GRUPO BLR

DEL CUMPLIMIENTO A LA CONFIANZA EMPRESARIAL: NORMATIVAS Y ÉTICA PROFESIONAL EN LAS TI

ISBN: 978-9907-852-11-0

Joofre Antonio Honores Tapia
Nicole Yeslaine Mora Encalada

2026

DEL CUMPLIMIENTO A LA CONFIANZA EMPRESARIAL: NORMATIVAS Y ÉTICA PROFESIONAL EN LAS TI

Joofre Antonio Honores Tapia

Nicole Yeslaine Mora Encalada

AUTORES

UTMACH

Este libro ha sido debidamente examinado y valorado en la modalidad doble par ciego con fin de garantizar la calidad científica.

©Grupo Editorial BLR
Universidad Técnica de Machala
Riobamba – Ecuador
Correo: publicaciones@grupoblr.com
https://grupoblr.com/libros-investigo
REPOSITORIO



Honores, J., Mora., N. (2026) Del cumplimiento a la confianza empresarial: Normativas y ética profesional en las TI. Grupo Editorial BLR.

© Joofre Antonio Honores Tapia
Nicole Yeslaine Mora Encalada

Del cumplimiento a la confianza empresarial: Normativas y ética profesional en las TI

ISBN:978-9907-852-11-0

El copyright promueve la libertad de expresión, protege la diversidad de ideas y conocimiento, además apoya la libre expresión. Se prohíbe de manera rigurosa la producción o el almacenamiento de esta publicación, ya sea en su totalidad o en parte, está estrictamente prohibido por ley, incluyendo el diseño de la portada, así como su difusión a través de cualquiera de sus medios, ya sean electrónicos, mecánicos, ópticos, de grabación o incluso de fotocopia, sin permiso de los propietarios de los derechos de autor.

Filiación de autores

Joofre Antonio Honores Tapia

Universidad Técnica de Machala

Correo Electrónico: jhonores@utmachala.edu.ec

ORCID: https://orcid.org/0000-0001-8612-3025

Nicole Yeslaine Mora Encalada

Universidad Técnica de Machala

Correo Electrónico:nymora@utmachala.edu.ec

ORCID: https://orcid.org/0009-0000-2960-7701

PREFACIO

La tecnología atraviesa hoy la educación, la salud, las finanzas, la gestión pública y las relaciones sociales. En este entorno, el profesional de Tecnologías de la Información no se limita a construir sistemas: también contribuye a crear o debilitar confianza. Una decisión de diseño, una configuración de seguridad, una política de acceso o una línea de código pueden afectar derechos como la privacidad, la equidad y la seguridad. De ahí parte la idea central de este libro: la ética y las normativas no son elementos accesorios del trabajo técnico, sino parte de su fundamento.

Los capítulos relacionan leyes, normas y mejores prácticas con la ética profesional aplicada. La normativa no se presenta como una lista rígida de verificación, sino como una estructura para actuar con responsabilidad, prevenir daños y rendir cuentas. El recorrido incluye marcos y organismos relevantes, la función social de la ética y dilemas contemporáneos vinculados con la ciberseguridad, la privacidad, la reputación digital, el uso responsable de los datos, la inteligencia artificial y las decisiones automatizadas en contextos empresariales y sociales.

El capítulo final funciona como un espacio de práctica profesional mediante casos, preguntas, análisis y propuestas de solución. Su propósito es que el lector no solo comprenda lo que establecen las normas, sino que pueda decidir responsablemente frente a presiones institucionales, recursos limitados, conflictos de interés, incidentes de

seguridad, relaciones con proveedores y decisiones que afectan a otras personas.

La obra se dirige a estudiantes, docentes y especialistas que buscan ejercer con integridad. Aspira a fortalecer el criterio ético, consolidar una cultura de cumplimiento y promover un desempeño responsable que proteja a los usuarios, mejore la calidad de los servicios y contribuya a instituciones más confiables.

La tecnología seguirá evolucionando, pero el verdadero desafío será asegurar que esa evolución esté alineada con el respeto a la dignidad humana y con una práctica profesional que merezca la confianza de la sociedad.

Objetivo general del libro

Analizar desde una perspectiva ética y normativa, los principios, estándares y buenas prácticas que guían el ejercicio profesional en Tecnologías de la Información, mediante el estudio de casos reales e hipotéticos, para fortalecer la toma de decisiones responsable, la protección de derechos y la rendición de cuentas en contextos empresariales y sociales.

ÍNDICE

PREFACIO ..... **i**

ÍNDICE ..... **iii**

ÍNDICE DE TABLAS ..... **vii**

ÍNDICE DE FIGURAS ..... **viii**

INTRODUCCIÓN ..... **xi**

JUSTIFICACIÓN ..... **xii**

CAPÍTULO I **13**

1 FUNDAMENTOS DE LAS NORMATIVAS EN TECNOLOGÍAS DE LA INFORMACIÓN **13**

1.1 Conceptos básicos de normativas y regulaciones 17

1.2 ¿Qué son las normativas y los estándares? 21

1.3 Diferencias entre leyes, normas y mejores prácticas 23

1.4 Principios éticos y legales en el uso de las TI 27

1.4.1 EduCloud: dilema de cumplimiento ético y técnico 29

1.5 Impacto de las normativas en las TI 42

1.5.1 SIGEDU: cumplir por obligación o por convicción 44

1.6 Síntesis transversal del capítulo 53

CAPÍTULO II 55

2 LA ÉTICA EN LA SOCIEDAD 55

2.1 Leyes universales de ética en la sociedad 57

2.2 Principios éticos y legales en el uso de las TI 60

2.2.1 TECNOSALUD S. A.: una brecha de seguridad 62

2.3 Derechos digitales y cibernéticos 69

2.4 Organismos certificadores internacionales 71

2.5 Organismos nacionales reguladores de las TI 75

2.5.1 SALUDNET: cumplimiento formal frente a seguridad real 79

2.6 Síntesis transversal del capítulo 88

CAPÍTULO III 90

3 ÉTICA EN TECNOLOGÍAS DE LA INFORMACIÓN 90

3.1 Introducción a la ética aplicada a las TI 92

3.2 Importancia de la ética en entornos tecnológicos 95

3.2.1 IA en reclutamiento: «El algoritmo reproduce nuestros sesgos» 97

3.3 Desafíos éticos emergentes ante el avance tecnológico 102

3.4 Rol del profesional de TI en la toma de decisiones éticas 104

3.5 Responsabilidad profesional en el ámbito tecnológico 108

3.5.1 SIGTAL y la responsabilidad del ingeniero en TI 114

3.6 Privacidad y protección de datos en entornos tecnológicos 120

3.7 Ética y reputación digital 125

3.7.1 CIVITAS: entre el cumplimiento y la confianza 127

3.8 Síntesis transversal del capítulo 133

CAPÍTULO IV 135

4 APLICACIÓN PRÁCTICA DE NORMAS Y ÉTICA EN EL EJERCICIO PROFESIONAL: CASOS, ANÁLISIS Y SOLUCIONES 135

4.1 Introducción a la práctica profesional ética 135

4.2 Aplicación de normas y ética en situaciones reales 137

4.3 Metodologías de análisis ético para la toma de decisiones 139

4.4 Casos prácticos: análisis y soluciones 142

4.4.1 FinNova Capital: brecha de datos en una empresa de tecnología financiera 143

4.4.2 VALORPAY: entre la prueba autorizada y el riesgo 150

4.4.3 TALENTOIA en Econofin: eficiencia, sesgo y decisiones 157

4.4.4 SIGCOMPRAS-EC: transparencia, eficiencia y dilemas éticos en la contratación pública 166

4.5 Metodologías de resolución y recomendaciones..... 173

4.6 Aprendizajes para el ejercicio profesional 176

4.7 Síntesis transversal del capítulo 178

GLOSARIO DE TÉRMINOS 180

REFERENCIAS BIBLIOGRÁFICAS 191

ÍNDICE DE TABLAS

Tabla 1. Tabla comparativa de conceptos y el ámbito de TI. 19

Tabla 2. Aspectos relevantes de las leyes, normas y mejores prácticas. 24

Tabla 3. Tabla de deberes y acciones del Ingeniero en TI. 109

Tabla 4. Áreas y razón de actualización profesional en TI. 112

Tabla 5. Dimensiones y controles éticos ante el uso de la IA. 123

ÍNDICE DE FIGURAS

Figura 1. Normativas en las tecnologías de la información. 14

Figura 2. Aspectos que garantizan la confianza y la seguridad de la información. 15

Figura 3. Aspectos que fomentan la responsabilidad y la rendición de cuentas. 16

Figura 4. Aspectos que impulsan la eficiencia y la innovación tecnológica. 17

Figura 5. Diferencias entre normativas y estándares. 23

Figura 6. Dilema de cumplimiento ético y técnico. 29

Figura 7. Impacto de las Normativas en TI. 43

Figura 8. SIGEDU: cumplir por obligación o por convicción. 44

Figura 9. Leyes universales de ética en la sociedad. 58

Figura 10. TECNOSALUD S. A.: una brecha de seguridad..... 62

Figura 11. Derechos digitales y cibernéticos. 70

Figura 12. ISO/IEC y las organizaciones. 72

Figura 13. ISACA y el marco que gobierna. 74

Figura 14. El alcance de NIST 75

Figura 15. Arcotel y sus regulaciones.....76

Figura 16. Visión general de MINTEL. 77

Figura 17. Los GAD y su función en la sociedad. 78

Figura 18. INEN y su función. 79

Figura 19. 1.1.1 SALUDNET: cumplimiento formal frente a seguridad real. 79

Figura 20. Función de la Ética en las TI. 92

Figura 21. Importancia de la ética en entornos digitales. 95

Figura 22. IA en reclutamiento: «El algoritmo reproduce nuestros sesgos». 97

Figura 23. Rol ético del profesional en TI. 104

Figura 24. Triángulo de responsabilidades. 111

Figura 25. Ciclo de actualización profesional. 112

Figura 26. SIGTAL y la responsabilidad del ingeniero en TI..... 114

Figura 27. Privacidad y protección de datos. 120

Figura 28. Flujo ético de contenido generado por el usuario. 126

Figura 29. CIVITAS: entre el cumplimiento y la confianza. 127

Figura 30. Aplicación de normas éticas en situaciones reales.....137

Figura 31. Ética profesional más allá de los checklist y las normas. 139

Figura 32. Ciclo de toma de decisiones éticas. 139

Figura 33. FinNova Capital: brecha de datos en una empresa de tecnología financiera. 143

Figura 34. VALORPAY: entre la prueba autorizada y el riesgo.. 150

Figura 35. TALENTOIA en Econofin: eficiencia, sesgo y decisiones. 157

Figura 36. SIGCOMPRAS-EC: transparencia, eficiencia y dilemas éticos en la contratación pública. 166

INTRODUCCIÓN

La ética ofrece criterios para distinguir entre conductas correctas e incorrectas y orienta las decisiones tanto personales como profesionales. Su relación con el bien común y la convivencia resulta especialmente relevante en ámbitos donde una decisión técnica puede afectar a muchas personas. Actuar con integridad, por tanto, no solo dignifica el ejercicio profesional: también sostiene la confianza social en quienes asumen responsabilidades sobre sistemas, datos y servicios.

En el trabajo, la ética profesional convierte esos principios generales en criterios para evaluar decisiones concretas. Permite examinar si una conducta es responsable, si respeta a las partes afectadas y si protege la calidad del servicio. Esta mirada ayuda a prevenir prácticas que deterioran la confianza pública, incluso cuando una acción pueda parecer técnicamente posible o conveniente a corto plazo.

Desde esa perspectiva, el libro se concentra en la práctica profesional y en las normas que la orientan. Presenta situaciones basadas en experiencias señaladas por los autores y escenarios hipotéticos que permiten examinar decisiones cuyas consecuencias éticas no fueron valoradas de manera suficiente.

El propósito es ofrecer una guía útil para estudiantes y profesionales. Las preguntas incluidas en cada caso invitan a contrastar criterios, argumentar decisiones y fortalecer una práctica responsable, coherente con las necesidades de la sociedad y de las organizaciones.

JUSTIFICACIÓN

La ética reúne valores y criterios que orientan la conducta en los espacios personales y profesionales, influye en la identidad moral proporcionando referencias para convivir y trabajar con responsabilidad y respeto.

El contenido del libro busca ayudar al lector a reconocer y prevenir las situaciones problemáticas expuestas. Las preguntas de análisis promueven una reflexión crítica en la que cada persona debe justificar sus respuestas a partir de los principios, las normas y las consecuencias presentes en cada caso de estudio.

La obra responde a una necesidad concreta: analizar por qué algunos profesionales participan en decisiones contrarias a los principios éticos y qué consecuencias producen esas actuaciones, haciendo reflexionar sobre el daño que puede alcanzar tanto la reputación profesional como los derechos y la integridad de las personas afectadas intentando con ello fortalecer la reflexión ética permitiendo anticipar esos efectos y sostener una práctica coherente con el bien común.

CAPÍTULO I

1 FUNDAMENTOS DE LAS NORMATIVAS EN TECNOLOGÍAS DE LA INFORMACIÓN

En el ámbito profesional, las normativas de la información reúnen leyes, regulaciones, estándares, políticas y directrices que orientan el ciclo de vida de los datos: su recopilación, almacenamiento, procesamiento, transmisión y eliminación.

Estas normativas pueden emanar de diversas fuentes:

1. Leyes gubernamentales: Leyes nacionales e internacionales diseñadas para proteger la privacidad de los datos (como la Ley Orgánica de protección de datos personales), la propiedad intelectual, la ciberseguridad y otros aspectos cruciales.
2. Estándares tecnológicos: Marcos de referencia y mejores prácticas desarrolladas por organizaciones y consorcios para garantizar la calidad, la seguridad y la interoperabilidad de los sistemas de información (por ejemplo, ISO 38500 para orientar a las organizaciones de cara a un gobierno que utilice de forma efectiva el uso de las Tecnologías de la Información).
3. Políticas internas de las organizaciones: Reglas y procedimientos específicos que las empresas implementan para asegurar el cumplimiento normativo, proteger sus activos de información y gestionar los riesgos de manera efectiva.



Figura 1. Normativas en las tecnologías de la información.

Fuente: Elaboración propia.

La relevancia de las normativas de la información en el ámbito profesional se puede articular a través de tres pilares fundamentales:

1. Garantía de la confianza y la seguridad: Las normativas establecen los lineamientos para la recopilación y el tratamiento de datos personales, asegurando la privacidad de los individuos y evitando el uso indebido de la información. Esto es crucial para mantener la confianza de los clientes, socios y empleados; además, promueven la adopción de prácticas que aseguran la exactitud, la consistencia y el acceso oportuno a la información crítica para la toma de decisiones y las operaciones empresariales mediante regulaciones y estándares que impulsan la implementación de medidas de seguridad robustas para proteger los sistemas de información contra amenazas cibernéticas, como ataques

maliciosos, fugas de datos y fraudes garantizando un entorno digital seguro para la continuidad del negocio y la reputación de la organización.

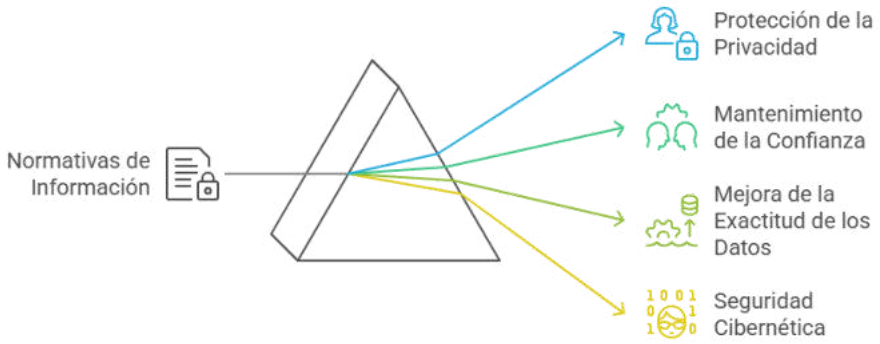


Figura 2. Aspectos que garantizan la confianza y la seguridad de la información.

Fuente: Elaboración propia.

2. Fomento de la Responsabilidad y la Rendición de Cuentas: El acatamiento de las normativas evita sanciones legales, multas y daños a la reputación que pueden resultar del incumplimiento; además, clarifica quién es la persona responsable de la gestión y protección de la información, facilitando la rendición de cuentas en caso de incidentes o incumplimiento. Para ello, es importante la implementación de mecanismos de auditoría y la documentación de prácticas de gestión de la información, promoviendo la transparencia y facilitando la identificación de áreas de mejora (National Institute of Standards and Technology, 2025; Center for Internet Security, 2024).



Figura 3. Aspectos que fomentan la responsabilidad y la rendición de cuentas.

Fuente: Elaboración propia.

3. Impulso a la eficiencia y la innovación tecnológica: al adoptar estándares, las organizaciones pueden optimizar sus procesos, mejorar la interoperabilidad de sus sistemas y reducir costos a largo plazo. También proporcionan un marco claro dentro del cual las organizaciones pueden innovar de manera segura y ética, considerando los impactos en la privacidad y la seguridad desde el diseño convirtiéndose en un diferenciador clave generando confianza entre clientes y socios comerciales.



Figura 4. Aspectos que impulsan la eficiencia y la innovación tecnológica.

Fuente: Elaboración propia.

1.1 Conceptos básicos de normativas y regulaciones

Cuando se trate temas de normativas y regulaciones en las Tecnologías de la Información es importante tener bien claro algunos conceptos que ayudarán a comprender el panorama de las normativas y regulaciones en las tecnologías de la información que se irá profundizando en cada uno de ellos con un enfoque técnico y fundamentado.

- Normativa: Directriz o especificación técnica que establece criterios para sistemas, procesos o productos de TI. Se basa en estándares técnicos definidos por organizaciones de normalización (IEEE, IETF, W3C) o estándares de facto surgidos por la práctica industrial.
- Regulación: Instrumento legal de carácter obligatorio, promulgado por entidades gubernamentales para gobernar actividades de TI dentro de su jurisdicción. Se fundamenta en la

legislación nacional e internacional con mecanismos oficiales y bases de datos jurídicas.

- Ley: Norma jurídica fundamental establecida por el poder legislativo de un estado, que sienta las bases para la regulación de las TI, deriva de la constitución y los principios generales del derecho. Las leyes específicas de TI abordan áreas como la protección de datos y la ciberseguridad.
- Estándar: Documento formalmente aprobado por un organismo de normalización reconocido, que define especificaciones técnicas, metodologías o directrices para garantizar la interoperabilidad, seguridad o calidad en TI. Es desarrollado a través de procesos de consenso técnico y basado en la investigación y la experiencia de expertos.
- Política: Declaración formal de principios, reglas y directrices internas de una organización, que definen el comportamiento esperado y los procedimientos para la gestión y el uso de los recursos de TI. Se alinea con los objetivos estratégicos de la organización y la necesidad de cumplir con las normativas y regulaciones externas.
- Cumplimiento: Estado de adherencia a las leyes, regulaciones, estándares y políticas de TI aplicables. Implica la implementación de controles y procesos para asegurar esta conformidad. Se basa en marcos de gestión de riesgos y la necesidad de evitar consecuencias legales, financieras y de reputación.
- Gobernanza: Sistema de dirección y control del uso de las TI dentro de una organización, asegurando que se alinean con los

objetivos estratégicos y se gestionan los riesgos, incluyendo el cumplimiento normativo. Se apoya en marcos de gobierno de TI como COBIT 2019 y principios de gobierno corporativo.

- Riesgo: Probabilidad de que una amenaza explote una vulnerabilidad en los activos de TI, con un impacto negativo en la confidencialidad, integridad, disponibilidad de la información o el cumplimiento normativo. Es evaluado mediante metodologías de análisis de riesgos basadas en identificación de activos, amenazas, vulnerabilidades y posibles impactos.
- Auditoría: Proceso sistemático e independiente para evaluar la eficacia de los controles de TI y el cumplimiento de las normativas, regulaciones y políticas establecidas. Se basa en estándares de auditoría de sistemas de información, metodologías de auditoría y principios de objetividad e independencia.

Tabla 1. Tabla comparativa de conceptos y el ámbito de TI.

Item	Descripción	Origen	Propósito
Normativa	Directriz o especificación técnica con criterios para sistemas, procesos o productos de TI.	Estándares técnicos (IEEE, IETF, W3C) o estándares de facto.	Asegurar coherencia técnica, interoperabilidad y buenas prácticas.
Regulación	Instrumento legal obligatorio emitido por entidades gubernamentales	Legislación nacional/internacional y bases jurídicas oficiales.	Establecer obligaciones y límites legales dentro de una jurisdicción.

	para controlar actividades de TI.		
Ley	Norma jurídica fundamental establecida por el poder legislativo; base para regular TI.	Constitución y principios del derecho.	Definir marcos legales generales, como protección de datos y ciberseguridad.
Estándar	Documento aprobado por un organismo reconocido que define especificaciones técnicas o metodologías.	Organismos de normalización (ISO, IEC, IEEE).	Garantizar interoperabilidad, calidad y seguridad mediante consenso técnico.
Política	Declaración interna de una organización que define reglas y comportamientos esperados en TI.	Objetivos estratégicos internos y obligaciones externas.	Guiar la gestión y uso responsable de los recursos de TI.
Cumplimiento	Estado de adherencia a leyes, regulaciones, estándares y políticas de TI aplicables.	Marcos de gestión de riesgos y requisitos normativos.	Evitar sanciones legales, pérdidas financieras y daños reputacionales.
Gobernanza	Sistema de dirección y control del uso de TI	Marcos como COBIT 2019 y gobierno corporativo.	Garantizar uso eficiente de TI y

	alineado con los objetivos organizacionales.		manejo adecuado de riesgos.
Riesgo	Probabilidad de que una amenaza explote una vulnerabilidad generando impacto negativo.	Metodologías de análisis de riesgos (identificación de activos, amenazas, impactos).	Identificar, evaluar y mitigar eventos adversos en TI.
Auditoría	Proceso independiente para evaluar controles de TI y el cumplimiento normativo.	Estándares y metodologías de auditoría de sistemas.	Verificar eficacia, objetividad y conformidad con políticas y normativas.

Fuente: Elaboración propia.

1.2 ¿Qué son las normativas y los estándares?

Las normativas en Tecnologías de la Información son como esas leyes y ordenanzas de nuestra ciudad digital. Son las reglas del juego, a veces impuestas por el "gobierno" (las autoridades legales y regulatorias) y otras veces acordadas por los propios "ciudadanos" (las organizaciones y la industria). Estas normativas nos indican qué se puede hacer, qué no se puede hacer y cómo se deben hacer las cosas para proteger a las personas (sus datos, su privacidad), asegurar que los servicios funcionen de manera confiable y evitar problemas mayores (National Institute of Standards and Technology [NIST], 2015; International Organization for Standardization, s. f.).

La normativa de protección de datos es como una ley que dice cómo debemos tratar la información personal de cada "habitante" de nuestra ciudad digital, asegurándonos de que se respete su privacidad y se use la información de forma justa y transparente.

Por otro lado, los estándares en Tecnologías de la Información son como los planos de construcción y los códigos de edificación. Son los acuerdos técnicos que definen cómo deben construirse y funcionar las cosas en nuestra ciudad digital. Estos estándares aseguran que diferentes "edificios" (sistemas y dispositivos) puedan comunicarse entre sí sin problemas (interoperabilidad), que sean seguros (siguiendo ciertos criterios de seguridad) y que tengan una calidad mínima aceptable.

Imagina que, en nuestra ciudad digital, además de leyes (normativas), necesitamos un "consejo de gobierno" que supervise cómo se gestiona y se utiliza la tecnología para el beneficio de todos los "ciudadanos" y el progreso de la ciudad en general. Aquí es donde entra en juego la ISO 38500, el estándar internacional para el "gobierno corporativo de las tecnologías de la información". La ISO 38500 no nos dice cómo construir un software específico ni cómo gestionar la calidad de ese software sino se enfoca en quién toma las decisiones importantes sobre la tecnología, cómo se toman esas decisiones y cómo se asegura que el uso de la tecnología esté alineado con los objetivos de toda la "ciudad" (la organización) y que se gestionen los riesgos de manera responsable.

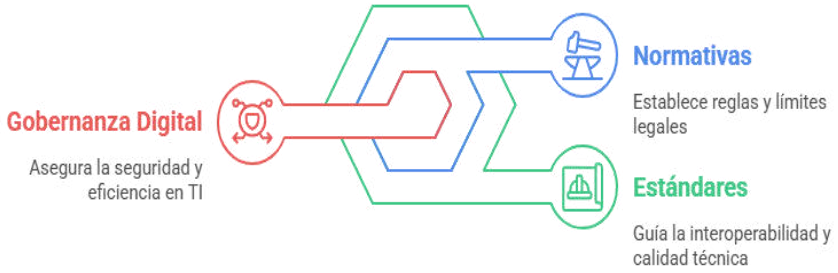


Figura 5. Diferencias entre normativas y estándares.

Fuente: Elaboración propia.

1.3 Diferencias entre leyes, normas y mejores prácticas

Pensemos primero en lo que significa en resumen lo que son las leyes, las normas y las buenas prácticas, entonces pongámonos en contexto:

Las leyes son el "debes hacer" obligatorio para mantener el orden y la legalidad con sentido de coacción, es decir el no hacerlo implicará tener una sanción, las normas son el "deberías hacer" para asegurar la calidad, la seguridad y la eficiencia, a menudo basadas en consenso y por último las mejores prácticas serían el "sería ideal hacer" para alcanzar la excelencia y la eficiencia óptima, basadas en la experiencia y el conocimiento para ello se basa en metodologías y técnicas.

Ahora bien, definamos lo que significa cada una de ellas y notemos la diferencia que tienen en sus definiciones.

Leyes: Son el marco regulatorio obligatorio promulgado por entidades gubernamentales. En el ámbito tecnológico, estas legislaciones definen los límites de las actividades digitales, estableciendo derechos,

responsabilidades y prohibiciones con consecuencias legales por su incumplimiento. Su objetivo principal es proteger a los individuos (privacidad de datos), las organizaciones (propiedad intelectual, seguridad de la información) y la sociedad en general (ciberseguridad, delitos informáticos).

Normas: Son documentos técnicos o de gestión establecidos por consenso por organismos de normalización reconocidos (ISO, IEEE, IETF) que definen especificaciones técnicas, metodologías, procesos o características para asegurar la interoperabilidad, la calidad, la seguridad y la eficiencia de los sistemas y servicios de TI. Su adopción puede ser voluntaria, pero a menudo se convierte en un requisito contractual o es referenciada por regulaciones.

Mejores prácticas: Representan las técnicas, metodologías o marcos de trabajo que han demostrado consistentemente generar resultados superiores en la gestión, el desarrollo y la operación de sistemas de TI. No son obligatorias ni formalmente especificadas como las normas, pero su adopción se basa en la experiencia de la industria y la búsqueda de la eficiencia, la seguridad y la innovación.

Tabla 2. Aspectos relevantes de las leyes, normas y mejores prácticas.

Aspecto	**Leyes**	**Normas**	**Mejores prácticas**
Naturaleza	Marco jurídico obligatorio promulgado por el Estado.	Documento técnico o de gestión aprobado por consenso en	Conjunto de técnicas/metodologías que la industria considera eficaces.

		organismos de normalización.	
Emisor / Origen	Poder legislativo (parlamentos, asambleas) y autoridades regulatorias.	Organismos como ISO, IEC, IEEE, IETF, W3C, ETSI, etc.	Comunidades profesionales, consorcios, cuerpos de conocimiento (ISACA, ITIL, OWASP, SANS, NIST SP como guía), experiencias sectoriales.
Proceso de elaboración	Proceso legislativo formal (debate, aprobación, promulgación).	Consenso técnico (comités, revisión pública, votación).	Evolutivo y empírico (lecciones aprendidas, benchmarking, marcos de referencia).
Propósito principal	Proteger derechos y el orden público: privacidad, propiedad intelectual, ciberseguridad, responsabilidades y sanciones.	Asegurar interoperabilidad, calidad, seguridad y eficiencia técnica y de gestión.	Optimizar resultados: eficacia operativa, seguridad, calidad, innovación y mejora continua.
Mecanismo de cumplimiento	Supervisión estatal, autoridades competentes, fiscalización y sistema judicial.	Auditorías de certificación (p. ej., ISO/IEC 27001), auditorías de clientes, revisiones de conformidad.	Autoevaluación, auditorías internas, evaluaciones de madurez, adopción voluntaria.

Consecuencias por incumplimiento	Sanciones legales: multas, inhabilitaciones, responsabilidad civil/penal.	Pérdida de certificación, incumplimiento contractual, afectación reputacional.	Ineficiencias, riesgos elevados y brechas, pérdida de competitividad/reputación.
Actualización / Ciclo de vida	Menos frecuente; requiere reforma legislativa.	Periódica y estructurada; ciclos multianuales de revisión.	Continua y ágil; responde a tendencias, incidentes, nuevas tecnologías.
Quién las exige	El Estado (autoridades y tribunales).	Clientes, certificadores, reguladores (cuando las referencian), mercados internacionales.	Dirección de TI, CISO/CTO, equipos de mejora continua, comunidades técnicas.
Ejemplos	Ley de Protección de Datos, leyes de ciberseguridad, firmas electrónicas, normas de propiedad intelectual.	ISO/IEC 27001, ISO/IEC 20000-1, ISO 22301, IEEE 802.11, IETF RFC 791/2460, W3C HTML/CSS.	ITIL 4, COBIT (como marco de gobierno y prácticas), DevOps/SRE, OWASP Top 10, CIS Controls, Kanban, Scrum.

