Custodia de documentos y registros probatorios	Alteración o destrucción de registros digitales	Borrado de archivos entregados como prueba o

Sector del Código Penal	Bien jurídico protegido	Aplicación informática frecuente	Ejemplo organizacional
		confiados a custodia	sujetos a conservación legal
Delitos contra la fe pública	Confianza en documentos, firmas y certificaciones	Falsedad documental digital, alteración de firma digital	Alteración de un archivo firmado digitalmente para simular una aprobación

Un mismo incidente puede exigir más de una lectura: un acceso no autorizado puede comprometer privacidad, un borrado deliberado puede constituir daño, y la alteración de un documento digital puede afectar la fe pública o la prueba, según el contexto.

1.4 Figuras penales frecuentes desde la mirada de TI

1.4.1 Acceso ilegítimo a sistemas o datos

Se presenta cuando una persona ingresa sin autorización o excede la autorización que tenía. En una organización puede ocurrir cuando alguien:

- Usa credenciales de otro usuario.
- Recupera claves de un archivo no protegido.
- Accede a un módulo para el cual no tenía permiso asignado.

Controles preventivos: gestión de accesos, contraseñas robustas, MFA, baja inmediata de cuentas inactivas y revisión periódica de privilegios.

1.4.2 Violación de secretos y privacidad

Incluye conductas sobre comunicaciones electrónicas, correspondencia digital y datos personales. Desde TI, se vincula con correos, mensajería interna, bases de clientes, legajos, información salarial, archivos financieros y registros de navegación.

Un empleado que publica una comunicación interna no destinada a publicidad puede generar un problema penal además de una falta laboral.

1.4.3 Fraude informático

Aparece cuando se defrauda mediante manipulación informática que altera el funcionamiento normal de un sistema o la transmisión de datos.

Ejemplo	Descripción
Cambio de CBU en el sistema de pagos	Modificar el número de cuenta bancaria de un proveedor para desviar una transferencia a una cuenta no autorizada
Alteración de datos de stock	Ocultar faltantes y generar movimientos contables falsos

Control clave: atender al circuito completo — solicitud, aprobación, carga, modificación, auditoría y ejecución — con segregación de funciones en cada etapa crítica.

1.4.4 Daño informático

Comprende la afectación de datos, documentos, programas o sistemas. Puede incluir borrar bases, inutilizar servidores, cifrar archivos sin autorización, alterar código o destruir respaldos.

Controles preventivos: copias de seguridad probadas, control de cambios, separación entre ambientes de prueba y producción, EDR (*Endpoint Detection and Response*), monitoreo y plan de recuperación ante desastres (DRP).

1.4.5 Interrupción de comunicaciones

No todo corte de servicio es delito: puede tratarse de falla técnica, saturación, error de configuración o caso fortuito. El análisis penal se activa cuando una persona interrumpe o entorpece deliberadamente una comunicación.

Controles preventivos: redundancia de red, monitoreo de conectividad, gestión de cambios y trazabilidad de configuraciones.

1.4.6 Alteración de documentos digitales

Un documento digital puede respaldar una contratación, una orden de compra, una aprobación presupuestaria, una factura o un informe de auditoría. Alterarlo puede afectar la fe pública, la prueba o la administración de justicia.

Controles preventivos: integridad mediante *hash* (huella digital de un archivo), firma digital, control de versiones y repositorios con permisos adecuados.

1.5 Criterios de análisis para administradores ante un incidente

Ante un posible incidente con relevancia penal, conviene formular preguntas en este orden:

Pregunta	Qué permite determinar
¿Qué activo fue afectado?	Datos, sistemas, redes, comunicaciones, documentos, credenciales o dinero
¿Qué conducta humana se detectó?	Ingreso, copia, borrado, modificación, publicación, interceptación, manipulación o interrupción
¿Existía autorización?	Rol asignado, perfil en el sistema, contrato, orden de trabajo, política interna y necesidad funcional

Pregunta	Qué permite determinar
¿Qué evidencia existe?	*Logs*, capturas, respaldos, registros de cambios, reportes de monitoreo, testimonios técnicos
¿Qué impacto produjo?	Pérdida patrimonial, exposición de datos, caída del servicio, daño documental, riesgo para la prueba

