Responsabilidad Institucional en Seguridad de la Información: Evidencia documental y diligencia debida

Institutional Responsibility in Information Security: Documentary evidence and due diligence

AUTOR:

Torres Ponce, Mariano Enrique
Abogado y Especialista en Derecho Informático

RESUMEN

El trabajo examina la seguridad de la información desde una perspectiva que integra derecho, auditoría interna y gestión organizacional. Se parte de la idea de que la protección de los activos informacionales no depende solo de controles operativos, sino de una estructura normativa que defina responsabilidades y conserve evidencia capaz de sostener decisiones. La auditoría interna permite interpretar esa estructura y revela la forma en que políticas, procedimientos y prácticas cotidianas se articulan dentro del funcionamiento real de la institución. El análisis muestra que la claridad documental, la trazabilidad y la consistencia en la ejecución son elementos que influyen de manera directa en la madurez del sistema de seguridad. También se identifican obstáculos

frecuentes vinculados con saturación normativa, desactualización documental y ausencia de ciclos de mejora. A partir de estos hallazgos se propone un enfoque de alineación jurídica y auditora que refuerza la coherencia del sistema y mejora la capacidad institucional para actuar con diligencia en escenarios de incertidumbre.

ABSTRACT

This paper examines information security through an integrated perspective that combines legal reasoning, internal auditing and organizational practice. The analysis assumes that effective protection does not depend solely on technical controls but on a coherent normative structure that assigns responsibilities and preserves reliable evidence. Internal auditing provides the vantage point to understand how policies, procedures and day-to-day practices interact within institutional operations. The findings show that documentary clarity, traceability and consistent execution are central elements in determining the maturity of an information security system. The study also identifies structural weaknesses related to normative saturation, outdated documentation and the absence of continuous improvement cycles. Based on these observations, the paper advances an alignment approach that links legal obligations with audit criteria and reinforces the organization's capacity to justify decisions in scenarios marked by uncertainty.

PALABRAS CLAVE

Seguridad de la información, auditoría interna, documentación normativa, responsabilidad institucional, evidencia digital, madurez organizacional, gestión del riesgo.

KEYWORDS

Information security, internal auditing, normative documentation, institutional responsibility, digital evidence, organizational maturity, risk management.

ÍNDICE

A. INTRODUCCIÓN

La seguridad de la información se fortaleció como un campo que articula los riesgos tecnológicos, por un lado, con obligaciones jurídicas y formas organizacionales de control. Su desarrollo estuvo impulsado por la necesidad de reducir la incertidumbre generada por sistemas cada vez más interdependientes. Los marcos normativos internacionales contribuyeron a ordenar ese proceso y ofrecieron criterios objetivos para interpretar responsabilidades y expectativas. Por eso, la noción de seguridad dejó de ser una función dispersa y se transformó en un componente estructural del gobierno institucional.

En este contexto, la auditoría interna comienza a ocupar un papel cada vez más relevante en la seguridad de la información. Su función de revisión independiente permite vincular el diseño documental con la práctica cotidiana y muestra la importancia de mantener coherencia entre políticas, procedimientos y controles como señal de madurez institucional. La observación del auditor sobre la asignación de responsabilidades y el comportamiento de los procesos frente a la incertidumbre ofrece una visión concreta del sistema. El análisis de la documentación revela la estructura de obligaciones internas que buscan sostener la protección de los activos informacionales.

El campo jurídico aportó una dimensión decisiva. La seguridad no solo se evalúa en términos operativos. También expresa una forma de responsabilidad institucional. La existencia de criterios claros, la trazabilidad documental y la consistencia en la ejecución configuran un estándar razonable de diligencia. La falta de definiciones o la ausencia de registros comprometen la capacidad de explicar y justificar decisiones. La trazabilidad se convierte en un mecanismo indispensable para reconstruir hechos y para sostener el cumplimiento normativo.

La literatura especializada ha resaltado la importancia de los marcos regulatorios y de las políticas internas como expresión del deber de cuidado organizacional. El desarrollo de estándares internacionales reflejó esta tendencia y consolidó prácticas que integran riesgo, controles y registros formales. Las obras dedicadas a la regulación de la seguridad y al análisis del ciberdelito facilitaron la comprensión de las obligaciones emergentes y de la necesidad de estructuras normativas que permitan sostener decisiones complejas. La interacción entre tecnología, procesos y derecho dejó de ser accesoria y pasó a representar un eje de gobierno institucional.

El enfoque de auditoría interna permite examinar este entramado de manera sistemática. La revisión de los documentos que organizan la seguridad revela no solo el estado del sistema sino también el grado de compromiso directivo. La cultura institucional influye en la eficacia de las medidas adoptadas y condiciona el cumplimiento real de los controles. La claridad en la asignación de roles, la difusión de las políticas y el mantenimiento del sistema se convierten en elementos que afectan el riesgo y determinan la calidad de la evidencia disponible.