Fuente: Elaboración propia.

Si bien cada una tiene su particularidad Conviene subrayar que todas buscan reducir riesgos y proteger a las partes interesadas, fomentan la

seguridad, calidad y confiabilidad en TI; todas ellas pueden complementarse para encontrar el equilibrio en la empresa es así que la Ley es una referencia y enmarca todo el tema legal, la norma establece las operaciones dentro de la empresa y las mejores prácticas elevan la madurez y facilitan el cumplimiento.

1.4 Principios éticos y legales en el uso de las TI

Estos principios se centran en el comportamiento responsable y moralmente correcto en el diseño, desarrollo, implementación y uso de las tecnologías de la información. Aunque no siempre estén codificados en leyes, su observancia es esencial para mantener la confianza y el bienestar de los individuos y la sociedad.

Los principios éticos en primer lugar se centran en:

- Privacidad: El respeto por la esfera personal y el derecho de los individuos a controlar la recopilación, el almacenamiento, el procesamiento y la divulgación de su información. Esto implica transparencia en las políticas de datos, minimización de la recopilación y obtención de consentimiento informado.
- Seguridad: La obligación de proteger la información y los sistemas contra accesos no autorizados, alteraciones, destrucción o divulgación. Esto requiere la implementación de medidas técnicas y organizativas robustas para salvaguardar los activos digitales.
- Transparencia y Honestidad: La necesidad de ser claros y veraces sobre el funcionamiento de los sistemas de TI, el uso de los datos

y las posibles implicaciones de la tecnología. Esto fomenta la confianza y permite a los usuarios tomar decisiones informadas.

- Equidad y No Discriminación: El imperativo de asegurar que el diseño, el desarrollo y la implementación de las tecnologías de la información no perpetúen ni amplifiquen sesgos injustos o discriminación basados en características protegidas.
- Responsabilidad y Rendición de Cuentas: La obligación de asumir la responsabilidad por las acciones y las consecuencias del uso de las TI, estableciendo mecanismos claros para la rendición de cuentas en caso de fallos o daños.

Por otro lado, los principios legales se centran en:

- Cumplimiento Normativo: La obligación de adherirse a las leyes y regulaciones aplicables en el ámbito de las TI, que abarcan áreas como la protección de datos, la propiedad intelectual, la ciberseguridad y el comercio electrónico.
- Propiedad Intelectual: El respeto por los derechos de autor, las patentes, las marcas registradas y otros derechos de propiedad intelectual relacionados con el software, el contenido digital y las innovaciones tecnológicas.
- Responsabilidad Legal: La obligación de responder legalmente por los daños causados por el uso negligente o indebido de las tecnologías de la información, especialmente en casos de brechas de seguridad o mal uso de datos.

- Jurisdicción y Ley Aplicable: La determinación de qué leyes rigen las actividades en línea y las transacciones digitales, un aspecto crucial en el contexto global de internet.
- Evidencia Digital y Admisibilidad Legal: La comprensión de cómo se considera la información digital como prueba en procesos legales y la necesidad de garantizar su autenticidad e integridad.

El siguiente caso permite aplicar los conceptos revisados:

1.4.1 EduCloud: dilema de cumplimiento ético y técnico



Figura 6. Dilema de cumplimiento ético y técnico.

La Empresa Desarrollo Inteligente implementa EduCloud, una plataforma digital diseñada para gestionar la información académica de los estudiantes de una prestigiosa universidad: calificaciones, historial académico, datos personales y archivos de investigación. El sistema fue desarrollado por el Departamento de Tecnologías de la Información, liderado por el ingeniero Carlos Mena.

Durante una auditoría interna, se detecta que EduCloud almacena información sensible sin aplicar técnicas adecuadas de cifrado. Además, se descubre que los registros de acceso no están siendo monitoreados correctamente, lo que vulnera los principios básicos de seguridad de la información.

Al revisar el proyecto, la auditora concluye lo siguiente:

- Incumplimiento de leyes
  - Se viola la legislación nacional sobre protección de datos personales y privacidad digital. La empresa tiene la obligación legal de salvaguardar la información de los estudiantes, y el almacenamiento sin cifrado constituye una infracción que puede acarrear sanciones económicas y administrativas.
- Incumplimiento de normas
  - El desarrollo de EduCloud no siguió las normas internacionales recomendadas, como:
    - ISO/IEC 27001 (gestión de la seguridad de la información).
    - ISO/IEC 27002 (controles de seguridad).
    - Estándares de interoperabilidad establecidos por organismos como IEEE.

Aunque estas normas no son obligatorias, su uso es reconocido como referencia técnica indispensable para garantizar calidad y seguridad.

- Falta de adopción de mejores prácticas
  - El equipo de desarrollo tampoco aplicó prácticas ampliamente aceptadas en la industria, como:

- Ciclos de desarrollo seguro.
- Revisión de código y pruebas de penetración.
- Control de versiones formal.
- Matrices de riesgos y planes de mitigación.

Estas prácticas, aunque no imponen sanciones legales ni normativas, ayudan a prevenir incidentes, optimizar procesos y asegurar la eficiencia del sistema.

Cuando Carlos es convocado para explicar las irregularidades, argumenta que la presión por lanzar la plataforma lo llevó a omitir algunos pasos técnicos, y que confiaba en que el sistema "funcionaría bien" mientras se completaban las mejoras previstas. Sin embargo, la situación se agrava cuando un estudiante denuncia que sus datos personales fueron accedidos por un tercero no autorizado. Aunque no se logra comprobar cómo ocurrió la filtración, el incidente provoca preocupación en la comunidad universitaria y genera desconfianza hacia EduCloud y hacia el equipo de TI.

Frente a esto, la rectoría toma la decisión de:

- Suspender temporalmente el uso de la plataforma.
- Notificar la brecha de seguridad ante la autoridad reguladora, como exige la ley.
- Solicitar una reconstrucción completa del sistema siguiendo normas y mejores prácticas.
- Abrir una investigación disciplinaria por negligencia profesional.

El caso evidencia que las consecuencias de ignorar leyes, normas y mejores prácticas pueden afectar no solo a la infraestructura tecnológica, sino también a la reputación institucional y a la confianza de los usuarios.

Preguntas para el análisis

1. ¿Qué responsabilidades legales incumplió el equipo de TI al almacenar datos sensibles sin cifrado y cómo afectan estas omisiones a la institución?
2. ¿De qué manera el desconocimiento o la falta de aplicación de normas internacionales (como ISO/IEC 27001 o 27002) contribuyó al incidente de seguridad presentado?
3. ¿Qué factores organizacionales pudieron influir en que el ingeniero Carlos Mena priorizara la rapidez del lanzamiento sobre la seguridad del sistema?
4. ¿Qué consecuencias éticas se derivan de haber implementado un sistema con vulnerabilidades conocidas, especialmente tratándose de información académica y personal?
5. ¿Cómo afecta este incidente la confianza de los estudiantes y de la comunidad universitaria en la gestión tecnológica de la institución?
6. ¿Qué mecanismos internos de control o auditoría pudieron haberse aplicado para detectar oportunamente las falencias antes del incidente?

7. ¿Qué mejores prácticas de la industria (como pruebas de penetración, revisiones de código o Siclos de Desarrollo Seguro) habrían evitado el acceso no autorizado a los datos?
8. ¿Cuál debería ser el rol de la rectoría y de la autoridad reguladora para asegurar que la universidad cumpla con leyes de protección de datos y prevención de delitos informáticos?
9. ¿Cómo puede el equipo de TI corregir las fallas detectadas y establecer un plan de mejora continua para garantizar que no se repitan incidentes similares?
10. ¿Qué medidas preventivas, tanto técnicas como administrativas, deberían implementarse para reconstruir EduCloud siguiendo leyes, normas y mejores prácticas (p. ej., cifrado, capacitación, políticas de seguridad, auditorías periódicas)?

Reflexión del caso

El caso de la plataforma EduCloud evidencia cómo las fallas técnicas no siempre son producto exclusivo de errores tecnológicos, sino del debilitamiento de principios éticos y profesionales fundamentales. A primera vista, la omisión del cifrado y la falta de controles de seguridad parecen simples descuidos técnicos, pero en realidad revelan un problema mayor: la ausencia de responsabilidad, rigor y compromiso con la protección de la información confiada a la institución.

En el campo de las tecnologías de la información, los profesionales gestionan datos que representan la identidad, la privacidad y, en muchos casos, la seguridad de las personas. Por ello, la ética no es un complemento, sino un componente esencial de la práctica profesional.

Cuando Carlos decide acelerar el lanzamiento de EduCloud sin implementar medidas básicas de seguridad, coloca en segundo plano la integridad y la protección de los usuarios. Esta acción implica un quiebre del principio ético de no maleficencia, pues expone a los estudiantes a riesgos previsibles y evitables.

Asimismo, el caso muestra cómo ignorar leyes, normas y mejores prácticas afecta directamente la confianza institucional. Una universidad debe ser un espacio seguro y confiable para el manejo de información académica. La filtración, aunque no se haya comprobado cómo ocurrió, genera un daño intangible pero profundo: la pérdida de credibilidad. Una plataforma que incumple estándares mínimos de seguridad compromete el vínculo de confianza con los usuarios y afecta el prestigio de la institución.

Por otra parte, la falta de adopción de normas como ISO 27001 o ISO 27002 pone en evidencia que la seguridad no es solo un asunto técnico, sino también de gestión y cultura organizacional. Las normas ofrecen estructura, los marcos legales establecen límites, y las mejores prácticas proporcionan el conocimiento acumulado de la industria. Ignorarlas no solo vulnera sistemas, sino que revela una actitud poco profesional hacia el deber de proteger la información. En un entorno donde la tecnología se entrelaza con la vida diaria, la ética tecnológica se vuelve tan importante como la capacidad técnica.

Finalmente, el caso nos recuerda que la competencia profesional no se mide solo en habilidades técnicas, sino también en la capacidad de tomar decisiones responsables, actuar preventivamente y mantener un

compromiso genuino con la seguridad y el bienestar de los usuarios. Lanzar un sistema “porque funcionará después” o “porque luego se corrige” es contrario a la ética del profesional en TI, cuyo deber es prever, prevenir y proteger.

Posible solución:

La solución al problema presentado debe abordarse desde una perspectiva integral que combine acciones inmediatas para mitigar los riesgos actuales y un plan estratégico que garantice la seguridad, cumplimiento y calidad del sistema a largo plazo. A continuación, se propone una solución estructurada en cuatro fases esenciales.

1. Fase de contención y mitigación inmediata
a. Suspensión temporal del sistema.
b. Notificación a la autoridad de protección de datos.
c. Comunicación transparente con la comunidad universitaria.
2. Fase de corrección técnica del sistema
a. Implementación de cifrado de datos.
b. Establecimiento de controles de acceso.
c. Auditoría externa de seguridad.
3. Fase de alimentación con leyes, normas y mejores prácticas
a. Cumplimiento estricto de leyes de protección de datos.
b. Implementación de un sistema de gestión de seguridad de la información.
c. Adopción de normas técnicas.
d. Aplicación de mejores prácticas de desarrollo.
4. Fase de fortalecimiento institucional y ético

a. Programa permanente de capacitación del equipo de TI.
b. Definición de políticas internas de seguridad.
c. Fomento de una cultura ética en TI.

Respuestas al caso práctico: La plataforma EduCloud y el dilema del cumplimiento ético y técnico

1. ¿Qué responsabilidades legales incumplió el equipo de TI al almacenar datos sensibles sin cifrado y cómo afectan estas omisiones a la institución?

El equipo incumplió deberes de protección de datos personales al almacenar información sensible sin cifrado y sin controles adecuados de acceso y registro. Esto vulnera principios como confidencialidad, integridad y disponibilidad, así como el deber de seguridad que toda institución tiene ante titulares de datos.

2. ¿De qué manera el desconocimiento o la falta de aplicación de normas internacionales (como ISO/IEC 27001 o 27002) contribuyó al incidente de seguridad presentado?

La ausencia de estas normas impidió contar con un marco sistemático de gestión de la seguridad de la información por lo que no existió un proceso formal para identificar riesgos, establecer controles obligatorios, documentar políticas de seguridad, monitorear accesos, y aplicar medidas preventivas; de igual manera, la falta de aplicación de normas dejó al sistema sin controles concretos, como cifrado de datos, registros de auditoría o segmentación de accesos.

3. ¿Qué factores organizacionales pudieron influir en que el ingeniero Carlos Mena priorizara la rapidez del lanzamiento sobre la seguridad del sistema?

Varios factores institucionales probablemente influyeron:

- Presión por cumplir fechas de entrega sin considerar criterios mínimos de seguridad.
- Ausencia de una política formal de ciberseguridad, lo que deja la seguridad a discreción del equipo.
- Falta de supervisión por parte de la gerencia o rectoría en temas de riesgo tecnológico.
- Escasez de recursos (tiempo, presupuesto, personal especializado).
- Una cultura institucional enfocada en "salir rápido", en lugar de "salir seguro".

4. ¿Qué consecuencias éticas se derivan de haber implementado un sistema con vulnerabilidades conocidas, especialmente tratándose de información académica y personal?

Las implicaciones éticas son severas:

- Se vulnera el principio de responsabilidad profesional, al no proteger adecuadamente información sensible.
- Se incumple el deber de no causar daño, pues se expone a los usuarios a riesgos previsibles.
- Se afecta la confianza que estudiantes y docentes depositan en la institución.

- Hay una falta de transparencia, pues no se informó sobre las debilidades del sistema.
- Se atenta contra la privacidad y dignidad humana, pilares fundamentales de la ética tecnológica.

5. ¿Cómo afecta este incidente la confianza de los estudiantes y de la comunidad universitaria en la gestión tecnológica de la institución?

El impacto en la confianza es significativo:

- Los estudiantes pierden seguridad al entregar datos personales o académicos.
- Surge la percepción de que la universidad no protege adecuadamente la información.
- La credibilidad del área de TI se deteriora, afectando futuros proyectos digitales.
- La comunidad cuestiona la competencia profesional del equipo responsable.
- Se genera un clima de desconfianza general hacia plataformas tecnológicas institucionales.

6. ¿Qué mecanismos internos de control o auditoría pudieron haberse aplicado para detectar oportunamente las falencias antes del incidente?

Entre los mecanismos que debieron implementarse están:

- Auditorías internas de seguridad antes del lanzamiento.
- Revisiones de código fuente enfocadas en seguridad.

- Pruebas de penetración regulares.
- Monitoreo activo de logs, con alertas de accesos inusuales.
- El uso de un gestor de eventos de seguridad.
- Un comité de seguridad encargado de validar los requisitos mínimos antes de la implementación.
- Evaluación de riesgos al inicio y cierre de cada fase del proyecto.

7. ¿Qué mejores prácticas de la industria (como pruebas de penetración, revisiones de código o Siclos de Desarrollo Seguro) habrían evitado el acceso no autorizado a los datos?

Las principales mejores prácticas que habrían prevenido el incidente son:

- Implementación de un Ciclo de Desarrollo de Software Seguro.
- Cifrado de datos en reposo y en tránsito.
- Pruebas automatizadas de seguridad.
- Revisiones de código entre pares.
- Principio de mínimo privilegio en los accesos.
- Autenticación multifactor.
- Pruebas de penetración periódicas.
- Gestión adecuada de contraseñas, llaves y credenciales.

8. ¿Cuál debería ser el rol de la rectoría y de la autoridad reguladora para asegurar que la universidad cumpla con leyes de protección de datos y prevención de delitos informáticos?

Ambas instancias son claves para evitar que el incidente se repita sin embargo tanto el Rectorado como la autoridad reguladora tienen labores diferentes De este modo:

El Rectorado debe:

- Garantizar el cumplimiento de leyes de protección de datos.
- Establecer políticas institucionales obligatorias de seguridad.
- Financiar capacitación y mejoras tecnológicas.
- Supervisar el plan de corrección y exigir informes periódicos.
- Fomentar una cultura ética en la gestión de información.

La autoridad reguladora debe:

- Exigir la notificación formal del incidente.
- Supervisar que la universidad implemente correcciones reales.
- Imponer sanciones si hubo negligencia.
- Emitir directrices obligatorias de cumplimiento.

9. ¿Cómo puede el equipo de TI corregir las fallas detectadas y establecer un plan de mejora continua para garantizar que no se repitan incidentes similares?

El equipo de TI debe:

- Aplicar cifrado robusto en toda la información sensible.
- Rediseñar los controles de acceso e implementar Múltiple Factor de Acceso.
- Integrar pruebas de seguridad en todas las fases del desarrollo.

- Realizar auditorías internas y externas periódicas.
- Documentar políticas y procedimientos de seguridad.
- Establecer un Sistema de Gestión de Seguridad de la Información basado en ISO 27001.
- Capacitarse constantemente en ciberseguridad y ética profesional.
- Implementar un sistema de monitoreo continuo (SIEM).

10. ¿Qué medidas preventivas, tanto técnicas como administrativas, deberían implementarse para reconstruir EduCloud siguiendo leyes, normas y mejores prácticas (p. ej., cifrado, capacitación, políticas de seguridad, auditorías periódicas)?

Medidas técnicas:

- Cifrado AES-256 en bases de datos y TLS para comunicaciones.
- Múltiple Factor de Acceso y control de accesos basados en roles.
- Monitoreo y registro de actividades.
- Pruebas de penetración y análisis de vulnerabilidades.
- Pruebas de servidores y aplicaciones.
- Gestión de parches y actualizaciones.
- Backups cifrados y probados regularmente.

Medidas administrativas

- Políticas institucionales de seguridad de la información.
- Procedimientos de respuesta ante incidentes.
- Política de clasificación de información.
- Capacitación continua para personal de TI y usuarios clave.

- Adopción formal de normas ISO/IEC 27001-27002.
- Auditorías periódicas internas y externas.

1.5 Impacto de las normativas en las TI

Las normativas tienen un impacto profundo y multifacético en las Tecnologías de la Información. Si bien pueden generar desafíos en términos de costos y complejidad, son fundamentales para construir un entorno digital más seguro, confiable, ético y de mayor calidad.

Son esenciales para establecer un marco de confianza en un mundo cada vez más interconectado y dependiente de los datos, la seguridad y la privacidad donde no se permite que sean meras ocurrencias tardías. Regulaciones como el Reglamento General de Protección de Datos o las leyes de ciberseguridad obligan a las organizaciones a tomarse en serio la protección de la información, lo que a su vez genera una mayor confianza por parte de los usuarios y los clientes, esto, a largo plazo, fomenta la adopción y el crecimiento de las tecnologías de la información.

Desde un punto de vista técnico, las normativas impulsan la adopción de mejores prácticas y estándares. La necesidad de cumplir con regulaciones específicas a menudo conlleva la implementación de marcos de gestión de seguridad (como ISO 27001) o la adopción de estándares técnicos para garantizar la interoperabilidad y la seguridad. Esto eleva el nivel general de calidad y profesionalismo en el desarrollo y la operación de sistemas de TI.

Si bien es cierto que el cumplimiento normativo puede imponer costos y complejidades adicionales a las organizaciones, especialmente a las más pequeñas o a los startups, creo que estos costos se ven superados por los beneficios a largo plazo. Evitar las consecuencias de una brecha de seguridad o una sanción por incumplimiento es significativamente más costoso que invertir en medidas preventivas.



Figura 7. Impacto de las Normativas en TI.

Fuente: Elaboración propia.

No obstante, también es importante reconocer que las normativas deben ser ágiles y adaptables al ritmo vertiginoso de la innovación tecnológica. Regulaciones demasiado rígidas o desactualizadas pueden frenar la experimentación y la adopción de nuevas tecnologías. Es crucial que los legisladores y los organismos reguladores trabajen en estrecha colaboración con la industria tecnológica para crear normativas que sean efectivas sin sofocar la innovación.

A continuación, un caso práctico traslada estos conceptos a una decisión profesional:

1.5.1 SIGEDU: cumplir por obligación o por convicción



Figura 8. SIGEDU: cumplir por obligación o por convicción.

La Universidad Horizonte lanza SIGEDU, un sistema web para administrar el ciclo de vida estudiantil (admisiones, matrícula, calificaciones, historial académico y certificados). El proyecto, liderado por la Dirección de TI, se ejecutó en ocho meses bajo fuerte presión institucional por "estar en producción antes del nuevo periodo académico".

Tres semanas después del despliegue, un estudiante reporta haber visto en su portal datos de otro alumno (nombres completos y asignaturas). El equipo de TI identifica que:

- Las bases de datos no estaban cifradas.

- La autenticación multifactor estaba planificada “para una fase posterior”.
- No existían registros de auditoría suficientes para trazar accesos.
- La codificación no siguió un ciclo de desarrollo seguro; tampoco se ejecutaron pruebas de penetración.
- La institución no tenía implantado un Sistema de Gestión de Seguridad de la Información basado en ISO/IEC 27001 ni controles específicos de ISO/IEC 27002.
- El contrato con el proveedor no exigía cumplimiento de normas internacionales, solo “buena práctica y esfuerzo razonable”.

La Asesoría Legal advierte que el incidente podría vulnerar leyes de protección de datos personales y exige: notificar a la autoridad, comunicar a los afectados y ejecutar medidas correctivas inmediatas.

El Rectorado solicita un informe técnico-ético donde se detallen:

Las causas, responsabilidades, plan de remediación, cronograma, políticas para prevenir la repetición.

El equipo de TI argumenta que “no hubo presupuesto suficiente”, que “la ventana de despliegue era inflexible” y que “se planeó completar la seguridad luego del go-live”.

Cuestiones para discutir

1. ¿Qué obligaciones legales fueron posiblemente vulneradas y por qué el incidente podría constituir una violación a la protección de datos personales?

2. ¿Cómo incidió la falta de adopción de normas ISO/IEC 27001 y 27002 en la materialización del incidente?
3. ¿Qué factores organizacionales explican que se priorizara la velocidad de entrega sobre la seguridad del sistema?
4. ¿Cuáles son las consecuencias éticas de desplegar un sistema con controles críticos diferidos (MFA, cifrado, auditoría)?
5. ¿Qué riesgos reputacionales y de confianza institucional emergen para la universidad y para el área de TI?
6. ¿Qué mecanismos de control interno y auditoría previa habrían detectado oportunamente las fallas antes del despliegue?
7. ¿Qué mejores prácticas (SSDLC, pentesting, code review, hardening, gestión de llaves) habrían prevenido el acceso indebido a datos?
8. ¿Qué rol deben asumir la Rectoría y la autoridad reguladora tras el incidente para asegurar cumplimiento y mejora?
9. ¿Cómo estructurar un plan de remediación y de mejora continua que integre aspectos legales, normativos y técnicos?
10. ¿Qué medidas preventivas, técnicas y administrativas, deben exigirse para la reconstrucción de SIGEDU conforme a leyes, normas y mejores prácticas?

Lectura ética del caso

SIGEDU evidencia que la seguridad no es un complemento del desarrollo tecnológico, sino su condición moral y funcional de posibilidad. Postergar controles esenciales en nombre de la velocidad niega el principio de no maleficencia y vulnera la confianza que la

comunidad deposita en la institución. Cumplir con la ley por obligación es insuficiente si no existe una convicción ética que ponga a la persona y su dignidad en el centro del diseño tecnológico. La excelencia institucional emerge cuando confluyen: leyes (protección y sanción), normas (calidad y consistencia) y mejores prácticas (aprendizaje y eficacia). No se trata solo de "evitar multas", sino de honrar la responsabilidad profesional, asegurar la privacidad y fortalecer el bien común.

Posible solución:

1. ¿Qué obligaciones legales fueron posiblemente vulneradas y por qué el incidente podría constituir una violación a la protección de datos personales?

- Deber de seguridad: ausencia de medidas técnicas y organizativas adecuadas (falta de cifrado, MFA, registros de auditoría, control de accesos).
- Principios de confidencialidad e integridad: exposición de datos personales de un estudiante a otro usuario.
- Responsabilidad demostrable: no hay evidencia técnica suficiente que pruebe cumplimiento diligente.
- Notificación de incidentes: obligación de informar a la autoridad y a titulares afectados dentro de plazos razonables.

2. ¿Cómo incidió la falta de adopción de normas ISO/IEC 27001 y 27002 en la materialización del incidente?

- Sin ISO/IEC 27001 (SGSI): no hubo ciclo PDCA (Plan-Do-Check-Act), ni análisis formal de riesgos, ni roles/políticas definidas, ni auditorías regulares.
- Sin ISO/IEC 27002: faltaron controles concretos (cifrado en reposo y tránsito, gestión de accesos y privilegios, monitoreo y retención de logs, pruebas de seguridad).
- Efecto agregado: La ausencia de marco de gestión sumado a los controles operativos dejó brechas previsibles sin tratar, habilitando el acceso indebido.

3. ¿Qué factores organizacionales explican que se priorizara la velocidad de entrega sobre la seguridad del sistema?

- Presión de calendario sin criterios de seguridad.
- Cultura de "salir y corregir después".
- Presupuesto y recursos limitados (equipo, tiempo, herramientas).
- Gobernanza de TI débil: sin comité de riesgos, sin patrocinios ejecutivos, sin KPIs de seguridad.
- Contratación deficiente: contratos sin cláusulas obligatorias de cumplimiento normativo y pruebas de seguridad.

4. ¿Cuáles son las consecuencias éticas de desplegar un sistema con controles críticos diferidos (MFA, cifrado, auditoría)?

- Quebranto del principio de no maleficencia: se expone a usuarios a riesgos evitables.
- Irresponsabilidad profesional: falta de diligencia debida con datos sensibles.
- Pérdida de confianza y legitimidad moral ante la comunidad.

- Falta de transparencia: no informar riesgos conocidos que afectan a terceros.
- Afectación a dignidad y privacidad de las personas titulares de datos.

5. ¿Qué riesgos reputacionales y de confianza institucional emergen para la universidad y para el área de TI?

- Erosión de credibilidad institucional y del equipo de TI.
- Resistencia de estudiantes a usar SIGEDU o entregar datos.
- Incremento de escrutinio de reguladores, prensa y comunidad.
- Posible impacto en matrícula, alianzas y proyectos tecnológicos futuros.
- Costo de recuperación de imagen (tiempo, recursos, comunicación, auditorías).

6. ¿Qué mecanismos de control interno y auditoría previa habrían detectado oportunamente las fallas antes del despliegue?

- Revisión de arquitectura y modelado de amenazas.
- Revisiones de código con foco en seguridad.
- SAST/DAST/IAST integrados al pipeline CI/CD.
- Pruebas de penetración pre - producción y tras cambios significativos.
- Puertas de seguridad obligatorios para “go - live”.
- Checklist de cumplimiento (mapeado a ISO 27001/27002) antes de liberar.
- Pruebas de privacidad (minimización de datos, control de acceso por contexto).

7. ¿Qué mejores prácticas (SSDLC, pentesting, code review, hardening, gestión de llaves) habrían prevenido el acceso indebido a datos?

- SSDLC: requisitos de seguridad, threat modeling, criterios de aceptación de seguridad, pruebas automatizadas, security sign-off.
- Cifrado en tránsito (TLS 1.2+) y en reposo (AES-256) + gestión de llaves (KMS/HSM, rotación, segregación).
- MFA y principio de mínimo privilegio (RBAC/ABAC, segregación de funciones).
- Hardening de plataformas y patch management.
- Code reviews sistemáticos y escaneo de dependencias (SCA).
- Pentesting interno/externo periódico y tras cambios críticos.
- Monitoreo y logs centralizados con alertas y retención adecuada (SIEM).

8. ¿Qué rol deben asumir El Rectorado y la autoridad reguladora tras el incidente para asegurar cumplimiento y mejora?

El Rectorado:

- Declarar la seguridad como prioridad estratégica.
- Asignar presupuesto para SGSI, herramientas y capacitación.
- Aprobar políticas institucionales (seguridad, privacidad, incidentes).
- Exigir plan de remediación con hitos y KPIs, además de generar reportes periódicos.
- Establecer comité de seguridad y riesgo tecnológico.

Autoridad reguladora:

- Verificar notificación del incidente y atención a titulares.

- Exigir acciones correctivas verificables y auditorías.
- Aplicar sanciones si hay negligencia.
- Emitir lineamientos y monitorizar madurez de seguridad.

9. ¿Cómo estructurar un plan de remediación y de mejora continua que integre aspectos legales, normativos y técnicos?

Fase 1 Contención inmediata (0 - 30 días)

- Suspender vectores de riesgo, implementar cifrado, MFA, logging y revisión de accesos.
- Notificar a autoridad y titulares; comunicación transparente a la comunidad.
- Pentest rápido y cierre de brechas críticas.

Fase 2 Corrección y formalización (30 - 90 días)

- Integrar SAST/DAST/SCA al pipeline.
- Establecer políticas (clasificación de información, incidentes, acceso, backups).
- Capacitar al equipo en ciberseguridad y ética.
- Alinear contratos con requisitos de seguridad medibles.

Fase 3 SGSI y gobernanza (90 - 180 días)

- Implementar SGSI (ISO 27001) con matriz de riesgos, controles (27002) y ciclo PDCA.
- Comité de seguridad, KPIs (MTTD, MTTR, cobertura de pruebas), auditorías internas.