1.5.1 Manejo de evidencia digital — La cadena de custodia

La evidencia digital debe tratarse con cuidado desde el primer momento:

Práctica	Por qué es necesaria
No modificar el equipo afectado sin registrar lo realizado	Cada cambio puede afectar la integridad de la evidencia
Preservar copias, fechas, usuarios, rutas y direcciones de red	Son los datos que permiten reconstruir el hecho
Mantener la **cadena de custodia**	Demuestra que la evidencia no fue alterada desde su obtención
Coordinar con dirección, asesoría legal y auditoría interna	El área de TI no debería actuar sola cuando el hecho puede tener relevancia penal

1.5.2 Lenguaje en los informes internos

No todo incidente debe ser calificado de delito en informes internos preliminares. Es preferible **describir hechos verificables** sin anticipar conclusiones jurídicas:

Forma incorrecta	Forma correcta
"Se detectó un acceso delictivo al sistema"	"Se detectó acceso desde una cuenta no autorizada"
"El empleado cometió fraude"	"Se modificaron 12 registros de proveedores sin aprobación registrada"
"Hubo un ataque criminal"	"Se interrumpió el servicio durante 2 horas con origen en modificaciones de configuración no autorizadas"

Esta forma de documentación permite el análisis posterior sin comprometer investigaciones ni anticipar conclusiones que corresponden a la autoridad judicial.

1.6 Casos integrados

1.6.1 Caso 1 — Acceso con credenciales ajenas

Un usuario de administración ingresa al módulo de sueldos con la clave de un compañero y consulta legajos salariales.

Elemento	Análisis
Conducta humana	Ingreso deliberado y consulta de información usando credenciales de otro
Tipicidad	Puede analizarse bajo acceso ilegítimo y violación de privacidad
Antijuridicidad	Dependería de la ausencia de autorización para ingresar con esas credenciales
Dolo	Puede surgir del uso consciente de credenciales ajenas

Elemento	Análisis
Evidencia clave	*Logs* de acceso con usuario, horario, dirección IP y módulo consultado

1.6.2 Caso 2 — Cambio de CBU para desviar pagos

Una persona modifica en el sistema de pagos el CBU de un proveedor para dirigir una transferencia a una cuenta distinta.

Elemento	Análisis
Conducta humana	Manipulación de datos bancarios en el sistema
Figura aplicable	Fraude informático
Evidencia útil	Historial de cambios, usuario, dirección IP, fecha, aprobaciones y trazabilidad bancaria
Control preventivo	Doble aprobación para cambios de datos bancarios; verificación por canal independiente

1.6.3 Caso 3 — Borrado por error durante migración autorizada

Un técnico borra por error una carpeta compartida durante una migración autorizada.

Elemento	Análisis
Conducta humana	Acción accidental dentro de una tarea autorizada

Elemento	Análisis
Dolo	Ausente si se demuestra error, autorización de tarea y ausencia de voluntad de destruir
Resultado penal probable	Sin delito si no hay dolo y la figura culposa no aplica
Acciones organizacionales	Analizar *backups*, recuperación, capacitación y controles de cambio

1.6.4 Caso 4 — Ransomware con exigencia de rescate

Una persona cifra deliberadamente archivos de producción y exige dinero para entregar la clave de descifrado.

Elemento	Análisis
Conducta humana	Cifrado deliberado de archivos ajenos; exigencia de rescate
Figuras posibles	Daño informático, afectación patrimonial; pueden concurrir otras según el caso
Acciones inmediatas	Preservar evidencia, aislar equipos, activar el plan de respuesta ante incidentes
Error crítico a evitar	No realizar acciones que destruyan rastros antes de documentar el estado del sistema

1.6.5 Caso 5 — Publicación de comunicaciones internas

Un empleado publica capturas de correos internos no destinados a publicidad.

