

ESTÁNDARES, NORMAS Y LEGISLACIÓN DE SEGURIDAD

Payment Card Industry Data Security Standard (PCI DSS)

La seguridad no solo es relevante para quienes trabajan directamente en el área, sino también para el **usuario final**, para **el ciudadano**, para **el empresario**, para **la empresa** y para cualquier **organización**.

Es fundamental tener en cuenta estos aspectos al momento de realizar acciones relacionadas con la **seguridad informática**. Para ello, es necesario conocer y aplicar **estándares** y **normativas** que pueden ser tanto **nacionales** como **internacionales**. Estas normas nos indican cómo actuar correctamente dentro del marco legal.

Como ciudadanos informados, debemos saber que toda actividad vinculada a la seguridad debe estar enmarcada dentro de la ley. Hoy en día, muchas de las prácticas relacionadas con la "cibercomunidad" o con pruebas de seguridad se tergiversan. Algunas incluso se convierten en prácticas ilegales, aunque se realicen con buena intención.

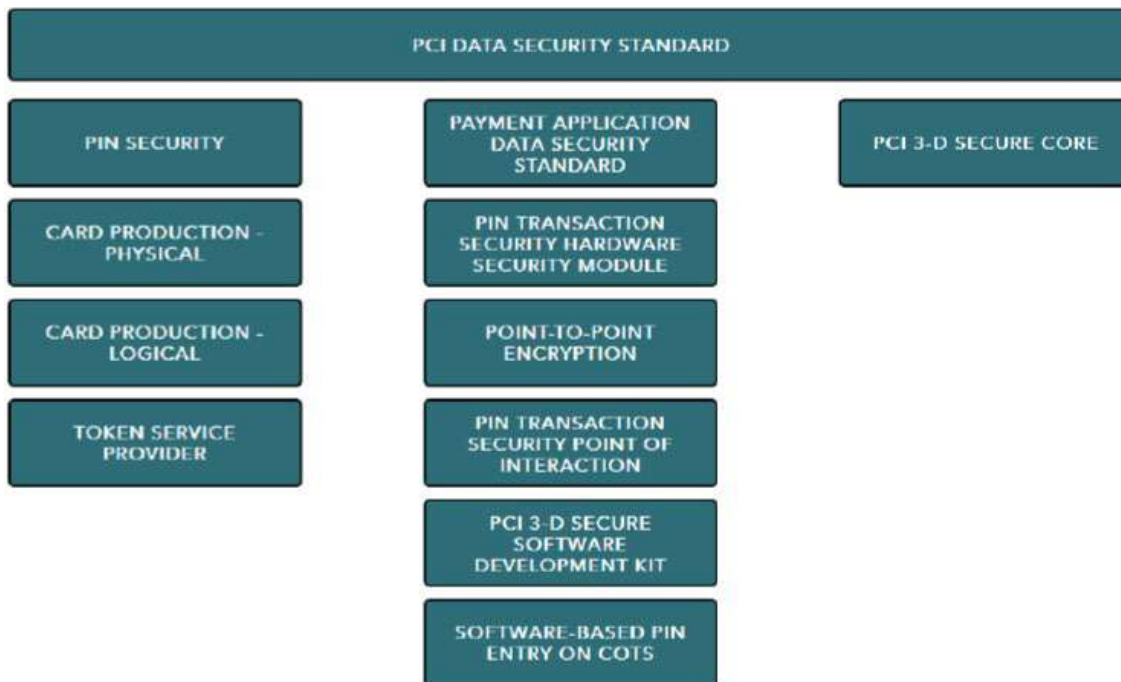
Por ejemplo, probar herramientas que se encuentran en internet sin autorización, o ejecutar ensayos sobre sistemas ajenos, es algo que **no está permitido**. Existen formas legales y éticas de realizar pruebas, análisis y estudios en el ámbito de la **seguridad defensiva u ofensiva**, pero siempre dentro del marco de la **legislación vigente** en temas de **derechos informáticos**.

Por eso, es crucial tener conciencia sobre la **legalidad** de nuestras acciones. Se pueden hacer pruebas, se puede estudiar el funcionamiento de sistemas, pero sin afectar a terceros ni violar la privacidad o integridad de otros dispositivos o plataformas.

Payment Card Industry Data Security Standard (PCI DSS)

PCI Security Standards Council

Es un foro mundial abierto destinado a la formulación, la mejora, el almacenamiento, la difusión y la aplicación permanente de las normas de seguridad para la protección de datos de cuentas correspondientes a tarjetas de pago.



<https://www.pcisecuritystandards.org>

Estándar Principal

PCI Data Security Standard (PCI DSS)

- Es el **estándar base y obligatorio** para cualquier organización que procese, almacene o transmita datos de tarjetas de crédito.
- Define controles técnicos y operativos para proteger los datos del titular de la tarjeta.

Segmento: Seguridad de PIN y Producción de Tarjetas

◆ PIN Security

- Asegura la protección del **PIN del titular de la tarjeta** desde el punto de entrada hasta el procesamiento.
- Aplica a cajeros automáticos, POS y redes bancarias.

◆ Card Production – Physical

- Controla la seguridad física en la **fabricación y personalización** de tarjetas (grabado, chip, empaque).

◆ Card Production – Logical

- Define requisitos para la **gestión digital de datos de tarjetas**, como personalización lógica, generación de claves y scripts.

◆ Token Service Provider

- Regula a quienes **reemplazan datos reales de tarjeta por “tokens”**, minimizando el riesgo en transacciones digitales.

Segmento: Aplicaciones, Hardware y Cifrado

◆ Payment Application Data Security Standard (PA-DSS)

- Normas para **aplicaciones de pago** (por ejemplo, software POS) que almacenan, procesan o transmiten datos de tarjetas.

◆ PIN Transaction Security Hardware Security Module (PTS HSM)

- Estándar para el **hardware criptográfico** que protege datos de PIN y claves de cifrado durante el procesamiento.

◆ Point-to-Point Encryption (P2PE)

- Define cómo **cifrar datos desde el punto de captura (POS)** hasta el entorno seguro del proveedor, protegiendo de sniffers o malware.

◆ PIN Transaction Security Point of Interaction (PTS POI)

- Aplica a dispositivos como **terminales POS o cajeros**, asegurando que el hardware cumple estándares de seguridad para capturar PIN.

Segmento: Seguridad en entornos digitales y móviles

◆ PCI 3-D Secure Software Development Kit (SDK)

- Guía para integrar **3-D Secure** (verificación de identidad del titular en e-commerce) en apps móviles y navegadores de forma segura.

◆ Software-Based PIN Entry on COTS

- Protege la **entrada de PIN en dispositivos comerciales** (como tablets o smartphones) mediante software seguro.

🛡️ Segmento: Autenticación avanzada

◆ PCI 3-D Secure Core

- Estándar que **mejora la autenticación del usuario** en transacciones online (e.g., 3DS 2.0), reforzando la experiencia sin comprometer la seguridad.

PCI DSS

El **PCI DSS** es un estándar de seguridad de información patentado para organizaciones que manejan tarjetas de crédito de las principales marcas, incluidas **Visa, MasterCard, AmericanExpress**, Discovery JCB. Las tarjetas de etiqueta privada, que no tienen el logotipo de una marca de tarjeta importante, no están incluidas en el alcance de PCI DSS.

Ahora bien, hablando de normativas, quiero empezar por una que tiene gran sensibilidad debido al tipo de información que protege: me refiero al estándar **PCI DSS** (*Payment Card Industry Data Security Standard*). Este estándar está relacionado con la **protección de datos de tarjetas de pago**, es decir, tarjetas de crédito y débito de marcas reconocidas a nivel global.

Este no es un estándar local ni exclusivo de Perú, sino una **normativa internacional**, creada por el sector financiero y bancario para garantizar la seguridad de los datos que manejan.

El PCI DSS no solo establece pautas técnicas, también es **certificable**. Existen certificaciones para **profesionales** de seguridad, así como para **empresas** que brindan servicios de auditoría, almacenamiento, administración o análisis de plataformas que procesan tarjetas de pago.

Es un foro global, una comunidad internacional que pone a disposición **documentación gratuita** sobre el estándar. Cualquiera puede descargarla y revisar los **requisitos** que se exigen.

Entre los distintos dominios que cubre PCI DSS, encontramos normativas específicas como las relacionadas con el manejo de **PINs**: cómo se generan, actualizan y protegen. También aborda la seguridad en la **producción física** de las tarjetas (microchips, banda magnética, materiales), así como en la **producción lógica**, que es la que más nos interesa.

En esta última se incluye, por ejemplo, la **protección de datos en aplicaciones de pago**, algo clave cuando se realizan transacciones bancarias o compras por internet. Si ustedes pagan su matrícula u otros servicios en línea usando una **pasarela de pago**, esa plataforma debe cumplir con el estándar PCI DSS.

Entonces, la gran pregunta es:
¿La universidad está tomando en cuenta este estándar para proteger nuestros datos cuando hacemos pagos en línea?

*Evidentemente, esta es una pregunta que como institución debemos plantearnos. Nosotros, por ejemplo, usamos una pasarela de pago —no recuerdo exactamente si se trata de **OpenPay**, **Culqi**, **Niubiz** u otra como **ProductCast**—, pero lo importante es que dicha pasarela **debe cumplir con los requisitos del estándar PCI DSS**, es decir, debe respetar los **lineamientos y exigencias internacionales** para proteger los datos de los usuarios durante las transacciones.*

El objetivo es que nuestros datos pasen **cifrados, seguros**, y se minimicen los riesgos de **fraudes, suplantaciones de identidad, transacciones maliciosas** u otros ataques. Por supuesto, un riesgo cero **no existe**, pero sí podemos **reducir** significativamente la posibilidad de incidentes con una correcta implementación de los controles de seguridad.