Fase 4 Mejora continua (180 días y posterior)

- Auditorías externas, pentesting anual, simulacros de incidentes, evaluación de proveedores, revisión de lecciones aprendidas.

10. ¿Qué medidas preventivas, técnicas y administrativas, deben exigirse para la reconstrucción de SIGEDU conforme a leyes, normas y mejores prácticas?

Técnicas:

- Cifrado en tránsito (TLS 1.2/1.3) y reposo (AES-256); KMS/HSM, rotación de llaves.
- MFA, RBAC/ABAC, principio de mínimo privilegio y segregación de funciones.
- Logs centralizados y correlación con SIEM; retención y monitoreo continuo.
- SAST/DAST/IAST, dependency scanning, pentesting planificado.
- Hardening de OS/DB/app, patch management, configuración segura por defecto.
- Backups cifrados, pruebas de restauración, BCP/DRP documentados y probados.
- Segregación de ambientes (dev/test/preprod/prod) y control de cambios.

Administrativas:

- Políticas de seguridad de la información, privacidad, clasificación de datos, gestión de incidentes, control de accesos, uso aceptable.

- SGSI ISO/IEC 27001 y controles 27002 adoptados formalmente.
- Capacitación continua en seguridad y ética para TI y usuarios clave.
- Acuerdos contractuales con proveedores (SLAs de seguridad, pruebas obligatorias, derecho de auditoría).
- Comité de seguridad con reportes ejecutivos y KPIs.
- Auditorías internas semestrales y externas anuales; seguimiento de hallazgos.

1.6 Síntesis transversal del capítulo

Los contenidos de este capítulo permiten comprender que el cumplimiento en Tecnologías de la Información no depende de una única clase de regla. Las leyes establecen obligaciones exigibles; las normas ofrecen criterios técnicos y de gestión; las mejores prácticas aportan métodos que ayudan a elevar la calidad y la madurez operativa; y las políticas internas traducen estos referentes al funcionamiento cotidiano de cada organización, aunque su fuerza y su origen son distintos, todos estos instrumentos convergen en la protección de la información, la reducción de riesgos y la continuidad de los servicios.

La dimensión ética atraviesa ese conjunto normativo y le da sentido; cumplir no consiste únicamente en evitar sanciones o completar una lista de controles, también implica preguntarse a quién puede afectar una decisión, qué derechos están en juego y si la solución técnica puede justificarse ante usuarios, directivos y organismos de control. Así, la privacidad, la seguridad, la transparencia, la equidad y la rendición de

cuentas se convierten en criterios que orientan el diseño, la implementación y la evaluación de los sistemas.

Los casos de EduCloud y SIGEDU muestran esta relación desde la práctica, evidenciando que la presión por entregar un sistema, la ausencia de cifrado, el monitoreo insuficiente o una adopción meramente formal de las normas pueden producir consecuencias que van más allá del fallo técnico se comprometen la confianza de los usuarios, la reputación institucional y la capacidad de demostrar que las decisiones fueron responsables. Para el estudiante, estos casos fortalecen la lectura crítica de problemas reales; para la empresa, evidencian que la gobernanza, la documentación y la prevención deben incorporarse desde el inicio y no después de un incidente.

Este capítulo establece una base para el resto del libro: la técnica, la norma y la ética no son ámbitos separados, su integración permite pasar del cumplimiento entendido como obligación a una práctica profesional capaz de generar confianza. El capítulo siguiente amplía esta mirada al examinar la ética en la vida social, los derechos digitales y el papel de las instituciones que regulan o certifican el entorno tecnológico.

CAPÍTULO II

2 LA ÉTICA EN LA SOCIEDAD

La ética constituye uno de los pilares fundamentales sobre los cuales se estructura la vida en sociedad. Su influencia se manifiesta en la manera en que los individuos regulan sus acciones, reconocen sus responsabilidades y asumen las consecuencias de sus decisiones. A través de normas y valores compartidos, la ética orienta la convivencia y permite que las relaciones humanas se desenvuelvan en un marco de respeto, justicia y equidad; por ello, no se reduce a reglas abstractas, sino que actúa como un factor dinámico que favorece la confianza social y la construcción de instituciones más transparentes y prácticas profesionales responsables (UNESCO, 2026; The Editors of Encyclopaedia Britannica, 2026).

En el ámbito social, la ética funciona como un mecanismo de cohesión. Sin ella, las interacciones cotidianas estarían expuestas a la arbitrariedad y al abuso de poder. La toma de decisiones en espacios públicos, la gestión de recursos, el cumplimiento de normas y la valoración de la dignidad humana dependen de principios éticos que orientan el comportamiento individual y colectivo. Por ello, sociedades con altos niveles de compromiso ético tienden a mostrar mayor confianza ciudadana, mejor funcionamiento institucional y un desarrollo sostenible más equitativo.

Esta realidad adquiere un significado aún más profundo en la formación de estudiantes universitarios, especialmente en las disciplinas de las

ciencias sociales. Quienes se preparan para desempeñarse en áreas como educación, sociología, trabajo social, psicología, administración pública o comunicación, están llamados a interactuar directamente con personas, instituciones y comunidades. Su quehacer profesional supone tomar decisiones que inciden en la vida de otros, y, por tanto, requiere una conciencia ética sólida que les permita actuar con responsabilidad, justicia y sensibilidad social.

La formación ética en estos campos no solo se limita a comprender códigos de ética o normativas profesionales. Implica también desarrollar la capacidad crítica para identificar dilemas morales, valorar la complejidad de los fenómenos sociales y reconocer los posibles impactos de sus intervenciones. Un profesional de las ciencias sociales debe ser capaz de analizar su propio rol dentro de la estructura social, cuestionar prácticas que reproduzcan desigualdades y promover acciones que contribuyan al bienestar colectivo.

En este proceso formativo, la ética se convierte en una herramienta para la toma de decisiones informadas y moralmente fundamentadas. Enseña a los estudiantes a diferenciar entre lo legal y lo legítimo, entre lo permitido y lo correcto, entre lo eficaz y lo justo. Asimismo, fomenta el compromiso con la transparencia, la inclusión, la responsabilidad social y el respeto por la diversidad humana, elementos indispensables para fortalecer las instituciones y mejorar las condiciones de vida de las comunidades.

En definitiva, la ética no solo influye en la sociedad como principio rector de la convivencia, sino que también desempeña un papel esencial

en la formación de futuros profesionales. Para los estudiantes de ciencias sociales, constituye un componente fundamental que les permitirá ejercer su profesión con integridad, sensibilidad humana y compromiso con el desarrollo social. Al cultivar una visión ética, los futuros profesionales no solo se preparan para enfrentar dilemas complejos, sino también para convertirse en agentes de cambio capaces de impulsar una sociedad más justa, consciente y solidaria.

La ética en la sociedad se sustenta en un conjunto de principios universales que orientan el comportamiento humano, permiten la vida en comunidad y dan sentido a la justicia, la responsabilidad y el respeto mutuo. Estas leyes no dependen de culturas o tiempos específicos, sino que reflejan valores que históricamente se reconocen como fundamentales para cualquier comunidad humana.

2.1 Leyes universales de ética en la sociedad

Existen 7 leyes universales necesarias para comprender la ética en la sociedad y son fundamentales porque permiten estructurar la convivencia social y orientan el comportamiento humano hacia acciones que promueven armonía, respeto y cooperación. Su función es profunda y abarca dimensiones individuales, comunitarias e institucionales.

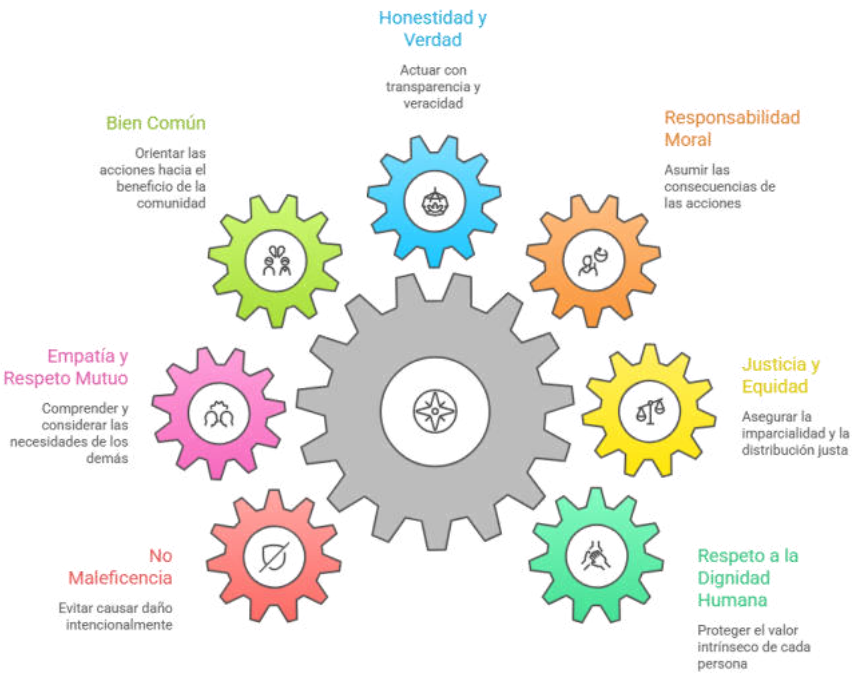


Figura 9. Leyes universales de ética en la sociedad.

Fuente: Elaboración propia.

Desde esta perspectiva se detallan estas 7 leyes universales que son:

1. Ley del respeto a la dignidad humana: Esta ley sostiene que toda persona tiene un valor intrínseco que debe ser protegido, implica reconocer la libertad, la igualdad y el derecho a ser tratado sin humillación, discriminación ni violencia, es claro que sin esta ley la convivencia sería imposible, pues se romperían los límites que protegen la vida humana.
2. Ley de la justicia y la equidad: Establece que las acciones deben regirse por criterios de imparcialidad, evitando privilegios y discriminaciones, promueve la distribución justa de

oportunidades, recursos y responsabilidades lo cual ayuda a prevenir abusos y garantiza orden social fortaleciendo la confianza en las instituciones.

3. Ley de la responsabilidad moral: Toda persona es responsable de las consecuencias de sus actos; ser ético implica asumir el impacto de las decisiones propias tanto a nivel personal como profesional y social; si no existiera la responsabilidad no existiría la ética.
4. Ley de la honestidad y la verdad: La ética exige actuar con transparencia, veracidad y coherencia, es claro que si se actúa a través de la mentira se está destruyendo la confianza mientras que si se actúa desde la honestidad se construye vínculos sólidos y sociedades más estables.
5. Ley del bien común: Toda acción ética debe orientarse no solo al beneficio personal, sino al bien de la comunidad; ser solidario, cooperar, ser servicial y empático promueve una sociedad pensante y ayuda a actuar por el bien común y evita el egoísmo social.
6. Ley de la empatía y el respeto mutuo: La ética requiere la capacidad de ponerse en el lugar del otro, comprender sus necesidades y actuar con consideración de tal forma que se potencie la convivencia, se humanice las interacciones sociales y se reduzca los conflictos.
7. Ley de la no maleficencia: Esta es una ley que se aplica en medicina, convivencia, en el trabajo y en cualquier relación humana que se basa principalmente en un principio ético universal que es no causar daño intencionalmente incluyendo daños físicos,

emocionales, económicos, psicológicos y sociales siendo una ley base en la construcción de cualquier código ético.

2.2 Principios éticos y legales en el uso de las TI

Estos principios se centran en el comportamiento responsable y moralmente correcto en el diseño, desarrollo, implementación y uso de las tecnologías de la información. Aunque no siempre estén codificados en leyes, su observancia es esencial para mantener la confianza y el bienestar de los individuos y la sociedad.

Los principios éticos en primer lugar se centran en:

- Privacidad: El respeto por la esfera personal y el derecho de los individuos a controlar la recopilación, el almacenamiento, el procesamiento y la divulgación de su información. Esto implica transparencia en las políticas de datos, minimización de la recopilación y obtención de consentimiento informado.
- Seguridad: La obligación de proteger la información y los sistemas contra accesos no autorizados, alteraciones, destrucción o divulgación. Esto requiere la implementación de medidas técnicas y organizativas robustas para salvaguardar los activos digitales.
- Transparencia y Honestidad: La necesidad de ser claros y veraces sobre el funcionamiento de los sistemas de TI, el uso de los datos y las posibles implicaciones de la tecnología. Esto fomenta la confianza y permite a los usuarios tomar decisiones informadas.

- Equidad y No Discriminación: El imperativo de asegurar que el diseño, el desarrollo y la implementación de las tecnologías de la información no perpetúen ni amplifiquen sesgos injustos o discriminación basados en características protegidas.
- Responsabilidad y Rendición de Cuentas: La obligación de asumir la responsabilidad por las acciones y las consecuencias del uso de las TI, estableciendo mecanismos claros para la rendición de cuentas en caso de fallos o daños.

Por otro lado, los principios legales se centran en:

- Cumplimiento Normativo: La obligación de adherirse a las leyes y regulaciones aplicables en el ámbito de las TI, que abarcan áreas como la protección de datos, la propiedad intelectual, la ciberseguridad y el comercio electrónico.
- Propiedad Intelectual: El respeto por los derechos de autor, las patentes, las marcas registradas y otros derechos de propiedad intelectual relacionados con el software, el contenido digital y las innovaciones tecnológicas.
- Responsabilidad Legal: La obligación de responder legalmente por los daños causados por el uso negligente o indebido de las tecnologías de la información, especialmente en casos de brechas de seguridad o mal uso de datos.
- Jurisdicción y Ley Aplicable: La determinación de qué leyes rigen las actividades en línea y las transacciones digitales, un aspecto crucial en el contexto global de internet.

- Evidencia Digital y Admisibilidad Legal: La comprensión de cómo se considera la información digital como prueba en procesos legales y la necesidad de garantizar su autenticidad e integridad.

El análisis se concreta en el siguiente caso:

2.2.1 TECNOSALUD S. A.: una brecha de seguridad



Figura 10. TECNOSALUD S. A.: una brecha de seguridad.

TecnoSalud S.A. es una empresa que desarrolla software para la gestión de historias clínicas electrónicas utilizado por clínicas y hospitales de varias ciudades del país. El sistema almacena datos sensibles de miles de pacientes, incluyendo diagnósticos, tratamientos, resultados de laboratorio y antecedentes médicos.

En enero de 2026, la empresa implementó un nuevo módulo de análisis predictivo basado en inteligencia artificial. Durante su fase inicial, varios empleados comenzaron a notar inconsistencias: el módulo

solicitaba acceso a más datos de los necesarios, y algunos informes internos mostraban sesgos en el tratamiento de información de ciertos grupos poblacionales.

A finales de febrero de 2026, un ciberdelincuente logró explotar una vulnerabilidad del módulo para extraer más de 50.000 registros clínicos. La brecha se hizo pública a través de redes sociales antes de que la empresa pudiera emitir un comunicado oficial.

Tras el incidente, se descubrió que:

- No existía una política clara de minimización de datos.
- El sistema carecía de controles de seguridad robustos (cifrado, segmentación de redes, monitoreo).
- El módulo IA no había sido sometido a auditorías de equidad y no discriminación.
- No había un plan de responsabilidad y rendición de cuentas, y la empresa no tenía claro qué ley aplicaba debido a que manejaba datos de pacientes de varios países.
- No existía un procedimiento para garantizar evidencia digital íntegra durante la investigación.

La autoridad de protección de datos inició un proceso sancionador, y varios pacientes interpusieron demandas colectivas.

Este escenario involucra directamente los principios éticos (privacidad, seguridad, transparencia, equidad, responsabilidad) y legales

(cumplimiento, propiedad intelectual, responsabilidad legal, jurisdicción y evidencia digital) descritos en el documento adjunto.

Problema central:

¿Cómo debe actuar TecnoSalud S.A. para responder éticamente y dentro del marco legal a la brecha de datos, corregir las fallas del sistema y evitar que incidentes similares vuelvan a ocurrir?

Analiza el caso y sugiere respuestas a las siguientes preguntas:

1. ¿Qué decisiones de la empresa evidencian una falta de respeto por la privacidad y el control de los datos de los pacientes?
2. ¿Cuáles fueron las principales fallas en las medidas de seguridad implementadas y cómo debieron haberse prevenido?
3. ¿Por qué es importante que TecnoSalud informe de forma clara y oportuna sobre el uso del nuevo módulo de IA y sus implicaciones para los pacientes?
4. ¿Qué riesgos existen al no auditar algoritmos predictivos en salud? ¿Por qué este principio ético es crucial?
5. ¿Quiénes deben asumir responsabilidades dentro de la organización por la brecha y por qué?
6. ¿Qué leyes o normativas debió considerar la empresa al manejar datos sensibles en múltiples países?
7. ¿Qué implicaciones de propiedad intelectual podrían estar involucradas en el desarrollo del módulo IA y su vulnerabilidad?
8. ¿Qué consecuencias legales puede enfrentar TecnoSalud por el uso negligente de TI?

9. ¿Cómo determina TecnoSalud qué leyes aplican cuando maneja datos de diferentes países y qué complicaciones surgen de ello?
10. ¿Qué procedimientos debieron seguirse para garantizar que la evidencia digital del ataque fuese íntegra y admisible legalmente?

Consideración final

El incidente de TecnoSalud demuestra cómo la falta de principios éticos y el incumplimiento de normas legales pueden convertir una innovación tecnológica en un riesgo social. La tecnología por sí sola no garantiza la protección ni el bienestar de las personas: requiere un diseño responsable, controles adecuados y una cultura organizacional basada en transparencia, responsabilidad y respeto. La brecha también evidencia que la ética y la legalidad no son elementos separados, sino componentes complementarios que determinan la confianza de la sociedad en las Tecnologías de la Información.

Un enfoque responsable implica anticiparse a los riesgos, establecer mecanismos de rendición de cuentas y priorizar siempre los derechos de las personas sobre las presiones comerciales o técnicas. Este caso refuerza que, en el ámbito de TI, la ética no es opcional y la legalidad no es negociable.

Posible solución:

1. ¿Qué decisiones de la empresa evidencian una falta de respeto por la privacidad y el control de los datos de los pacientes?

TecnoSalud permitió que el módulo de IA solicitara y procesara más datos de los necesarios, incumpliendo el principio de minimización de

datos. Tampoco informó adecuadamente a los pacientes sobre el nuevo tratamiento de información, lo cual vulnera el deber de transparencia asociado al derecho a la privacidad. Estas acciones van en contra del principio ético de Privacidad, que exige respetar la esfera personal y el control de los individuos sobre sus datos.

2. ¿Cuáles fueron las principales fallas en las medidas de seguridad implementadas y cómo debieron haberse prevenido?

Faltaron controles básicos como cifrado, monitoreo, segmentación de redes y restricciones de acceso. Estas debilidades facilitaron el acceso no autorizado del atacante. El principio ético de Seguridad exige implementar medidas técnicas y organizativas robustas para proteger los activos digitales. Una auditoría previa del módulo, gestión de vulnerabilidades y pruebas de penetración habrían prevenido el incidente.

3. ¿Por qué es importante que TecnoSalud informe de forma clara y oportuna sobre el uso del nuevo módulo de IA y sus implicaciones para los pacientes?

Porque los principios de transparencia y honestidad exigen que la empresa comunique de forma clara el funcionamiento del sistema, qué datos utiliza y cuáles son sus implicaciones. Sin esa transparencia, los pacientes no pueden tomar decisiones informadas ni otorgar consentimiento real respecto al uso de su información. Además, la falta de comunicación deteriora la confianza en la organización. ¿Qué riesgos existen al no auditar algoritmos predictivos en salud? ¿Por qué este principio ético es crucial?

4. ¿Quiénes deben asumir responsabilidades dentro de la organización por la brecha y por qué?

Sin auditorías periódicas, los algoritmos pueden incorporar o amplificar sesgos injustos, generando decisiones discriminatorias contra ciertos grupos. El principio de equidad y no discriminación exige evitar impactos desproporcionados basados en características protegidas. En salud, estos sesgos pueden afectar diagnósticos, tratamientos o el acceso a servicios, agravando desigualdades.

5. ¿Qué leyes o normativas debió considerar la empresa al manejar datos sensibles en múltiples países?

Deben asumir responsabilidad los directivos, los responsables de TI, el equipo de desarrollo del módulo IA y quienes supervisan el cumplimiento normativo. El principio de Responsabilidad y Rendición de Cuentas establece que las organizaciones deben asumir las consecuencias de sus decisiones tecnológicas y definir mecanismos claros de responsabilidad en caso de fallos. [PRINCIPIOS.DE LAS TI | Word]

6. ¿Qué implicaciones de propiedad intelectual podrían estar involucradas en el desarrollo del módulo IA y su vulnerabilidad?

TecnoSalud debió considerar las leyes locales e internacionales de protección de datos, las regulaciones de manejo de datos sensibles en salud, normativas de comercio electrónico y legislación de ciberseguridad vigentes en cada país. El principio legal de Cumplimiento Normativo obliga a adherirse a las leyes aplicables en cada jurisdicción donde se procesan datos.

7. ¿Qué consecuencias legales puede enfrentar TecnoSalud por el uso negligente de TI?

El software del módulo IA está protegido por derechos de autor y posiblemente por patentes. Una vulnerabilidad puede comprometer componentes privados o revelar información protegida, generando conflictos legales o infracciones a licencias. El principio de Propiedad Intelectual exige respetar los derechos asociados al software y a las innovaciones tecnológicas implicadas.

8. ¿Cómo determina TecnoSalud qué leyes aplican cuando maneja datos de diferentes países y qué complicaciones surgen de ello?

Debe realizar un análisis jurídico detallado para determinar qué leyes de protección de datos, ciberseguridad y transacciones digitales aplican a su actividad en distintos países. Esto es complejo porque las normativas pueden superponerse, diferir o entrar en conflicto, haciendo que la gestión del cumplimiento sea un desafío significativo en entornos transfronterizos. Este punto está fundamentado directamente en el principio legal de Jurisdicción y Ley Aplicable. Podría fijarse primordialmente en los siguientes puntos:

- Identificando el país de residencia de los titulares de los datos.
- Analizando dónde se realiza el tratamiento efectivo de los datos.
- Revisando contratos, acuerdos de servicio y condiciones transfronterizas.
- Identificando leyes sectoriales específicas.

9. ¿Qué procedimientos debieron seguirse para garantizar que la evidencia digital del ataque fuese íntegra y admisible legalmente?

Debe evaluar las leyes de cada país donde residen los titulares de datos y determinar cuál es la jurisdicción aplicable. Esto incluye analizar el tipo de transacción digital y dónde ocurre el tratamiento de los datos. Las complicaciones incluyen diferencias normativas, conflictos entre legislaciones y requisitos adicionales de almacenamiento, reporte y consentimiento. Esto se relaciona con el principio de Jurisdicción y Ley Aplicable.

10. ¿Qué procedimientos debieron seguirse para garantizar que la evidencia digital del ataque fuese íntegra y admisible legalmente?

Deben aplicarse prácticas de preservación forense:

- Cadena de custodia.
- Registro de auditoría.
- Copia bit a bit de discos.
- Protección contra alteraciones.
- Documentación detallada del proceso.

2.3 Derechos digitales y cibernéticos

Los derechos digitales son una extensión y adaptación de los derechos humanos fundamentales al entorno digital y en línea. Se centran en garantizar que las personas disfruten de las mismas protecciones y libertades en el ciberespacio que tienen en el mundo físico. En esencia, buscan trasladar los derechos humanos al ámbito digital.

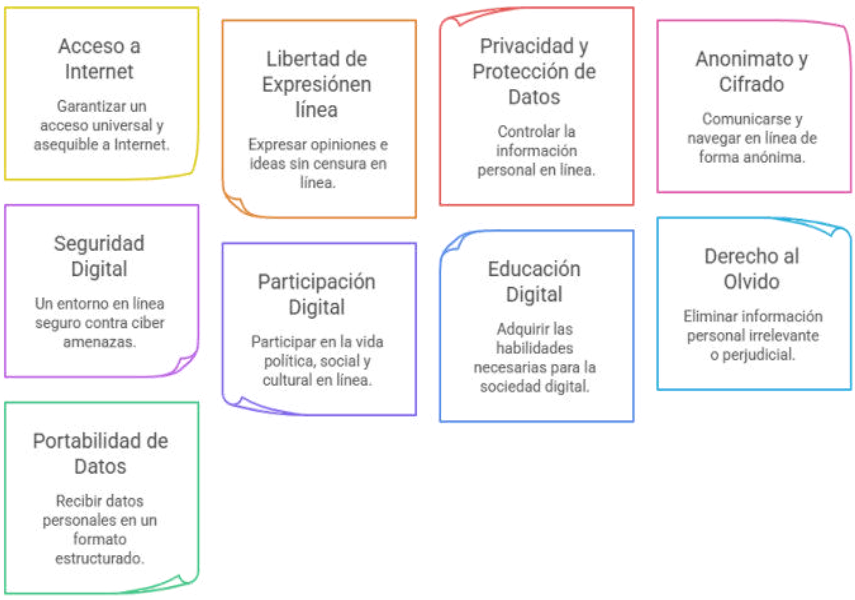


Figura 11. Derechos digitales y cibernéticos.

Fuente: Elaboración propia.

Algunos de los principales derechos digitales incluyen:

- Derecho de acceso a Internet: Considerado cada vez más como un derecho fundamental para la participación en la sociedad moderna. Implica la necesidad de superar la brecha digital y garantizar un acceso universal y asequible.
- Libertad de expresión en línea: El derecho a expresar opiniones, ideas e información sin censura en el entorno digital, sujeto a las mismas limitaciones que existen en el mundo físico (por ejemplo, incitación a la violencia, difamación).
- Derecho a la privacidad y protección de datos: El derecho a controlar la recopilación, el almacenamiento, el procesamiento y

la divulgación de la información personal en línea. Esto abarca el consentimiento informado, la minimización de datos y el derecho al olvido o supresión.

- Derecho al anonimato y al cifrado: En ciertos contextos, el derecho a comunicarse y navegar en línea de forma anónima y a utilizar herramientas de cifrado para proteger la confidencialidad de las comunicaciones.
- Derecho a la seguridad digital: El derecho a un entorno en línea seguro, protegido contra ciber amenazas como el hacking, el fraude y el robo de identidad.
- Derecho a la participación digital: El derecho a participar en la vida política, social y cultural a través de medios digitales.
- Derecho a la educación digital: El derecho a adquirir las habilidades necesarias para participar plenamente en la sociedad digital.
- Derecho al olvido: El derecho a que se elimine información personal que ya no es relevante o que perjudica la reputación de un individuo de los motores de búsqueda y otras plataformas en línea.
- Derecho a la portabilidad de datos: El derecho a recibir los datos personales en un formato estructurado y de uso común para poder transmitirlos a otro proveedor de servicios.

2.4 Organismos certificadores internacionales

Son entidades gubernamentales o intergubernamentales con la autoridad legal para establecer y hacer cumplir leyes, regulaciones y directrices

relacionadas con las tecnologías de la información. Su objetivo principal es proteger los intereses públicos, garantizar la competencia justa, fomentar la innovación responsable y abordar los desafíos sociales y económicos derivados del uso de las TI.

- ISO (International Organization for Standardization) / IEC (International Electrotechnical Commission): A través de su Comité Técnico Conjunto, desarrollan estándares internacionales que sirven de base para diversas certificaciones en alrededor de 140 países, promoviendo el desarrollo de la estandarización e intercambio internacional de bienes y servicios. Si bien ISO/IEC no certifica directamente a individuos, las organizaciones pueden obtener certificaciones (a través de organismos acreditados) que demuestran el cumplimiento de estándares ISO/IEC como ISO/IEC 27001 (seguridad de la información) e ISO/IEC 20000 (gestión de servicios de TI).

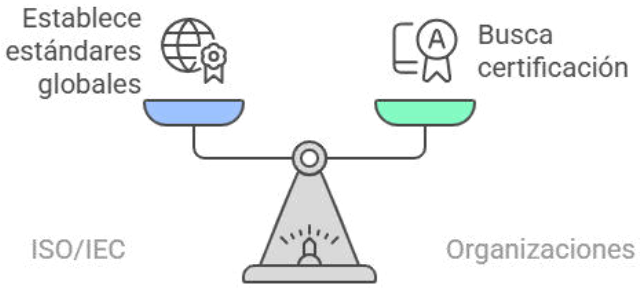


Figura 12. ISO/IEC y las organizaciones.

Fuente: Elaboración propia

- ISACA (Information Systems Audit and Control Association): Es una asociación sin fines de lucro que proporciona conocimiento, estándares, certificación, comunidad, defensa y educación a profesionales de la auditoría de sistemas de información, seguridad de la información, gestión de riesgos y gobernanza de TI. Su misión es fomentar la confianza en la tecnología de la información.

Si bien ISACA no es un organismo regulador en el sentido gubernamental, desarrolla marcos, estándares, guías y procedimientos que son ampliamente adoptados como buenas prácticas y marcos de referencia por organizaciones y profesionales de TI a nivel mundial, ayudando a gestionar y controlar sus sistemas de información asegurando el cumplimiento normativo y optimizar el valor de sus inversiones en TI.

Incluye varios marcos y estándares como COBIT, ITAF, Risk IT Framework, así como marcos y guías para gestión de riesgos de TI, seguridad de la información e implementación de blockchain desarrollando además un código de ética profesional para guiar la conducta de los miembros y titulares de certificaciones promoviendo la integridad, objetividad, competencia, confidencialidad y apoyo a los estándares profesionales.