El objetivo de este trabajo es articular una mirada que combine auditoría interna y análisis jurídico para comprender cómo se estructura la seguridad de la información dentro de las organizaciones. El sistema documental, los controles y la cultura institucional se examinan como parte de un entramado que define responsabilidad, coherencia y capacidad de respuesta. Este enfoque permite entender que la seguridad depende tanto de los controles instrumentales como del diseño normativo que orienta la conducta institucional

B. MARCO TEÓRICO Y ESTADO DEL ARTE

El campo de la seguridad de la información se apoyó en una serie de ideas que no aparecieron de manera ordenada. Surgieron a partir de prácticas dispersas, de problemas concretos y de intentos de las organizaciones por entender fenómenos que avanzaban más rápido que sus propias estructuras. La literatura que acompañó ese proceso ayudó a darle un sentido más claro a lo que, en la práctica, eran esfuerzos aislados por conservar estabilidad. Ese recorrido permitió advertir que la protección de la información no depende solo de soluciones técnicas. Requiere un marco conceptual que permita organizar criterios y que ofrezca una base común para interpretar decisiones. Los estándares internacionales aportaron esa base al proponer métodos que vinculan riesgo, roles y documentación de manera más coherente (International Organization for Standardization [ISO], 2013). Con el tiempo, la seguridad dejó de funcionar como un conjunto de respuestas improvisadas y empezó a consolidarse como un sistema que necesita cierta continuidad conceptual para sostenerse.

Los enfoques técnicos y jurídicos coincidieron en que la seguridad se vuelve más robusta cuando las organizaciones reconocen que los controles no operan en el vacío. Dependen

de prácticas, de expectativas internas y de un modo particular de gestionar la información. La literatura técnica señaló que los controles adquieren sentido cuando forman parte de una estructura organizacional que los ubica dentro de procesos estables y conocidos (National Institute of Standards and Technology [NIST], 2013). La producción académica sobre gobernanza reforzó esta lectura al mostrar que la protección de la información no se limita a un conjunto de herramientas, sino que exige una interpretación institucional sostenida en reglas claras y en criterios consistentes (von Solms, 2005). Desde esa perspectiva, la seguridad se fortalece cuando la organización logra integrar estos elementos en un marco que permita justificar decisiones y demostrar la razonabilidad de sus actos.

B.1. FUNDAMENTOS CLÁSICOS DE LA SEGURIDAD Y SU ESTRUCTURA NORMATIVA

Los principios de confidencialidad, integridad y disponibilidad constituyen el marco conceptual que organiza la disciplina de la seguridad de la información. Estos principios ofrecen un punto de referencia relativamente estable que permite evaluar controles con cierta objetividad. La literatura técnica temprana advirtió que estos conceptos solo resultan operativamente útiles cuando la organización los transforma en reglas claras y en procesos reproducibles que no dependan de interpretaciones cambiantes (Schneier, 2015). Desde una perspectiva jurídica, esta transformación adquiere relevancia adicional. Las obligaciones de seguridad no pueden cumplirse mediante compromisos abstractos. Requieren concreción en políticas específicas, procedimientos documentados y controles verificables que permitan acreditar su aplicación efectiva.

Estudios posteriores mostraron que la seguridad alcanza mayor efectividad cuando existe equilibrio entre tecnología, procesos y cultura institucional (Dhillon, 1997). Este equilibrio resulta particularmente relevante desde el punto de vista de la responsabilidad institucional. Los tribunales no evalúan la diligencia únicamente por la sofisticación técnica de los controles implementados. Evalúan si la organización logró integrar esos controles dentro de una estructura coherente que incluya políticas claras, procesos estables y capacitación efectiva del personal. Las obras dedicadas al análisis de normas internacionales y nacionales de seguridad aportaron claridad sobre cómo se estructura ese lenguaje normativo y sobre cómo se relaciona con las obligaciones internas que asumen las organizaciones (Maggiore y Prandini, 2017). Las discusiones sobre ciberdelito

reforzaron esta perspectiva al mostrar que la capacidad para investigar incidentes depende en gran medida de la calidad de la documentación interna y de las garantías que rodean la conservación de evidencia digital relevante (Prandini y Maggiore, 2013).

B.2. LA FUNCIÓN DE AUDITORÍA INTERNA Y EL CONTROL DE LAS ESTRUCTURAS DOCUMENTALES

La auditoría interna incorporó este marco conceptual y lo transformó en un criterio para evaluar el comportamiento institucional. La disciplina auditora parte de una premisa sencilla. La organización solo puede demostrar lo que documenta y solo puede documentar lo que está definida para hacer. Los estándares profesionales reforzaron esta visión al señalar que la evidencia es el elemento central del trabajo auditor y que la calidad de esa evidencia depende de la consistencia de los documentos que describen procesos y responsabilidades (The Institute of Internal Auditors [IIA], 2017). Investigaciones en comportamiento organizacional mostraron que las políticas solo alcanzan su propósito cuando se integran en la práctica diaria y cuando las personas las internalizan como parte de su actividad normal (Siponen, 2000). La auditoría observa este punto porque muestra el grado de madurez institucional. La distancia entre lo escrito y lo ejecutado revela fallas estructurales que afectan la protección de los activos informacionales.

La literatura sociológica destacó que la seguridad es una construcción colectiva que depende de la forma en que la organización distribuye roles, reconoce riesgos y establece mecanismos de control (Dhillon, 1997). Este enfoque permite entender por qué la auditoría interna presta tanta atención a la redacción de las políticas y a la claridad de los procedimientos. La interpretación de un documento condiciona la interpretación del control. Una política ambigua o desordenada puede producir más incertidumbre que protección. Por eso, la documentación se convierte en una pieza central del análisis auditor.