Ahora, ¿a qué tipo de tarjetas aplica realmente el estándar PCI DSS? Este estándar se aplica a las tarjetas más reconocidas a nivel mundial: **Visa, MasterCard, American Express, Discover, JCB**, entre otras. Es decir, aquellas que operan con marcas globales y no con tarjetas privadas o locales emitidas exclusivamente por una tienda o comercio.

*Por ejemplo, hace unos diez años, algunas tiendas tenían sus propias tarjetas privadas. Estas solo podían usarse dentro del negocio emisor, y como no se vinculaban a redes globales de pago, **no estaban obligadas a cumplir con PCI DSS**. Pero hoy en día, muchas de esas tarjetas privadas han migrado a plataformas como **MasterCard** o **Visa**, lo que las obliga a alinearse con el estándar.*

Entonces, **todo el ecosistema** que interviene en el procesamiento de pagos —bancos, comercios, emisores, adquirientes, pasarelas de pago, plataformas de comercio electrónico— debe garantizar el cumplimiento de PCI DSS, especialmente en transacciones con tarjetas de crédito o débito.

ALCANCE:

- Las Normas de Seguridad de Datos de PCI se desarrollaron para fomentar y mejorar la seguridad de los datos del **titular de la tarjeta** y facilitar la adopción de medidas de seguridad uniformes a nivel mundial.
- La PCI DSS proporciona una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de cuentas.
- La PCI DSS se aplica a **todas** las entidades que participan en el procesamiento de las tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios.
- La PCI DSS se aplica a **todas** las entidades que almacenan, procesan o transmiten datos del titular de la tarjeta (CHD) y/o datos confidenciales de autenticación (SAD).

¿Cuál es el alcance del PCI DSS?

Principalmente, el estándar busca asegurar que **los datos del titular de la tarjeta** estén protegidos de forma uniforme en **todo el mundo**. Esto garantiza que, sin importar en qué país o plataforma se realice la transacción, existan **medidas de seguridad consistentes**.

Los participantes obligados a cumplir con este estándar son:

- Comercios y tiendas físicas o virtuales
- Entidades procesadoras de pagos
- Bancos emisores
- Adquirentes (bancos o instituciones que procesan las tarjetas para los comercios)
- Proveedores de servicios de tecnología o pasarelas de pago

Cada uno de ellos, en la parte del proceso que le corresponde, debe seguir los **lineamientos de PCI DSS** para garantizar la integridad, confidencialidad y disponibilidad de los datos del titular.

REQUISITOS:

Desarrolle y mantenga redes y sistemas seguros	1	Instale y mantenga una configuración de firewall para proteger los datos del titular de la tarjeta
	2	No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad
Proteger los datos del titular de la Tarjeta	3	Proteja los datos del titular de la tarjeta que fueron almacenados
	4	Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas
Mantener un programa de administración de Vulnerabilidad	5	Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente
	6	Desarrollar y mantener sistemas y aplicaciones seguros

Desarrolle y mantenga redes y sistemas seguros	1	Instale y mantenga una configuración de firewall para proteger los datos del titular de la tarjeta
	2	No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad
Proteger los datos del titular de la Tarjeta	3	Proteja los datos del titular de la tarjeta que fueron almacenados
	4	Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas
Mantener un programa de administración de Vulnerabilidad	5	Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente
	6	Desarrollar y mantener sistemas y aplicaciones seguros
Implementar medidas sólidas de control de acceso	7	Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.
	8	Identificar y autenticar el acceso a los componentes del Sistema.
Supervisar y evaluar las redes con regularidad	9	Restringir el acceso físico a los datos del titular de la tarjeta.
	10	Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta.

Mantener una política de seguridad de información	11	Probar periódicamente los sistemas y procesos de seguridad.
	12	Mantener una política que aborde la seguridad de la información para todo el personal.

¿Cuáles son los requisitos del PCI DSS?

Como cualquier estándar serio de seguridad, PCI DSS tiene una estructura detallada. Aunque cuenta con **12 requisitos principales**, estos se agrupan en **6 dominios clave**. Un ejemplo es el primer dominio: **mantener una red y sistemas seguros**.

Este dominio incluye, por ejemplo:

1. **Instalar y mantener firewalls apropiados.**
2. **Evitar el uso de contraseñas predeterminadas** en sistemas y dispositivos.

Parece algo obvio, ¿verdad? Pero muchos dispositivos siguen operando con credenciales por defecto como admin/admin, root/root, 123456, entre otras. Esto representa una gran vulnerabilidad y es una de las razones por las que existen los estándares: para **establecer un mínimo aceptable de buenas prácticas**.

Ahora bien, **el estándar no siempre te dice “cómo” hacerlo**, sino **qué se espera que cumplas**.

*Por ejemplo, te dirá que necesitas proteger el firewall, pero no te dirá con qué marca, tecnología ni configuración específica. Esa decisión queda en manos del implementador, lo que muchas veces puede provocar que una organización **cumpla con el estándar en papel**, pero no de forma **efectiva**.*

*Lo mismo sucede con las contraseñas: no basta con que una contraseña sea compleja (ej. tenga letras, números y símbolos), también debe ser **robusta** (larga, única, no repetida, no fácil de adivinar). La **complejidad** y la **fortaleza** no son lo mismo.*

Cuando hablamos de **contraseñas seguras**, muchas veces nos encontramos con formularios que nos indican el nivel de "fortaleza" de la contraseña: **débil**, **media** o **fuerte**. Estos niveles suelen depender de ciertos **parámetros**, como:

- Longitud (mínimo 8–12 caracteres).
- Uso de **mayúsculas y minúsculas**.
- Inclusión de **números**.
- Inclusión de **caracteres especiales** (como @, #, !, etc.).

Sin embargo, algo importante que debemos considerar es que **complejidad no es igual a fortaleza**. Una contraseña como Holamundo123! puede cumplir con los requisitos mínimos de complejidad, pero si es fácil de adivinar o ya ha sido filtrada en bases de datos públicas, sigue siendo débil.

Por eso, el estándar PCI DSS no solo establece que las contraseñas deben ser "complejas", sino que también deben ser **robustas**, únicas y difíciles de predecir. Y aunque la norma no siempre especifica "cómo" hacer esto, sí exige **políticas claras de gestión de contraseñas** y control de acceso.

Cifrado de datos: almacenamiento vs. transmisión

Otro punto clave del estándar PCI DSS es el **uso de criptografía** para proteger los datos sensibles de las tarjetas. Aquí es importante distinguir dos momentos:

1. **Transmisión:** cuando los datos viajan por internet o redes públicas.
2. **Almacenamiento:** cuando los datos quedan guardados en servidores o bases de datos.

En el primer caso, muchos piensan que usar **HTTPS** ya es suficiente. Es cierto que HTTPS protege la información **en tránsito**, pero el **navegador** (cliente) puede capturar la contraseña en texto plano **antes de que sea cifrada**.

*Por ejemplo, si hay un **script malicioso** o un ataque tipo **Man-in-the-Browser**, la contraseña podría ser robada **incluso antes de que salga cifrada**.*

Por eso, el estándar insiste en proteger la información **desde su origen**: no solo confiar en HTTPS, sino también asegurar el **frontend**, validar los formularios, evitar scripts de terceros, y cifrar adecuadamente **desde la propia aplicación**.

En cuanto al **almacenamiento**, hay casos donde los datos se guardan cifrados, pero se transmiten en texto claro, lo cual es un **grave error de implementación**. Ambas partes deben protegerse: **en tránsito** y **en reposo**.

Buenas prácticas adicionales (aunque obvias)

Aunque muchas de estas prácticas parecen obvias, el estándar las **menciona explícitamente** para evitar ambigüedades. Por ejemplo:

- **Actualizar frecuentemente el software**, especialmente sistemas operativos, antivirus y herramientas antimalware.
- **Evitar contraseñas por defecto** como admin, root, 123456, etc.
- **Configurar correctamente los firewalls**, no solo instalarlos.

- **Implementar desarrollo seguro** en la construcción de sistemas y aplicaciones.

Estas recomendaciones están incluidas en los **12 requisitos principales de PCI DSS**, y su cumplimiento es obligatorio para todas las entidades que procesan, almacenan o transmiten datos de tarjetas.

Cuando implementamos medidas de seguridad en aplicaciones, es fundamental considerar que **estas pueden impactar en la calidad del software**, especialmente en aspectos como la **usabilidad**. Es decir, aplicar muchos requisitos de seguridad puede dificultar o incomodar la experiencia del usuario.

Por ejemplo, algunos bancos y comercios, con el fin de que sus usuarios utilicen sus aplicaciones de forma más fluida, a veces **sacrifican ciertas medidas de seguridad** como:

- El uso obligatorio del **dobles factor de autenticación**.
- El **cierre automático de sesión** tras minutos de inactividad.
- Requisitos estrictos de contraseñas o validaciones recurrentes.

¿Por qué hacen esto? Porque saben que, si bien estas medidas mejoran la seguridad, también **pueden hacer que el usuario se sienta menos cómodo o más frustrado**, lo que reduce la adopción de la aplicación.

Entonces, surge una **pregunta clave**:

¿Hasta qué punto debemos aplicar estas medidas de seguridad?
¿Y en qué momento se decide asumir o trasladar parte del riesgo al usuario?