Figura 13. ISACA y el marco que gobierna.

Fuente: Elaboración propia.

- NIST (National Institute of Standards and Technology): Es una agencia del Departamento de Comercio de los Estados Unidos. Su misión principal es promover la innovación estadounidense y la competitividad industrial mediante el avance de la ciencia de la medición, los estándares y la tecnología de manera que mejoren la seguridad económica y nuestra calidad de vida.

En el contexto de las tecnologías de la información desempeña un papel fundamental puesto que es la encargada del desarrollo de estándares, directrices y mejores prácticas además de desarrollar marcos de trabajo para ayudar a las organizaciones a gestionar los riesgos de seguridad de la información y a implementar sistemas de TI seguros y confiables.



Figura 14. El alcance de NIST

Fuente: Elaboración propia.

2.5 Organismos nacionales reguladores de las TI

- ARCOTEL (Agencia de Regulación y Control de las Telecomunicaciones): Es el principal ente regulador y de control de las telecomunicaciones y del espectro radioeléctrico en Ecuador, su ámbito de acción abarca los servicios de telecomunicaciones fijas y móviles, internet, radiodifusión, televisión y, en general, los aspectos de la gestión de los medios de comunicación que utilizan frecuencias del espectro radioeléctrico.

Su función principal es regular y controlar el espectro radioeléctrico, además de normar, sustanciar y resolver los procedimientos para el otorgamiento, administración y extinción de títulos habilitantes como concesiones, autorizaciones y registros.

Es una agencia que ha logrado establecer regulaciones para garantizar la seguridad de las comunicaciones y la protección de datos personales en el ámbito de su competencia, así como la regulación y control de las actividades relacionadas con el comercio y la firma electrónica.

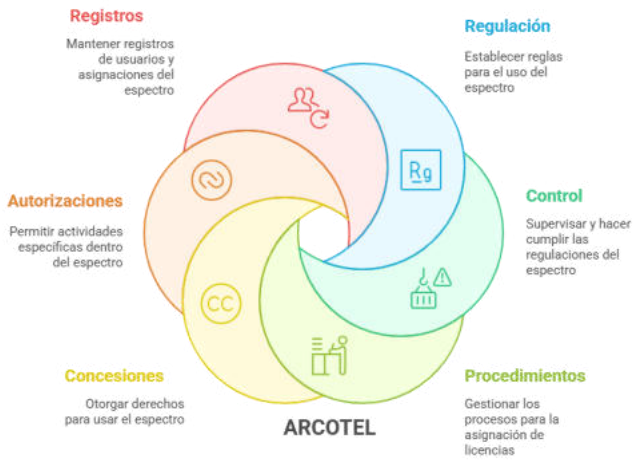


Figura 15. Arcotel y sus regulaciones.

Fuente: Elaboración propia.

- MINTEL (Ministerio de Telecomunicaciones y de la Sociedad de la Información): Es un órgano rector de las políticas de telecomunicaciones y de la sociedad de la información en Ecuador, es el encargado de establecer las políticas, directrices y planes a nivel nacional para el desarrollo de la Sociedad de la información y el sector de las telecomunicaciones.

Su función es vital para definir la política pública de telecomunicaciones, así como para la elaboración del Plan Nacional de Telecomunicaciones y Tecnologías de la Información promoviendo el

desarrollo de la infraestructura de telecomunicaciones y la adopción de las TIC coordinando con otras entidades gubernamentales en telas relacionados con la transformación digital.



Figura 16. Visión general de MINTEL.

Fuente: Elaboración propia.

- GADS (Gobiernos Autónomos Descentralizados Municipales y Metropolitanos): Tienen ciertas facultades de regulación y control sobre la infraestructura de telecomunicaciones y el uso de espacio público para el despliegue de redes.

Su función en el tema de tecnologías de la información en sí no está directamente relacionado sin embargo son los entes encargados de emitir ordenanzas y regulaciones sobre el uso del suelo y del espacio aéreo para la instalación de infraestructura de telecomunicaciones como antemas, cableado, postes, ductos y otras infraestructuras públicas para el despliegue de redes de telecomunicaciones además de la gestión de

permisos de construcción e instalación de infraestructuras de telecomunicaciones dentro de su jurisdicción.



Figura 17. Los GAD y su función en la sociedad.

Fuente: Elaboración propia.

- INEN (Servicio Ecuatoriano de Normalización): Es el organismo encargado de desarrollar y publicar normas técnicas que pueden incluir estándares relacionados con las tecnologías de la información, tiene una función clave en la elaboración, adopción y publicación de normas técnicas en diversos sectores incluyendo las TI. Además, promueve la adopción de estándares para mejorar la calidad y la competitividad, así como actuar como punto de contacto con organismos internacionales de normalización.



Figura 18. INEN y su función.

Fuente: Elaboración propia.

Para relacionar la teoría con la práctica, considérese el siguiente caso:

2.5.1 SALUDNET: cumplimiento formal frente a seguridad real



Figura 19. 1.1.1 SALUDNET: cumplimiento formal frente a seguridad real.

El Hospital Universitario Andino implementa SALUDNET, una plataforma clínica integral (HCE, agenda, farmacia, laboratorio y facturación). El proyecto se ejecutó en 10 meses, con un proveedor externo y un equipo interno de TI. Para “cumplir con estándares”, el proveedor entregó una matriz donde declara alineación a ISO/IEC 27001, ISO/IEC 27002, NIST CSF e ITIL.

Dos meses después de la puesta en marcha, una doctora reporta que, al consultar la historia clínica de un paciente, visualiza documentos de otro, incluyendo resultados de laboratorio y diagnósticos sensibles. El equipo encuentra lo siguiente:

- Autorización deficiente: el módulo de historia clínica no valida de forma estricta el contexto de acceso (control ABAC mal configurado).
- Cifrado inconsistente: la base de datos tiene cifrado a nivel de disco, pero no a nivel de campos sensibles (diagnóstico, resultados).
- Logging incompleto: existen registros, pero sin integridad y sin correlación centralizada.
- Pruebas de seguridad limitadas: no se ejecutaron pentests externos ni pruebas de explotación sobre controles de autorización; solo pruebas funcionales.
- Gobernanza difusa: no existe SGSI formal en la institución; el proveedor declaró “equivalencia” con ISO 27001, pero no tiene políticas aprobadas ni roles definidos en seguridad.

- Continuidad y DR: hay backups, pero no pruebas de restauración ni plan BCP/DRP operativo (ISO/IEC 22301).
- Gestión de proveedores: el contrato exige “mejores esfuerzos” pero no SLA de seguridad, ni derechos de auditoría, ni conformidad verificable con estándares.

El hospital debe cumplir obligaciones legales de protección de datos sensibles y normas éticas del sector. La Dirección solicita un informe técnico - ético donde se detallen las causas, responsabilidades, acciones de contención, plan de remediación y fortalecimiento de gobierno y cultura de seguridad.

Analiza el caso y sugiere respuestas a las siguientes preguntas:

1. ¿Qué obligaciones legales y principios de protección de datos sensibles pudieron vulnerarse y por qué el incidente califica como violación de datos?
2. ¿Cómo habría mitigado el riesgo la adopción efectiva (no declarativa) de ISO/IEC 27001 y 27002 a nivel institucional?
3. ¿Qué carencias de gobernanza y gestión de proveedores explican que el cumplimiento fuera solo “documental”?
4. ¿Qué consecuencias éticas emergen al exponer información clínica por fallas previsibles (autorización, cifrado, logging)?
5. ¿Qué impactos reputacionales y de confianza enfrentan el hospital y el equipo de TI ante pacientes, personal clínico y reguladores?
6. ¿Qué controles técnicos y de proceso (previos al go-live) habrían detectado la falla de autorización y el cifrado insuficiente?

7. ¿Qué mejores prácticas (SSDLC, pentesting, gestión de llaves, ABAC/RBAC, SIEM) habrían prevenido y/o limitado el incidente?
8. ¿Qué rol deben asumir la Dirección del hospital y la autoridad reguladora para asegurar corrección, cumplimiento y aprendizaje institucional?
9. ¿Cómo diseñar un plan de remediación y mejora continua que integre aspectos legales, normativos, técnicos y culturales?
10. ¿Qué medidas preventivas técnicas y administrativas deben exigirse para la "reconstrucción segura" de SALUDNET conforme a normas y estándares?

Reflexión del caso

SALUDNET demuestra la diferencia entre cumplir en papel y proteger en la práctica. Declarar alineación a estándares sin gobernanza, pruebas y métricas es una forma de cumplimiento ilusorio. En salud, la información es especialmente sensible: su exposición vulnera la dignidad, la confianza clínica y el derecho a la privacidad.

La excelencia tecnológica surge cuando confluyen: leyes, normas, mejores prácticas y ética profesional. Proteger datos en salud no es un requisito accesorio: es una obligación moral y un indicador de calidad asistencial.

Posible solución:

1. ¿Qué obligaciones legales y principios de protección de datos sensibles pudieron vulnerarse y por qué el incidente califica como violación de datos?

El hospital vulneró principios esenciales de protección de datos personales sensibles tales como:

- Confidencialidad: información clínica expuesta a una persona no autorizada.
- Integridad: registros accesibles sin controles adecuados.
- Seguridad: ausencia de medidas técnicas razonables (cifrado granular, autorización estricta).
- Finalidad y acceso legítimo: datos clínicos utilizados fuera del contexto permitido.

2. ¿Cómo habría mitigado el riesgo la adopción efectiva de ISO/IEC 27001 y 27002 a nivel institucional?

   Una implementación real de estos estándares habría mitigado el incidente, con ello la falla de autorización y el cifrado insuficiente habrían sido detectados antes del lanzamiento.

- ISO/IEC 27001 exige un Sistema de Gestión de Seguridad con:
  - Evaluación de riesgos.
  - Políticas formales.
  - Gobernanza clara.
  - Auditorías internas y mejora continua.
  - Revisión por la alta dirección.

- ISO/IEC 27002 proporciona controles específicos, tales como:

- Cifrado de información sensible.
- Controles de acceso RBAC/ABAC.
- Segregación de funciones.
- Registros de auditoría íntegros.
- Pruebas de seguridad y validación previa al despliegue.

3. ¿Qué carencias de gobernanza y gestión de proveedores explican que el cumplimiento fuera solo "documental"?

Los factores clave son:

- Alta presión institucional por cumplir plazos operativos del hospital.
- Cultura de "liberar primero y asegurar después".
- Ausencia de una estructura formal de gobernanza de TI.
- Falta de supervisión ejecutiva del riesgo tecnológico.
- Contratos con proveedores sin requisitos de seguridad verificables.
- Escasa capacitación en estándares de ciberseguridad y privacidad.

4. ¿Qué consecuencias éticas emergen al exponer información clínica por fallas previsibles (autorización, cifrado, logging)?

- Violación del principio de no maleficencia (evitar daño).
- Afectación de la dignidad humana al exponer datos sensibles.
- Minar la confianza médica-paciente, base del sistema de salud.
- Falta de responsabilidad profesional al no prever riesgos conocidos.
- Incumplimiento del deber moral de proteger información crítica.

5. ¿Qué impactos reputacionales y de confianza enfrentan el hospital y el equipo de TI ante pacientes, personal clínico y reguladores?

- Pérdida de credibilidad del hospital ante pacientes y personal clínico.
- Rechazo o temor a utilizar sistemas informáticos del hospital.
- Posible disminución de pacientes que confían su información al centro.
- Mayor escrutinio regulatorio y auditorías externas.
- Deterioro de la reputación profesional del equipo de TI.
- Costos elevados de recuperación de la imagen institucional.

6. ¿Qué controles técnicos y de proceso (previos al go-live) habrían detectado la falla de autorización y el cifrado insuficiente?

- Modelado de amenazas (STRIDE, LINDDUN).
- Revisión de arquitectura de seguridad antes del despliegue.
- Pruebas de penetración realizadas por terceros.
- SAST/DAST/IAST integrados al pipeline de desarrollo.
- Pruebas específicas de autorización ABAC/RBAC.
- Auditoría de cumplimiento basada en 27001 y 27002.
- Validación de cifrado granular en datos sensibles.

7. ¿Qué mejores prácticas (SSDLC, pentesting, gestión de llaves, ABAC/RBAC, SIEM) habrían prevenido y/o limitado el incidente?

- SSDLC: seguridad incorporada en todas las fases del desarrollo.
- Privacy by Design y Privacy by Default.
- Cifrado por campo y gestión de llaves KMS/HSM.
- Uso adecuado de ABAC/RBAC y principio de mínimo privilegio.
- Pentesting recurrente y escaneo continuo de vulnerabilidades.
- Implementación de SIEM para correlación y alertas.

- Hardening, patch management y segregación de ambientes.

8. ¿Qué rol deben asumir la Dirección del hospital y la autoridad reguladora para asegurar corrección, cumplimiento y aprendizaje institucional?

Dirección del hospital:

- Declarar la seguridad como prioridad estratégica.
- Financiar adecuadamente la ciberseguridad.
- Implantar un SGSI ISO 27001 completo.
- Exigir evidencia verificable a proveedores (auditorías, pruebas).
- Supervisar el plan de remediación con KPIs claros.

Autoridad reguladora:

- Verificar notificación del incidente.
- Exigir y revisar un plan de corrección verificable.
- Sancionar si hubo negligencia técnica.
- Emitir lineamientos sectoriales y auditorías de seguimiento.

9. ¿Cómo diseñar un plan de remediación y mejora continua que integre aspectos legales, normativos, técnicos y culturales?

Fase 1 Contención inmediata:

- Corregir autorización ABAC/RBAC.
- Cifrar campos sensibles.
- Activar MFA, logging reforzado y revisar accesos.
- Comunicar a usuarios y notificar a regulador.

Fase 2 Reforzamiento (30 - 90 días):

- Integrar SAST/DAST/SCA al pipeline.
- Implementar políticas formales de seguridad y privacidad.
- Revisar contratos con requisitos de seguridad verificables.
- Capacitar a todo el personal involucrado.

Fase 3 Implementación SGSI (90 - 180 días):

- Estructurar ISO 27001 y controles 27002.
- Comité de seguridad, métricas, reportes a dirección.

Fase 4 Mejora continua:

- Auditorías periódicas.
- Pentesting anual.
- Simulacros de incidentes y pruebas de continuidad (ISO 22301).

10. ¿Qué medidas preventivas técnicas y administrativas deben exigirse para la "reconstrucción segura" de SALUDNET conforme a normas y estándares?

Técnicas

- Cifrado TLS 1.2/1.3 y AES-256 (también por campo).
- MFA, RBAC/ABAC, segregación de funciones.
- Hardening, parches, control de cambios.
- SIEM, registros íntegros y monitoreo continuo.
- Pentesting, SAST/DAST/IAST, escaneo de dependencias.
- Backups cifrados, pruebas de restauración, continuidad y DR.

Administrativas

- SGSI completo ISO/IEC 27001.
- Controles ISO/IEC 27002 adoptados formalmente.
- Políticas: seguridad, clasificación de información, incidentes, desarrollo seguro, privacidad.
- Gestión de proveedores con SLA de seguridad y derecho de auditoría.
- Comité de seguridad y reportes ejecutivos periódicos.
- Capacitación continua en ética, ciberseguridad y protección de datos.

2.6 Síntesis transversal del capítulo

Este capítulo sitúa la ética tecnológica dentro de un marco social más amplio, examinando principios como el respeto, justicia, responsabilidad, honestidad y búsqueda del bien común permitiendo valorar la tecnología no solo por su funcionamiento, sino también por la forma en que modifica relaciones, distribuye oportunidades y afecta derechos. Desde esta perspectiva, las decisiones sobre datos, plataformas o servicios digitales forman parte de la convivencia social y deben analizarse por sus efectos sobre personas y organizaciones.

Los derechos digitales conectan esa reflexión con obligaciones concretas como la privacidad, la seguridad, el acceso, la participación y la posibilidad de cuestionar decisiones tecnológicas las cuales requieren mecanismos institucionales que los hagan efectivos, resaltando la intervención de los organismos internacionales, las entidades nacionales

y las autoridades reguladoras las cuales cumplen funciones complementarias desarrollando estándares y marcos de referencia; otros establecen reglas, supervisan actividades o promueven su aplicación dentro de una jurisdicción.

La relación entre principios, derechos e instituciones tiene una consecuencia directa para el ámbito empresarial. Una organización no construye confianza solo mediante declaraciones éticas; necesita políticas comprensibles, responsabilidades definidas, controles verificables y canales para responder ante errores o afectaciones. Del mismo modo, el futuro profesional debe aprender a reconocer cuándo una decisión aparentemente eficiente puede entrar en tensión con la privacidad, la equidad o la dignidad de las personas.

La lectura transversal del capítulo muestra que la ética social proporciona el criterio, los derechos digitales delimitan aquello que debe protegerse y las instituciones aportan mecanismos de orientación y control estableciendo la base del capítulo siguiente trasladando la discusión al ejercicio específico del profesional de TI y a los dilemas que surgen durante el diseño, la operación y la evolución de los sistemas.

CAPÍTULO III

3 ÉTICA EN TECNOLOGÍAS DE LA INFORMACIÓN

A medida que los sistemas digitales se vuelven más complejos, autónomos e influyentes en la vida cotidiana, la ética deja de ser un elemento accesorio para convertirse en un pilar que orienta la toma de decisiones, la gestión de riesgos y la responsabilidad social del profesional tecnológico.

La interacción entre datos, algoritmos, infraestructuras y usuarios genera nuevas tensiones éticas que no existían en escenarios tecnológicos tradicionales. Entre ellas destacan la protección de la privacidad, la gestión responsable de datos personales, la seguridad de la información, la equidad algorítmica, la eliminación de sesgos discriminatorios, la transparencia en los procesos automatizados y la obligación de garantizar que la tecnología no cause daño a individuos ni comunidades. Estas preocupaciones no solo tienen una dimensión técnica, sino también moral, jurídica y social, lo que exige al profesional una visión multidisciplinaria del impacto de su trabajo.

Además, el papel de la ética aplicada frente al avance acelerado de tecnologías disruptivas como la inteligencia artificial, el aprendizaje automático, los sistemas de vigilancia digital y la automatización inteligente introducen dilemas relacionados con la autonomía de los sistemas, la rendición de cuentas, la explicabilidad de los modelos y las repercusiones no intencionales de la toma de decisiones algorítmicas. Comprender estos dilemas permite evaluar de manera crítica cómo

equilibrar innovación y responsabilidad en un entorno donde los límites éticos se están redefiniendo constantemente.

Asimismo, es importante analizar y definir la importancia de los marcos normativos y los códigos de conducta profesional que guían al especialista en TI hacia una práctica responsable. Códigos como los que promueven organismos internacionales, junto con estándares de seguridad y privacidad, ofrecen lineamientos concretos para integrar principios éticos desde las etapas de diseño y desarrollo hasta la operación y el mantenimiento de sistemas tecnológicos. El capítulo enfatiza la necesidad de que estos principios no se limiten a declaraciones formales, sino que se traduzcan en políticas, procesos, controles y métricas verificables.

Por esta razón se plantea la ética como una competencia transversal que debe cultivarse de manera continua. El profesional de TI debe ser consciente de que cada decisión técnica puede tener consecuencias sociales, económicas o incluso legales. Es importante adoptar una postura crítica y reflexiva que considere el bienestar humano, el respeto a los derechos fundamentales, la inclusión, la transparencia y la sostenibilidad como ejes centrales del ejercicio profesional; solo así es posible construir un ecosistema digital confiable, seguro y orientado al bien común.

3.1 Introducción a la ética aplicada a las TI



Figura 20. Función de la Ética en las TI.

Fuente: Elaboración propia.

La ética aplicada a las Tecnologías de la Información permite comprender cómo los principios morales orientan el diseño, desarrollo, operación y gobierno de los sistemas digitales. No se limita a "hacer lo correcto" en abstracto, sino a traducir valores como responsabilidad, transparencia, justicia y no maleficencia en decisiones técnicas concretas, desde el modelado de datos hasta los controles que se implementan para protegerlos. En entornos donde la información es un activo crítico, la ética se integra al criterio de ingeniería mediante enfoques de gestión del riesgo, promoviendo prácticas como privacy by design, el análisis del ciclo de vida del dato (recolección-uso-retención-eliminación) y la priorización de salvaguardas para minimizar consecuencias adversas sobre las personas. Así, conceptos como trazabilidad, consentimiento informado, minimización de datos y

limitación de uso dejan de ser ideales y se convierten en requisitos verificables de arquitectura y operación (Boeckl & Lefkovitz, 2020; Organisation for Economic Co-operation and Development [OECD], s. f.).

En la práctica, la ética se integra con la gobernanza y la seguridad a través de normas y marcos de referencia. Un SGSI alineado con ISO/IEC 27001 y controles de ISO/IEC 27002 materializa el deber de cuidado sobre la información (confidencialidad, integridad y disponibilidad), mientras que marcos como NIST CSF, COBIT o ITIL ayudan a balancear riesgo, valor y continuidad del servicio. La privacidad por diseño y por defecto exige decisiones técnicas como cifrado por campo, gestión de llaves (KMS/HSM), control de acceso contextual (RBAC/ABAC), registros inmutables y segregación de ambientes. El SSDLC incorpora seguridad y privacidad en todas las fases del ciclo de vida del software mediante threat modeling, SAST/DAST/SCA/IAST, revisiones de código y pruebas de penetración, cerrando la brecha entre intención ética y ejecución técnica.

La irrupción de datos masivos e inteligencia artificial eleva el listón ético. Modelos que toman decisiones sobre personas requieren gobernanza de datos, gestión de sesgos para mitigar discriminación, y explicabilidad para justificar resultados. La ética de Inteligencia Artificial demandas prácticas como evaluaciones de impacto algorítmico, validación y monitoreo posdespliegue, límites claros de uso y disyuntores para detener sistemas ante comportamientos anómalos. Del lado de la ciberseguridad, la ética impone proporcionalidad en la

vigilancia, protección contra abusos internos, principio de mínimo privilegio y respuesta responsable a incidentes, porque la confianza social se construye con evidencia y coherencia, no solo con promesas.

La rápida expansión de tecnologías como la inteligencia artificial, los sistemas autónomos y el análisis masivo de datos ha colocado nuevos desafíos éticos en la agenda contemporánea. Los modelos automatizados pueden amplificar sesgos, afectar decisiones críticas o vulnerar derechos fundamentales si no se desarrollan bajo criterios éticos sólidos. Aquí, la ética exige implementar metodologías de evaluación de impacto, controles de equidad, auditorías algorítmicas y transparencia en los procesos de decisión. De igual modo, la ciberseguridad plantea dilemas complejos relacionados con vigilancia, acceso privilegiado, monitoreo de usuarios y uso responsable de herramientas de protección.

La ética en TI es también cultura organizacional. Requiere liderazgo que priorice la seguridad y la privacidad, políticas claras, formación continua y métricas que midan lo que importa; implica diseñar contratos con proveedores que incluyan SLA de seguridad, derecho de auditoría y evidencia verificable de conformidad. La meta no es el "cumplimiento en papel", sino sistemas que resisten fallos, protejan a las personas y sostengan el bien común. En un mundo hiperconectado, la ética aplicada a TI no es un accesorio: es el marco que convierte la innovación en un servicio confiable, seguro y socialmente responsable.

3.2 Importancia de la ética en entornos tecnológicos



Figura 21. Importancia de la ética en entornos digitales.

Fuente: Elaboración propia.

La ética en entornos tecnológicos es el marco que convierte la capacidad de crear sistemas en la responsabilidad de hacerlo sin causar daño y maximizando el bien común; en la práctica, esto significa tomar decisiones correctas desde el diseño hasta la operación diaria: recolectar solo los datos necesarios, usarlos con un propósito legítimo y explícito, protegerlos con controles robustos, garantizar trazabilidad y asegurar que los usuarios conserven control real, porque cada elección técnica tiene consecuencias humanas, legales y sociales; en ciberseguridad, la ética se traduce en deber de cuidado y no maleficencia: diferir "para después" el cifrado o las pruebas de penetración cuando se manejan datos sensibles es una omisión que expone a riesgos previsibles (ej., un portal académico que libera sin MFA y filtra calificaciones), y la

respuesta a incidentes exige transparencia responsable, notificación oportuna, contención eficaz y reparación, porque la confianza se sostiene con hechos.

En Ciencia de Datos e Inteligencia Artificial, la ética obliga a gobernar el ciclo de vida, evaluar y mitigar sesgos que puedan discriminar, justificar decisiones automatizadas, establecer límites de uso y supervisión humana en decisiones de alto impacto, y monitorear en producción para detectar daños, con disyuntores para detener modelos si es necesario (pj., un sistema de selección de personal que sobre valora estatus socioeconómico debe auditar variables, ofrecer mecanismos de apelación y ajustar el modelo); en experiencia de usuario, actuar éticamente implica evitar consentimientos preconfigurados, cancelaciones ocultas, diseñar con accesibilidad y mantener simetría de fricción, mientras que en la cadena de suministro se requiere diligencia con terceros: contratos con cláusulas de seguridad, derecho de auditoría, pruebas obligatorias y mínima exposición de datos.

La ética también abarca sostenibilidad, propiedad intelectual y gobernanza, formación continua en seguridad, privacidad y sesgos, comités de riesgo con voz ejecutiva, y una práctica profesional guiada por integridad y responsabilidad, porque la excelencia tecnológica no consiste solo en funcionar, sino en funcionar con justicia, protección y respeto por la dignidad de las personas.

Analicemos el siguiente caso práctico:

3.2.1 IA en reclutamiento: «El algoritmo reproduce nuestros sesgos»



Figura 22. IA en reclutamiento: «El algoritmo reproduce nuestros sesgos».

Una empresa adopta un sistema de IA para filtrar currículums. Tras seis meses, la directora de Talento Humano observa que los candidatos de zonas rurales son rechazados en un 70 % más que los urbanos, y que egresados de universidades públicas casi no pasan el primer umbral. El proveedor explica que el modelo "aprendió de datos históricos de éxito". No existe auditoría algorítmica, ni explicación de decisiones, ni revisión humana de casos por lo que pone en riesgo que suceda una discriminación indirecta, falta de equidad, carencia de explicación y ausencia de supervisión humana significativa.

Preguntas de reflexión

1. ¿Qué datos o variables podrían actuar como filtros discriminatorios?
2. ¿Cómo implementar una auditoría algorítmica?

3. ¿Cuándo debe exigirse revisión humana y derecho de apelación?
4. ¿Qué políticas deben regular el uso de IA en decisiones de alto impacto?
5. ¿Cómo documentar la calidad y procedencia de datos?
6. ¿Qué responsabilidades legales y éticas recaen sobre la empresa y el proveedor?

Lectura ética del caso

Este caso ilustra una verdad central: los algoritmos aprenden de nuestras historias y, si esas historias están atravesadas por desigualdades, la IA puede amplificarlas bajo una apariencia de objetividad. La ética no se limita a evitar variables "prohibidas"; exige examinar filtros, medir efectos reales por subgrupos y garantizar supervisión humana significativa donde hay vidas y trayectorias en juego. Operacionalizar la ética implica gobernanza, auditorías con métricas de equidad, explicaciones accionables, derechos de apelación, y contratos con proveedores que permitan ver, medir y corregir. Innovar con responsabilidad no frena al negocio; lo hace sostenible, legítimo y socialmente justo. En reclutamiento, eso se traduce en un compromiso explícito: seleccionar talento sin reproducir barreras de origen, porque un buen sistema no solo predice "éxito pasado", construye oportunidades futuras.

Orientación para el análisis

1. ¿Qué datos o variables podrían actuar como filtros discriminatorios?

Pueden ser variables aparentemente neutrales que, al correlacionarse con factores socioeconómicos o geográficos, terminan discriminando indirectamente como código postal, universidad de procedencia, trayectoria laboral, idiomas o certificaciones, participación en actividades extracurriculares, disponibilidad horaria, duración de estudios, edad, etc.

2. ¿Cómo implementar una auditoría algorítmica?

   Para poder implementar una auditoría algorítmica se podría realizar un plan que involucre métricas de equidad, prueba de estrés y sensibilidad, revisión de datos y revisión de impacto y gobernanza.

- Métricas de equidad:
  - Paridad demográfica, igualdad de oportunidades, calibración por subgrupos.
- Pruebas de estrés y sensibilidad
  - Alterar solo la variable sensible o su filtro y observar si cambia el resultado, realizar perturbaciones controladas y quitar variables candidatas a filtros y medir impacto en sesgo/rendimiento.
- Revisión de datos
  - Auditoría de sesgo de entrenamiento, balanceo/reponderación, limpieza de variables que no agregan valor predictivo y elevan riesgo ético.
- Revisión de impacto y gobernanza
  - Evaluación de impacto algorítmico, mapa de riesgos, afectados, mitigaciones, responsables, validación externa a través de un comité ético o auditor independiente.

3. ¿Cuándo debe exigirse revisión humana y derecho de apelación?
   En decisiones de alto impacto, en umbrales cercanos a corte, cuando existan señales de sesgo, si la explicación es insuficiente y cuando existan apelaciones.
4. ¿Qué políticas deben regular el uso de IA en decisiones de alto impacto?