B.3. IMPLICANCIAS JURÍDICAS Y PROBATORIAS DEL SISTEMA DE SEGURIDAD

La seguridad incorpora una dimensión jurídica que se vuelve evidente cuando la organización necesita reconstruir hechos o explicar decisiones. La literatura sobre evidencia digital remarcó la importancia de contar con registros íntegros, fiables y completos que permitan sostener conclusiones (Casey, 2004). La integridad probatoria

no se construye de manera improvisada. Surge de la manera en que la organización gestiona sus documentos y de la estabilidad de los procesos que generan esa información. Estudios jurídicos sobre responsabilidad demostraron que la capacidad para explicar actos depende de la existencia de reglas claras y de la trazabilidad de las decisiones (Hildebrandt, 2015). La literatura en privacidad también aportó elementos para comprender cómo la documentación se transforma en evidencia que permite valorar la diligencia institucional (Solove, 2008). Las obras que abordaron el ciberdelito reforzaron esta idea al mostrar que la ausencia de documentos adecuados dificulta la investigación y genera vacíos probatorios que se traducen en mayores riesgos (Prandini y Maggiore, 2013).

B.4. MARCOS Y GUÍAS VIGENTES EN EL PERÍODO ANALIZADO

Los estándares internacionales ofrecieron un método sistemático para organizar la seguridad y consolidaron una visión cíclica que articula planificación, implementación, monitoreo y mejora continua. Estos marcos entregaron criterios objetivos que facilitan evaluar riesgos, seleccionar controles proporcionales y revisar periódicamente su efectividad real (ISO, 2013). Las guías técnicas de ese período reforzaron la centralidad de la continuidad del negocio, la gestión estructurada de incidentes y, sobre todo, la documentación como herramienta esencial para sostener decisiones y acreditar diligencia (European Union Agency for Network and Information Security [ENISA], 2018). La literatura de auditoría interna aportó un análisis crítico sobre la lógica del control y demostró cómo las organizaciones adoptan estos marcos no solo por cumplimiento formal, sino para fortalecer de verdad su estructura de gobernanza (Power, 1999). Este enfoque logró integrar de manera más clara el análisis de riesgo técnico con el análisis de responsabilidad institucional. La documentación dejó de ser un mero requisito burocrático y se convirtió en el instrumento que orienta acciones, facilita la revisión independiente y permite sostener conclusiones sólidas frente a cualquier cuestionamiento.

C. AUDITORÍA INTERNA Y SEGURIDAD JURÍDICA

La auditoría interna ofrece una mirada que integra lo técnico y lo institucional en un escenario donde la seguridad de la información continúa consolidándose como función estratégica. Los controles requieren una estructura que dé sentido a su aplicación y

permita demostrar que la organización actúa con coherencia. Esta estructura se expresa en la documentación interna y en la manera en que los procesos se aplican realmente. La auditoría transforma ese entramado en evidencia sobre el comportamiento institucional, especialmente cuando resulta necesario reconstruir hechos y justificar decisiones.

C.1. RELACIÓN ENTRE MARCO NORMATIVO INTERNO Y RESPONSABILIDAD

El marco normativo interno organiza la seguridad mediante políticas, normas y procedimientos que asignan responsabilidades y describen formas de actuación. Estos documentos cumplen una función que trasciende su contenido técnico. Establecen criterios que orientan la conducta institucional y permiten interpretar cómo la organización entiende sus obligaciones. Sin embargo, cuando esos criterios son ambiguos o cuando coexisten múltiples fuentes normativas sin jerarquía clara, la responsabilidad se vuelve objeto de disputa.

La Corte Suprema de Justicia de la Nación argentina abordó esta cuestión en 2016 al resolver un caso de fraude bancario electrónico. Un cliente del Banco Galicia sufrió transferencias no autorizadas por más de 400.000 pesos a cuentas utilizadas para lavado. El banco alegó que el cliente había entregado sus claves y que, por tanto, era responsable exclusivo. La Corte confirmó la condena a la entidad por falta de controles adecuados y por no haber demostrado con registros técnicos y documentales que su sistema de prevención de fraude cumplía con los estándares exigidos por la Comunicación A 4609 del Banco Central, vigente desde 2007. El tribunal destacó que el banco no pudo aportar logs ni documentación interna que acreditara que sus sistemas de monitoreo de operaciones sospechosas funcionaban correctamente y estaban alineados con sus propias políticas de seguridad. La falta de trazabilidad de los controles internos impidió acreditar que la institución había actuado con la diligencia debida (Corte Suprema de Justicia de la Nación, 2016).

Este fallo consolidó la doctrina según la cual las entidades financieras tienen un deber reforzado de cuidado que no se satisface con la mera existencia de políticas formales. La responsabilidad institucional requiere demostrar que los controles descriptos operaban efectivamente y que la documentación interna permitía verificar su aplicación. La literatura especializada destacó la importancia de que estos documentos sean claros y consistentes para evitar interpretaciones que generen incertidumbre o que habiliten decisiones contradictorias (ISO, 2013). Los estudios sobre ciberdelito reforzaron esta idea

al mostrar que la falta de reglas adecuadas dificulta la identificación de responsabilidades y compromete la reconstrucción de incidentes (Prandini y Maggiore, 2013). La auditoría interna trabaja sobre este conjunto documental para determinar si la organización definió con claridad sus expectativas y si esas expectativas se aplican en la práctica diaria.

C.2. ROL DE LA ALTA DIRECCIÓN Y DEBER DE DILIGENCIA

La alta dirección establece el tono del sistema de seguridad. El grado de compromiso directivo influye en la calidad del marco documental y en la estabilidad de los controles. Los estándares profesionales insistieron en que la seguridad solo adquiere consistencia cuando la dirección reconoce sus responsabilidades y sostiene procesos de revisión que acompañan la evolución del entorno (IIA, 2017). La literatura jurídica analizó esta cuestión desde la perspectiva del deber de diligencia y mostró que la conducción institucional se evalúa según la razonabilidad de las decisiones adoptadas frente a los riesgos identificados (Hildebrandt, 2015). Investigaciones en regulación de datos destacaron que la dirección tiene un papel central en la construcción de accountability y que esta responsabilidad exige explicaciones claras sobre la forma en que se adoptan medidas de protección (Bygrave, 2014). La auditoría interna observa estos elementos para determinar si la dirección mantiene una conducción efectiva del sistema y si el marco documental refleja ese liderazgo.