Por ejemplo, si un usuario deja su sesión abierta en un dispositivo compartido, o permite que otros usen su teléfono sin protección, el problema ya no está en la aplicación, sino en el **uso indebido por parte del usuario**. Aun así, la empresa debe prever estas situaciones y proteger al usuario incluso de sus propios descuidos.

Control de acceso y almacenamiento seguro

Una parte crítica del estándar **PCI DSS** es la implementación de **controles de acceso estrictos**. Solo el **personal autorizado** debe poder ver o manejar los datos sensibles del titular de la tarjeta. No cualquiera dentro de una organización debe tener acceso a esta información. Y aún menos si hablamos del código **CVV** (código de verificación) que se usa para confirmar transacciones.

Cuando haces una compra en línea y eliges la opción de “guardar tarjeta para futuras compras”, **los datos quedan almacenados en algún lugar**. Entonces la pregunta que debemos hacernos es:

¿Cómo se están almacenando esos datos?

Muchas filtraciones de tarjetas han ocurrido porque las bases de datos contenían los números **en texto plano**, sin cifrado ni medidas de protección. Si un atacante accede a esa base, obtiene toda la información lista para ser usada o vendida (como ha ocurrido en foros de la dark web o grupos de Telegram).

Y aquí hay una **clave esencial**:

El usuario no es el responsable de proteger la base de datos. La responsabilidad recae en la empresa o proveedor de servicios que almacena esos datos.

Trazabilidad y autenticación

El estándar también exige que **todo acceso esté debidamente identificado, autenticado y registrado**. No debe haber ambigüedad en los accesos. Cada cuenta debe ser única, con trazabilidad garantizada. Esto permite saber exactamente **quién accedió, cuándo, desde dónde y qué hizo** en el sistema.

Todo lo que hace un usuario autenticado debe estar **registrado**, especialmente si tiene acceso a datos sensibles. Esto forma parte de una buena política de **auditoría y monitoreo**.

Seguridad física y segmentación de redes

Además del software y las bases de datos, es crucial proteger el **acceso físico a los datos**, especialmente en plataformas como **cajeros automáticos, datáfonos** o servidores que procesan pagos.

Uno de los conceptos clave en este aspecto es la **segmentación de red**. ¿Qué significa esto? Que **no todas las partes de una red deben estar conectadas entre sí**. Por ejemplo:

- Un **cajero automático** no debería estar en el mismo segmento de red que los servidores de desarrollo o las computadoras administrativas.
- Solo dispositivos autorizados, con reglas claras de firewall y control de acceso, deberían poder comunicarse con estos sistemas críticos.

Una **red bien segmentada** impide que un atacante que compromete un equipo común (por ejemplo, un computador de oficina) pueda escalar fácilmente y acceder a los sistemas que manejan datos sensibles de tarjetas.

Cuando un **dispositivo o máquina permite tráfico inusual**, esto debe ser detectado y controlado rápidamente. En una red bien segmentada, un ataque a una zona específica —como la red de servidores— **no debería afectar otras áreas**, por ejemplo, la red de cajeros automáticos.

Y aunque hablar de **restricciones y controles** de seguridad a veces puede parecer exagerado o “limitante”, lo cierto es que las **políticas de seguridad** son fundamentales para **organizar, direccionar y dar coherencia** a las acciones de protección dentro de una organización.

Sin embargo, es importante entender que **la política por sí sola no es suficiente**. Si no se traduce en **mecanismos concretos**, en **controles técnicos o administrativos efectivos**, su aplicación será meramente decorativa.

¿Cómo se prueban las defensas?

Las defensas de un sistema no se validan únicamente con documentos o configuraciones. Se prueban mediante técnicas ofensivas, como el **pentesting (pruebas de penetración)** o el uso de **herramientas de auditoría defensiva** como **plugins de seguridad**.

- **Pentesting:** forma parte del enfoque ofensivo, necesario para saber si las medidas defensivas realmente funcionan.
- Es como **simular un ataque** para medir la capacidad de respuesta y resistencia del sistema.

Además, debe haber una política clara de **concienciación del personal**, porque no basta con proteger las máquinas: **el ser humano sigue siendo uno de los puntos más vulnerables**.

Técnicas como el **phishing**, la **ingeniería social** y los **engaños por mensajería** siguen siendo de los ataques más efectivos. Por eso, capacitar al personal **es tan importante como actualizar los antivirus o configurar los firewalls**.

Estándares y sectores sensibles: financiero y salud

En el sector **financiero**, ya hemos hablado del estándar **PCI DSS**, que rige la protección de datos de tarjetas de crédito y débito. Esta norma es ampliamente reconocida y muchas instituciones en todo el mundo deben cumplirla.

Cada país, sin embargo, puede tener sus **regulaciones internas**, pero cuando hablamos de operaciones internacionales y tarjetas de pago, el estándar más citado sigue siendo **PCI DSS**.

=====

Health Insurance Portability and Accountability Act (HIPAA)

Health Insurance Portability and Accountability Act (HIPAA)

Desde el punto de vista de la **atención médica**, la legislación HIPAA (Ley de Responsabilidad y Portabilidad de Seguros Médicos), promulgada en 1996, exige que el Departamento de Salud y Servicios Humanos de EE. UU. desarrolle un conjunto de estándares nacionales para **las transacciones de atención médica**. Estos estándares **brindan seguridad de que la transferencia electrónica de información confidencial del paciente** será tan segura o más segura que los registros en papel del paciente.

ALCANCE:

- Otorga derechos sobre la información de la salud personal, incluso el derecho a obtener una copia de esa información, a asegurarse de que es correcta y a saber quién la ha visto.
- En PERÚ no existe una ley similar, sin embargo se tienen Resoluciones Ministeriales (MINSA) que especifican el procesamiento y gestión de las Historias Clínicas.

Algunas RM-MINSA-PERÚ

- RM 776-2004/MINSA: Norma técnica número 022-MINSA/DGSP-V.01: Norma Técnica de la Historia Clínica de los Establecimientos de Salud del Sector Público y Privado
 - RM 466-2011/MINSA: Directiva Administrativa que aprueba las especificaciones para la estandarización del registro en la Historia Clínica Electrónica.
 - RM 732-2008/MINSA: Norma Técnica número 022-MINSA/DGSP-V.03: Norma Técnica de Salud para la Gestión de la Historia Clínica.
-

Por otro lado, en el sector **salud**, existen también normativas específicas que regulan la privacidad y seguridad de los **datos médicos personales**. Un ejemplo internacional es la ley **HIPAA** de Estados Unidos, que establece:

- Portabilidad de datos de salud.
- Seguridad y confidencialidad.
- Responsabilidad sobre su uso.

En el caso de **Perú**, no contamos aún con una ley tan robusta como HIPAA, pero existen algunos **decretos y directivas** sobre:

- Uso de historias clínicas.
- Interoperabilidad entre sectores públicos de salud.

Sin embargo, el sistema aún es **débil e incompleto**, especialmente en lo que respecta a la seguridad digital de la información médica. Por ejemplo, en muchos centros de salud, los datos siguen siendo accesibles para **personal no autorizado**, lo que representa un grave riesgo para la **confidencialidad e integridad** de los pacientes.

Caso ilustrativo: datos sensibles en salud

Imagina que un periodista desea saber cuántas personas viven con VIH en una región determinada. Es válido que se publique una estadística **anónima** para informar a la población, pero nunca deben divulgarse **datos personales** que permitan identificar a esos pacientes. Los **datos de salud** son considerados **sensibles y protegidos**, y su uso está regulado incluso cuando no exista una ley tan específica como HIPAA.

Por lo tanto, cualquier acceso a estos datos debe estar:

- **Controlado y limitado.**
- **Justificado por rol o función.**
- **Registrado (trazabilidad del acceso).**

El hecho de que alguien trabaje en un hospital **no le da derecho automático** a ver todas las historias clínicas.

Protección de datos en salud e interoperabilidad clínica

La **información clínica** de los pacientes, como sus **historias médicas**, debe ser accedida exclusivamente por **personal autorizado**. Esto incluye médicos, enfermeras u otros profesionales que estén directamente involucrados en el tratamiento del paciente. Sin embargo, en la práctica, muchas veces personas no autorizadas acceden a esta información.

Esto puede ocurrir, por ejemplo, durante la transferencia de datos de un hospital a otro o entre establecimientos de salud. En estos casos, la **seguridad de la transmisión** es clave, ya que los registros pueden ser manipulados o interceptados si no se emplean los **mecanismos adecuados de cifrado y autenticación**.

*La historia clínica debe ser **protegida**, tanto en su almacenamiento como en su transferencia. La regulación internacional como **HIPAA (Health Insurance Portability and Accountability Act)** en EE.UU. establece estándares estrictos para garantizar que solo personas autorizadas accedan a la información, y que cada acceso esté registrado y controlado.*

En **Perú**, lamentablemente, no existe aún una ley unificada y robusta similar a HIPAA. Lo que tenemos son **normas aisladas**, resoluciones emitidas por el MINSA en distintos años:

- Una **Norma Técnica de 2004** sobre la estructura y uniformización de historias clínicas.
- Una resolución de **2011** que impulsa el registro electrónico de historias clínicas.
- Otras disposiciones sueltas en 2008, 2016 y 2020.

Este enfoque fragmentado genera un sistema **desorganizado y poco interoperable**. Por ejemplo:

- Si un paciente se atiende en un hospital público, se crea una historia clínica.
- Si luego acude a un centro de salud de Essalud o una clínica privada, **se crea otra historia clínica nueva**, independiente de la anterior.

Esto revela una grave **falta de interoperabilidad**. No hay un sistema integrado que permita a los médicos acceder al historial completo del paciente, lo cual afecta la **continuidad del tratamiento** y la **seguridad del paciente**.