- Política de uso responsable de IA con:
  - Propósito legítimo y límites de uso.
  - Principios de equidad, no discriminación y explicabilidad.
  - Revisión humana significativa obligatoria y derecho de apelación.
  - Criterios de umbrales definidos.
  - Ciclo de vida seguro.
  - Registro de decisiones.
  - Auditorías periódicas internas/externas y divulgación de hallazgos clave a la dirección.
  - Gestión de terceros y protección de datos.

5. ¿Cómo documentar la calidad y procedencia de datos?

- Limpieza de datos:
  - Origen (fuentes, periodos, coberturas geográficas y poblacionales).
  - Transformaciones (limpieza, imputación, normalización).
  - Selección de variables (justificación y evaluación de riesgo de filtro).
  - Versionado de datasets (fechas, cambios, responsables).
- Calidad:
  - Tasas de faltantes, inconsistencias, desbalance de clases.

- Representatividad por subgrupos (rural/urbano, universidades).

- Sesgos conocidos:
- Reporte de limitaciones y potenciales discriminaciones.
- Matriz de riesgos (probabilidad/impacto) y mitigaciones.

- Artefactos de gobernanza:
- Ficha de conjunto de datos (datasheets for datasets).
- Modelado de credenciales con desempeño y banderas por subgrupos.
- Registros de acceso y control de cambios.

6. ¿Qué responsabilidades legales y éticas recaen sobre la empresa y el proveedor?

- Empresa (responsable del tratamiento y de la decisión):
- Debida diligencia antes de usar IA (evaluación de impacto, pruebas de banderas).
- Transparencia con candidatos (uso de IA, criterios generales, derechos).
- Revisión humana y canal de apelación.
- Monitoreo continuo y corrección de sesgos detectados.
- Protección de datos (seguridad, minimización, finalidad).
- Responsabilidad: puede delegar tareas, no la responsabilidad final.

- Proveedor (encargado / desarrollador del modelo):
- Explicabilidad técnica (herramientas, documentación, diseño de credenciales).
- Soporte para métricas de banderas y controles de sesgo.
- Evidencias de validación (datasets, pruebas, resultados por subgrupos).

- Mecanismos de auditoría y derecho de revisión contractual.
- Actualizaciones y parches ante hallazgos de sesgo o fallas.
- Cumplimiento contractual con estándares éticos y de seguridad.

3.3 Desafíos éticos emergentes ante el avance tecnológico

El acelerado despliegue de sistemas digitales y algoritmos de inteligencia artificial ha amplificado tensiones clásicas entre innovación y protección de derechos, revelando nuevas zonas grises como sesgos algorítmicos, opacidad decisional, manipulación informativa a escala, impactos ambientales y riesgos de ciberseguridad. Las respuestas institucionales combinan principios globales con marcos de gestión de riesgos y regulaciones vinculantes para lograr una IA responsable y centrada en la persona.

Existen varios aspectos relevantes a tomar en cuenta:

1. Privacidad y autonomía en la sociedad de datos.

La recopilación masiva y el tratamiento automatizado de datos personales reconfiguran la relación entre cliente y empresas. Modelos regulatorios establecen principios de licitud, finalidad, minimización de datos y derechos ampliados de los titulares. Sistemas de gestión de seguridad y privacidad permiten operacionalizar controles técnicos y organizativos con mejora continua.

2. Sesgos, discriminación y justicia algorítmica

Los modelos entrenados con datos históricos pueden reproducir exclusiones sistémicas. Guías internacionales enfatizan equidad, transparencia y supervisión humana, mientras marcos de riesgo ayudan a identificar y mitigar sesgos a lo largo del ciclo de vida.

3. Opacidad, explicabilidad y rendición de cuentas

La opacidad de ciertos modelos dificulta auditar, impugnar o atribuir responsabilidades. La explicabilidad y la transparencia son atributos esenciales para sistemas confiables y responsables.

4. Integridad informacional y contenidos sintéticos

La proliferación de deepfakes y contenido generado por IA plantea riesgos para la deliberación pública y la confianza social. Las regulaciones recientes exigen etiquetado y controles de transparencia.

5. Ciberseguridad, resiliencia y uso dual

La expansión tecnológica amplía también la superficie de ataque. Sistemas de gestión de seguridad de la información permiten gestionar riesgos, proteger infraestructuras y resguardar datos sensibles.

6. Impactos ambientales y sostenibilidad

El entrenamiento de modelos y la operación de centros de datos generan impactos ambientales significativos. Las recomendaciones globales promueven TI verde y evaluación de huellas ambientales.

7. Gobernanza integral y ética operativa

La ética tecnológica requiere pasar de principios declarativos a prácticas operativas, con políticas, procesos, métricas y responsables claramente definidos.

3.4 Rol del profesional de TI en la toma de decisiones éticas

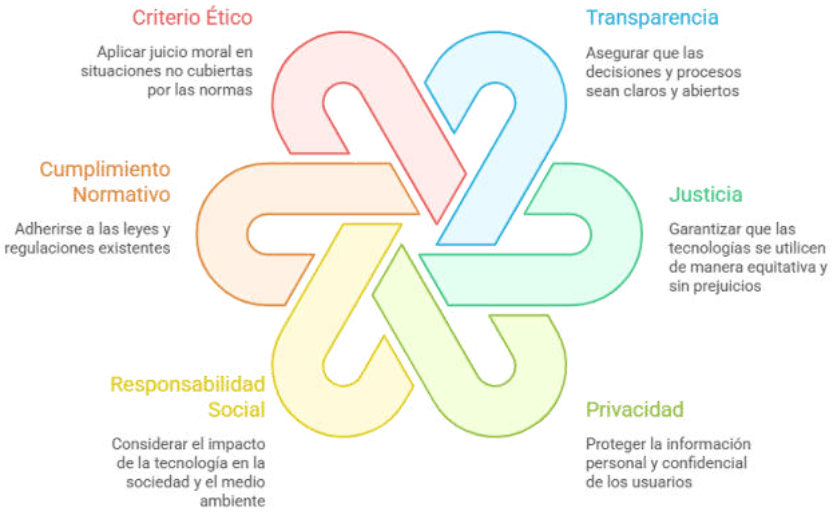


Figura 23. Rol ético del profesional en TI.

Fuente: Elaboración propia.

La labor del profesional de Tecnologías de la Información trasciende la mera implementación de sistemas y herramientas tecnológicas. En un entorno donde los datos, la automatización y la inteligencia artificial tienen un impacto directo en las personas, la toma de decisiones éticas se convierte en un componente esencial del ejercicio profesional. El profesional TI actúa no solo como tecnólogo, sino también como garante de principios éticos fundamentales como la transparencia, la justicia, la privacidad y la responsabilidad social.

Su responsabilidad no se limita al cumplimiento normativo; incluye también la aplicación de criterio ético cuando una norma no contempla explícitamente una situación emergente.

Desde esta perspectiva es importante recalcar la importancia que tiene al tener que desarrollar varias actividades tales como:

1. Custodio de la información y la privacidad.

El profesional TI tiene acceso privilegiado a datos sensibles Por esta razón su responsabilidad no se limita al cumplimiento normativo sino también incluye la aplicación de criterio ético cuando una norma no contempla explícitamente una situación emergente. Por esta razón debe:

- Salvaguardar la confidencialidad, integridad y disponibilidad de la información.
- Garantizar que el uso de los datos se ajuste a regulaciones como protección de datos personales.
- Evaluar proactivamente los riesgos de exposición, abuso o tratamiento indebido.

2. Mediador entre tecnología y sociedad.

Las decisiones tecnológicas influyen directamente en derechos individuales y colectivos siendo el profesional en TI el puente entre las capacidades tecnológicas y el bienestar social y para conseguirlo debe:

- Comprender el impacto social de las soluciones que desarrolla o administra.

- Cuestionar decisiones organizacionales que puedan generar exclusión, discriminación o afectación a grupos vulnerables.
- Asegurar que las innovaciones tecnológicas respeten principios éticos y no solo objetivos comerciales.

3. Promotor de transparencia y rendición de cuentas.

La opacidad tecnológica puede favorecer abusos o desigualdades Por esta razón para fortalecer la confianza y permitir corregir desviaciones antes de que escalen es necesario que el profesional TI se responsabilice de:

- Diseñar sistemas auditables y explicables, especialmente cuando incluyen algoritmos de decisión automática.
- Facilitar la comprensión del funcionamiento de las soluciones a usuarios, colaboradores y directivos.
- Registrar las decisiones técnicas relevantes y justificar sus implicaciones éticas.

4. Evaluador de riesgos éticos en proyectos tecnológicos.

Antes de implementar una tecnología, el profesional TI debe identificar riesgos y es justamente por ello que deben sugerir alternativas más seguras, promover evaluaciones de impacto ético y participar en comités de gobernanza tecnológica asociados al:

- Sesgo algorítmico.
- Uso indebido de datos.
- Vigilancia excesiva.
- Erosión de derechos digitales.

- Manipulación de información.

5. Ejecutor de principios de equidad y no discriminación.

La tecnología puede amplificar sesgos humanos si no se evalúa adecuadamente por lo que el sol del profesional en Tecnologías es clave como actor del reclutamiento, calificación crediticia, seguridad ciudadana y educación debido a que este profesional debe:

- Verificar que los modelos y sistemas no reproduzcan exclusiones por género, cultura, edad u otros factores.
- Proponer ajustes o rediseños cuando detecte inequidades.
- Mantener una postura crítica ante “lo que el algoritmo dice”, reconociendo que la IA no es neutral.

6. Compromiso con la actualización profesional

Las tecnologías evolucionan más rápido que las leyes y Por esta razón el conocimiento actualizado permite anticipar problemas y actuar con criterio informado, debiendo el profesional en TI:

- Mantenerse actualizado en tendencias, riesgos emergentes y buenas prácticas éticas.
- Participar en espacios de formación continua.
- Promover dentro de la organización una cultura de ética tecnológica y mejora permanente.

7. Voz ética dentro de la organización

El rol como “consciencia tecnológica” del profesional en TI es fundamental para organizaciones que buscan la sostenibilidad y legitimidad, Por esta razón debe tener la valentía de:

- Señalar prácticas inadecuadas.
- Negarse a participar en proyectos que violen principios éticos claros.
- Proponer soluciones más responsables, aunque impliquen mayores costos o cambios en la planificación.

3.5 Responsabilidad profesional en el ámbito tecnológico

La profesión del ingeniero en Tecnologías de la Información implica una responsabilidad que trasciende lo puramente técnico. Cada decisión tomada, cada sistema diseñado y cada línea de código escrita tiene impacto en organizaciones, ecosistemas digitales y, más importante aún, en la vida de las personas que confían en la tecnología. Desde este enfoque, la responsabilidad profesional no es solo un componente ético: es parte esencial de la gobernanza tecnológica, la seguridad de la información y el cumplimiento normativo.

Se debe tener bien en claro que no somos simples solucionadores de problemas técnicos sino somos garantes de integridad, seguridad y justicia tecnológica. La responsabilidad profesional exige actuar con competencia, honestidad y compromiso con el bienestar social. Esto implica un profundo respeto por las normativas, una práctica alineada con estándares de calidad, una actualización constante y una

comprensión ética de las decisiones que se toman en entornos altamente digitalizados.

La tecnología, por sí sola, no es buena ni mala; adquiere valor moral a través de quienes la diseñan, implementan y gestionan. Por ello, debemos siempre asumir un rol con plena conciencia de que cada decisión técnica puede transformar vidas, instituciones y sociedades enteras.

Desde esta perspectiva se puede identificar brevemente los deberes y obligaciones del ingeniero en Tecnologías de la Información siendo conscientes que todos los actos desarrollados tienen una responsabilidad directa con la calidad, seguridad y transparencia de los sistemas que construyen o administran, y para un mejor entendimiento podría resumirse en esta tabla dividida en tres niveles: técnicos, éticos y sociales.

Tabla 3. Tabla de deberes y acciones del Ingeniero en TI.

Categoría	**Deberes/Obligaciones**	**Descripción**
Técnica	Diseño seguro	Aplicar principios de seguridad por diseño, cifrado, autenticación robusta, privacidad por defecto.
	Cumplimiento normativo	Alinear procesos con estándares como ISO/IEC 27001, 27002, COBIT, ITIL, NIST.

	Calidad del software	Garantizar funcionalidad, confiabilidad y mantenimiento del código.
Ética	Transparencia	Comunicar riesgos, limitaciones y efectos potenciales de las soluciones tecnológicas.
	No maleficencia	Evitar exponer a usuarios a daños previsibles (brechas, discriminación, fallos críticos).
	Equidad	Hay que asegurar que sistemas e IA no generen sesgos o exclusiones injustas.
Social	Protección de datos	Resguardar la información personal y sensible según leyes vigentes.
	Responsabilidad	Asumir consecuencias de las decisiones y actuar con diligencia profesional.
	Impacto social	Considerar efectos de la tecnología en comunidades, economía y justicia social.

Un profesional de TI no solo debe actuar desde lo técnico, sino debe tener un equilibrio entre competencias, valores y conciencia del impacto social.

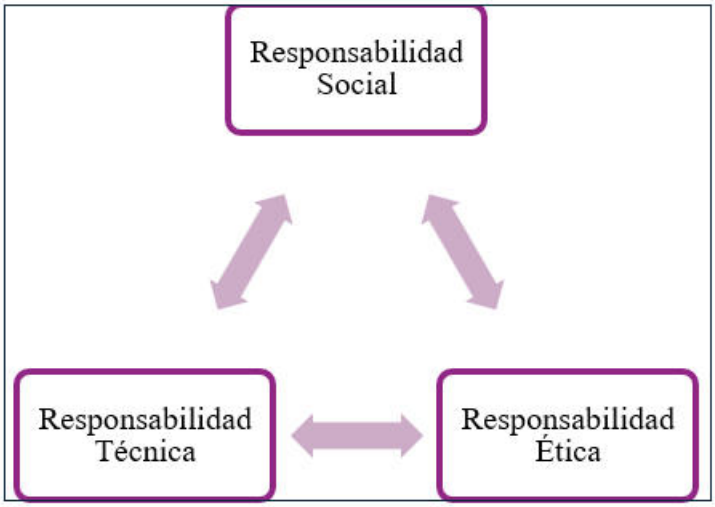


Figura 24. Triángulo de responsabilidades.

Fuente: Elaboración propia.

Las tecnologías evolucionan con una velocidad que no tiene precedentes y por ende su influencia en otras disciplinas es incuestionable. Por ello, el profesional de TI tiene un deber explícito de actualización continua, no solo como recomendación, sino como requisito para ejercer la profesión con responsabilidad, existiendo áreas críticas en las que debiera actuar con mayor énfasis como se describen en la siguiente tabla.

Tabla 4. Áreas y razón de actualización profesional en TI.

Área	Razón de actualización	Ejemplo
Ciberseguridad	Amenazas cambian constantemente.	Nuevos ataques, vulnerabilidades, metodologías de hacking ético.
Normativas y cumplimiento	Leyes y estándares se actualizan.	ISO/IEC 27001:2022, leyes de datos, marcos NIST.
Desarrollo de software	Nuevas metodologías y herramientas.	DevSecOps, microservicios, contenedores.
Cloud Computing	Modelos de nube en transformación.	AWS, Azure, GCP, gobernanza en la nube.
IA y datos	Riesgos éticos y técnicos emergentes.	Sesgos, explicabilidad, auditoría algorítmica.

Fuente: Elaboración propia.

Es importante en este sentido que todo profesional en TI sepa conocer su ciclo de actualización profesional que empieza con una evaluación de conocimientos hasta la retroalimentación como se ve en el siguiente gráfico:

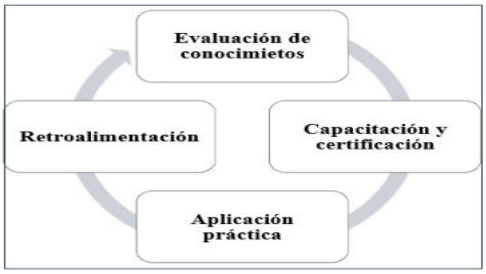


Figura 25. Ciclo de actualización profesional.

Fuente: Elaboración propia.

Los deberes, obligaciones y razones de actualización vienen apegado de igual manera al conflicto de interés en el sector tecnológico que pudieran surgir a partir de la incidencia directa que se tiene sobre decisiones importantes, Por esta razón se debe tener bien claro que a pesar de que las decisiones son empresariales, se debe tener como prioridad el interés social.

Habrían de aparecer intereses de tipo económicos como beneficiar directamente a un proveedor o la elección de un software tomando decisiones técnicas sesgadas, o dando accesos a sistemas donde se puede tomar ventajas y tener que hacer violaciones a la privacidad, pudiendo administrar sistemas donde seamos jueces y parte habiendo falta de transparencia o favorecer a empresas o algún otro profesional con lo que podría perderse la objetividad.

La responsabilidad del ingeniero en tecnologías de la información es muy grande dado que sus decisiones afectan a empresas y sociedad directamente, Por esta razón hay que tener siempre en cuenta ciertas alertas como:

- Falta de transparencia en decisiones técnicas.
- Recomendación de soluciones sin justificación documental.
- Acceso innecesario a datos sensibles.
- Negativa a auditorías o revisiones independientes.
- Incentivos ocultos o no declarados.

Y, para ello es necesario tener en cuenta estas estrategias para gestionar los conflictos de interés:

- Declaración obligatoria de intereses personales y laborales.
- Auditorías técnicas externas para decisiones críticas.
- Separación clara entre roles (como desarrollo vs. seguridad).
- Documentación exhaustiva de decisiones arquitectónicas.
- Mecanismos de supervisión ética o comités internos.

El siguiente caso plantea un dilema para el análisis:

3.5.1 SIGTAL y la responsabilidad del ingeniero en TI

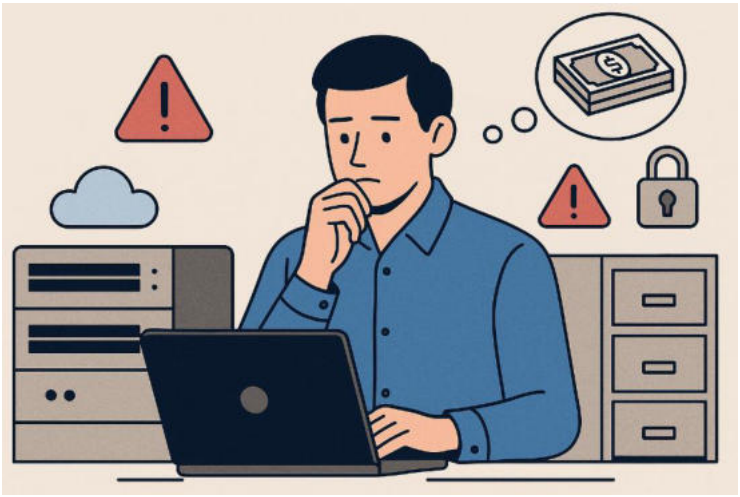


Figura 26. SIGTAL y la responsabilidad del ingeniero en TI.

La empresa pública SIGTAL administra información crítica relacionada con licencias comerciales, datos tributarios y registros de permisos municipales. Su departamento de TI está conformado por cinco profesionales, dirigidos por el ingeniero Luis Andrade, responsable de

infraestructura y seguridad de la información. La institución se encuentra en un proceso de modernización tecnológica que incluye migración a la nube, implementación de un sistema de gestión documental y adopción de nuevas normativas internas de seguridad basadas en ISO/IEC 27001. Durante la fase de pruebas del sistema en la nube, un analista detecta que varios archivos con información sensible estaban almacenados sin cifrado y accesibles para personal no autorizado.

Al informar a Luis, este decide ignorar el hallazgo temporalmente, afirmando que “el lanzamiento no puede detenerse por detalles técnicos” y que “la seguridad se reforzará más adelante”. Además, Luis mantiene un acuerdo informal con un excompañero que trabaja en un proveedor externo: recomienda sus servicios a la empresa sin informar que recibirá un porcentaje por cada contratación.

Días después del lanzamiento, ocurre un incidente: un funcionario accede accidentalmente a documentos de otra dependencia y descarga información tributaria que no debía ver. La Dirección exige un informe del incidente y descubre la omisión de controles mínimos como:

- Cifrado en reposo y en tránsito.
- Segregación de accesos basada en roles.
- Auditorías de acceso.
- Gestión de incidentes documentada.

El informe también revela la relación económica entre Luis y el proveedor recomendado, lo cual se considera un posible conflicto de interés.

Frente a esta situación, la institución solicita evaluar el comportamiento profesional del equipo de TI y reforzar competencias clave relacionadas con: responsabilidad profesional, competencia técnica, ética, gestión de riesgos, toma de decisiones y cumplimiento normativo.

Guía de análisis

1. ¿Qué deberes profesionales incumplió el ingeniero Luis durante el proyecto?
2. ¿Qué competencias técnicas faltaron para evitar el incidente?
3. ¿Por qué almacenar datos sensibles sin cifrado constituye una falta grave?
4. ¿Cómo influyó la ausencia del control basado en roles en el incidente?
5. ¿Qué tipo de conflicto de interés se evidencia en la conducta de Luis?
6. ¿Qué riesgos enfrenta la institución al ignorar vulnerabilidades conocidas?
7. ¿Qué debió hacer el analista que detectó el problema en primera instancia?
8. ¿Qué medidas inmediatas debió adoptar la Dirección tras conocerse el incidente?
9. ¿Qué aprendizajes deben integrarse al proceso de desarrollo y migración a la nube?

10. ¿Qué políticas y normativas deben reforzarse institucionalmente?

Consideración final

Este caso evidencia que la responsabilidad profesional en TI va mucho más allá del dominio técnico. La negligencia en la implementación de controles básicos y la falta de ética en la relación con proveedores comprometen no solo un sistema, sino la confianza en toda la organización. La ética profesional, la transparencia y la gestión responsable del riesgo deben guiar cada decisión. En un entorno tecnológico donde pequeñas omisiones pueden tener impactos masivos, el ingeniero de TI debe actuar con integridad, actualización constante, respeto por estándares internacionales y plena conciencia del valor social de la información que protege. La excelencia técnica es fundamental, pero la excelencia ética es lo que garantiza que dicha técnica se ponga realmente al servicio del bien común.

Propuesta de respuesta

1. ¿Qué deberes profesionales incumplió el ingeniero Luis durante el proyecto?

Incumplió su deber de cuidado, diligencia, transparencia y responsabilidad profesional, al ignorar fallas críticas de seguridad y no priorizar la protección de datos. Además, vulneró la obligación ética de evitar conflictos de interés.

2. ¿Qué competencias técnicas faltaron para evitar el incidente?

- Implementación de controles de seguridad.

- Aplicación del SGSI basado en ISO/IEC 27001.
- Gestión de riesgos tecnológicos.
- Auditoría y monitoreo efectivo.

3. ¿Por qué almacenar datos sensibles sin cifrado constituye una falta grave?

Porque expone información crítica a accesos no autorizados, pudiendo generar consecuencias legales, reputacionales y operativas. El cifrado es un control obligatorio en cualquier entorno seguro.

4. ¿Cómo influyó la ausencia del control basado en roles en el incidente?
5. Permitió que un funcionario con permisos básicos accediera a información tributaria. La falta de control basado en roles generó un acceso horizontal no autorizado.
6. ¿Qué tipo de conflicto de interés se evidencia en la conducta de Luis?
7. Un conflicto de interés económico, ya que Luis obtiene beneficios personales al recomendar un proveedor sin declararlo a la institución.
8. ¿Qué riesgos enfrenta la institución al ignorar vulnerabilidades conocidas?

- Incidentes de fuga de información.
- Sanciones legales.
- Daños reputacionales.
- Interrupción de servicios.
- Pérdida de confianza interna y externa.

9. ¿Qué debió hacer el analista que detectó el problema en primera instancia?

Escalar formalmente la alerta, documentar el hallazgo y solicitar activación del proceso de gestión de incidentes. Si no era atendido, debía reportar a un nivel superior siguiendo el protocolo interno.

10. ¿Qué medidas inmediatas debió adoptar la Dirección tras conocerse el incidente?

- Suspender accesos riesgosos.
- Activar gestión de incidentes.
- Evaluar el impacto.
- Notificar a las partes afectadas.
- Ordenar medidas correctivas y auditorías técnicas.
- Abrir investigación sobre conducta del ingeniero.

11. ¿Qué aprendizajes deben integrarse al proceso de desarrollo y migración a la nube?

- Seguridad desde el diseño.
- Revisiones técnicas obligatorias antes del despliegue.
- Auditorías continuas.
- Documentación exhaustiva del proceso.
- Capacitación en normativas y ética.

12. ¿Qué políticas y normativas deben reforzarse institucionalmente?

- Política de seguridad de la información.
- Política de gestión de incidentes.
- Política de conflicto de interés.
- Política de acceso a la información.
- Estándares de desarrollo seguro.

- Marco normativo basado en ISO/IEC 27001 y 27002.

3.6 Privacidad y protección de datos en entornos tecnológicos



Figura 27. Privacidad y protección de datos.

Fuente: Elaboración propia.

La privacidad y la protección de datos en entornos tecnológicos exigen un enfoque integral que combine principios éticos y controles técnicos desde el diseño hasta la operación: respetar la autonomía del usuario mediante consentimiento informado y granular; aplicar proporcionalidad y minimización para recolectar solo lo estrictamente necesario; asegurar la no maleficencia con cifrado en tránsito y en reposo, gestión segura de llaves, autenticación multifactor y principio de mínimo privilegio; garantizar transparencia y responsabilidad con avisos claros, trazabilidad mediante registros inmutables, auditorías periódicas y métricas que midan cumplimiento.

En la recolección y uso ético, toda finalidad debe estar documentada y ser legítima; los formularios deben evitar campos superfluos, habilitar opciones sin penalización y clasificar los datos por sensibilidad para aplicar controles diferenciados; el almacenamiento debe incluir

segmentación de ambientes, acceso controlado y contextualizado por roles, tokenización o seudonimización para analítica y políticas de retención con eliminación verificable, complementadas por evaluaciones de impacto cuando exista alto riesgo.

La privacidad digital no es solo un requisito legal: es una obligación moral que protege autonomía, dignidad y libertad, se debe tener claro el propósito de almacenamiento de los datos, recolectando y clasificando la información, haciendo uso legítimo y garantizando la seguridad y acceso, debiendo hacer una retención limitada de los datos y una eliminación verificable.

Ante esto es importante incluir algo como la Ciberseguridad éticamente responsable definiéndola como una disciplina técnica y un compromiso moral. Un sistema puede "funcionar", pero si su defensa se basa en prácticas opacas, pruebas sin consentimiento o explotación de fallos sin notificación, la seguridad se vuelve antagónica a la confianza.

Cuando se habla se privacidad digital y ciberseguridad hay que dejar bien en claro que no basta "no hacer daño"; en ciberseguridad profesional se exige consentimiento informado y trazabilidad. Puede que en algún momento decisivo hagamos una decisión que tenga las mejores intenciones sin embargo es importante reconocer que si no se tiene los permisos sigue siendo antiético y potencialmente ilegal.

También es importante topar el tema de la inteligencia artificial y la ética logarítmica pues en un mundo donde los sistemas automatizados influyen cada vez más en decisiones que antes eran exclusivamente

humanas, la importancia de la ética en este campo se ve afectada, debiendo siempre garantizar que la IA se diseñe y utilice bajo principios de equidad, transparencia y responsabilidad. Un algoritmo no es neutral: reproduce patrones presentes en los datos con los que fue entrenado, por lo que es esencial aplicar criterios éticos que aseguren que las decisiones automatizadas respeten la dignidad humana, no vulneren derechos y actúen dentro de un marco verificable y auditable. En este sentido, la ética algorítmica constituye un componente crítico para la confiabilidad tecnológica y para la protección de los usuarios en entornos cada vez más automatizados.

La afectación a la sociedad es profunda, ya que los algoritmos pueden influir en múltiples esferas: desde la salud y la educación hasta la justicia y el acceso a servicios financieros. Una IA sin supervisión ética puede amplificar desigualdades, replicar estereotipos o favorecer grupos privilegiados sin que nadie lo note a simple vista. Por ello, la ética algorítmica demanda procesos de evaluación de impacto, análisis de sesgos, explicabilidad de modelos y mecanismos de corrección continua. También requiere transparencia en el uso de datos y límites claros para evitar decisiones que afecten gravemente a individuos o comunidades. Así, la sociedad necesita sistemas de IA que sean no solo eficaces, sino también justos, verificables y alineados con valores democráticos.

En el ámbito del reclutamiento, la IA puede generar selección injusta de personal cuando aprende de datos históricos cargados de sesgos o desigualdades laborales. Un sistema entrenado con perfiles

mayoritariamente urbanos, de universidades privadas o provenientes de sectores específicos tenderá a reproducir esos patrones, excluyendo automáticamente a candidatos de zonas rurales, instituciones públicas o trayectorias no tradicionales. Sin mecanismos éticos como auditorías algorítmicas, análisis justos, revisión humana significativa y transparencia en los criterios de evaluación, la IA puede rechazar talento valioso sin motivos legítimos, perpetuando inequidades laborales. Por ello, la ética algorítmica en recursos humanos no es opcional: es un requisito esencial para garantizar procesos de selección inclusivos, respetuosos y libres de discriminación oculta.

Podríamos entonces resumir toda esta información en una tabla donde se pueda tomar en cuenta ciertas dimensiones y controles necesarios para salvaguardar los principios.

Tabla 5. Dimensiones y controles éticos ante el uso de la IA.