C.3. TRAZABILIDAD DOCUMENTAL Y VALIDEZ PROBATORIA

La trazabilidad se vuelve un elemento decisivo cuando la organización necesita reconstruir hechos o justificar acciones. La calidad de los registros condiciona la capacidad para demostrar que un proceso se ejecutó como estaba previsto. La literatura forense remarcó la importancia de conservar evidencia íntegra, fiable y comprensible para sostener conclusiones basadas en datos verificables (Casey, 2004). La doctrina vinculada a privacidad destacó que la validez probatoria depende de la manera en que se gestionan los documentos y de la estabilidad de los procesos que generan los registros (Solove, 2008). La auditoría interna analiza estos criterios con detenimiento y verifica si los documentos permiten seguir el recorrido de una acción, identificar a los responsables y comprender cómo se aplicaron los procedimientos. La ausencia de trazabilidad afecta la consistencia del sistema y debilita la capacidad institucional para sostener decisiones frente a cuestionamientos.

C.4. GESTIÓN DEL RIESGO Y ACCOUNTABILITY ORGANIZACIONAL

El análisis del riesgo se integró a la seguridad como una forma de ordenar la toma de decisiones. Los marcos técnicos propusieron métodos para identificar amenazas, valorar impactos y seleccionar medidas proporcionales (NIST, 2012). La literatura jurídica vinculó este enfoque con la noción de *accountability* y mostró que la responsabilidad institucional depende de la capacidad de justificar decisiones y de demostrar que estas surgieron de un proceso razonado (Bygrave, 2002). Investigaciones en comportamiento organizacional señalaron que la gestión del riesgo solo resulta efectiva cuando se articula con prácticas institucionales capaces de sostener controles y de adaptar procesos cuando cambian las condiciones (Dhillon, 1997). La auditoría interna revisa si la organización incorporó estos criterios y si la documentación refleja una integración real entre el análisis de riesgo y los controles que se aplican.

C.5. CULTURA INSTITUCIONAL, CONCIENTIZACIÓN Y CAPACITACIÓN

La cultura institucional influye de manera decisiva en la efectividad de la seguridad. Las políticas pueden estar bien redactadas y los procedimientos pueden describir con precisión cada paso. Sin embargo, estos documentos pierden fuerza cuando no forman parte de la práctica cotidiana. La literatura dedicada al comportamiento organizacional mostró que la actitud de los usuarios determina, en buena medida, la eficacia de los controles (Siponen, 2000). Estudios sobre cultura institucional explicaron que las organizaciones desarrollan patrones de comportamiento que condicionan la forma en que se interpretan las reglas y se aplican los procesos (Schein, 1985). Investigaciones sobre fallas sistémicas demostraron que muchos incidentes se originan en errores humanos que la organización no logró anticipar ni mitigar (Reason, 1990). La auditoría interna analiza estos factores porque revelan el grado de madurez del sistema y la medida en que la cultura instaura hábitos favorables a la seguridad.

D. EVALUACIÓN DE CONTROLES DE SEGURIDAD

La auditoría interna interpreta los controles como piezas que expresan el modo en que la organización protege la información. Cada control refleja decisiones previas sobre riesgo, responsabilidades y capacidad operativa. Dado que la seguridad no puede sostenerse solo

con configuraciones aisladas, la literatura técnica mostró que los controles pierden eficacia cuando se aplican sin un marco que los organice o cuando carecen de documentación que permita entender su propósito (ISO, 2013). La auditoría trabaja sobre estos elementos y examina la consistencia entre las políticas, los procedimientos y las prácticas reales. La revisión no se limita al funcionamiento técnico del control. También incluye una lectura más amplia que conecta decisiones directivas, cultura institucional y calidad de la evidencia disponible. Podemos determinar que la coherencia entre estos factores define el grado de madurez del sistema y la capacidad de la organización para sostener sus decisiones frente a escenarios de incertidumbre.

D.1. CONTROL DE ACCESOS Y SEGREGACIÓN DE FUNCIONES

El control de accesos representa uno de los núcleos clásicos de la seguridad. Su función consiste en regular quién puede hacer qué dentro de los sistemas y en establecer límites que preserven la información. La literatura señaló que la consistencia en este punto depende de la claridad del modelo de roles y de la capacidad para mantener registros que permitan reconstruir cada cambio en los permisos otorgados (ISO, 2013). Estudios sobre riesgo organizacional mostraron que la acumulación de privilegios en una misma persona genera vulnerabilidades que pueden comprometer la integridad del sistema (Power, 1999). Investigaciones sobre errores humanos demostraron que muchas fallas en los accesos surgen de prácticas que no fueron supervisadas de manera adecuada o de decisiones aisladas que no respondieron a criterios documentados (Reason, 1990).

La auditoría interna analiza cómo se asignan los accesos y cómo se mantienen a lo largo del tiempo. Revisa procesos de altas, modificaciones y bajas. Verifica si los privilegios se ajustan a las responsabilidades reales y si los registros permiten reconstruir el historial de los permisos otorgados. La calidad del control depende de la combinación entre claridad documental, supervisión constante y cultura institucional orientada a mantener la coherencia entre rol y acceso.