Reflexión crítica sobre el estado actual

Este problema demuestra que, aunque existen esfuerzos normativos, **no hay una estandarización ni una política nacional clara y efectiva**. Cada institución maneja sus datos por separado, con distintas plataformas y sin integración, lo que:

- **Aumenta el riesgo de errores clínicos.**
- **Genera duplicidad de pruebas y gastos.**
- **Excluye al paciente del control sobre su información.**

Además, las debilidades en la seguridad y la trazabilidad hacen que estos datos queden **vulnerables a accesos no autorizados**. Esto no solo es un riesgo técnico, sino también **un atentado contra el derecho a la privacidad**.

Sarbanes-Oxley Act (SOX)

Sarbanes-Oxley Act(SOX)

La Ley SOX de 2002 es una legislación aprobada por el Congreso de los EE. UU. para proteger a los accionistas y al público en general contra errores contables y prácticas fraudulentas en la empresa, así como para mejorar la precisión de las divulgaciones corporativas.

La ley fue creada en respuesta a varios escándalos corporativos y contables importantes, incluidos los que afectan a **Enron**, **Tyco International**, **Peregrine Systems** y **WorldCom**. Estos escándalos resultaron en una disminución de la confianza pública en las prácticas contables y de información.

ALCANCES:

- La ley de Sarbanes-Oxley crea un nuevo organismo supervisor de la contabilidad, nuevas reglas de independencia del auditor, una reforma de la contabilidad corporativa.
- La Nueva Junta Supervisora Contable tiene el deber de:
 - * Registrar las firmas de la contabilidad.
 - * Establecer y/o adoptar normas de auditoria.
 - * Conducir inspecciones, investigaciones, y procedimientos disciplinarios.
 - * Hacer cumplir la ley.
- La creación del “*Public Company Accounting Oversight Board*” (**Comisión encargada de supervisar** las auditorias de las compañías que cotizan en bolsa).
- El requerimiento de que las compañías que cotizan en bolsa garanticen la **veracidad de las evaluaciones de sus controles internos en el informe financiero**, así como que los auditores independientes de estas compañías constaten esta transparencia y veracidad.
- **Certificación de los informes financieros**, por parte del comité ejecutivo y financiero de la empresa.
- **Independencia de la empresa auditora.**

- El requerimiento de que las compañías que cotizan en bolsa tengan un **comité de auditores** completamente independientes.
 - **Prohibición de préstamos personales** a directores y ejecutivos.
 - Transparencia de la información de acciones y opciones, de la compañía en cuestión, que puedan tener los directivos, ejecutivos y empleados claves de la compañía y consorcios, en el caso de que posean más de un 10% de acciones de la compañía. Asimismo estos **datos deben estar reflejados en los informes** de las compañías.
 - **Endurecimiento de la responsabilidad civil** así como las penas, ante el incumplimiento de la Ley. Se alargan las penas de prisión, así como las multas a los altos ejecutivos que incumplen y/o permiten el incumplimiento de las exigencias en lo referente al informe financiero.
 - La ley SOX afecta a sociedades cotizadas en EE.UU. Sin embargo aquellas empresas **extranjeras que cotizan** en las bolsas de Estados Unidos deben cumplir la Ley SOX.
-

El caso de Sarbanes-Oxley (SOX): cómo un escándalo cambió la ley

Un ejemplo potente sobre cómo los **escándalos pueden originar leyes estrictas** lo encontramos en el caso de **Sarbanes-Oxley (SOX)**, promulgada en EE.UU. en **2002**.

Durante los años 90 e inicios del 2000, varias empresas gigantes como **Enron**, **WorldCom** y **Tyco** protagonizaron fraudes contables a gran escala. Simulaban tener rentabilidad mediante empresas fantasmas, manipulaban balances y engañaban a inversionistas y empleados.

Estas empresas incluso eran reconocidas por su “cultura corporativa” ejemplar, premiaban a sus trabajadores y eran recomendadas como lugares ideales para trabajar. Sin embargo, todo estaba sostenido sobre **fraude financiero sistemático**.

¿Cómo lograron hacerlo sin ser descubiertos?

Principalmente porque **los auditores eran pagados por las mismas empresas auditadas**, lo que generaba un conflicto de interés evidente. A pesar de tener ciertas normativas, la dependencia económica anulaba la imparcialidad de las auditorías.

Cuando estos escándalos salieron a la luz, **la confianza en los mercados financieros se desplomó**, y fue necesario legislar con urgencia. Así nació la **Ley Sarbanes-Oxley (SOX)**.

¿Qué cambió con SOX?

SOX introdujo reformas fundamentales:

- Se creó un **organismo regulador independiente (PCAOB)** para supervisar las auditorías.
- Se exigió que los auditores ya **no sean contratados directamente por la empresa auditada**.
- Se establecieron sanciones penales por falsificación de información contable.
- Se obligó a que los altos directivos **firmen y respondan legalmente por la veracidad de los reportes financieros**.

Esto marcó un antes y un después en la **gestión de la información financiera**, obligando a las empresas a implementar **controles internos confiables**, y a mantener registros auditables y transparentes.

Supervisión, auditoría y transparencia: lo que cambió después de SOX

Uno de los pilares de la **Ley Sarbanes-Oxley (SOX)** fue romper con la dependencia entre las empresas y sus auditores. Antes, las empresas contrataban y pagaban directamente a los auditores, lo cual comprometía la **imparcialidad** del proceso. Es decir, el auditor difícilmente denunciaría a la empresa que le paga.

Con la implementación de SOX:

- **La contratación de auditores pasó a ser externa y regulada.**
- Se creó un **organismo supervisor independiente**.
- Se estableció la obligación de publicar información detallada sobre el estado financiero de las empresas que cotizan en bolsa, incluyendo:
 - Estados financieros.
 - Proyectos ejecutados.
 - Planillas de trabajadores (nombre, puesto, sueldo, bonificaciones).
 - Préstamos internos, premios y beneficios otorgados por los directorios.

Esto marcó un cambio radical, apuntando a **transparencia, trazabilidad y responsabilidad corporativa**.

¿Qué pasa en Perú?

En el contexto peruano, **no existe una ley como SOX**, pero sí contamos con mecanismos de control como los establecidos por la **Contraloría General de la República**, que fiscaliza el comportamiento financiero de las entidades públicas.

Además:

- La Contraloría **contrata auditores externos**, y estos **no dependen de las instituciones auditadas** (como universidades u hospitales).
- Aunque algunos de estos auditores tengan oficinas dentro de las instituciones, **su salario es pagado directamente por la Contraloría**, lo cual busca preservar su independencia.

En el caso de las **empresas privadas**, la fiscalización recae sobre entidades como:

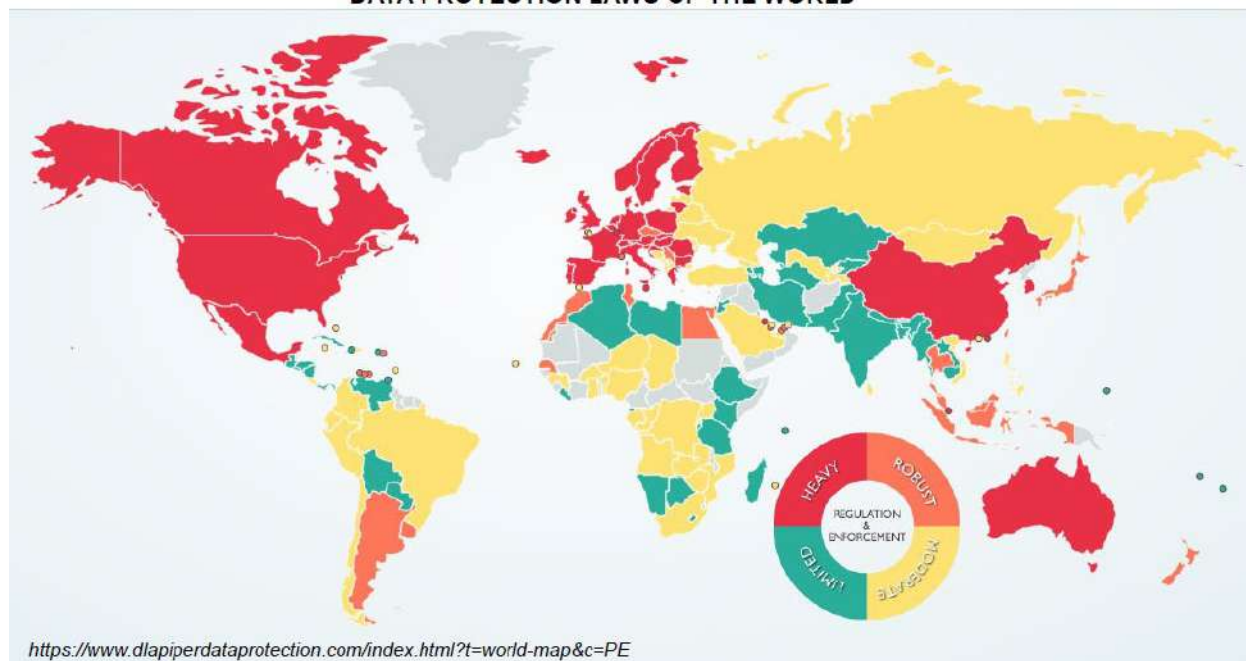
- **SUNAT** (tributación).
- **Superintendencia del Mercado de Valores (SMV)**.
- **Unidad de Inteligencia Financiera (UIF)**, entre otras.