Elemento	Análisis
Conducta humana	Difusión de comunicaciones reservadas
Figuras posibles	Pueden comprometerse secretos, privacidad, datos personales y deberes laborales
Variables relevantes	Contenido del correo, forma de obtención, existencia de autorización, perjuicio producido y figura penal aplicable
Acciones organizacionales	Preservar los correos originales, documentar cómo se accedió a ellos y coordinar con asesoría legal

1.7 Ideas clave

- Un incidente informático y un delito informático son categorías distintas. El perjuicio operativo no es suficiente para configurar un delito: se requieren **conducta humana, tipicidad, antijuridicidad y culpabilidad**.
- El **medio digital** no define el delito en el Código Penal argentino: lo define el bien jurídico afectado y la conducta tipificada. Un mismo incidente puede involucrar privacidad, propiedad, fe pública y administración pública simultáneamente.
- La **autorización** es un concepto operativo y jurídico. Determina cuándo un acceso es legítimo y cuándo es ilegítimo. Los controles de IAM, los perfiles de usuario y la segregación de funciones no solo reducen riesgos: también generan evidencia de quién podía hacer qué.
- La mayoría de las figuras penales informáticas relevantes requieren **dolo**: quien actúa por error, negligencia o desconocimiento generalmente no reúne el elemento subjetivo necesario para el reproche penal. Eso no elimina la responsabilidad civil, laboral o administrativa.

- La **cadena de custodia** es tan importante como la evidencia en sí misma. Una evidencia bien preservada pero sin cadena de custodia puede perder valor en una investigación. El área de TI no debe actuar sola cuando el hecho puede tener relevancia penal.

- El **lenguaje en los informes internos** importa: describir hechos verificables sin calificar jurídicamente la conducta preserva la objetividad y evita comprometer investigaciones o anticipar conclusiones que corresponden a la autoridad judicial.

- Los controles organizacionales — *logs*, segregación de funciones, MFA, *backups* probados, gestión de accesos y procedimientos de cadena de custodia — no solo previenen incidentes: también **mejoran la capacidad de análisis legal** cuando ocurren.

- La administración debe distinguir cuándo un hecho requiere solo una respuesta interna (disciplinaria, contractual, técnica) y cuándo debe derivarse a asesoramiento jurídico especializado con preservación de evidencia.

1.8 Preguntas de evaluación

1. ¿Por qué un incidente informático no constituye automáticamente un delito? Identifique los cuatro elementos que debe reunir una conducta para ser penalmente relevante.

2. ¿Qué significa que una conducta sea típica en el Código Penal? Proporcione un ejemplo de conducta informática típica y uno de conducta que genera daño pero que podría no ser típica.

3. ¿Cómo se diferencia la conducta humana del medio técnico utilizado para ejecutarla? ¿Por qué esa distinción es importante para el análisis penal?

4. ¿Qué importancia tiene la autorización en el análisis de accesos a sistemas informáticos? ¿Qué diferencia existe entre autorización técnica y autorización funcional?

5. ¿Cuál es la diferencia entre culpabilidad, dolo y culpa? Proporcione un ejemplo de cada uno en el contexto de un incidente en un sistema contable.

6. ¿Por qué el Código Penal argentino no agrupa los delitos informáticos en una sección única? ¿Qué consecuencia práctica tiene esa distribución para el análisis de un incidente?

7. Analice el Caso 2 (cambio de CBU): ¿qué controles administrativos habrían podido prevenir la conducta y qué evidencia debería preservarse para la investigación?

8. ¿Qué controles internos ayudan a prevenir el fraude informático en un sistema de pagos? ¿Por qué la segregación de funciones es el más importante?

9. ¿Por qué la cadena de custodia es relevante cuando se investiga un incidente digital? ¿Qué errores frecuentes pueden invalidar la evidencia digital?

10. ¿Por qué el lenguaje en los informes internos preliminares debe describir hechos verificables en lugar de calificaciones jurídicas? ¿Qué riesgos genera anticipar la calificación de delito?

1.9 Glosario

Término	Traducción / Explicación
Acceso ilegítimo	*Unauthorized access*. Ingreso a un sistema o dato informático sin autorización o excediendo la autorización que se tenía.
Antijuridicidad	Condición de una conducta que, además de ser típica, resulta contraria al ordenamiento jurídico y no está cubierta por una causa de justificación.