D.2. GESTIÓN DE INCIDENTES, RESPUESTA Y DOCUMENTACIÓN

Los incidentes revelan el estado real del sistema de seguridad. El modo en que la organización responde a un evento adverso expresa la calidad de sus procesos y el grado de claridad del marco documental. Un fallo de la Corte de Apelaciones de Santiago (2017) sobre phishing bancario ilustra esta dinámica. Una clienta recibió un correo fraudulento

que solicitaba actualizar datos de seguridad. Ingresó credenciales y códigos de su dispositivo de autenticación. Minutos después se ejecutaron tres operaciones no autorizadas por $3.558.570. La afectada solicitó bloqueo inmediato, denunció ante la policía y objetó las transacciones.

El banco argumentó que su sistema no había sido vulnerado y que las operaciones cumplían todas las validaciones técnicas. La clienta demostró mediante documentación que había actuado inmediatamente al detectar la anomalía. El tribunal consideró que la entidad debía mantener mecanismos de detección de patrones fraudulentos conforme a la regulación de la superintendencia local, lo que implicaba algo más que validar credenciales formalmente correctas. La ausencia de estos controles fue interpretada como incumplimiento del deber de cuidado institucional (Corte de Apelaciones de Santiago, 2017).

La capacidad de reconstrucción dependió de la documentación conservada por ambas partes. Registros de transacciones, comunicaciones, denuncias y logs del sistema permitieron establecer la secuencia temporal completa. Los marcos técnicos han señalado que la respuesta ante incidentes requiere procedimientos definidos que organicen la identificación de eventos, su contención y la preservación de evidencia (NIST, 2012). La literatura forense destacó que la integridad de los registros condiciona la posibilidad de sostener conclusiones verificables (Casey, 2004). La auditoría interna examina si la organización mantiene procesos ordenados que generen documentación suficiente para reconstruir hechos y sostener decisiones bajo presión.

D.3. CONTINUIDAD DEL NEGOCIO Y RESILIENCIA ORGANIZACIONAL

La continuidad del negocio se vincula con la necesidad de sostener operaciones esenciales frente a eventos que afectan la disponibilidad de los sistemas. La literatura especializada mostró que este análisis requiere comprender cuáles son los procesos críticos, cuáles son los impactos derivados de una interrupción y cuáles son los recursos necesarios para recuperar la actividad dentro de plazos razonables (ENISA, 2018). Estudios sobre cultura institucional señalaron que la resiliencia depende tanto de la planificación como de la manera en que la organización internaliza procedimientos y mantiene capacidad para adaptarse en situaciones adversas (Schein, 1985).

La auditoría interna revisa si la organización realizó análisis de impacto, si mantiene planes vigentes y si ejecuta pruebas periódicas que permitan verificar la efectividad de esos planes. También analiza si los resultados de estas pruebas se documentan y si generan acciones de mejora. La continuidad del negocio se transforma así en un indicador que muestra el grado de estabilidad del sistema de seguridad y la capacidad institucional para sostener operaciones en escenarios de incertidumbre.

D.4. SEGURIDAD FÍSICA, AMBIENTAL Y DE PROVEEDORES

La seguridad física y ambiental conserva un papel relevante dentro de la disciplina. La literatura técnica señaló que la protección de los activos depende tanto de los controles lógicos como de las medidas destinadas a regular el acceso físico a las instalaciones y a conservar condiciones adecuadas para el funcionamiento de los equipos (ISO, 2013). La auditoría evalúa si la organización mantiene estos controles de manera consistente y si los documentos internos describen con precisión las responsabilidades asociadas.

La relación con proveedores introduce riesgos adicionales. Estudios de riesgo organizacional advirtieron que la tercerización sin controles adecuados puede generar vulnerabilidades que afectan la seguridad general del sistema (Power, 1999). Las guías técnicas destacaron que los contratos deben incluir criterios que regulen la protección de la información y que permitan verificar el cumplimiento de las obligaciones asumidas por los terceros (NIST, 2014). La auditoría interna analiza estos contratos y revisa si la organización mantiene registros de seguimiento que permitan evaluar la calidad del servicio y la coherencia entre riesgos y controles aplicados.

D.5. RECURSOS HUMANOS, PROCESOS DISCIPLINARIOS Y DESVINCULACIÓN

El comportamiento de las personas constituye un factor determinante en la seguridad. Las políticas de seguridad pueden ser correctas y los procedimientos pueden estar bien definidos. Sin embargo, la efectividad del sistema depende del modo en que los equipos incorporan estas reglas en sus prácticas diarias. La literatura sobre comportamiento organizacional mostró que la capacitación continua y la claridad normativa influyen en la forma en que las personas ejecutan sus tareas (Siponen, 2000). Estudios sobre fallas humanas demostraron que muchos incidentes se originan en hábitos que no fueron corregidos o en desconocimiento de procedimientos básicos (Reason, 1990).

La auditoría interna revisa procesos de ingreso, formación y desvinculación. Observa la existencia de verificaciones previas, programas de concientización y mecanismos disciplinarios que permitan abordar incumplimientos. También examina cómo se gestionan los accesos cuando un empleado deja la organización y cómo se documenta la recuperación de activos. La coherencia entre estos procesos revela la capacidad institucional para reducir riesgos asociados al factor humano y para sostener prácticas de protección que acompañen la actividad diaria.