Cabe señalar que algunas **empresas peruanas que cotizan en la Bolsa de Nueva York** (como ciertos bancos o mineras) **sí están obligadas a cumplir con SOX**, ya que aceptan regulaciones extranjeras al ingresar a mercados internacionales.

Ley 29733 – Ley de Protección de Datos Personales

Ley 29733 –Ley de Protección de Datos Personales

DATA PROTECTION LAWS OF THE WORLD



Publicación de la Ley

Reglamento de la Ley

D.L. 1353 Modifica
Ley 29733

3 julio 2011

22 Marzo 2013

07 enero 2017

DECRETO LEGISLATIVO QUE CREA LA
AUTORIDAD NACIONAL DE TRANSPARENCIA Y
ACCESO A LA INFORMACIÓN PÚBLICA,
FORTALECE EL RÉGIMEN DE PROTECCIÓN DE
DATOS PERSONALES Y LA REGULACIÓN DE LA
GESTIÓN DE INTERESES

Ley N.º 29733 – Ley de Protección de Datos Personales (Perú)

Esta ley, vigente desde 2011, busca proteger los **datos personales** de los ciudadanos peruanos.
Sin embargo, **su aplicación práctica sigue siendo débil y muy limitada**.

A pesar de que en países como **EE. UU., China y la Unión Europea** se han desarrollado leyes con altos niveles de exigencia, Perú se encuentra todavía en un nivel medio o bajo, similar al de países como Bolivia, India o Venezuela, en términos de **madurez normativa y capacidad de fiscalización efectiva**.

Problemas comunes en Perú:

- La ley existe, pero **muchas empresas la utilizan solo como adorno legal**.

- Se solicita la firma de formularios de consentimiento para el uso de datos, pero **no se explica claramente para qué se usarán**.
- En muchos casos, **si no firmas, no puedes acceder al servicio**, por lo que el consentimiento es prácticamente forzado.
- Algunas entidades, incluso estatales, **no cumplen ni con el mínimo de transparencia ni protección**.

Un ejemplo claro de esto es la adquisición de servicios como:

- **Líneas telefónicas.**
- **Cuentas bancarias.**
- **Afiliaciones a seguros o aplicativos móviles.**

Allí se firman formularios extensos con letra diminuta, en los que el usuario **ni lee ni entiende realmente** qué datos está cediendo y con qué finalidad.

El uso de datos personales: consentimiento aparente y vulnerabilidad del ciudadano

En la práctica cotidiana, es común encontrar formularios en los que la **casilla de “sí acepto”** el uso de mis datos personales **ya viene marcada por defecto**. Muchas veces, por apuro, por desinformación o simplemente por presión del entorno, las personas firman sin leer, o aceptan sin entender lo que están autorizando.

Esto ocurre en:

- Empresas de telefonía.
- Apertura de cuentas bancarias.
- Formularios en tiendas, clínicas, seguros, redes sociales, y más.

Aunque por ley debe existir la **opción de negar el consentimiento** y el derecho a **retractarse posteriormente**, en la práctica:

- Si no marcas "sí acepto", no puedes acceder al servicio.
- El consentimiento deja de ser libre y se convierte en **forzado**.
- Se convierte en una **condición encubierta** para obtener un producto o servicio.

La Ley N.º 29733 – Protección de Datos Personales

Promulgada en 2011, con su reglamento en 2013 y una modificación en 2017, esta ley establece los principios, derechos y obligaciones sobre el **tratamiento de datos personales**. La

entidad encargada de su aplicación es la **Autoridad Nacional de Protección de Datos Personales**, que forma parte del Ministerio de Justicia y Derechos Humanos.

Fundamento constitucional:

La ley está alineada con el **artículo 2° de la Constitución Política del Perú**, que reconoce como derecho fundamental:

“Que los servicios informáticos, públicos o privados, no suministren información que afecte la intimidad personal o familiar”.

Sin embargo, el problema no está en la ley en sí, sino en:

- La **falta de fiscalización y sanciones efectivas**.
 - La **escasa difusión** entre la población.
 - La **asimetría de poder** entre empresas e individuos.
-

¿Qué son los datos personales?

Según la ley, son:

“Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a una persona natural que la identifique o la haga identificable.”

Ejemplos:

- Nombre y apellidos.
 - DNI, RUC.
 - Dirección domiciliaria o laboral.
 - Correo electrónico personal.
 - Número telefónico.
 - Huellas digitales, voz, imagen.
-

Datos personales sensibles

La ley también distingue un grupo especial de datos llamados **sensibles**, los cuales requieren **mayor protección** por su naturaleza íntima y el potencial de discriminación o vulneración de derechos que implican.

Ejemplos de datos sensibles:

- Estado de salud o historial médico.

- Discapacidad.
- Orientación sexual.
- Creencias religiosas o filosóficas.
- Origen étnico o racial.
- Afiliación sindical o política.
- Información genética o biométrica.

Estos datos **no deben solicitarse salvo que exista una justificación válida**, y el consentimiento debe ser **explícito y específico**.

Reflexión crítica

Aunque la Ley 29733 existe hace más de **14 años**, muchas personas **ni siquiera saben que tienen derecho a oponerse** al tratamiento de sus datos. Y peor aún, muchos servicios — incluso públicos— no ofrecen una alternativa real. El consentimiento se vuelve una **formalidad impuesta**.

Además:

- Los formularios son extensos, con letra pequeña y lenguaje técnico.
- Se firman sin leer, por apuro o por confianza.
- El ciudadano queda **desprotegido ante un uso indebido de sus datos**.

ALCANCE:

Constitución Política del Perú

Toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, **no suministren informaciones que afecten la intimidad personal y familiar.**

Artículo 1. Objeto de la Ley

Garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú.

Datos personales: Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados.

- ☐ **Datos personales relacionados con la salud:** Es aquella información concerniente a la salud pasada, presente o pronosticada, física o mental, de una persona, incluyendo el grado de discapacidad y su información genética.
- ☐ **Datos sensibles:** Es aquella información relativa a datos personales referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la salud física o mental u otras análogas que afecten su intimidad.

Principios de la Ley

Reglamento de la Ley

Artículo 4. Principio de legalidad

Artículo 5. Principio de consentimiento

Artículo 6. Principio de finalidad

Artículo 8. Principio de calidad

Artículo 9. Principio de seguridad

Consentimiento:

- 🔗 Sobre el **consentimiento expreso** observar que: Tratándose del entorno digital, también se considera **expresa** la manifestación consistente en “hacer clic”, “clickear” o “pinchar”, “dar un toque”, “touch” o “pad” u otros similares.
- 🔗 También: “el consentimiento escrito podrá otorgarse mediante firma electrónica, mediante escritura que quede grabada, ... o que por cualquier otro mecanismo o procedimiento ... Permita identificar al titular y recabar su consentimiento, a través de texto escrito. También podrá otorgarse mediante texto preestablecido, fácilmente visible, legible y en lenguaje sencillo,

que el titular pueda hacer suyo, o no, mediante una respuesta escrita, gráfica o mediante clic o pinchado.”

(art. 12, numeral 3 del Reglamento de la Ley 29733)

Sobre el **consentimiento informado** observar que: Al titular de los datos personales se le debe comunicar claramente:

- ☐ La identidad y domicilio o dirección del titular del banco de datos personales o del responsable del tratamiento al que puede dirigirse para revocar el consentimiento o ejercer sus derechos.
- ☐ La finalidad o finalidades del tratamiento a las que sus datos serán sometidos.
- ☐ La identidad de los que son o pueden ser sus destinatarios, de ser el caso.
- ☐ La existencia del banco de datos personales en que se almacenarán, cuando corresponda.
- ☐ El carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, cuando sea el caso.
- ☐ Las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo.

Tratamiento de Datos Personales

Artículo 13. Alcances sobre el tratamiento de datos personales

- ☐ Se dictan medidas especiales para tratamiento de D.P. de los niños y adolescentes.
- ☐ Las telecomunicaciones, sistemas informáticos, cuando sean de carácter privado, solo pueden ser intervenidos por mandamiento del juez o con autorización de su titular. Se guarda secreto de los asuntos ajenos al hecho.
- ☐ En datos sensibles, el consentimiento para su tratamiento debe ser por escrito.
- ☐ El titular de D.P. puede revocar su consentimiento en cualquier momento
- ☐ El tratamiento de D.P. relativos a la comisión de infracciones penales o administrativas solo puede ser efectuado por las entidades públicas competentes-Poder Judicial o el Ministerio Público

No es necesario el consentimiento

- ☐ Cuando los D.P. se recopilen o transfieran para el **ejercicio de las funciones de las entidades públicas.**
- ☐ Cuando se trate de D.P. contenidos o destinados a ser contenidos en **fuentes accesibles para el público.**

- ☐ Cuando se trate de datos personales relativos a la solvencia **patrimonial y de crédito, conforme a ley.**
- ☐ Cuando medie norma para **la promoción de la competencia** en los mercados regulados..., siempre que la información brindada no sea utilizada en perjuicio de la privacidad del usuario.
- ☐ Cuando los D.P. sean necesarios para la preparación, celebración y ejecución de una **relación contractual** en la que el titular de datos personales sea parte, o cuando se trate de datos personales que derive de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento.
- ☐ Cuando se trate de datos personales **relativos a la salud** y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, siempre que dicho tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud, observando el secreto profesional.
- ☐ Cuando el tratamiento sea efectuado por organismos sin fines de lucro cuya **finalidad sea política, religiosa o sindical** y se refiera a los datos personales recopilados de sus respectivos miembros.
- ☐ Cuando el tratamiento sea para fines vinculados al **sistema de prevención de lavado de activos y financiamiento del terrorismo** u otros que respondan a un mandato legal.
- ☐ En el caso de grupos económicos conformados por empresas que son consideradas sujetos obligados a informar, conforme a las normas que regulan a la **Unidad de Inteligencia Financiera**,
- ☐ Cuando el tratamiento se realiza en ejercicio constitucionalmente válido del derecho fundamental a la **libertad de información.**
- ☐ Otros que deriven del ejercicio de competencias expresamente establecidas por Ley

¿Quién tiene la obligación de proteger nuestra información personal?