Término	Traducción / Explicación
Audit Log	Registro de auditoría. Registro cronológico e inmutable de las acciones realizadas en un sistema: quién accedió, qué modificó y cuándo.
Backup	Copia de respaldo. Copia de datos destinada a recuperar información ante pérdida, daño o corrupción.
CBU	Clave Bancaria Uniforme. Identificador bancario argentino de 22 dígitos que identifica una cuenta. Su modificación fraudulenta es un vector frecuente de fraude informático.
Chain of custody	Cadena de custodia. Registro documentado que acredita cómo fue obtenida, preservada y transferida la evidencia, permitiendo demostrar que no fue alterada.
Computer crime	Delito informático o ciberdelito. Conducta penalmente tipificada cometida mediante tecnología, contra tecnología o en un entorno digital.
Computer data	Dato informático. Representación digital de hechos, instrucciones o conceptos susceptible de ser procesada por un sistema.
Computer system	Sistema informático. Conjunto de *hardware*, *software*, redes, datos y procedimientos que procesan información.
Culpabilidad	Categoría jurídico-penal que habilita el reproche penal cuando una persona comprendía la ilicitud del hecho y pudo actuar de otro modo.

Término	Traducción / Explicación
Culpa	Modalidad subjetiva del delito basada en imprudencia, negligencia o impericia. Solo es penalmente relevante cuando la ley prevé expresamente esa modalidad.
DRP	*Disaster Recovery Plan*. Plan de recuperación ante desastres. Plan técnico para restaurar sistemas, datos e infraestructura luego de una interrupción grave.
Dolo	Conocimiento y voluntad de realizar la conducta típica. Elemento subjetivo requerido por la mayoría de las figuras penales informáticas.
EDR	*Endpoint Detection and Response*. Detección y respuesta en dispositivos finales. Herramienta que monitorea equipos para detectar comportamientos maliciosos y responder ante amenazas.
Evidencia digital	Información almacenada o transmitida en formato digital que puede ser utilizada como prueba en una investigación o proceso judicial.
Hash	Huella digital de un archivo. Valor calculado matemáticamente sobre un archivo que permite verificar si fue modificado. Fundamental para demostrar integridad de evidencia.
IAM	*Identity and Access Management*. Gestión de identidades y accesos. Sistema y procesos para administrar usuarios, roles, permisos, altas, bajas y modificaciones de acceso.

Término	Traducción / Explicación
IP	*Internet Protocol*. Dirección numérica que identifica un dispositivo en una red. Clave para reconstruir desde qué equipo o conexión se realizó una acción.
Log	Registro técnico de actividad en un sistema: accesos, cambios, errores, operaciones y eventos relevantes. Fundamental para investigar incidentes.
Malware	*Malicious software*. Software malicioso diseñado para dañar, espiar, secuestrar o tomar control de sistemas.
MFA	*Multi-Factor Authentication*. Autenticación multifactor. Mecanismo que exige más de un factor de verificación para acceder a un sistema.
Principio de legalidad	Garantía penal que establece que no hay delito sin ley penal previa que lo tipifique. Determina que la tipicidad debe cotejarse contra el texto legal vigente.
Ransomware	Tipo de malware que cifra archivos o sistemas y exige un pago para restituir el acceso. Puede comprometer figuras penales de daño informático y afectación patrimonial.
Script	Secuencia de instrucciones automatizadas que un sistema ejecuta. Puede ser el medio técnico de una conducta penalmente relevante.
Segregation of Duties	Segregación de funciones. Principio de control interno que evita que una misma persona concentre todas las etapas de un proceso crítico, reduciendo el riesgo de fraude.

Término	Traducción / Explicación
SIEM	*Security Information and Event Management*. Gestión de información y eventos de seguridad. Sistema que centraliza y analiza registros para detectar patrones anómalos.
TI	Tecnologías de la Información. Conjunto de recursos tecnológicos utilizados para procesar, almacenar, transmitir y proteger información.
Tipicidad	Característica de una conducta que encuadra en una descripción prevista por la ley penal. Elemento esencial para el análisis del delito.