Dimensión	Descripción	Riesgos/Impactos	Controles éticos
Importancia de la IA y la ética algorítmica	La IA debe diseñarse y usarse con equidad, transparencia y responsabilidad; los modelos aprenden patrones de los datos y pueden replicar sesgos.	Decisiones opacas, errores sistemáticos con gran escala, pérdida de confianza, afectación de derechos.	Equidad, trazabilidad; gobernanza de modelos; auditorías internas/externa; registro de decisiones.

Afectación a la sociedad	La IA incide en salud, educación, justicia, finanzas y servicios públicos. Sin ética, amplifica desigualdades y estereotipos.	Discriminación de colectivos, exclusión de servicios, decisiones injustas difíciles de impugnar.	Evaluaciones de Impacto Algorítmico (AIA/DPIA); políticas de límites de uso; supervisión humana significativa en decisiones de alto impacto.
Selección injusta de personal	Modelos de reclutamiento aprenden de datos históricos (p. ej., preferencia por zonas urbanas o universidades privadas) y replican sesgos.	Rechazo sistemático de candidatos de zonas rurales, universidades públicas o trayectorias no tradicionales; riesgo legal y reputacional.	Auditoría de sesgos (paridad demográfica, igualdad de oportunidades); exclusión/regularización de código postal, universidad; revisión humana y derecho de apelación.
Supervisión humana significativa	Humanos con competencia y autoridad revisan y pueden modificar o revocar decisiones del modelo.	Automatización sin control; errores persistentes.	Mecanismos aplicables para detener despliegues ante sesgo.

Mecanismos de apelación y reparación	Canales formales para impugnar decisiones y corregir perjuicios.	Daños no remediados; percepción de injusticia.	Portal de apelaciones, plazos garantizados, revisión independiente; documentación de resoluciones.

Fuente: Elaboración propia.

3.7 Ética y reputación digital

En los entornos digitales contemporáneos, la reputación de una organización, medio o plataforma no solo depende de sus publicaciones oficiales, sino también de aquello que permiten, fomentan o toleran en los espacios de interacción: comentarios, foros, reseñas, imágenes, videos, streams y mensajes. El contenido generado por usuarios amplifica la voz de la comunidad, pero también introduce riesgos: desinformación, incitación al odio, difusión de datos personales sin consentimiento, violaciones de propiedad intelectual o publicidad engañosa. Gestionar éticamente el contenido generado por los usuarios significa proteger derechos, cuidar a las audiencias y preservar la confianza sin sofocar la libre expresión, estableciendo reglas claras, procesos de moderación proporcionados y mecanismos de apelación.

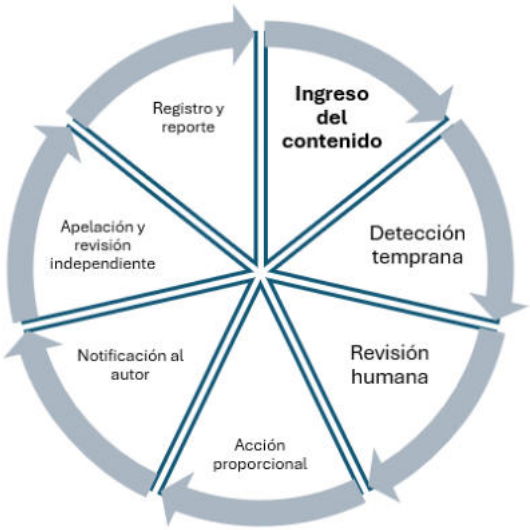


Figura 28. Flujo ético de contenido generado por el usuario.

Fuente: Elaboración propia.

La ética del contenido generado por el usuario es muy importante, De este modo una organización responsable delimita reglas, modera con proporcionalidad, explica lo que hace, permite apelar y mide sus decisiones. De este modo, se equilibra la libertad de expresión con el deber de proteger a las personas y a la comunidad, consolidando una reputación basada en la confianza y la coherencia entre valores y prácticas.

Considérese ahora este caso práctico:

3.7.1 CIVITAS: entre el cumplimiento y la confianza



Figura 29. CIVITAS: entre el cumplimiento y la confianza.

La municipalidad de CIVITAS implementa un portal de servicios en línea para trámites ciudadanos (pagos, certificados, solicitudes). El proyecto fue liderado por el Área de TI y un proveedor externo. Para cumplir fechas, el equipo liberó la versión 1.0 sin completar todos los controles previstos: se postergaron la autenticación multifactor (MFA) y el cifrado por campo en la base de datos; tampoco se formalizó un Sistema de Gestión de Seguridad de la Información (SGSI) ISO/IEC 27001 ni un plan de continuidad (ISO 22301). Tres semanas después, se reporta que algunos contribuyentes pudieron visualizar por error los datos de terceros al descargar comprobantes.

En la revisión post-incidente se detecta: Control de acceso basado en funciones incompleto, registros de auditoría sin integridad, ausencia de pruebas de penetración externas, contratos con el proveedor sin

seguridad, ni derecho de auditoría, ni exigencias de divulgación responsable de vulnerabilidades. Además, se descubre que la jefatura de TI aceptó recomendaciones técnicas del proveedor, aunque el comité de riesgo solicitó retrasar el lanzamiento hasta completar MFA y cifrado por campo.

La alcaldía solicita un informe por competencias: responsabilidad profesional, gestión de riesgos, cumplimiento normativo, privacidad y ética digital, arquitectura segura, gobierno con terceros, respuesta a incidentes y mejora continua. Se requiere un plan de corrección en 90 días y métricas para demostrar avances.

Preguntas para el análisis

1. ¿Qué deberes profesionales y éticos se incumplieron al liberar CIVITAS sin MFA ni cifrado por campo?
2. ¿Qué brechas de cumplimiento normativo y de estándares son evidentes?
3. ¿Qué controles de arquitectura debieron ser requisitos de “no-go” antes del lanzamiento?
4. ¿Cómo debería gestionarse el riesgo detectado en términos de priorización y mitigación?
5. ¿Qué acciones de respuesta a incidentes y comunicación son éticamente esperables?
6. ¿Qué medidas de privacidad por diseño deben incorporarse para el portal?
7. ¿Cómo debió gobernarse al proveedor para evitar las fallas detectadas?

8. Propón un plan de corrección en 90 días con hitos y métricas.
9. ¿Qué evidencias objetivas demostrarían mejora continua y rendición de cuentas?
10. ¿Qué lecciones deben institucionalizarse para futuros proyectos digitales?

Reflexión del caso

El caso de la plataforma CIVITAS expone con claridad cómo las decisiones apresuradas en entornos tecnológicos pueden erosionar la confianza pública y revelar debilidades profundas en la gestión ética de la información. La liberación de un sistema crítico sin controles de seguridad indispensables como autenticación multifactor, cifrado por campo o registros auditables demuestra que la presión por cumplir plazos no puede justificar la omisión de responsabilidades profesionales fundamentales. La tecnología que maneja datos sensibles de la ciudadanía debe nacer sobre principios de seguridad, privacidad y transparencia; de lo contrario, se convierte en un riesgo para quienes busca servir.

Este caso también evidencia que la ética no es un complemento, sino un componente operativo de la gestión tecnológica. La ausencia de un SGSI, la falta de auditorías previas y la negligencia en la gobernanza con proveedores muestran que los riesgos no emergen únicamente por fallas técnicas, sino por fallas en el juicio profesional y la cultura organizacional. Cuando el liderazgo consiente prácticas que “se reforzarán más adelante”, se normaliza la idea de que la seguridad puede

ser opcional, debilitando el ecosistema de protección y abriendo puertas a incidentes evitables.

Asimismo, la afectación a los ciudadanos revela que la privacidad no puede entenderse como un tema administrativo, sino como un derecho cuya vulneración genera daños reales: exposición de información personal, pérdida de confianza en servicios públicos y percepción de negligencia institucional. La transparencia en la respuesta, la corrección oportuna y la disposición a aprender de los errores se vuelven esenciales para reconstruir credibilidad y demostrar madurez tecnológica.

Finalmente, este caso deja una enseñanza crucial: la competencia técnica debe ir siempre acompañada de responsabilidad ética. Un ingeniero de TI, un jefe de proyecto o un proveedor no solo diseñan sistemas, sino también las condiciones en las que una comunidad deposita su confianza. La verdadera profesionalidad se mide no por la rapidez del despliegue, sino por la capacidad de anticipar riesgos, proteger a las personas y actuar íntegramente ante decisiones difíciles. CIVITAS recuerda que la seguridad y la ética no son retrasos en el proceso, sino la base para construir tecnología que sirva genuinamente al bien común.

Criterios para una posible solución

1. ¿Qué deberes profesionales y éticos se incumplieron al liberar CIVITAS sin MFA ni cifrado por campo?

Se vulneró el deber de cuidado y la no maleficencia al exponer a los ciudadanos a riesgos previsibles; se omitió la transparencia al no

comunicar adecuadamente impactos; y se subordinó la seguridad a la presión del calendario, afectando el principio de responsabilidad profesional. Técnicamente, se ignoraron controles básicos de confidencialidad y trazabilidad.

2. ¿Qué brechas de cumplimiento normativo y de estándares son evidentes?

Ausencia de SGSI ISO/IEC 27001, falta de controles de ISO/IEC 27002, carencia de BCP/DRP según ISO 22301, y deficiencias de privacidad. También faltó evidenciar prácticas NIST/OWASP para aplicaciones web.

3. ¿Qué controles de arquitectura debieron ser requisitos de “no-go” antes del lanzamiento?

MFA obligatoria; RBAC/ABAC con mínimo privilegio; cifrado TLS 1.2/1.3, en reposo (AES-256) y por campo para PII sensible; segregación dev/test/pre-prod/prod; logs inmutables (WORM/hashing) con monitoreo SIEM; secrets management y rotación de llaves; rate limiting y protecciones OWASP.

4. ¿Cómo debería gestionarse el riesgo detectado en términos de priorización y mitigación?

Valorar severidad con CVSS y contexto de negocio. Acciones inmediatas: activar MFA, corregir RBAC, aplicar cifrado por campo, endurecer endpoints y reglas WAF, revisar accesos y forzar rotación de credenciales. Paralelamente, ejecutar un pentest externo y cerrar hallazgos críticos menores o igual a 30 días.

5. ¿Qué acciones de respuesta a incidentes y comunicación son éticamente esperables?

Contención y verificación del alcance; notificación oportuna a afectados y autoridad competente; comunicación clara de lo ocurrido y de medidas de remediación; habilitar soporte a ciudadanos; y realizar revisión posterior al incidente sin culpabilizar con plan de mejora verificable.

6. ¿Qué medidas de privacidad por diseño deben incorporarse para el portal?

Minimización de formularios; finalidad y base legal documentadas; centro de preferencias; políticas de retención limitada y eliminación verificable (TTL, crypto-shredding); seudonimización/tokenización para analítica; revisión de third-party scripts y CSP para evitar exfiltraciones; DPIA/PIA para cambios de alto riesgo.

7. ¿Cómo debió gobernarse al proveedor para evitar las fallas detectadas?

Contratos con SLA de seguridad, derecho de auditoría, evidencia de controles, VDP con plazos de corrección, requerimientos de DevSecOps y obligación de cumplir con ISO/IEC 27001/27002 y buenas prácticas OWASP.

8. Propón un plan de corrección en 90 días con hitos y métricas.

- 0 - 30 días: MFA, RBAC completo, cifrado por campo, hardening, rotación de llaves, quick pentest, canal VDP; KPIs: % controles críticos implementados, hallazgos críticos abiertos.
- 31 - 60 días: Integrar SAST/DAST/SCA al pipeline, secure logging + SIEM, políticas de retención y centro de preferencias, contratos actualizados con SLA; KPIs: cobertura CI/CD, MTTD/MTTR.

- 61 - 90 días: Formalizar SGSI ISO 27001 (políticas, matriz de riesgos, SoA), pruebas BCP/DRP (RTO/RPO), auditoría interna; KPIs: cierre de hallazgos, éxito de simulacros, % sistemas con DPIA.

9. ¿Qué evidencias objetivas demostrarían mejora continua y rendición de cuentas?

Políticas aprobadas y vigentes; registros de riesgo y SoA; reportes SIEM; resultados de pentests con cierres documentados; métricas de tiempo de remediación; actas de comité de seguridad; registros de DPIA; bitácoras de incidentes y post-mortems; contratos con anexos de seguridad; reportes de transparencia.

10. ¿Qué lecciones deben institucionalizarse para futuros proyectos digitales?

Seguridad y privacidad por defecto; puertas de liberación con criterios "no-go"; participación temprana de legal/compliance/seguridad; gobierno de terceros riguroso; cultura de divulgación responsable; pruebas y simulacros periódicos; formación continua en ética digital; y métricas que alineen objetivos de negocio con reducción de riesgo.

3.8 Síntesis transversal del capítulo

La ética aplicada a las Tecnologías de la Información acompaña todo el ciclo de vida de un sistema, está presente cuando se seleccionan los datos, se definen requisitos, se diseña una arquitectura, se prueban controles, se despliega una solución y se atienden sus consecuencias, por ello, la responsabilidad profesional no puede reducirse a corregir errores después de que ocurren; exige anticipar riesgos, documentar

decisiones y revisar de manera continua si la tecnología sigue respondiendo a los fines para los que fue creada.

Los desafíos asociados con la inteligencia artificial, la privacidad, la protección de datos y la reputación digital refuerzan esta necesidad, mostrando que un sistema puede ser técnicamente eficiente y, al mismo tiempo, producir resultados poco transparentes, discriminatorios o difíciles de impugnar. La competencia técnica debe complementarse con capacidad de análisis ético, comunicación clara, actualización profesional y disposición para detener o modificar una solución cuando sus riesgos no han sido controlados de forma suficiente.

Los casos abordados en el capítulo muestran que el profesional de TI actúa dentro de organizaciones sometidas a presiones de tiempo, presupuesto y resultados; en esas condiciones, los controles, los registros, la segregación de funciones y la revisión independiente ofrecen respaldo para tomar decisiones justificables, sin embargo; ninguna herramienta sustituye el juicio profesional por lo que corresponde identificar a las personas afectadas, explicar las limitaciones de la solución y asumir responsabilidad por sus efectos.

De manera transversal, el capítulo vincula integridad, competencia y rendición de cuentas como dimensiones inseparables del ejercicio profesional, esa integración protege a los usuarios y también fortalece la continuidad y la credibilidad de la organización convirtiendo estos criterios en métodos de análisis, alternativas de respuesta y planes de acción aplicables a situaciones empresariales concretas.

CAPÍTULO IV

4 APLICACIÓN PRÁCTICA DE NORMAS Y ÉTICA EN EL EJERCICIO PROFESIONAL: CASOS, ANÁLISIS Y SOLUCIONES

4.1 Introducción a la práctica profesional ética

La práctica profesional ética es el punto donde convergen el conocimiento técnico, el criterio normativo y la responsabilidad moral del ingeniero en Tecnologías de la Información. En este capítulo, la ética deja de ser una abstracción filosófica o un conjunto de buenas intenciones, y se convierte en una guía concreta para actuar correctamente ante dilemas reales que involucran datos, sistemas, usuarios, instituciones y proveedores. La verdadera competencia profesional no se evalúa únicamente por la capacidad de diseñar software eficiente o implementar infraestructuras robustas, sino por la habilidad de tomar decisiones responsables bajo presión, anticipar riesgos, proteger a las personas y sostener la confianza en cada proyecto tecnológico.

A medida que las organizaciones dependen más de plataformas digitales, la aplicación práctica de normas y marcos como ISO/IEC 27001, 27002, 22301, NIST, COBIT, ITIL y principios de ética profesional se vuelve indispensable. Estos estándares no solo orientan el diseño y operación de sistemas seguros, sino que establecen límites claros sobre cómo debe actuar un profesional frente a vulnerabilidades, incidentes, conflictos de interés, manejo de datos sensibles o uso de inteligencia artificial. La

ética profesional se expresa en acciones concretas: rechazar el lanzamiento de un sistema inseguro, reportar una vulnerabilidad de manera responsable, garantizar la privacidad de los ciudadanos o resistir presiones que comprometan la integridad del servicio.

Este capítulo aborda casos de estudio, análisis críticos y soluciones estructuradas que permiten comprender cómo las normas y principios éticos se aplican en la vida real. Cada situación narrada pone en evidencia que la ética profesional no es opcional ni secundaria, sino la base sobre la cual se sostiene la reputación del ingeniero, la confiabilidad de los sistemas y la credibilidad de las instituciones. Aquí, la teoría se transforma en práctica: el lector analizará incidentes, identificará fallas en la toma de decisiones, evaluará riesgos y propondrá planes de remediación que integren seguridad, privacidad, gobernanza y responsabilidad social.

En última instancia, este capítulo busca fortalecer la capacidad del futuro profesional para actuar con integridad incluso en escenarios ambiguos o complejos. El objetivo no es solo resolver problemas técnicos, sino comprender las consecuencias humanas, legales y organizacionales de cada decisión. La ética aplicada al ejercicio profesional es el elemento que convierte a un ingeniero competente en un ingeniero confiable, capaz de construir tecnología que no solo funcione, sino que también honre la dignidad, la seguridad y los derechos de las personas que dependen de ella.

4.2 Aplicación de normas y ética en situaciones reales

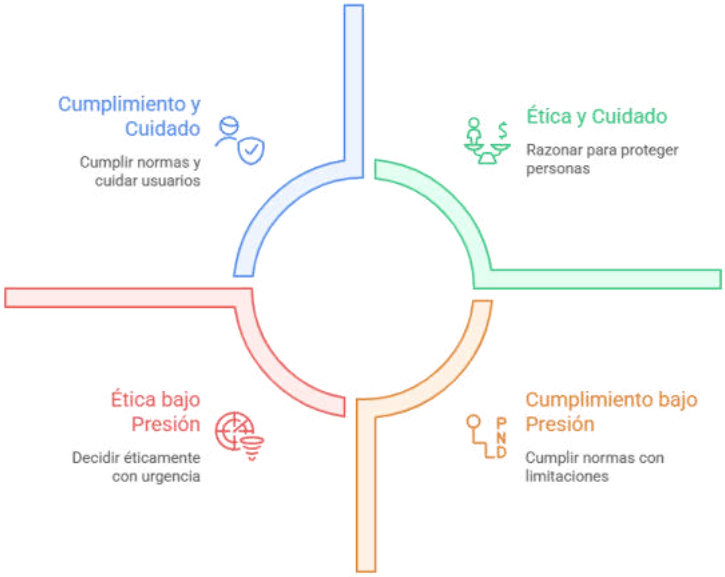


Figura 30. Aplicación de normas éticas en situaciones reales.

Fuente: Elaboración propia.

La aplicación de normas y ética en escenarios reales del ejercicio profesional requiere más que conocer marcos como ISO/IEC 27001, ISO/IEC 27002, COBIT, ITIL o lineamientos de privacidad: demanda la capacidad de interpretarlos en el contexto de decisiones concretas, especialmente en situaciones donde la presión operativa, las limitaciones técnicas y los intereses institucionales pueden entrar en conflicto. En la práctica cotidiana, los profesionales de TI deben equilibrar requisitos normativos, expectativas del usuario, viabilidad técnica y principios éticos fundamentales como no maleficencia, justicia, responsabilidad y transparencia. Así, cuando una organización

enfrenta un incidente de seguridad, un dilema sobre el uso de información sensible o una migración tecnológica urgente no basta con saber qué norma aplicar; se requiere razonar éticamente para determinar qué acción protege mejor a las personas, preserva la integridad del sistema y respeta el valor social de la tecnología.

En situaciones reales, la ética actúa como un marco de navegación que orienta decisiones cuando la norma no es explícita o cuando existen varias alternativas técnicamente viables. Por ejemplo, un ingeniero puede estar autorizado a acceder a ciertos registros internos, pero la ética le exige preguntarse si ese acceso es necesario, proporcional y seguro. De igual forma, un proyecto puede cumplir formalmente con un checklist de seguridad, pero la ética demanda evaluar si las decisiones tomadas reducen verdaderamente los riesgos para usuarios y comunidades. En la práctica profesional, el buen juicio ético consiste en anticipar consecuencias, identificar impactos en grupos vulnerables, cuestionar decisiones técnicamente aceptables, pero socialmente dañinas y actuar bajo un principio de debido cuidado que vaya más allá del cumplimiento mínimo.



Figura 31. Ética profesional más allá de los checklist y las normas.

Fuente: Elaboración propia

4.3 Metodologías de análisis ético para la toma de decisiones

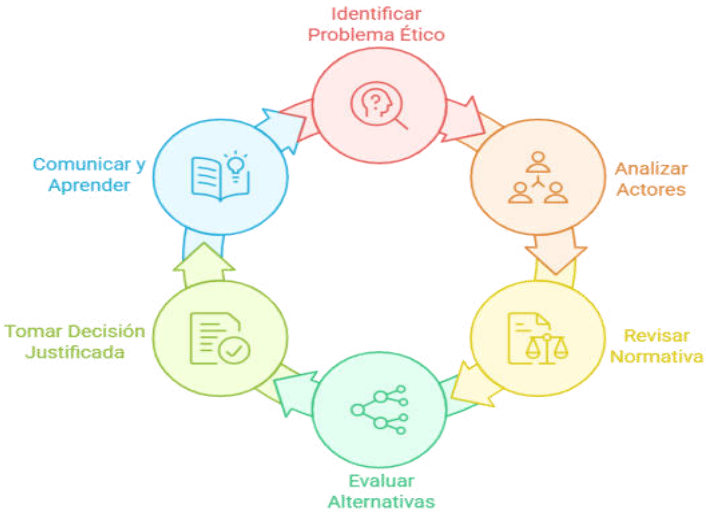


Figura 32. Ciclo de toma de decisiones éticas.

Fuente: Elaboración propia.

La toma de decisiones éticas en el ámbito tecnológico requiere un procedimiento estructurado que permita evaluar no solo la viabilidad técnica de una acción, sino también su impacto humano, organizacional y social. Una metodología formal evita decisiones impulsivas, sesgadas o basadas únicamente en requisitos funcionales, y promueve un enfoque profesional guiado por valores, responsabilidad y prevención del daño. A continuación, se presenta un modelo en seis etapas, diseñado para ser aplicado en situaciones reales que involucran privacidad, seguridad, inteligencia artificial, uso de datos, riesgos operativos y dilemas profesionales.

1. Identificación del problema ético y tecnológico.

El primer paso consiste en definir con precisión el dilema, distinguiendo entre el problema técnico (fallo, vulnerabilidad, acceso indebido, automatización, etc.) y el problema ético (riesgo a personas, afectación a la confianza, conflicto de interés, decisión injusta, manipulación, vigilancia desproporcionada, etc.).

En esta etapa es importante conocer qué está ocurriendo realmente, qué daños previsibles o potenciales existen y quienes podrían verse afectados.

2. Análisis de actores y partes afectadas.

Toda decisión tecnológica impacta a múltiples grupos: usuarios finales, ciudadanos, empleados, terceros, proveedores, la organización y la sociedad. Esta etapa se busca mapear intereses, vulnerabilidades y asimetrías de poder para comprender el alcance del dilema, además de detectar quienes son los posibles ganadores o perdedores con la decisión

a tomar y prever quienes son los actores que quedan vulnerables y a quienes se debe proteger especialmente.

3. Revisión normativa y marcos técnicos aplicables.

Aquí se evalúa qué leyes, estándares, políticas internas y mejores prácticas resultan pertinentes. La decisión ética debe estar alineada con obligaciones legales, normativas internacionales, códigos de conducta profesional y estándares de seguridad.

Se podría incluir análisis como lo determinan algunas normas tales como:

- ISO/IEC 27001 (gestión de seguridad)
- ISO/IEC 27002 (controles de seguridad)
- ISO/IEC 27701 (privacidad)
- ISO 22301 (continuidad)
- NIST CSF (ciberseguridad)
- Principios éticos de IA (equidad, no discriminación, explicabilidad)

De esta manera se puede identificar aquellas normas o políticas que resulten más relevantes y analizar los controles mínimos obligatorios.

4. Evaluación de alternativas y consecuencias.

Se deben construir varias opciones posibles, no solo la solución inmediata. Cada alternativa se analiza desde su impacto técnico, ético, legal y social utilizando métodos complementarios como análisis de consecuencias a corto, mediano y largo plazo, evaluaciones de riesgos con su probabilidad de impacto, identificación se sesgos y efectos colaterales; todo ese análisis podrá ayudar a minimizar el daño, proteger

la dignidad, privacidad y seguridad de las personas, injusticia y discriminación.

5. Toma de decisión ética justificada.

La decisión final debe estar basada en evidencia técnica, análisis normativo y un razonamiento ético explícito, de esta manera se deberá justificar las razones por las que se elige la alternativa, que valores y normas respaldan la decisión, que riesgos se eliminan y cuales permanecerán y si se deberá aplicar algún control adicional.

6. Comunicación, documentación y aprendizaje.

Finalmente hay que tener en cuenta que la ética también implica comunicar de forma clara lo ocurrido y documentar la decisión para auditorías futuras. Además, cada caso debe convertirse en una oportunidad de mejora para procesos, políticas y capacidades del equipo, Por esta razón en esta etapa final se deberá documentar el análisis realizado, detallar las lecciones aprendidas, actualizar las políticas y métricas para el seguimiento de las normas aplicadas.

4.4 Casos prácticos: análisis y soluciones

- Caso práctico sobre privacidad y protección de datos.

4.4.1 FinNova Capital: brecha de datos en una empresa de tecnología financiera



Figura 33. FinNova Capital: brecha de datos en una empresa de tecnología financiera.

FinNova Capital es una fintech que otorga microcréditos a trabajadores independientes. Su modelo de riesgo usa fuentes tradicionales (historial de pagos, ingresos declarados) y datos alternativos (geolocalización de cobros, comportamiento en la aplicación). Los datos residen en la nube y se comparten con un tercero de marketing para campañas de reenganche.

Un investigador de seguridad reporta que un contenedor de almacenamiento público expone un archivo CSV de 2,3 GB con 121 548 registros que incluyen: identificación, nombre, ingresos declarados, score interno, geolocalizaciones de cobros, teléfonos, correo, y estado de mora. El tercero de marketing había creado temporalmente el

contenedor para “pruebas A/B”, y la política de acceso quedó pública por error. Se detectan descargas no autorizadas durante 18 horas. Algunos clientes reportan phishing y solicitudes falsas de pago.

Todo ello recae en posibles multas por protección de datos, caída de confianza, mayor costo de fondeo, pérdida de clientes, y deterioro del valor de la cartera por fraude y suplantación. La dirección ejecutiva solicita: respuesta a incidentes inmediata, análisis ético-normativo, estimación del impacto económico, plan de remediación y lecciones para incorporar en el SGSI.

Cuestiones para discutir

1. ¿Qué datos fueron comprometidos y cómo se clasifican?
2. ¿Qué obligaciones legales y normativas aplican y qué acciones exige el cumplimiento?
3. ¿Cuáles son las causas raíz técnicas y organizacionales?
4. Propón un plan de respuesta a incidentes con hitos temporales (0-24 h, 24-72 h, 3-14 días).
5. ¿Cómo estimar el impacto económico de la brecha?
6. ¿Qué medidas de privacidad por diseño previenen recurrencia?
7. ¿Cómo debe fortalecerse el gobierno de terceros?
8. ¿Qué consideraciones éticas aplican al uso de datos en campañas comerciales?
9. ¿Qué KPI demuestran mejora y responsabilidad tras el incidente?
10. Define un plan de 90 días y competencias a reforzar.

Lectura ética del caso

El incidente de FinNova revela que la confianza económica se sostiene en la confianza digital. La brecha no solo expuso datos; expuso decisiones apresuradas, controles incompletos y un gobierno de terceros insuficiente. En una fintech, donde el producto es información y riesgo, la ética no es decorativa: exige minimizar la recopilación, justificar los usos, proteger con rigor, y comunicar con transparencia. La respuesta adecuada combina cumplimiento normativo, cuidado del cliente y criterio económico: contener y notificar rápido, compensar de forma proporcional, y demostrar con métricas que el sistema es hoy más seguro que ayer. La lección central es inequívoca: el valor de mercado de una organización financiera depende de su capacidad de prevenir daño, asumir responsabilidad y aprender; sin ello, cualquier ventaja competitiva se evapora junto a la confianza de sus usuarios.

Ruta de solución sugerida

1. ¿Qué datos fueron comprometidos y cómo se clasifican?

- Datos personales: nombre, número de cédula, correo electrónico, números telefónicos.
- Datos financieros sensibles: ingresos declarados, valores en la cuenta, estado de mora.
- Datos de comportamiento: geolocalización de cobros/visitas.
- Clasificación: Confidenciales/Sensibles (financieros y geolocalización), Confidenciales. Requieren cifrado en reposo y en tránsito, acceso bajo y registro de accesos.

2. ¿Qué obligaciones legales y normativas aplican y qué acciones exige el cumplimiento?

- Ley de protección de datos personales: deber de seguridad, notificación a la autoridad y a titulares en plazo razonable, registro del incidente y medidas de mitigación.
- ISO/IEC 27001/27002: controles de gestión de accesos, cifrado, relación con proveedores y respuesta a incidentes.
- ISO/IEC 27701 (privacidad): identificar roles para gestionar el alto riesgo y registro de solicitudes de titulares.
- NIST SP 800-61 (IR) / NIST CSF: ciclo de respuesta (preparar, detectar, contener, erradicar, recuperar, aprender).
- Acciones: notificar, contener, ofrecer medidas a usuarios, documentar, y demostrar responsabilidades.