La **protección de la privacidad, la identidad y la dignidad** de las personas no es opcional: es un derecho respaldado por la **Constitución del Perú** y regulado específicamente por la **Ley N.º 29733 – Ley de Protección de Datos Personales.**

Esta ley **obliga a todas las entidades, públicas y privadas**, a proteger los datos que recopilan de los ciudadanos. Es decir, toda persona o empresa que almacene, procese o transfiera información personal **debe cumplir con esta norma.**

Principios fundamentales de la Ley de Protección de Datos

La Ley N.º 29733 se basa en **cuatro principios clave**:

1. Legalidad

El tratamiento de datos debe tener **base legal**. No se pueden recolectar datos por simple costumbre o conveniencia. Todo uso debe estar justificado y registrado.

2. Consentimiento

La persona debe otorgar su **consentimiento libre, previo, informado y expreso** para que su información sea usada. Marcar una casilla, hacer clic en “aceptar” o firmar un formulario son formas válidas de consentimiento, **pero deben estar bien informadas**.

3. Finalidad

El uso del dato debe ser **específico y declarado**. Si te piden tu correo para enviarte una boleta de compra, **no pueden usarlo luego para enviarte promociones o compartirlo con terceros**, a menos que lo hayan indicado y tú lo hayas autorizado.

4. Calidad del dato

Los datos deben ser **veraces, exactos y actualizados**. El titular también tiene la responsabilidad de no proporcionar datos falsos. La empresa debe almacenarlos de forma segura y emplearlos solo en función de su finalidad.

¿Para qué piden nuestros datos?

Muchas veces te piden tu nombre, correo o número telefónico en:

- Eventos públicos.
- Ingresos a centros comerciales o recreacionales.
- Hoteles o plataformas en línea.

¿Con qué fin?

Generalmente con fines de **marketing**: para enviarte promociones, publicidad o cruzar tu información con otras bases de datos.

¿Te han explicado por qué los necesitan?

Muchas veces no. Te lo presentan como un trámite obligatorio, sin mayor detalle. Pero **si tú preguntas, están obligados a responder** de forma clara.

¿Qué pasa si los usan para otra cosa?

Esto es una violación al principio de **finalidad**. Por ejemplo:

- Si dejas tu correo para recibir un comprobante, pero luego te llaman de una agencia de viajes que recibió tus datos del hotel... eso es uso indebido.
 - Si te registras en un sitio y sin tu permiso comparten tu información con sus "aliados comerciales", eso también infringe la ley.
-

¿Qué pasó con empresas de telecomunicaciones?

Durante la apertura del mercado de telecomunicaciones en Perú, se estableció —por ley— que empresas como Telefónica **debían compartir cierta información de sus clientes con otras operadoras** para asegurar la libre competencia.

Esto, que comenzó como una medida para evitar monopolios, terminó **normalizando el intercambio de datos** entre compañías. Así, al contratar una línea, a los pocos días te empiezan a llamar de otras operadoras.

Y aunque esto parece una práctica común, **no debería hacerse sin tu consentimiento claro**.

¿Qué se considera consentimiento expreso?

El consentimiento no siempre es una firma física. También puede ser:

- Marcar una casilla que diga “Acepto los términos”.
- Hacer clic en “Aceptar”.
- Usar un dispositivo para registrar tu aprobación (iPad, smartphone, quiosco digital).

Pero ojo: **ese consentimiento solo es válido si fue informado**.

No puede ser por omisión, ni puede venir marcado por defecto. Si no te explican claramente qué estás aceptando, **el consentimiento no es legalmente válido**.

¿Qué son los datos personales?

Son **toda información que permita identificarte directa o indirectamente**:

- Nombre, DNI, correo electrónico.
- Huellas, voz, rostro, dirección.
- Datos de salud, orientación sexual, creencias religiosas o políticas.

Entre estos, existen los **datos sensibles**, que por su naturaleza requieren **mayor protección**. Estos incluyen:

- Información médica o sobre discapacidades.
 - Datos sobre orientación sexual.
 - Creencias religiosas o filosóficas.
 - Origen étnico o racial.
-

Autoridad Nacional de Protección de Datos Personales



Buscar en ANPD



[Inicio](#) > [El Estado](#) > [MINJUSDH](#) > [ANPD](#) > Información institucional

[Inicio](#)

[Categorías](#) ▼

[Trámites y servicios](#) ▼

[Normas y documentos](#) ▼

[Noticias y campañas](#) ▼

[Información Institucional](#) ▼

[Contacto](#) ▼

[Autoridad Nacional de Protección de Datos Personales](#)

Información institucional

¿Qué hacemos?

La Autoridad Nacional de Protección de Datos Personales debe cumplir y hacer cumplir la normatividad vigente en materia de protección de datos personales.

En cumplimiento de la [Ley de Protección de Datos Personales 29733](#) y su [Reglamento](#).

Funciones

- Normativa
- Supervisora/Fiscalizadora
- Consultiva/orientadora
- Promotora /de representación
- Resolutiva/ Coactiva
- Administradora

[Normativa de Protección de Datos Personales](#)

[Organigrama](#)

[Organización](#)

[Directorio de funcionarios](#)

[Autoridad Nacional de Protección de Datos Personales](#)

Formulario de denuncia contra la Ley de Datos Personales 29733 - ANPD

Formulario

25 de marzo de 2013

Formulario de denuncia por actos contrarios a la Ley N° 29733 y su reglamento aprobado por Decreto Supremo N° 03-2013-JUS

Esta publicación pertenece al compendio [Formularios ANPD](#)

Documentos



**Formulario de denuncia
contra la Ley de Datos
Personales 29733**

PDF | 4.3 MB



Descargar

<https://www.gob.pe/institucion/anpd/informes-publicaciones/685141-formulario-de-denuncia-contra-la-ley-de-datos-personales-29733-anpd>



PERÚ

Ministerio
de Justicia
y Derechos Humanos

Despacho
Viceministerial
de Justicia

Dirección General de Transparencia,
Acceso a la Información Pública y
Protección de Datos Personales

Dirección de
Fiscalización e Instrucción

**FORMULARIO DE DENUNCIA POR ACTOS CONTRARIOS A LA LEY N° 29733 Y SU
REGLAMENTO APROBADO POR DECRETO SUPREMO N° 03-2013-JUS**

Dirigido a la Dirección de Fiscalización e Instrucción

I. DATOS DEL DENUNCIANTE

Nombres:

Apellidos:

N° de Documento de Identidad

DNI Pasaporte CE/CI

Avenida

Distrito: Provincia:

Departamento:

Referencia:

Teléfono:

Acepto que todo acto administrativo derivado del presente procedimiento se me notifique a mi correo electrónico (numeral 4 del artículo 20° del Texto Único Ordenado de la Ley N° 27444).

SI ☐

NO ☐

Si la respuesta es positiva, indicar dirección de correo electrónico:

**II. DATOS DEL DENUNCIADO (TITULAR DEL BANCO DE DATOS PERSONALES O
RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES)**

Titular del banco de datos personales ☐ Responsable del tratamiento ☐

Nombres:

Modelo de consentimiento de tratamiento de datos personales

CONDICIONES DEL TRATAMIENTO DE DATOS PERSONALES

En cumplimiento de lo dispuesto por la Ley N° 29733, Ley de Protección de Datos Personales y su reglamento aprobado por Decreto Supremo N° 003-2013-JUS, (la ENTIDAD) desea poner en conocimiento de sus usuarios, los siguientes aspectos relacionados con sus datos personales:

- 1. IDENTIDAD Y DOMICILIO DEL TITULAR DEL BANCO DE DATOS PERSONALES O ENCARGADO DEL TRATAMIENTO:** El titular del presente banco de datos en el que se almacenarán los datos personales facilitados en la presente solicitud es (indicar) con domicilio en (indicar).

La existencia de este banco de datos personales ha sido declarada a la Autoridad Nacional de Protección de Datos Personales, mediante su inscripción en el Registro Nacional de Protección de Datos Personales con la denominación (indicar) y el código: RNPDP N° (indicar).

Se informa al usuario que, cualquier tratamiento de datos personales, se ajusta a lo establecido por la legislación vigente en PERÚ en la materia (Ley N° 29733 y su reglamento).

- 2. FINALIDAD:** (indicar al titular del banco de datos personales) tratará sus datos con la finalidad de gestionar la presente solicitud y/o contrato. (Se hará constar una referencia al contrato o tipo de contrato de que se trate, con el detalle suficiente para que no quepa ninguna ambigüedad sobre lo que se refiere).

Adicionalmente, usted autoriza a (indicar al titular del banco de datos personales) para: (indicar en detalle cada finalidad no vinculada a la ejecución de la relación contractual para la cual necesita el consentimiento, por ejemplo, envío de comunicaciones referidas a promociones, comunicaciones comerciales de sus productos, entre otros).

Ejemplo:

Autorizo el envío de comunicaciones referidas a promociones. Sí acepto ☐

No acepto ☐

Sus datos personales sólo serán utilizados con propósitos limitados, tal como los expuestos precedentemente.