E. OBSTÁCULOS Y FALLAS COMUNES IDENTIFICADAS EN AUDITORÍA

La auditoría interna permite observar dónde se debilita la seguridad y por qué ciertas estructuras documentales pierden efectividad con el tiempo. Estas observaciones no surgen de eventos extraordinarios. Surgen de prácticas cotidianas que se desalinean del marco normativo o de decisiones que se acumulan sin la revisión necesaria. Dado que la documentación debe orientar la operación, la literatura técnica y organizacional señaló que la seguridad falla cuando esos documentos dejan de cumplir esa función y cuando los controles se aplican de manera irregular (ISO, 2013). De esta manera, las experiencias de auditoría confirman esta tendencia y muestran que muchas vulnerabilidades se originan en problemas estructurales que se consolidan sin que la organización lo advierta. Es así que, la lectura de estos patrones permite comprender cómo se construye el riesgo y cómo se deteriora la capacidad institucional para sostener evidencia. Podemos determinar que esta dinámica expresa una combinación de fallas acumuladas que requieren una intervención más profunda que un simple ajuste operativo.

E.1. SATURACIÓN NORMATIVA Y AMBIGÜEDAD

La saturación documental es una de las fallas más frecuentes. La organización suma políticas, normas y procedimientos que intentan cubrir todos los escenarios posibles. Este crecimiento desordenado genera un sistema difícil de interpretar. Los documentos se superponen, se contradicen o dejan vacíos que habilitan lecturas incompatibles. La literatura dedicada a la gobernanza de la seguridad advirtió que el exceso de normas puede producir el efecto contrario al buscado y debilitar la capacidad de control (von Solms, 2005). Estudios técnicos señalaron que la ambigüedad en la redacción genera incertidumbre en la aplicación de los controles y favorece decisiones que no responden a

criterios uniformes (Schneier, 2015). La auditoría interna interpreta este escenario como una señal de deterioro institucional porque revela una estructura normativa que perdió coherencia.

E.2. FALTA DE ALINEACIÓN ENTRE POLÍTICAS Y PRÁCTICA REAL

La falta de alineación entre políticas y práctica aparece cuando las obligaciones descriptas en los documentos no se ejecutan de manera consistente. Esta brecha deteriora la credibilidad del sistema porque transforma los controles en declaraciones formales sin consecuencias operativas. Los equipos internalizan que el incumplimiento carece de efectos reales y que las reglas escritas funcionan como referencia nominal sin impacto en la actividad cotidiana.

Las investigaciones sobre comportamiento organizacional mostraron que esta desconexión surge cuando las políticas no se integran en los procesos diarios y cuando los responsables no las reconocen como parte natural de su tarea (Schein, 1985). Los marcos técnicos señalaron que un control bien diseñado pierde efectividad si su aplicación depende de decisiones improvisadas o si carece de mecanismos que aseguren su ejecución consistente (ISO, 2013). La distancia entre documento y práctica genera dos problemas simultáneos. Primero, la organización carece del control que supuso haber implementado. Segundo, pierde capacidad para demostrar diligencia porque la evidencia documental contradice la realidad operativa.

La auditoría interna identifica estos desajustes porque revelan riesgo estructural. Una política que no se aplica anticipa fallas posteriores y limita la posibilidad de sostener decisiones frente a cuestionamientos. La contradicción entre lo establecido y lo ejecutado debilita tanto la protección efectiva de los activos informacionales como la capacidad institucional para justificar sus actos mediante evidencia suficiente.

E.3. DOCUMENTACIÓN DESACTUALIZADA Y RIESGO JURÍDICO

La falta de actualización se convierte en un problema crítico cuando los documentos dejan de reflejar el estado real de la organización. Un procedimiento desactualizado no solo afecta la eficacia operativa. También deteriora la capacidad jurídica para sostener decisiones. El Tribunal Supremo de España resolvió en 2013 un caso que ilustra esta consecuencia. Una entidad financiera ejecutó transferencias fraudulentas por 5.800 euros

mediante phishing. El banco alegó que las operaciones se realizaron con claves correctas y que disponía de sistemas de detección de fraude. El tribunal condenó a la institución por incumplimiento del deber de diligencia establecido en el Código Civil y en la normativa de servicios de pago. La sentencia destacó que el banco no pudo aportar prueba suficiente de que su sistema detectara patrones anómalos de horario, origen de conexión o importe, pese a tener obligación normativa de hacerlo. La documentación interna sobre procedimientos antifraude era genérica y no reflejaba la configuración real del sistema de seguridad implementado (Tribunal Supremo de España, 2013).

Este caso muestra cómo la desactualización documental genera riesgo jurídico concreto. La entidad disponía de políticas formales, pero esas políticas no describían con precisión qué controles operaban ni cómo se configuraban. Esta brecha impidió demostrar que la institución había actuado con la diligencia esperable. La literatura centrada en responsabilidad institucional explicó que la diligencia se evalúa a partir del marco normativo vigente y de la coherencia entre ese marco y las acciones adoptadas (Bygrave, 2014). Los estándares técnicos señalaron que la actualización periódica se vuelve necesaria para evitar desfasajes que afecten la efectividad de los controles (NIST, 2012).

La auditoría interna identifica estos desfasajes con rapidez. Un documento obsoleto revela un proceso que perdió conducción y que dejó de acompañar la evolución del entorno. La distancia entre la descripción documental y la realidad operativa debilita tanto la protección efectiva como la capacidad de acreditar diligencia frente a cuestionamientos posteriores.

E.4. FALLAS EN LOS CICLOS DE MEJORA Y EN LA CONTINUIDAD DE LOS PROCESOS

La seguridad necesita ciclos de revisión que permitan ajustar controles y adoptar medidas correctivas. La ausencia de estos ciclos debilita la capacidad institucional para adaptarse. Investigaciones sobre resiliencia mostraron que las organizaciones que no revisan sus procesos pierden capacidad para enfrentar eventos adversos y tienden a repetir errores conocidos (Schein, 1985). Las guías especializadas remarcaron la importancia de conservar registros que documenten pruebas, resultados y acciones de mejora (ENISA, 2018). La auditoría interna analiza estos elementos para determinar si el sistema mantiene

una dinámica de mejora o si se volvió estático. Las fallas en este punto revelan una estructura que conserva documentos, pero no conserva aprendizaje.