3. ¿Cuáles son las causas raíz técnicas y organizacionales?

- Técnicas: contenedor en la nube con ACL pública, ausencia de DLP y de guardrails en IaC; falta de encriptación por campo y llaves gestionadas (KMS) en los extractos compartidos.
- Organizacionales: gobierno de terceros débil (sin revisión de permisos ni privilegios), falta de checklist de publicación de datos, ausencia de VDP formal, presión comercial para acelerar campañas.

4. Propón un plan de respuesta a incidentes con hitos temporales (0-24 h, 24-72 h, 3-14 días).

- 0-24 h (contención): cerrar acceso público, rotar llaves y credenciales, invalidar tokens, activar equipo de coordinación del incidente, conservar evidencias, reglas de bloqueo para dominios de phishing.

- 24-72 h (notificación y erradicación): confirmar alcance, notificar a autoridad y titulares; forzar cambio de contraseñas; habilitar línea de ayuda; IOC a socios; hardening del bucket.
- 3-14 días (recuperación y aprendizaje): pentest focalizado, revisión de permisos en la nube, implementar DLP, CSPM, políticas de tagging y cifrado en reposo, ejecutar DPIA post-incidente, plan de compensación.

5. ¿Cómo estimar el impacto económico de la brecha?

- Directos: respuesta, notificación, protección a clientes, multas y sanciones.
- Indirectos: caída en nuevos orígenes, incremento del costo de capital, tiempo improductivo, revisiones de aliados.
- Riesgos operacionales: fraude por suplantación, interrupciones por contención.
- Fórmula orientativa: Impacto total = Costos directos + (Clientes perdidos × tiempo de permanencia de clientes en la empresa) + Costo de fondeo × Volumen + Pérdidas por fraude estimado.

6. ¿Qué medidas de privacidad por diseño previenen recurrencia?

- Minimización y particionado de datasets por finalidad; tokenización/seudonimización para entornos de marketing.
- Cifrado por campo (PII/finanzas/geo) con KMS/HSM; almacenamiento privado con políticas denegación predeterminada.
- RBAC/ABAC con mínimo privilegio y vencimiento de permisos (JIT/JEA).

- DLP y CSPM para detectar exposición; pre-commit hooks y escaneo IaC.
- Retención limitada (TTL) y borrado verificable; clean rooms de datos para terceros.

7. ¿Cómo debe fortalecerse el gobierno de terceros?

- Contratos con SLA de seguridad, cifrado obligatorio, cláusula de protección para la VDP, derecho de auditoría, subprocesadores aprobados, notificación de incidentes ≤72 h.
- DPA (acuerdo de procesamiento de datos) con finalidad exclusiva, prohibición de uso secundario, y estándares mínimos (ISO 27001/27701 o equivalentes).
- incorporación con evaluación de riesgo, pentest/attestation y revisión periódica; acceso a datos solo tokenizados.

8. ¿Qué consideraciones éticas aplican al uso de datos en campañas comerciales?

- Autonomía y consentimiento: fines claros y opt-out real; no reutilizar datos de crédito para marketing sin base legítima.
- Proporcionalidad: evitar variables excesivas (geo granular histórica) si no aportan valor explicable.
- No maleficencia y justicia: evaluar sesgos en scoring por zona/ingresos; excluir proxies discriminatorios.
- Transparencia: informar criterios generales y canales de reclamo; AIA (evaluación de impacto algorítmico) en modelos críticos.

9. ¿Qué KPI demuestran mejora y responsabilidad tras el incidente?

- MTTD/MTTR de incidentes; % de buckets con cifrado + private ACL; cobertura de DLP/CSPM.

- Porcentaje de datos sensibles tokenizados.
- Porcentaje de accesos con MFA; Zero Standing Privileges.
- Porcentaje de terceros con auditoría vigente y SLA firmado; tiempo de notificación a titulares; tasa de phishing posterior.
- Cierre de hallazgos críticos menores o igual a 30 días y resultados de pentest.

10. Define un plan de 90 días y competencias a reforzar.

- 0-30 días: contención completada; DLP + CSPM activos; cifrado por campo; IAM mínimo privilegio; VDP público; capacitación express a marketing/ventas.
- 31-60 días: DPIA/AIA de modelos; contratos con terceros actualizados (SLA, auditoría, DPA); playbooks IR revisados; simulacro de breach.
- 61-90 días: Análisis de brechas y plan de certificación ISO 27001/27701; revisión posterior al incidente institucional; tablero de KPIs al comité.
- Competencias: responsabilidad profesional, gestión de riesgos, arquitectura segura, TPRM, respuesta a incidentes, comunicación ética y análisis económico.
- Caso de estudio sobre ciberseguridad.

4.4.2 VALORPAY: entre la prueba autorizada y el riesgo

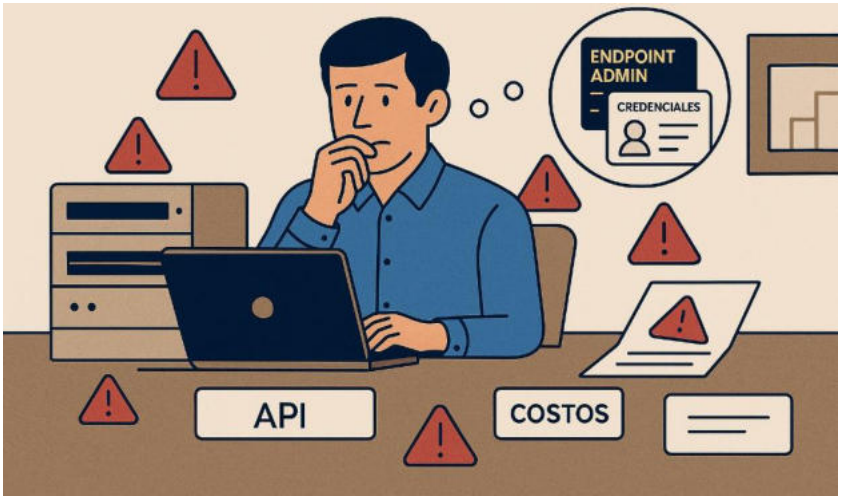


Figura 34. VALORPAY: entre la prueba autorizada y el riesgo.

VALORPAY es una fintech que procesa pagos para pequeños comercios. Para crecer, abre una API pública y contrata un pentest con alcance firmado sobre la API de pruebas y el portal de desarrolladores. A la par, el equipo comercial presiona para lanzar rápido una campaña que requiere analítica en tiempo real.

Una analista de seguridad detecta en producción un endpoint de administración expuesto por error tras un rollback de emergencia. El fallo permite enumerar claves de integración si se encadenan dos errores de validación. La analista documenta, reporta y propone bloquear temporalmente altas de nuevos comercios.

Durante la contención del incidente, el sistema alerta extracciones inusuales de logs hacia una IP residencial. El responsable de datos

afirma estar “corriendo diagnósticos” para ayudar a la analista. El patrón no cuadra con los runbooks y su cuenta no tiene ticket asociado.

Dos días después, un consultor externo envía por correo un “informe urgente” con capturas de producción y credenciales, alegando que “se adelantó” con pruebas no contempladas en el alcance para “mostrar proactividad”.

La interrupción parcial de la incorporación y las revisiones forenses elevan costos, mientras que tres comercios reportan intentos de fraude con claves antiguas. Hay presión de Dirección por “no parar el negocio”, pero el comité de riesgo exige decisiones éticas y responsables.

Preguntas de reflexión

1. ¿Cómo clasificar técnicamente la vulnerabilidad y qué medidas inmediatas tomar sin “romper” el negocio?
2. Ante la sospecha de extracción de logs por un empleado, ¿cómo actuar sin caer en cacerías de brujas?
3. ¿Qué diferencia ética y legal existe entre simulación controlada bajo contrato y pruebas fuera de contrato?
4. ¿Se debe detener totalmente la plataforma mientras se corrige?
5. ¿Cómo comunicar a clientes y aliados sin crear pánico ni opacidad?
6. ¿Qué gobierno de terceros faltó y cómo corregirlo?
7. ¿Cómo estimar el impacto económico de los tres incidentes combinados?
8. ¿Qué controles deben institucionalizarse para evitar repetición?

9. ¿Cómo cerrar el caso del consultor externo que probó fuera de alcance?
10. ¿Qué plan de 30/60/90 días y KPIs/KRIs propone el equipo?

Consideración final

VALORPAY nos recuerda que la ética profesional no es un adorno, sino el cimiento de la confianza económica. Una vulnerabilidad mal gestionada, una sospecha interna ignorada o una "prueba" entusiasta fuera de contrato pueden dañar más que un bug: erosionan la relación con clientes, encarecen el capital y comprometen la reputación. Actuar con responsabilidad significa frenar a tiempo, aunque cueste una métrica de crecimiento, escuchar las alertas sin prejuzgar a las personas, y respetar los límites incluso cuando la intención sea "ayudar". La práctica madura integra técnica y humanidad: contener sin paralizar, comunicar sin ocultar, aprender sin culpar, y convertir cada incidente en un peldaño de mejora. De este modo la seguridad deja de ser un gasto y se vuelve valor: menos pérdidas, más lealtad, mejores condiciones financieras y, sobre todo, un negocio que merece la confianza que recibe.

Orientación para el análisis

1. ¿Cómo clasificar técnicamente la vulnerabilidad y qué medidas inmediatas tomar sin romper el negocio?

Clasificación:

- Crítica: endpoint de administración expuesto y posibilidad de enumerar claves encadenando dos fallos de validación. Impacta confidencialidad e integridad y es explotable remotamente.

- Severidad: alta por alcance en producción y datos de alto valor (claves/credenciales de integración).

Medidas inmediatas:

Contención granular:

- Regla en WAF/ACL para bloquear el endpoint y/o segmentarlo.
- Rotar de forma preventiva todas las claves potencialmente afectadas.
- Congelar únicamente el alta de nuevos comercios por una ventana breve; mantener operaciones de pago ya activas.

2. Ante la sospecha de extracción de logs por un empleado, ¿cómo actuar sin caer en cacerías de brujas?

- Proporcionalidad y debido proceso:
- Congelar sesiones y tokens de la cuenta sin despedir ni exponer públicamente a nadie.
- Ajustar a mínimo privilegio mientras dura la revisión.
- Entrevista formal con registro, verificar ticket, cambios y justificación técnica.

3. ¿Qué diferencia ética y legal existe entre simulación controlada bajo contrato y pruebas fuera de contrato?

- Bajo contrato (válido): alcance definido, ventanas horarias, datos sintéticos, contactos 24/7, cadena de custodia y reporte coordinado.
- Fuera de contrato: no hay consentimiento ni límites; el riesgo de daño es real, aunque la intención sea ayudar. Es antiético y puede ser ilegal (acceso no autorizado, tratamiento indebido de datos, incumplimiento contractual).

- Acción: suspender accesos del consultor, exigir destrucción certificada de evidencias, abrir investigación y aplicar cláusulas contractuales (sanción/terminación).

4. ¿Se debe detener totalmente la plataforma mientras se corrige?

- Bloquear solo el flujo corporativo y rotar claves de integraciones afectadas.
- Mantener pagos en curso con telemetría reforzada (alertas sobre uso de claves antiguas).
- Reabrir progresivamente cuando: Primera línea de defensa activa, claves rotadas, métricas de intentos/errores a la baja y doble verificación.

5. ¿Cómo comunicar a clientes y aliados sin crear pánico ni opacidad?

- Mensaje claro y humano sin detalles explotables: Qué pasó, qué hicimos, qué debes hacer, rotar credenciales, revisar conciliaciones, activar alertas.
- Plazos y garantías con monitoreo reforzado a 30 días y un canal dedicado.
- Compensación proporcional si hubo impacto directo.
- Mantener coherencia con lo que dices a clientes y aliados.

6. ¿Qué gobierno de terceros faltó y cómo corregirlo?

- Faltó:
  - Alcance y límites de pruebas por escrito, SLA de seguridad, política de divulgación de vulnerabilidades, derecho de auditoría, cláusulas de manejo de datos
- Corregir:

- Anexos contractuales con consecuencias por violación (penalidades/terminación).
- Evidencias periódicas de controles (pentests, reportes de seguridad del proveedor).
- Acceso solo a ambientes no productivos y datos sintéticos.

7. ¿Qué tipo de escenarios plantearías y cada qué tiempo harías un control de incidentes?

- Se plantean res escenarios (conservador/base/adverso), actualizándolos semanalmente y vinculándolos al plan de mitigación a KPIs financieros.

8. ¿Qué controles deben institucionalizarse para evitar repetición?

Técnicos:

- Bloquear despliegues con endpoints y admin expuestos.
- Zero Trust en accesos privilegiados y rotación automática de secretos (KMS/secret manager).
- DLP más detección de anomalías para exfiltración de logs/datos.
- RBAC/ABAC y recertificación trimestral de accesos.
- Secure logging y retención limitada.

Procesos:

- Change management con puertas de seguridad y peer review.
- Parada ética: derecho/deber de frenar un lanzamiento inseguro.
- Programa de divulgación de vulnerabilidades con límites claros.

Personas:

- Formación continua en ética, respuesta a incidentes y privacidad.
- Runbooks actualizados y simulacros.

9. ¿Cómo cerrar el caso del consultor externo que probó fuera de alcance?

- Inmediato: revocar accesos, requerir entrega/destrucción de material, documentar cadena de custodia.
- Contractual: aplicar penalidades o terminación, según cláusulas; comunicar a su organización y registrar en lista de riesgo de proveedores.
- Aprendizaje: actualizar plantillas de contrato, reforzar el programa de divulgación de vulnerabilidades y diferenciar formalmente "investigación coordinada" vs. "acceso no autorizado".

10. ¿Qué plan de 30/60/90 días y KPIs/KRIs propone el equipo?

0 - 30 días (contención y saneamiento)

- WAF/ACL y hotfix auditados; rotación completa de claves; segmentación de endpoints admin; recertificación de accesos sensibles; tabletop de insider.
- KPIs: % claves rotadas, MTTR de la vulnerabilidad, intentos de enumeración bloqueados, identificar cuentas privilegiadas recertificadas.
- KRIs: alertas de exfiltración, errores de validación en endpoints críticos.

31 - 60 días (fortalecimiento y contratos)

- IaC con controls-as-code (bloqueos automáticos), DLP/CSPM activos, secure logging; actualización contractual con terceros (SLA/VDP/auditoría).

- KPIs: número de despliegues bloqueados por guardrails, número de proveedores con anexos firmados y evidencias, tiempo medio de notificación a clientes/regulador.
- KRIs: tasa de findings repetidos en pentest, frecuencia de accesos fuera de horario en cuentas privilegiadas.

61-90 días (auditoría y cultura)

- Auditoría interna, simulacro integral de crisis, tablero financiero de riesgo operativo; programa de formación y parada ética.
- KPIs: cierre de hallazgos críticos dentro de los primeros 30 días, cobertura de formación, satisfacción de clientes afectados.
- KRIs: variación mensual de incidentes, recurrencia por categoría.
- Casos de estudio sobre inteligencia artificial

4.4.3 TALENTOIA en Econofin: eficiencia, sesgo y decisiones



Figura 35. TALENTOIA en Econofin: eficiencia, sesgo y decisiones.

Econofin S.A. es una empresa del sector financiero - comercial que gestiona créditos y servicios para pequeñas y medianas empresas. En los últimos dos años, la organización ha sufrido un aumento de costos operativos (por gestión manual de reclutamiento y atención al cliente) y una presión creciente por mejorar productividad, reducir tiempos de contratación y disminuir la morosidad asociada a errores de evaluación. Para responder, la Dirección aprueba un programa de automatización con dos componentes: un sistema de IA para selección de personal llamado TALENTOIA y un módulo de decisión automática para asignar cupos y beneficios en el portal de clientes (por ejemplo, extensiones de plazo, reestructuraciones y límites transaccionales), ambos entrenados con datos históricos de "buen desempeño" y "baja pérdida crediticia".

Como primer incidente se evidenció un algoritmo discriminatorio en reclutamiento. A los seis meses, el área de RR. HH. observa que TALENTOIA rechaza con mayor frecuencia a postulantes provenientes de universidades públicas y a personas de zonas rurales, aun cuando cumplen con requisitos técnicos. Un auditor interno identifica que el modelo usa variables como código postal, institución de procedencia, continuidad laboral y tiempo hasta graduación, que funcionan como proxies socioeconómicos. Además, el proveedor no entregó evidencia de auditorías de equidad ni explicaciones claras. Los reclutadores, presionados por la meta de tiempo de contratación, aceptan la recomendación del algoritmo sin revisión.

Luego existió un segundo incidente teniendo una automatización que afectó derechos de usuarios. Paralelamente, el módulo de decisión

automática del portal reduce límites transaccionales y niega reestructuraciones a ciertos clientes sin explicación comprensible. Clientes reportan perjuicios económicos: retrasos en pagos a proveedores, penalidades contractuales y deterioro de reputación comercial. Se detecta que el modelo interpretó incorrectamente un patrón de comportamiento como riesgo elevado, y activó medidas restrictivas sin intervención humana.

Como un tercer incidente se tiene la responsabilidad ante decisiones autónomas incorrectas. Un cliente estratégico presenta una queja formal por trato injusto y solicita revisión. El área legal advierte que, aunque el sistema automatiza, la organización sigue siendo responsable. La Dirección enfrenta un dilema: detener la automatización reduciría riesgos reputacionales y legales, pero aumentaría costos operativos y retrasaría decisiones; mantenerla sin cambios podría profundizar daños y desconfianza. Se solicita un análisis basado en competencias para definir acciones correctivas, gobierno de IA y un plan de mitigación con indicadores económicos.

Guía de análisis

1. ¿Qué elementos del caso evidencian discriminación algorítmica en el reclutamiento?
2. ¿Qué variables son candidatas a “proxy” y por qué deben revisarse?
3. ¿Qué acciones inmediatas (0 - 72 h) son éticamente responsables ante los hallazgos?

4. ¿Cuándo debe exigirse supervisión humana significativa y derecho de apelación?
5. ¿Cómo aplicar normas y ética para analizar el dilema y decidir una solución?
6. ¿Qué medidas técnicas corrigen el sesgo sin destruir el valor predictivo del modelo?
7. En el portal de clientes, ¿por qué una decisión autónoma incorrecta afecta derechos y economía?
8. ¿Quién es responsable cuando la IA toma una decisión injusta o equivocada?
9. ¿Cómo evaluar el impacto económico del problema sobre reclutamiento y portal sin reducirlo a costos?
10. Propón un plan 30/60/90 días con KPIs/KRIs de ética y economía.

Reflexión del caso

El caso de Econofin muestra que la inteligencia artificial no solo automatiza procesos sino también puede ser capaz de automatizar consecuencias. Cuando un algoritmo decide quién accede a un empleo o quién mantiene su capacidad de operar económicamente, la ética deja de ser un discurso y se convierte en una obligación práctica. La discriminación algorítmica no siempre se presenta como una intención explícita; a menudo aparece como una eficiencia que replica desigualdades históricas con apariencia de objetividad. Por ello, gobernar IA no es un lujo sino es un requisito para sostener la legitimidad de la organización y la confianza del mercado.

En términos económicos, el costo de un sistema injusto no se limita a multas o incidentes: se manifiesta en pérdida de talento, deterioro de reputación, aumento en la tasa de abandono de clientes, aumento de soporte, y un riesgo acumulativo que encarece el negocio. La lección central es que la responsabilidad no se delega a la máquina: la institución que implementa IA debe garantizar transparencia, revisión humana significativa, mecanismos de apelación y auditorías que verifiquen equidad y corrección. Una empresa verdaderamente madura no pregunta solo ¿cuánto ahorra automatizando?, sino ¿qué daño podría causar si automatizo sin ética, sin controles y sin rendición de cuentas? En ese equilibrio entre eficiencia y dignidad se decide la calidad moral y también la sostenibilidad económica de la innovación tecnológica.

Propuesta de respuesta

1. ¿Qué elementos del caso evidencian discriminación algorítmica en el reclutamiento?

La evidencia está en el patrón estadístico de rechazo más alto hacia grupos específicos (universidades públicas y zonas rurales), junto con el uso de variables que actúan como proxies socioeconómicos (código postal, institución, continuidad laboral, tiempo hasta graduación). La discriminación puede ser indirecta ya que el sistema no usa una categoría prohibida, pero produce un efecto desigual sostenido. Éticamente, esto vulnera justicia y equidad, y profesionalmente exige revisión inmediata.

2. ¿Qué variables son candidatas a “proxy” y por qué deben revisarse?

Código postal, institución educativa, historial laboral lineal, tipo de empleo previo, duración de la carrera, certificaciones costosas o disponibilidad horaria total. Estas variables se correlacionan con acceso desigual a oportunidades y pueden excluir perfiles competentes. Deben revisarse porque pueden introducir sesgo estructural: el modelo premia privilegios históricos en vez de habilidades reales.

3. ¿Qué acciones inmediatas (0 - 72 h) son éticamente responsables ante los hallazgos?

- Pausar el uso del modelo como filtro final y pasar a modo asistido.
- Activar revisión humana de candidatos rechazados por el algoritmo en las últimas semanas.
- Congelar reglas automáticas del portal que restringen derechos sin explicación y habilitar un modo de uso humano.
- Comunicar internamente el incidente y abrir un expediente formal de análisis, preservando evidencia y registros de decisiones. Estas acciones minimizan daño y restablecen control.

4. ¿Cuándo debe exigirse supervisión humana significativa y derecho de apelación?

Siempre que la decisión tenga alto impacto como contratación/empleo, acceso a servicios financieros, límites transaccionales, reestructuraciones o restricciones que afecten continuidad de negocio del usuario.

5. ¿Cómo aplicar normas y ética para analizar el dilema y decidir una solución?

Podríamos implementar un modelo donde integre tres capas definidas tales como:

- Ética: Aplicando los principios de no maleficencia, justicia, transparencia y responsabilidad.
- Normas/estándares: gobernanza de seguridad y privacidad y marcos de IA responsable como la evaluación de impacto, trazabilidad y monitoreo.
- Decisión profesional: documentar alternativas, evaluar consecuencias, seleccionar la que reduzca más daño con viabilidad técnica y económica con la finalidad de convertir la ética en un procedimiento replicable, no solo en intención.

6. ¿Qué medidas técnicas corrigen el sesgo sin destruir el valor predictivo del modelo?

- Auditoría de datos: balance por subgrupos, identificación de variables proxy, limpieza de inconsistencias.
- Reentrenamiento con técnicas de reponderación o muestreo estratificado para representación justa.
- Ajustes de umbral por equidad y evaluación de métricas.
- Pruebas contrafactuales: cambiar solo la variable proxy (p. ej., código postal) y revisar si el resultado varía injustificadamente.
- Monitoreo continuo: detectar deriva y sesgos nuevos con el tiempo.

7. En el portal de clientes, ¿por qué una decisión autónoma incorrecta afecta derechos y economía?

Porque restringe capacidades transaccionales y acceso a reestructuración sin explicación ni revisión humana, causando daños reales: penalidades, retrasos de pago, pérdida de reputación comercial y ruptura de contratos. El error del algoritmo no es neutro: puede generar

consecuencias económicas en cascada. Éticamente se vulnera el principio de no maleficencia y el derecho del usuario a un trato justo y comprensible.

8. ¿Quién es responsable cuando la IA toma una decisión injusta o equivocada?

La organización sigue siendo responsable, siendo la IA una herramienta. La responsabilidad se distribuye operativamente entre los diferentes equipos de la organización, pero la responsabilidad final recae en la institución que decide usar el sistema, define su propósito y ejecuta decisiones con sus resultados. Por ello se requiere responsables, roles claros, trazabilidad, auditoría y posibilidad de revertir decisiones.

9. ¿Cómo evaluar el impacto económico del problema sobre reclutamiento y portal sin reducirlo a costos?

Se puede evaluar con un enfoque de costo total y riesgo:

- Reclutamiento: pérdida de talento, rotación por malas contrataciones, reputación empleadora, costos legales, disminución de diversidad y creatividad.
- Portal: Desvinculación de clientes, caída de ingresos de la empresa, aumento de quejas y soporte, riesgo de sanciones, pérdida de alianzas, incremento de morosidad por restricciones injustas.
- Se recomienda modelar escenarios y cuantificar costos operativos, pérdidas por incidentes y efectos reputacionales.

10. Propón un plan 30/60/90 días con KPIs/KRIs de ética y economía.

0 - 30 días (contención y control humano):

- IA en modo asistido; revisión humana para decisiones de alto impacto; canal de apelación; congelar reglas autónomas del portal más sensibles.
- KPIs: número de decisiones con revisión humana en casos críticos; tiempo de respuesta a apelaciones; reducción de quejas.
- KRIs: disparidad de tasas de rechazo por subgrupo; decisiones erróneas detectadas por muestreo.

31 - 60 días (auditoría y reentrenamiento):

- Auditoría de datos y variables proxy; reentrenamiento; métricas de imparcialidad; explicabilidad operativa, documentación y comité de IA.
- KPIs: mejora de métricas de equidad, cobertura de explicaciones, porcentaje de modelos auditados.
- KRIs: deriva de datos, incremento de rechazos desbalanceados.

61-90 días (gobernanza y sostenibilidad):

- Política de IA responsable, gestión de terceros, auditoría externa, monitoreo continuo, simulacros de incidentes, reportes ejecutivos.
- KPIs económicos: pérdida de clientes, pérdida de ingresos por clientes, tiempo de contratación, tasa de rotación temprana, costo de soporte por usuario.
- KRIs económicos: litigios/quejas formales, pérdidas por decisiones autónomas incorrectas, caída de confianza.
- Casos de estudio sobre decisiones éticas en proyectos tecnológicos reales.

4.4.4 SIGCOMPRAS-EC: transparencia, eficiencia y dilemas éticos en la contratación pública



Figura 36. SIGCOMPRAS-EC: transparencia, eficiencia y dilemas éticos en la contratación pública.

Una entidad pública en Ecuador decide modernizar su sistema de contratación pública mediante la implementación de SIGCOMPRAS-EC, una plataforma tecnológica para gestionar el ciclo completo de adquisiciones: planificación anual, términos de referencia, publicación de procesos, recepción de ofertas, evaluación, adjudicación, firma, ejecución contractual y seguimiento. El objetivo institucional es reducir tiempos, disminuir costos administrativos, mejorar la trazabilidad y fortalecer la transparencia. La presión es alta porque el presupuesto anual debe ejecutarse dentro de plazos definidos y la entidad busca evidenciar eficiencia ante órganos de control y ciudadanía.

Durante el despliegue piloto, el equipo de proyecto detecta tres tensiones principales:

- Riesgo de sesgo y discrecionalidad: el módulo de evaluación automatizada permite ponderaciones y criterios configurables; algunos responsables piden ajustes para favorecer proveedores habituales por confiabilidad, aun cuando esto podría afectar la libre competencia.
- Conflicto entre rapidez y control: la Dirección solicita habilitar un modo rápido que reduce pasos de validación para acelerar adjudicaciones, argumentando que si no se ejecuta el presupuesto se perdería.
- Integridad de datos y auditoría: se descubre que un proveedor externo propone una integración que permite editar registros post - adjudicación para corregir errores de forma, sin dejar trazabilidad completa. Esto podría abrir una puerta a manipulaciones.
- Además, el equipo recibe una alerta: un usuario interno con permisos amplios intentó exportar masivamente expedientes y ofertas incluyendo información sensible. La justificación verbal es que se requiere para un informe urgente, pero no existe solicitud formal ni ticket de soporte.

La Entidad exige que el proyecto se conduzca con decisiones éticas, alineadas a normativas internas, estándares de seguridad y buenas prácticas, garantizando que el sistema no solo funcione, sino que sea confiable y legítimo.

Preguntas para el análisis

1. ¿Cuál es el dilema ético central del caso y por qué tiene impacto económico?
2. ¿Qué riesgos se generan si se ajustan criterios para favorecer proveedores habituales?
3. ¿Qué controles técnicos y de gobernanza son no negociables antes de la puesta en marcha del sistema?
4. ¿Cómo evaluar éticamente el modo rápido propuesto por la Dirección?
5. ¿Qué debe hacerse ante la integración que permite editar registros post - adjudicación sin trazabilidad completa?
6. ¿Cómo actuar ante la alerta de exportación masiva de expedientes por un usuario interno?
7. ¿Qué indicadores económicos permiten medir si SIGCOMPRAS-EC está generando valor sin comprometer la ética?
8. ¿Qué metodología de análisis ético aplicar para tomar decisiones en este proyecto?
9. ¿Cómo gestionar la relación con el proveedor externo para garantizar integridad y transparencia?
10. Propón un plan para los 30, 60 y 90 días con KPIs/KRIs para ética, seguridad y economía.

Lectura ética del caso

El caso SIGCOMPRAS-EC evidencia que en la contratación pública la tecnología no solo automatiza trámites: automatiza confianza o desconfianza. Cuando un sistema permite ajustes discrecionales o

modificaciones sin trazabilidad, la plataforma deja de ser una herramienta de eficiencia y se convierte en un riesgo institucional. La presión por ejecutar presupuesto es real y tiene implicaciones económicas, pero no puede justificar la eliminación de controles que protegen el interés público. De hecho, los costos más altos no suelen venir del proceso lento, sino de las consecuencias de un proceso opaco: sobreprecios, impugnaciones, auditorías, litigios y pérdida de legitimidad.