Firma electrónica y consentimiento expreso

La Ley N.º 29733 reconoce que el **consentimiento expreso** no solo se da a través de una firma manuscrita. También puede manifestarse mediante:

- Una **firma electrónica** (con mecanismos criptográficos),
- Una **firma digitalizada** (imagen de la firma escaneada),
- O una acción directa del usuario como **hacer clic en “acepto”** o marcar una casilla.

Incluso, el acto de **“pinchar” un botón**, registrarse en una aplicación o realizar una acción específica en un dispositivo se considera un **acto afirmativo inequívoco**, y por tanto, un consentimiento válido según la ley.

Consentimiento informado

El titular de los datos personales tiene derecho a ser **debidamente informado** antes de entregar su información. Esto implica que se le debe comunicar:

- **La identidad y dirección del responsable del banco de datos,**
- **La finalidad exacta** para la cual se solicitan los datos,
- **Qué tipo de tratamiento se dará** a su información,
- **Cómo puede ejercer su derecho a revocar** ese consentimiento más adelante.

Esto está estipulado claramente en el artículo 18 de la ley y **el titular tiene derecho a saber a quién debe dirigirse para cancelar o modificar el uso de sus datos.**

El derecho a revocar el consentimiento

Muchas personas no saben que tienen derecho a decir **“ya no quiero que usen mis datos”**, incluso si firmaron o marcaron “acepto” en algún momento.

El titular puede presentar una **solicitud de revocación** ante la empresa u organización que está usando sus datos. Esta tiene un plazo legal —generalmente entre **60 y 90 días hábiles**— para procesar la solicitud y responder.

El problema es que **muy pocas organizaciones indican claramente cómo ejercer este derecho**, ni quién es el encargado interno de gestionar solicitudes de datos personales.

¿Dónde están nuestros datos? ¿Quién los gestiona?

Toda entidad que recolecte datos personales debe tener un **Banco de Datos Personales inscrito** ante la **Autoridad Nacional de Protección de Datos Personales (ANPDP)**. Este banco de datos debe:

- Estar documentado,

- Tener reglas de acceso,
- Informar quién tiene permiso para consultarlo o modificarlo,
- Proteger la información almacenada en sus servidores (por ejemplo, dentro de la OTI – Oficina de Tecnologías de la Información, en el caso de universidades).

En el ámbito educativo, por ejemplo, los **formularios de matrícula** recopilan datos sensibles:

- Datos de salud,
- Datos socioeconómicos,
- Información familiar,
- Nivel de ingresos,
- Lugar de residencia.

¿Dónde se almacenan esos datos? ¿Quién accede a ellos? ¿Quién puede modificarlos?

Todo eso **debe ser informado al titular**, aunque en la práctica, **casi nunca se cumple**.

Tratamiento de datos sensibles

Los **datos sensibles** incluyen:

- Orientación sexual,
- Creencias religiosas,
- Discapacidad,
- Estado de salud,
- Datos biométricos,
- Condenas o antecedentes penales,
- Información sobre infracciones administrativas.

Para que estos datos puedan ser tratados:

- El consentimiento debe ser **expreso y por escrito**.
- Debe detallarse **la finalidad específica** del tratamiento.
- El titular **puede revocar su consentimiento** en cualquier momento.

Además, el artículo 15 indica que **las telecomunicaciones y sistemas informáticos de carácter privado** solo pueden ser intervenidos **por mandato judicial**, por ejemplo:

- Levantamiento de comunicaciones,

- Acceso a cuentas bancarias,
 - Información financiera o historial penal.
-

¿Y qué sucede en la práctica?

Muchas organizaciones:

- **No informan al titular** sobre el uso exacto de sus datos,
- **No tienen canales visibles** para ejercer el derecho de revocatoria,
- **Reutilizan o comparten la información** sin consentimiento real.

La ley es clara, pero su cumplimiento **es débil**. Falta:

- Fiscalización activa del Estado,
- Formación del ciudadano sobre sus derechos,
- Transparencia real en las instituciones públicas y privadas.

¿Qué datos no necesitan consentimiento para su tratamiento?

Aunque la **Ley N.º 29733** establece que el consentimiento del titular es esencial para tratar sus datos personales, también contempla **excepciones**. Es decir, hay **casos específicos en los que no es necesario que la persona autorice expresamente** el uso de su información.

1. Entidades públicas en el ejercicio de sus funciones

No se requiere consentimiento cuando los datos personales son tratados por:

- La **Contraloría General de la República**,
- El **Poder Judicial**,
- La **Policía Nacional**,
- El **Ministerio Público**,
- Y otros organismos del Estado que actúan dentro de su marco legal.

Por ejemplo:

- Antecedentes penales, judiciales o civiles **pueden ser verificados por estas entidades** sin pedir permiso.
- **Cuando postulas a un trabajo**, muchas veces te piden presentar certificados de antecedentes.
Pero solo el **Poder Judicial o el Ministerio del Interior** puede emitirlos oficialmente.

El empleador **no tiene derecho a acceder directamente a tus datos penales** sin tu consentimiento o sin el documento oficial.

2. Publicaciones por transparencia

Cuando los datos personales aparecen en:

- Portales de transparencia,
- Registros de acceso público,
- Listas de servidores públicos,
- Boletines institucionales,

No se requiere consentimiento, ya que se considera que:

- **La información tiene un fin público,**
- Forma parte del principio de **transparencia del Estado,**
- Y está protegida por la **Ley de Transparencia y Acceso a la Información Pública.**

Ejemplo: los sueldos y cargos de los funcionarios públicos son datos personales, **pero deben ser publicados** por mandato de ley.

3. Evaluación de solvencia crediticia

Cuando solicitas un préstamo o crédito, las entidades financieras pueden consultar:

- Tu historial crediticio,
- Tus propiedades registradas,
- Deudas vigentes o pasadas.

No necesitas autorizar expresamente ese acceso, porque forma parte del análisis de riesgo de la entidad. Esto es legal mientras se haga con fines de **evaluación crediticia** y a través de **centrales de riesgo autorizadas** como Infocorp.

4. Promoción de la competencia en sectores regulados

Por ejemplo, en el sector de telecomunicaciones:

- Se obliga a operadoras como Telefónica o Claro a compartir cierta información de clientes con otras operadoras, para fomentar la **libre competencia** y evitar monopolios.
-

5. Relaciones contractuales

Cuando vas a firmar un contrato (de compra-venta, alquiler, trabajo, etc.), **no necesitas autorizar** por separado que tus datos sean usados. Su tratamiento es **necesario y legítimo** para:

- Preparar el contrato,
 - Validar tu identidad,
 - Emitir recibos, facturas, escrituras u otros documentos legales.
-

¿Cómo nacen las leyes? ¿Siempre responden a la realidad?

Esta es una pregunta **clave** para entender el sistema legal.

Las leyes deberían nacer como respuesta a:

- **Necesidades sociales reales,**
- **Conflictos legales sin solución clara,**
- **Vacíos normativos,**
- Y situaciones que requieren regulación específica.

Sin embargo, **no siempre ocurre así**. En muchos casos, las leyes:

- Se generan **por conveniencia política,**
- Responden a **intereses de grupos económicos,**
- O son propuestas que **no tienen sustento técnico ni jurídico sólido.**

Ejemplo:

Hay congresistas que presentan leyes para temas que los benefician directamente. Incluso, algunas propuestas **reproducen ideas privadas** (de bancos, empresas, gremios), lo cual distorsiona la finalidad pública de la legislación.

¿Quién crea las leyes?

En Perú, el **Congreso de la República** es el encargado de legislar. Los congresistas:

- Presentan proyectos de ley,
- Debaten en comisiones,
- Aprueban en el pleno.

Sin embargo, **la calidad de las leyes depende de la preparación y visión de los legisladores**, así como del asesoramiento técnico que reciben.

Históricamente, en Perú existía una **bicameralidad** (Senado y Cámara de Diputados), pero ahora el Congreso es **unicameral**, lo cual ha generado tanto ventajas como desafíos.

Derechos ARCO



¿Qué son los derechos ARCO?


Los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) permiten al ciudadano obtener información sobre sus propios datos y el tratamiento que les dan: cuál es su origen, finalidad y de qué forma se están comunicando o compartiendo.

- **Acceso:** el derecho a saber qué datos personales tienen sobre ti, preguntar cómo los obtuvieron, para qué los utilizaron, con quién los han compartido y todos los detalles de su uso.
- **Rectificación:** el derecho a modificar y actualizar tus datos personales, cuando estos sean erróneos, inexactos o incompletos.
- **Cancelación:** el derecho a cancelar el uso de tus datos personales cuando la finalidad para la que los entregaste ha concluido, venció el plazo establecido para su tratamiento, o revocaste el consentimiento.
- **Oposición:** el derecho a oponerte al uso de tus datos porque te están generando un perjuicio en diversos ámbitos, situación que se presenta con mayor frecuencia en plataformas digitales.

Si una persona no está de acuerdo con la respuesta, puede hacer un reclamo **solicitando el procedimiento trilateral** a la **Autoridad Nacional de Protección de Datos Personales (ANPD)**.