E.5. TERCERIZACIÓN SIN CONTROLES SUFICIENTES

La tercerización introduce actores externos cuyas prácticas pueden no alinearse con el marco normativo interno. Esta desalineación genera vulnerabilidades que permanecen inadvertidas hasta que se materializa un incidente o hasta que la auditoría solicita evidencia de cumplimiento. Los contratos suelen establecer compromisos genéricos sin especificar cómo se verificarán ni qué evidencia deberá aportar el tercero para acreditar que cumple las obligaciones asumidas.

Los estudios sobre riesgo organizacional señalaron que la falta de controles sobre proveedores incrementa la exposición institucional porque transfiere actividades críticas sin transferir responsabilidades de manera proporcional (Power, 1999). Las guías técnicas indicaron que la gestión de terceros requiere mecanismos de evaluación continua, cláusulas contractuales que definan obligaciones verificables y procedimientos de supervisión que permitan detectar desviaciones (NIST, 2014). Muchas organizaciones carecen de estos elementos y dependen de servicios esenciales sin capacidad efectiva de control sobre aspectos que consideran críticos para la seguridad de la información.

La auditoría interna examina si la institución mantiene trazabilidad sobre las obligaciones asumidas por proveedores y si conserva registros que permitan demostrar supervisión efectiva. La ausencia de controles contractuales verificables, de procesos de seguimiento documentados o de evidencia sobre el cumplimiento de compromisos críticos limita la capacidad institucional para sostener que actuó con diligencia cuando un proveedor genera un incidente que afecta la protección de los activos informacionales.

F. PROPUESTA DE ALINEACIÓN JURÍDICA Y AUDITORA

El análisis de los controles y de la estructura documental muestra que la seguridad de la información depende de decisiones que deben sostenerse en el tiempo y que requieren un equilibrio entre claridad normativa, madurez organizacional y capacidad de revisión. Dado que estos elementos no siempre evolucionan de manera pareja, la auditoría interna permite observar cómo se articulan y revela patrones que pueden transformarse en líneas

de mejora. De esta manera, la propuesta que se desarrolla en esta sección busca reforzar ese equilibrio a partir de un enfoque que integre criterios jurídicos, técnicos y organizacionales. No se trata de sumar documentos sin necesidad. Es así que el objetivo es fortalecer la coherencia del sistema y asegurar que los textos normativos expresen prácticas reales. Podemos determinar que la estabilidad del sistema depende de esa correspondencia y de la capacidad de la organización para sostenerla de manera continua.

F.1. REDACCIÓN NORMATIVA CLARA Y CRITERIOS DE REVISIÓN

La claridad documental constituye un punto de partida indispensable. Una política bien redactada reduce la incertidumbre y facilita la comprensión de las obligaciones. La literatura técnica subrayó la importancia de contar con marcos normativos que describan procesos sin ambigüedades y que definan responsabilidades de manera comprensible (ISO, 2013). La experiencia de auditoría confirma esta idea. Los documentos que expresan decisiones con lenguaje directo permiten verificar acciones y sostener conclusiones. La organización necesita un proceso de revisión que acompañe la evolución operativa y que permita ajustar los documentos cuando cambian las condiciones. La actualización periódica evita desfasajes y refuerza la correspondencia entre documento y práctica.

F.2. INTEGRACIÓN DEL RIESGO JURÍDICO, OPERATIVO Y ORGANIZACIONAL

La gestión del riesgo se fortalece cuando integra dimensiones jurídicas, operativas y organizacionales. Los marcos técnicos propusieron métodos para identificar amenazas y valorar impactos que permiten ordenar la toma de decisiones (NIST, 2012). La literatura jurídica señaló que la responsabilidad institucional requiere justificar actos y demostrar que las decisiones surgieron de un análisis razonado (Bygrave, 2014). Los estudios en comportamiento organizacional mostraron que la eficacia del riesgo depende de la capacidad para integrar criterios técnicos con prácticas internas que sostengan los controles y acompañen el funcionamiento real de la institución (Dhillon, 1997). La auditoría interna puede reforzar esta integración revisando si el análisis de riesgo se refleja en los documentos, si orienta la asignación de recursos y si se traduce en controles que acompañan la operación con la estabilidad necesaria para sostener decisiones incluso en momentos de presión y dinamismo institucional creciente.

F.3. EVIDENCIA, TRAZABILIDAD Y PRESERVACIÓN

La evidencia constituye el sustento del análisis auditor y el soporte de la responsabilidad institucional. La literatura forense remarcó la necesidad de conservar registros íntegros y de documentar procesos que permitan reconstruir hechos con precisión (Casey, 2004). La doctrina vinculada a la privacidad sostuvo que la validez probatoria depende de la estabilidad de estos registros y de la coherencia entre procedimientos y evidencia (Solove, 2008). La organización necesita prácticas de trazabilidad que permitan seguir el recorrido de cada acción y que garanticen que los registros se generen y se mantengan de manera consistente. La auditoría interna puede reforzar estas prácticas señalando vacíos documentales y promoviendo procesos que aseguren la integridad de la información.