Desde una perspectiva ética, el profesional de TI en el sector público debe recordar que su responsabilidad no se limita a que el sistema funcione; debe garantizar que el sistema sea justo, auditable y defendible. La decisión correcta no siempre es la más rápida, sino la que puede sostenerse ante la ciudadanía y los órganos de control con evidencia objetiva. Integrar normas, seguridad y ética convierte la plataforma en un activo económico: mejora la competencia, reduce riesgos y fortalece el uso eficiente de recursos públicos. En última instancia, la contratación pública digital solo cumple su promesa cuando la innovación tecnológica se alinea con la transparencia, la equidad y la rendición de cuentas.

Criterios para una posible solución

1. ¿Cuál es el dilema ético central del caso y por qué tiene impacto económico?

El dilema central es elegir entre eficiencia operativa inmediata e integridad del proceso. El impacto económico es directo ya que una plataforma manipulable aumenta el riesgo de compras ineficientes,

sobrecostos, sanciones, litigios, pérdida de competencia y desconfianza ciudadana. Además, eleva el costo de auditorías y correcciones futuras.

2. ¿Qué riesgos se generan si se ajustan criterios para favorecer proveedores habituales?

Se generan riesgos de discriminación y restricción de competencia, podría cancelarse el sistema debido a intereses particulares, ocasionar daño reputacional e incremento de auditorías y controversias, además de correr riesgo financiero teniendo adquisiciones más caras, menor calidad y potenciales nulidades o impugnaciones, cayendo en la pérdida de confianza del proveedor por no reemplazar reglas justas y verificables.

3. ¿Qué controles técnicos y de gobernanza son no negociables antes de la puesta en marcha del sistema?

Trazabilidad completa, segregación de funciones, control de cambios y aprobaciones formales, gestión de accesos, integridad documental, además del monitoreo y alertas.

4. ¿Cómo evaluar éticamente el modo rápido propuesto por la Dirección?

Aplicando proporcionalidad ya que, si el modo rápido elimina validaciones críticas, aumenta el riesgo de errores, favoritismos y fraude, una alternativa ética sería optimizar sin eliminar controles, por ejemplo: automatizar validaciones, usar plantillas estandarizadas, y habilitar un modo rápido solo para procesos de bajo riesgo y bajo monto con trazabilidad reforzada, dejando procesos sensibles con controles completos.

5. ¿Qué debe hacerse ante la integración que permite editar registros post - adjudicación sin trazabilidad completa?

Cualquier edición post - adjudicación debe quedar registrada documentando el motivo, responsable, aprobación, además de mantener historial de versiones, permitir auditoría y control.

6. ¿Cómo actuar ante la alerta de exportación masiva de expedientes por un usuario interno?

Suspender temporalmente la exportación masiva o limitarla por política, sin acusaciones inmediatas, solicitar justificación formal y ticket; revisar permisos y necesidad real, preservar evidencias y activar investigación interna con enfoque de debido proceso, además de ajustar accesos al mínimo necesario.

7. ¿Qué indicadores económicos permiten medir si SIGCOMPRAS-EC está generando valor sin comprometer la ética?

- Ahorro por competencia: variación entre presupuesto referencial y adjudicado.
- Tiempo de ciclo del proceso.
- Número promedio de oferentes por proceso.
- Costo administrativo por proceso.
- Tasa de impugnaciones/observaciones y su costo asociado.
- Cumplimiento de entregas y penalidades.

8. ¿Qué metodología de análisis ético aplicar para tomar decisiones en este proyecto?

- Identificar el dilema.
- Mapear afectados.
- Revisar normas internas y controles mínimos.

- Evaluar alternativas y consecuencias.
- Decidir con justificación y documentación.
- Comunicar y medir.

9. ¿Cómo gestionar la relación con el proveedor externo para garantizar integridad y transparencia?

- Contrato con SLA de seguridad y trazabilidad, derecho de auditoría y entrega de documentación técnica.
- Requisitos de control de cambios, evidencias de pruebas, y prohibición de funcionalidades que reduzcan auditabilidad.
- Revisiones técnicas y legales antes de integraciones sensibles.
- Plan de capacitación y transferencia de conocimiento para reducir dependencia.
- La relación debe basarse en evidencias verificables, no solo en confianza.

10. Propón un plan para los 30, 60 y 90 días con KPIs/KRIs para ética, seguridad y economía.

0-30 días (control y estabilización)

- Implementar trazabilidad fuerte, MFA, segregación de roles, límites de exportación.
- KPIs: número de módulos con auditoría activa; número de roles con mínimo privilegio; tiempo de detección de actividad anómala.
- KRIs: número de intentos de exportación masiva; cambios en criterios sin aprobación; accesos privilegiados fuera de horario.

31-60 días (optimización sin perder controles)

- Rediseñar el modo rápido con límites por riesgo/monto; automatizar validaciones; tablero de transparencia.

- KPIs: tiempo promedio de proceso con controles completos; número promedio de oferentes; ahorro estimado por competencia.
- KRIs: aumento de procesos con un solo oferente; incremento de observaciones o impugnaciones.

61-90 días (gobernanza y mejora continua)

- Auditoría interna, simulacro de incidente, comité de gobierno, capacitación a usuarios.
- KPIs: reducción de costos administrativos por proceso; cumplimiento de cronogramas; satisfacción de usuarios internos.
- KRIs: reincidencia de cambios no autorizados; incidentes de integridad; desviaciones presupuestarias repetitivas.

4.5 Metodologías de resolución y recomendaciones

Una metodología replicable para analizar dilemas reales sobre casos donde interviene la tecnología aplicando criterios éticos, con evidencia y trazabilidad priorizará siempre varios principios como: No maleficencia, justicia y equidad, transparencia, responsabilidad, proporcionalidad, legalidad y cumplimiento.

Las fases que intervienen son:

Fase 1. Definir el caso y el dilema:

- ¿Qué ocurrió? ¿Qué decisión está en juego?
- ¿Qué se considera éxito (técnico, legal, social, económico)?

Fase 2. Identificar actores y posibles afectados:

- Mapea partes interesadas y vulnerabilidades: Usuarios/ciudadanos, colaboradores, proveedores, entidad, reguladores, terceros.

Fase 3. Recopilar evidencia y hechos verificables:

- Logs, contratos, configuraciones, actas, versiones de software, correos, tickets.
- Evidencia con integridad (fecha, responsable, hash si aplica).

Fase 4 Revisar normas y marcos aplicables:

- Leyes vigentes, políticas internas, estándares (seguridad, privacidad, continuidad, auditoría), códigos profesionales.

Fase 5 Evaluar alternativas con análisis de riesgo ético:

- Define de 2 a 4 opciones reales.

Paso 6 Decidir, justificar y documentar:

- Seleccionar la opción con menor daño y mejor defendibilidad.
- Registrar: por qué se eligió, qué riesgos quedan, y cómo se mitigarán.

Paso 7 Comunicar, ejecutar y aprender:

- Comunicación proporcional (internos, usuarios, autoridad, proveedores).
- Plan de acción con responsables y plazos.

- Lecciones aprendidas y actualización de políticas.

Taxonomía rápida de riesgos éticos en TI:

- Privacidad: recolección excesiva, retención indefinida, acceso indebido.
- Seguridad: negligencia, exposición de datos, ausencia de controles mínimos.
- Equidad: sesgos en IA, reglas de evaluación manipulables, favoritismos.
- Transparencia: decisiones opacas, falta de trazabilidad, cambios sin registro.
- Integridad profesional: conflictos de interés, comisiones, presión indebida.
- Derechos: automatización sin revisión humana, ausencia de apelación.

Recomendaciones operativas para casos éticos:

- Definir dilema y alcance (qué está en juego).
- Identificar afectados y riesgos (personas/organización/terceros).
- Preservar evidencia (logs, tickets, contratos).
- Revisar normas/políticas aplicables.
- Generar alternativas y evaluar impactos.
- Aplicar mitigación inmediata si hay daño probable.
- Documentar decisión y responsables.
- Implementar canal de revisión/apelación si lo amerita el caso.

- Medir KPIs/KRIs y auditar cierre.
- Lecciones aprendidas y actualización de políticas.

La ética se vuelve operativa cuando existen un método, evidencia y funciones claramente asignadas. Auditar no consiste únicamente en comprobar requisitos; también permite demostrar que las decisiones fueron razonables, proporcionales y defendibles.

Los comités reducen arbitrariedad, controlan presiones internas y protegen a la institución ante terceros; sin embargo, el análisis de riesgo ético es el que conecta valores con impacto económico y evita costos futuros por incidentes, sanciones, litigios o pérdida de confianza.

4.6 Aprendizajes para el ejercicio profesional

La excelencia técnica resulta insuficiente si no está respaldada por integridad ética y cumplimiento normativo. Cuando los sistemas administran datos sensibles, automatizan decisiones o sostienen servicios críticos, la responsabilidad del profesional de TI se refleja en su capacidad para anticipar riesgos, proteger a las personas y rendir cuentas con evidencia verificable. Postergar la seguridad, la privacidad o la trazabilidad por razones de tiempo o presupuesto puede convertir un ahorro inmediato en incidentes, sanciones, litigios y pérdida de confianza.

Un aprendizaje clave es que las normas y estándares no deben verse como burocracia, sino como una forma de convertir la ética en práctica operativa: políticas, controles, procesos, métricas y responsabilidades.

Este libro deja claro que el cumplimiento real se logra cuando convergen: leyes (obligaciones mínimas), normas (estructura y consistencia) y mejores prácticas (eficiencia probada), guiadas por principios éticos como no maleficencia, justicia, transparencia, responsabilidad y bien común. Esa convergencia se traduce en decisiones concretas: detener un despliegue inseguro, incorporar revisión humana en automatización crítica, auditar un modelo de IA por sesgos, o rechazar integraciones que permitan cambios sin trazabilidad.

Otro aprendizaje central es que la ética no se limita a "intenciones correctas"; exige método, evidencia y gobernanza. La toma de decisiones éticas se fortalece cuando la organización institucionaliza el análisis de riesgos, auditorías y registros, mecanismos de respuesta a incidentes, comités con autoridad real, y seguimiento con KPIs/KRIs. Esto reduce la arbitrariedad, hace el control defendible ante auditorías y, sobre todo, protege derechos (privacidad, acceso justo, dignidad) en contextos digitales donde un error puede escalar a miles de personas.

Finalmente, el ejercicio profesional ético se consolida cuando el ingeniero en TI asume su rol como garante de integridad, seguridad y justicia tecnológica. Esto implica actuar con competencia y actualización continua, resistir presiones que comprometan controles críticos, gestionar conflictos de interés, y comunicar de forma transparente.

4.7 Síntesis transversal del capítulo

Los casos de este capítulo reúnen los principales hilos desarrollados a lo largo del libro: obligaciones legales, normas técnicas, principios éticos, derechos digitales, responsabilidad profesional y gobierno organizacional. Aunque los escenarios pertenecen a sectores diferentes, comparten una misma dificultad sobre las decisiones tecnológicas las cuales deben adoptarse bajo presión y con información que puede ser incompleta, mientras sus consecuencias alcanzan a usuarios, empleados, clientes, proveedores e instituciones.

El análisis transversal permite reconocer una secuencia común. Primero se define el dilema y se identifican las partes afectadas; después se reúnen evidencias, se revisan las normas aplicables y se comparan alternativas; finalmente se decide, se documenta, se comunica y se evalúan los resultados, esta secuencia evita respuestas improvisadas y facilita que una decisión pueda ser explicada, auditada y corregida.

Los casos de los ámbitos financiero, laboral, educativo, sanitario y de contratación pública también evidencian que la confianza constituye un resultado acumulativo, se fortalece cuando la organización protege los datos, reconoce límites, escucha alertas, controla los conflictos de interés y ofrece mecanismos de revisión en contraste se debilita cuando la rapidez, el beneficio inmediato o la apariencia de cumplimiento desplazan la seguridad, la transparencia y la equidad.

Para estudiantes y profesionales la conclusión práctica es que el cumplimiento debe convertirse en una capacidad organizacional lo cual

requiere personas competentes, responsabilidades claras, controles proporcionales, documentación útil y espacios donde los dilemas puedan discutirse antes de causar daño, de este modo, la ética deja de ser un discurso separado de la ingeniería y se integra en decisiones que sostienen servicios confiables, organizaciones responsables y relaciones empresariales duraderas.

GLOSARIO DE TÉRMINOS

Accesibilidad digital: Conjunto de prácticas para que sistemas y contenidos sean utilizables por todas las personas, incluyendo aquellas con discapacidad, sin barreras técnicas o de diseño.

Acceso basado en atributos (ABAC): Modelo de control de acceso que autoriza según atributos (rol, contexto, ubicación, hora, sensibilidad del dato) y reglas.

Acceso basado en roles (RBAC): Modelo de control de acceso que asigna permisos según roles (administrador, analista, usuario, etc.) para aplicar mínimo privilegio.

Accountability (Responsabilidad demostrable): Capacidad de una organización o profesional para explicar y evidenciar decisiones, controles y resultados ante auditoría o incidentes.

Amenaza: Evento o actor potencial que puede explotar una vulnerabilidad y causar impacto en información o servicios.

Análisis de riesgos: Proceso para identificar amenazas, vulnerabilidades, impactos y probabilidad; base para decidir controles y prioridades.

Análisis ético: Evaluación estructurada de un dilema considerando afectados, normas, consecuencias y principios éticos para decidir de forma justificable.

Apelación (en decisiones automatizadas): Mecanismo para impugnar una decisión de un sistema y solicitar revisión humana y corrección.

Arquitectura segura: Diseño de sistemas incorporando controles de seguridad y privacidad desde el inicio (security/privacy by design).

Auditoría (de TI): Proceso independiente y sistemático para evaluar controles, cumplimiento y eficacia de la gestión tecnológica.

Auditoría algorítmica: Evaluación de modelos de IA para verificar equidad, sesgos, trazabilidad, explicabilidad y desempeño por subgrupos.

Backups (copias de seguridad): Copias de datos para recuperación; deben ser cifradas, probadas y alineadas a las métricas de continuidad y recuperación del negocio ante los desastres.

Bien común: Principio ético que orienta decisiones hacia beneficios colectivos, no solo individuales.

Brecha de seguridad / Brecha de datos: Evento que expone o compromete información por acceso no autorizado, pérdida, alteración o divulgación indebida.

Cadena de custodia: Procedimiento para preservar evidencia digital con integridad y trazabilidad (quién la tuvo, cuándo y cómo).

Ciberseguridad: Disciplina que protege sistemas, redes y datos frente a ataques, fallos o usos indebidos mediante controles técnicos y organizativos.

Cifrado: Técnica que protege datos transformándolos para que solo sean legibles con una clave autorizada (en tránsito y en reposo).

Cifrado por campo: Cifrado aplicado a atributos específicos, útil cuando el cifrado de disco no es suficiente.

CI/CD: Integración y entrega/despliegue continuo; facilita automatizar pruebas, controles y puertas antes de liberar cambios.

Ciclo PDCA: Modelo de mejora continúa usado en sistemas de gestión como ISO 27001.

Clasificación de la información: Etiquetado de datos según sensibilidad para aplicar controles adecuados.

COBIT: Marco de gobierno y gestión de TI orientado a alinear tecnología con objetivos, riesgos y valor.

Comité de seguridad / Comité de ética tecnológica: Órgano colegiado que define criterios “no-go”, gestiona excepciones, revisa riesgos y decide con evidencia.

Consentimiento informado: Aceptación libre y comprensible del titular de datos sobre recolección y uso, con posibilidad de revocar.

Contención (respuesta a incidentes): Acciones inmediatas para frenar un incidente (bloquear accesos, rotar claves, aislar sistemas) y evitar propagación.

Continuidad del negocio (BCP): Plan para mantener servicios críticos ante interrupciones.

Control de cambios: Proceso formal para aprobar, registrar y auditar cambios en sistemas, configuraciones y despliegues.

Conflicto de interés: Situación donde beneficios personales/económicos pueden sesgar decisiones técnicas o institucionales.

Cumplimiento (Compliance): Estado de adherencia a leyes, regulaciones, normas y políticas aplicables; requiere controles y evidencia.

Datos sensibles: Datos de mayor riesgo por su naturaleza (salud, finanzas, ubicación, etc.); exigen controles reforzados.

Debida diligencia: Actuación profesional responsable y preventiva; implica anticipar riesgos y aplicar controles razonables.

Derecho al olvido (supresión): Derecho del titular a solicitar eliminación de datos cuando procede por normativa o política.

Derechos digitales: Extensión de derechos humanos al entorno digital (privacidad, acceso, seguridad, participación, etc.).

DevSecOps: Integración de seguridad en DevOps: seguridad embebida en el ciclo de vida con automatización y controles continuos.

DLP (Data Loss Prevention): Controles para prevenir fuga/exfiltración de datos.

DPIA/PIA (Evaluación de impacto en privacidad): Análisis formal de riesgos para derechos y libertades al tratar datos personales, con mitigaciones.

DRP (Plan de recuperación ante desastres): Estrategia para restaurar sistemas y datos tras fallos graves.

Evidencia digital: Registros, logs, artefactos y documentos que prueban hechos y decisiones; debe preservarse con integridad.

Equidad / No discriminación: Principio ético que exige evitar sesgos injustos en sistemas y decisiones, especialmente en IA.

Escalamiento: Proceso de elevar una alerta o caso crítico a niveles de autoridad (comité, dirección, regulador).

Estándar: Documento técnico aprobado por organismos reconocidos (ISO, IEC, IEEE) que define especificaciones o metodologías.

Ética algorítmica: Aplicación de principios éticos al diseño y uso de algoritmos/IA: equidad, explicabilidad, trazabilidad y control humano.

Fairness (equidad algorítmica): Conjunto de criterios y métricas que evalúan si un modelo trata de forma justa a distintos grupos.

Firma/Integridad documental: Mecanismos para asegurar que documentos no se alteren sin rastro.

Forense digital: Técnicas para investigar incidentes preservando evidencia y reconstruyendo eventos con rigor.

Fuera de alcance (out-of-scope): Actividades no autorizadas en pruebas que vulneran el contrato y la ética.

Gobernanza de TI: Sistema de dirección y control para alinear TI con objetivos, valor y gestión de riesgos.

Gobierno de terceros (TPRM): Gestión de riesgos de proveedores: SLA de seguridad, derecho de auditoría, evidencias y controles contractuales.

Grey hat / White hat / Black hat: Tipos de hacking por intención y autorización: ético (white), ambiguo (grey), malicioso (black).

Hardening: Endurecimiento de sistemas para reducir superficie de ataque.

Hito (plan 30/60/90): Entregable y fecha verificable dentro de un plan de remediación por etapas.

IA (Inteligencia artificial): Sistemas que aprenden patrones de datos para apoyar o automatizar decisiones; requiere controles éticos y de gobernanza.

Impacto económico del riesgo: Costos directos e indirectos de incidentes (multas, pérdida de clientes, fraude, pérdida reputacional, costo de capital).

Incidente de seguridad: Evento que compromete confidencialidad, integridad o disponibilidad; activa respuesta y notificación.

INEN: Organismo ecuatoriano de normalización que promueve estándares técnicos.

ISO/IEC 27001: Norma para implementar un Sistema de Gestión de Seguridad de la Información (SGSI).

ISO/IEC 27002: Guía de controles de seguridad que complementa 27001.

ISO/IEC 27701: Extensión orientada a gestión de privacidad y controles para datos personales.

ISO 22301: Norma para gestión de continuidad del negocio.

ITIL: Marco de gestión de servicios de TI para calidad, operación y mejora continua.

Jurisdicción y ley aplicable: Determinación de qué marco legal rige el tratamiento de datos o servicios, especialmente en contextos transfronterizos.

KMS/HSM: Servicios/dispositivos para gestión y custodia segura de claves criptográficas (control, rotación, auditoría).

KPI/KRI: Indicadores: KPI mide desempeño; KRI mide exposición al riesgo, por ejemplo: intentos de exportación masiva, hallazgos críticos.

Logs inmutables (WORM): Registros protegidos contra alteración, esenciales para auditoría y forense.

MFA (Autenticación multifactor): Control de acceso que combina dos o más factores y reduce suplantación.

Mejores prácticas: Técnicas/metodologías probadas que elevan calidad y seguridad; suelen complementar normas y leyes.

Minimización de datos: Recolectar y tratar solo lo estrictamente necesario para una finalidad legítima.

Mitigación: Medida preventiva o correctiva que reduce probabilidad o impacto de un riesgo.

NIST: Marco y guías para gestión de riesgos y ciberseguridad; referencia técnica ampliamente utilizada.

No maleficencia: Principio ético: "no causar daño", especialmente ante riesgos previsibles en TI.

Norma: Documento técnico/gestión por consenso (ISO, IEEE, IETF) para interoperabilidad, calidad y seguridad.

Normativa: Directriz o especificación que regula criterios técnicos y de gestión en TI.

OWASP: Referencia de riesgos y prácticas de seguridad para aplicaciones por ejemplo OWASP Top 10.

Organismos reguladores nacionales: Entidades estatales que emiten políticas/regulación vinculada a TI y telecomunicaciones por ejemplo ARCOTEL, MINTEL.

Pentest (Prueba de penetración): Evaluación controlada de seguridad para identificar vulnerabilidades explotables, con alcance y autorización.

Política (interna): Regla institucional que define comportamientos esperados, responsabilidades y procedimientos sobre TI.

Portabilidad de datos: Derecho a recibir datos en formato estructurado y transferible a otro servicio.

Privacidad por defecto: Configuración inicial que protege datos sin requerir acción del usuario.

Privacidad por diseño: Integración de privacidad desde la arquitectura y el ciclo de vida del sistema.

Proxy: Variable aparentemente neutral que representa indirectamente un rasgo sensible (p. ej., código postal como proxy socioeconómico).

Regulación: Instrumento legal obligatorio emitido por autoridades para gobernar actividades TI en una jurisdicción.

Rendición de cuentas: Obligación de responder y demostrar acciones, decisiones y resultados con evidencia verificable.

Retención de datos: Periodo durante el cual se conservan datos; debe ser limitado y justificado, con eliminación verificable.

RTO/RPO: Objetivos de recuperación (tiempo máximo de recuperación y pérdida máxima de datos aceptable).

Runbook: Guía operativa paso a paso para responder a incidentes o ejecutar procedimientos críticos.

Segregación de funciones: Separación de responsabilidades para evitar que una misma persona controle todo el proceso.

Sesgo algorítmico: Distorsión sistemática en resultados de IA que produce efectos injustos en ciertos grupos.

SIEM: Plataforma para correlación y análisis de eventos de seguridad, alertas y monitoreo centralizado.

SGSI: Sistema de Gestión de Seguridad de la Información que contiene políticas, riesgos, controles y mejora continua.

SLA (seguridad): Acuerdo de nivel de servicio con proveedores que fija obligaciones de seguridad, tiempos y evidencia.

SSDLC (Ciclo de desarrollo seguro): Integración de seguridad en todas las etapas del desarrollo tales como requisitos, diseño, pruebas, despliegue.

Trazabilidad: Capacidad de reconstruir qué ocurrió, quién actuó y por qué, clave para auditoría.

TPRM (Third-Party Risk Management): Gestión de riesgos por terceros; incluye auditorías, contratos, controles y monitoreo.

UGC (Contenido generado por usuarios): Publicaciones de usuarios (comentarios, reseñas, imágenes) que requieren moderación proporcional, transparencia y apelación.

VDP (Política de divulgación de vulnerabilidades): Canal y reglas para recibir reportes de fallos y gestionar divulgación responsable con plazos.

Vulnerabilidad: Debilidad que puede ser explotada por una amenaza; requiere evaluación, priorización y remediación.

WAF: Firewall de aplicaciones web; filtra y bloquea ataques comunes.

WORM (Write Once Read Many): Modelo de almacenamiento inmutable para registros/auditoría.

Zero Trust: Enfoque de seguridad que no confía por defecto; verifica cada acceso y segmenta privilegios continuamente.

Zero Standing Privileges (ZSP): Eliminación de privilegios permanentes; se otorgan solo cuando son necesarios.

REFERENCIAS BIBLIOGRÁFICAS

Boeckl, K. R., & Lefkovitz, N. B. (2020). NIST Privacy Framework: A tool for improving privacy through enterprise risk management, Version 1.0 (NIST CSWP 01162020). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.01162020

Center for Internet Security. (2024). NIST Cybersecurity Framework policy template guide (MS-ISAC). https://www.cisecurity.org/-/media/project/cisecurity/cisecurity/data/media/files/uploads/2024/08/cis-ms-isac-nist-cybersecurity-framework-policy-template-guide-2024.pdf

International Organization for Standardization. (s. f.). Standards in our world: What are standards and how do they help? ISO. https://www.iso.org/sites/ConsumersStandards/1_standards.html

National Institute of Standards and Technology. (2015, September 29). Cybersecurity Framework FAQS: Framework basics. https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-basics

National Institute of Standards and Technology. (2025, April 2). Assessment & auditing resources (NIST Cybersecurity Framework). https://www.nist.gov/cyberframework/assessment-auditing-resources

Organisation for Economic Co-operation and Development. (s. f.). Privacy principles. OECD. https://www.oecd.org/en/topics/privacy-principles.html

The Editors of Encyclopaedia Britannica. (2026, February 6). Ethics. In Encyclopaedia Britannica. https://www.britannica.com/topic/ethics-philosophy

UNESCO. (2026, January 30). Constitution [Constitution of the United Nations Educational, Scientific and Cultural Organization]. https://www.unesco.org/en/legal-affairs/constitution

Del cumplimiento a la confianza empresarial: Normativas y ética profesional en las TI, se publicó en el mes de noviembre de 2026.

ISBN: 978-9907-852-11-0

Grupo Editorial BLR
Ecuador
Cel: +593 98 320 4362
https://grupoblr.com/
publicaciones@grupoblr.com

BIOGRAFÍA DE AUTORES

Joofre Antonio Honores Tapia:

Es Ingeniero de Sistemas, Magíster en Docencia y Gerencia en Educación Superior, además, magíster en Ciencia de Datos Aplicada. Ha ejercido la docencia universitaria en áreas de programación, sistemas operativos, redes, ética profesional y Normativas en Tecnologías de la Información.

Entre la producción bibliográfica destacan dos manuales de referencia editados por UTMACH: Nociones de Ingeniería de Software (2015) y Fundamentos de base de datos (2016). Estas obras han servido como apoyo curricular y base metodológica en la enseñanza de ingeniería de software y bases de datos. En 2018 amplió su aporte con el libro SNAIL: una metodología híbrida para el desarrollo de aplicaciones web, publicado por 3 Ciencias/Área de Innovación y Desarrollo, ese mismo año participó en la CERI 2018 (ACM) con el trabajo "Trends in the creation of Spanish web sites and their active service", resultado de colaboración con investigadores de la Universidad de da Coruña.

Nicole Yeslaine Mora Encalada:

Es Economista con mención en Gestión Empresarial por la Universidad Técnica de Machala y Magíster en Administración Pública con mención en Desarrollo Institucional por la Universidad Estatal de Milagro. Actualmente cursa su segunda maestría en Compras Públicas.

En el ámbito profesional, se ha desempeñado en la Universidad Técnica de Machala como Analista de Refrendación y Registro de Títulos, y como Analista de Gestión de Actas y Resoluciones, desarrollando funciones relacionadas con gestión documental, control normativo, archivo institucional y formalización de actos administrativos. Asimismo, cuenta con experiencia en el Gobierno Autónomo Descentralizado Municipal de Machala en procesos vinculados con compras públicas, ínfimas cuantías, reforma al PAC, POA y subasta inversa electrónica.

DEL CUMPLIMIENTO A LA CONFIANZA EMPRESARIAL: NORMATIVAS Y ÉTICA PROFESIONAL EN LAS TI

Estimado lector, este libro fundamenta la ética y la regulación jurídica no como anexos burocráticos del quehacer técnico, sino como el principio estructural sobre el cual se edifica la confianza en las Tecnologías de la Información.

En un contexto donde el software y la conectividad median en la salud, las finanzas y la gestión pública, la obra sostiene que cada decisión de diseño algorítmico, directriz de acceso o arquitectura de ciberseguridad incide directamente sobre derechos fundamentales como la privacidad, la equidad y la seguridad de las personas.

A lo largo de sus capítulos, el texto articula los marcos legales, estándares internacionales y mejores prácticas con dilemas contemporáneos de la sociedad digital: la reputación en línea, la gobernanza y uso responsable de datos, la mitigación de brechas informáticas y los desafíos éticos derivados de la inteligencia artificial y las decisiones automatizadas en contextos corporativos y sociales.

El capítulo final consolida un entorno de entrenamiento profesional mediante el análisis de casos reales, preparando al lector para resolver conflictos de interés, presiones institucionales y fallos de seguridad bajo condiciones operativas restringidas.

Dirigida a estudiantes, docentes y especialistas del área, la obra busca formar un criterio deontológico riguroso que promueva la rendición de cuentas, la protección de los usuarios y una evolución tecnológica alineada con la dignidad humana.

GRUPO BLR

Grupo Editorial BLR
Ecuador
Cel: +593 98 320 4362
https://grupoblr.com/
publicaciones@grupoblr.com

ISBN: 978-9907-852-11-0

UNIVERSIDAD TÉCNICA DE MACHALA
1969