F.4. MODELO DE MADUREZ PARA LA AUDITORÍA INTERNA

La madurez del sistema de seguridad se evalúa a partir de la correspondencia entre políticas, prácticas y evidencia. La literatura organizacional mostró que las instituciones consolidadas mantienen procesos estables y criterios que guían decisiones en escenarios diversos (Schein, 1985). Las guías técnicas señalaron que la madurez se expresa en la capacidad para sostener controles, revisar procedimientos y adaptar medidas cuando cambian las condiciones (ENISA, 2018). La auditoría interna puede utilizar este enfoque para identificar el lugar que ocupa la organización dentro de ese continuo y para formular recomendaciones que permitan avanzar hacia un estado más consistente. La revisión de estos elementos no implica un diagnóstico rígido. Representa una herramienta para orientar mejoras graduales y sostenidas.

F.5. RECOMENDACIONES PARA LA ALTA DIRECCIÓN

El compromiso directivo condiciona la calidad del sistema de seguridad. La literatura en auditoría destacó que la dirección influye de manera directa en la asignación de recursos, en la estabilidad de los procesos y en la forma en que se interpretan las obligaciones internas (IIA, 2017). La responsabilidad institucional exige que las decisiones acompañen el análisis de riesgo y que los documentos expresen criterios que puedan sostenerse frente a cuestionamientos. La dirección puede fortalecer este proceso consolidando espacios de revisión, promoviendo la actualización documental y fomentando una cultura que

incorpore la seguridad en las prácticas diarias. La auditoría interna puede colaborar con este objetivo señalando vacíos, recomendando ajustes y aportando evidencia que permita orientar decisiones. Este trabajo conjunto refuerza la coherencia del sistema y mejora la capacidad institucional para enfrentar incidentes y justificar acciones.

G. CONCLUSIÓN

El análisis de los tres precedentes jurisprudenciales revela un patrón común: las entidades fueron condenadas porque no pudieron acreditar que sus controles operaban como habían declarado. La existencia de políticas formales o certificaciones resultó insuficiente. Los tribunales exigieron registros verificables que demostraran ejecución efectiva.

Los tribunales, cada uno con su estilo, repitieron el mismo mensaje. El banco argentino no logró presentar los registros que acreditaran que su sistema de monitoreo de operaciones sospechosas funcionaba conforme a la Comunicación A 4609 y a sus propias políticas internas. El banco chileno se refugió en que las credenciales eran correctas y recibió la respuesta de que eso no exime de detectar patrones fraudulentos evidentes. El banco español presentó políticas genéricas y obsoletas que no describían la configuración real de sus controles, y la sentencia fue tajante al declarar que tales documentos carecían de todo valor probatorio.

Este mismo error se repite en la práctica cotidiana de empresas privadas y organismos públicos. Se acumulan manuales que nadie consulta, se aprueban procedimientos que nadie aplica, se archivan evidencias que nadie revisa y, sobre todo, se confunde la existencia formal del documento con su efectividad real. La experiencia demuestra que no funciona así. El papel solo protege cuando refleja con exactitud lo que ocurre y cuando alguien se encarga periódicamente de comprobarlo y actualizarlo.

La madurez en seguridad de la información no consiste en multiplicar normas ni en acumular certificados. Consiste en escribir lo imprescindible con claridad, ejecutar fielmente lo escrito y conservar prueba suficiente de esa ejecución. Todo lo demás (controles sofisticados, certificaciones, comités de alto nivel) es accesorio si falta alguna de estas tres patas. Los jueces ya lo entendieron. Ahora nos toca entenderlo a nosotros.

H. BIBLIOGRAFIA

Bygrave, L. (2002). *Data protection law*. Kluwer Law International.

Bygrave, L. (2014). *Information privacy: Law or policy?* Oxford University Press.

Casey, E. (2004). *Digital evidence and computer crime* (2nd ed.). Academic Press.

Corte de Apelaciones de Santiago. (2017). *Nannig Tuchie con Banco de Chile*, Recurso de Protección N.° 44.191-2017. Chile.

Corte Suprema de Justicia de la Nación (Argentina). (2016). *Galicia y Buenos Aires, Banco de v. Dasso, Pablo Martín s/ daños y perjuicios*, Fallos 339:691. Argentina.

Dhillon, G. (1997). *Managing information system security*. Macmillan.

European Union Agency for Network and Information Security. (2018). *Threat landscape report 2018*.

Hildebrandt, M. (2015). *Smart technologies and the end(s) of law*. Edward Elgar.

Institute of Internal Auditors. (2017). *International standards for the professional practice of internal auditing*.

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements.*

Maggiore, M., & Prandini, P. (2017). *Normas internacionales y nacionales de seguridad de la información* (1ra ed.). Fundación Vía Libre.

National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments* (SP 800-30 Rev. 1).

National Institute of Standards and Technology. (2013). *Security and privacy controls for federal information systems and organizations* (SP 800-53 Rev. 4).

National Institute of Standards and Technology. (2014). *Assessing security and privacy controls in federal information systems and organizations* (SP 800-53A Rev. 4).

Power, M. (1999). *The audit society*. Oxford University Press.

Prandini, P., & Maggiore, M. (2013). *Ciberdelito en América Latina y el Caribe. Una visión desde la sociedad civil*. Proyecto Amparo.

Reason, J. (1990). *Human error*. Cambridge University Press.

Schein, E. (1985). *Organizational culture and leadership*. Jossey-Bass.

Schneier, B. (2015). *Data and Goliath*. W. W. Norton.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management and Computer Security*, 8(1), 31-41.

Solove, D. (2008). *Understanding privacy*. Harvard University Press.

Tribunal Supremo de España. (2013). *Sentencia 582/2013*, Recurso 1683/2010. Sala de lo Civil. España.