<https://www.gob.pe/9270-que-son-los-derechos-arco>

<https://www.gob.pe/9269-iniciar-procedimiento-para-el-ejercicio-de-derechos-de-acceso-rectificacion-cancelacion-y-oposicion>



```
graph TD; A[Presentar solicitud] --> B[Esperar respuesta  
(derecho de acceso: 20 días hábiles;  
derecho de rectificación, cancelación  
u oposición: 10 días hábiles).]; B --> C[Si no responden o deniegan la solicitud]; C --> D[Si no responden o deniegan la solicitud,  
puede presentar RECLAMO]; D --> E[Esperar 30 días hábiles  
por respuesta de la ANPD];
```

INFRACCIONES:

Son infracciones leves:

- ☐ Dar tratamiento a D.P sin el consentimiento de sus titulares, cuando lo requiere.
- ☐ Obstruir el ejercicio de la función fiscalizadora de la A.N.P.D.P

Son infracciones graves:

- ☐ Incumplir la obligación de confidencialidad establecida en el artículo 17.

- ☐ Impedir en forma sistemática, ejercicio de derechos del titular de D.P y funciones A.N.P.D.P
- ☐ No inscribir el B.D.P en el Registro Nacional de Protección de D.P.

Son infracciones muy graves:

- ☐ Crear, modificar, cancelar o mantener B.D.P sin cumplir con lo establecido
- ☐ Suministrar documentos o información falsa o incompleta a la A.N.P.D.P.
- ☐ No cesar en el tratamiento ilícito de D.P, cuando lo ha requerido la A.N.P.D.P.
- ☐ No inscribir el B.D. en el R.N.P.D, no obstante haber sido requerido para ello por la A.N.P.D.P.

SANCIONES:

1. Las infracciones leves son sancionadas con una multa mínima desde **0.5** de una UIT hasta **5** UIT.
 2. Las infracciones graves son sancionadas con multa desde más de **5 UIT** hasta **50 UIT**.
 3. Las infracciones muy graves son sancionadas con multa desde más de **50 UIT** hasta **100 UIT**.
 4. En ningún caso, la multa impuesta puede exceder del diez por ciento de los ingresos brutos anuales que hubiera percibido el presunto infractor durante el ejercicio anterior.
- (art. 39 de la Ley 29733)

¿Para qué sirve una ley si no se entiende su espíritu?

Muchos jóvenes se preguntan:

“¿Para qué sirve una ley si se contradice con otra, o si no se cumple de verdad?”

Y es una pregunta legítima. Porque en Perú, **tenemos leyes para casi todo**, pero también muchos **vacíos, contradicciones, parches y malas interpretaciones**.

El problema no es que haya leyes, sino **cómo se hacen** y **quiénes las hacen**. Hoy en día, cualquiera puede postular al Congreso:

- Basta con tener **25 años**,
- **Saber leer y escribir**,
- Y ser peruano de nacimiento.

No es necesario tener estudios superiores, ni experiencia legislativa, ni formación técnica. **Así se legisla en un país donde los problemas son complejos, pero las soluciones son simples... o improvisadas.**

¿Por qué nacen las leyes?

Idealmente, una ley debe nacer por:

- Una necesidad social real,
- Un vacío normativo,
- Un problema que requiere regulación formal,
- O como evolución de un derecho fundamental.

Pero muchas veces, las leyes en Perú:

- Nacen **por presión política o popular**,
 - Responden a **intereses particulares o coyunturales**,
 - Y **no tienen un análisis técnico profundo**.
-

Casos reales: el sistema universitario y sus contradicciones

Un ejemplo claro es lo que ha pasado con la **Ley Universitaria** y sus múltiples ajustes:

- Se implementó el **bachillerato automático**, pero no se respetó el criterio del “espíritu” de la ley.
- Se pidió que los estudiantes lleven un curso llamado “**Trabajo de investigación**”, como si el **nombre del curso** fuera lo más importante.
- Universidades que ya tenían cursos con enfoques metodológicos o seminarios de tesis, **tuvieron que cambiar de nombre solo para “cumplir” con la ley**.
- Algunas instituciones —como mencionaste en tu caso— **no cambiaron el nombre**, porque comprendieron que **lo que importa es el contenido y la competencia desarrollada**, no el rótulo del curso.

Luego, para mayor ironía, **el mismo SUNEDU emitió una resolución (diciembre 2024)** interpretando que:

“De acuerdo con la autonomía universitaria, el nombre del curso lo define cada institución.”

Entonces... ¿cuántas universidades **modificaron sus planes, temarios y currículos innecesariamente** por una interpretación forzada de la ley?

¿Y cuántos estudiantes se vieron **perjudicados o confundidos** por estos cambios mal ejecutados?

Lecciones de fondo

Lo que esto revela es algo más grande:

- Las **formas legales** no deben imponerse sobre el **fondo pedagógico**.
- Las leyes deben ser **claras, coherentes y viables**.
- Las instituciones deben tener **autonomía técnica**, pero también **criterio profesional** para interpretar y aplicar la ley con sentido.
- Y sobre todo, **los legisladores deben ser verdaderos técnicos del bien común**, no solo figuras políticas.

Cuando el nombre importa más que el fondo: una ley mal entendida

En Perú, se han “matado” —literalmente— por **el nombre de un curso**. El fondo se olvidó. Lo que importó fue cómo se llamaba, no **qué competencias desarrollaba** el estudiante.

La famosa exigencia del curso “**Trabajo de Investigación**” para el bachillerato automático, originada en la Ley Universitaria, fue malinterpretada y aplicada de manera mecánica por muchas universidades. ¿Qué ocurrió?

- Algunas instituciones tenían **semilleros de investigación, seminarios, proyectos de titulación**, pero se vieron **obligadas a cambiar el nombre del curso** solo para “cumplir”.
- Incluso se aceptó que estudiantes lleven ese curso **sin haber cumplido requisitos básicos**.
- Y se olvidó por completo lo que el **espíritu de la ley** buscaba: formar estudiantes capaces de **investigar, argumentar y proponer**.

Todo eso fue el resultado de una **ley imprecisa**, de libre interpretación, **mal entendida por asesores, autoridades y operadores**.

El idioma: otro requisito vaciado de sentido

Lo mismo ha pasado con el **requisito del idioma**. Se supone que un profesional debe tener competencias mínimas en un segundo idioma —generalmente inglés—, al menos en lectura técnica.

Pero en la práctica:

- **Se aprueba con un solo semestre**, en muchos casos con contenido básico.
- **Se validan certificados de academias privadas** sin criterios estandarizados.
- **No se evalúa comprensión lectora real** ni capacidad para interpretar textos especializados.

La consecuencia: cuando llega el momento de **leer papers, sustentar tesis o postular a posgrados**, muchos estudiantes **no comprenden lo que leen**. Y el requisito fue simplemente **un trámite cumplido en papel**, no en la práctica.

El consentimiento y la salud: ¿cuándo se vuelve opcional?

Volviendo al tema de la **protección de datos personales**, la ley reconoce **excepciones** donde **no se necesita el consentimiento del titular**. Por ejemplo:

En salud:

- Cuando existe **riesgo para la salud pública**.
- Para **prevención, diagnóstico o tratamiento médico**.
- En contextos de **emergencia sanitaria**, como la **pandemia del COVID-19**.

Ejemplo real:

Durante el COVID, se publicaban listas de personas contagiadas, zonas de riesgo, contactos cercanos. Se vulneraba parcialmente la privacidad, **pero con justificación legal y sanitaria**.

Datos en organizaciones sin fines de lucro

La ley también exime del consentimiento en casos como:

- **Organizaciones religiosas,**
- **Sindicatos,**
- **Partidos políticos.**

Es decir, si una persona pertenece a una de estas entidades, **la institución puede tratar sus datos sin autorización previa**, siempre que se limite a sus fines específicos.

Sin embargo, eso no impide que existan **abusos o filtraciones**. Y muchas veces el ciudadano **ni siquiera sabe que está firmando una autorización amplia** al inscribirse en una comunidad religiosa o club político.

Lavado de activos, terrorismo y fiscalización financiera

Hay contextos donde la privacidad **deja de ser protegida** por el bien común:

- **Investigaciones por lavado de activos,**
- **Financiamiento del terrorismo,**
- **Operaciones sospechosas detectadas por la Unidad de Inteligencia Financiera (UIF).**

En estos casos:

- Se puede **levantar el secreto bancario y tributario,**
 - Acceder a tus **bienes, propiedades, cuentas y vínculos familiares,**
 - Y construir un **perfil financiero completo,** sin necesidad de tu consentimiento.
-

Conclusión reflexiva

Una ley mal entendida puede causar más daño que su ausencia.

En Perú, muchas veces el sistema legal **prioriza la forma antes que el fondo:**

- Se cambia el nombre de un curso, pero **no se fortalece su contenido.**
- Se exige saber inglés, pero **no se comprueba la competencia.**
- Se exige cumplir requisitos, pero **no se forma un verdadero profesional.**

Y en paralelo:

- Tenemos leyes como la N.º 29733 que **protegen nuestros datos personales,**
- Pero con tantas **excepciones, vacíos y falta de fiscalización,** que el ciudadano queda **desprotegido.**

El reto no es solo tener más leyes.

El reto es **tener buenas leyes, bien aplicadas y mejor comprendidas.**

Y, sobre todo, que quienes las hagan **sepan para qué las hacen.**

¿Protección de datos... o exposición legalizada?

Aunque la **Ley de Protección de Datos Personales (N.º 29733)** establece una serie de mecanismos para cuidar nuestra privacidad, **la realidad muchas veces muestra lo contrario.**

En la práctica, nuestros datos **se venden, se filtran o se reutilizan sin consentimiento claro.**

Un ejemplo preocupante es lo que sucede en **Telegram**, donde se ofrecen servicios como:

“Borramos tu historial crediticio por 2000 soles”.

Esto **no lo hacen piratas externos.** Muchas veces, los mismos trabajadores internos de instituciones (como centrales de riesgo, bancos o financieras) **usan su acceso autorizado para ofrecer servicios ilegales.**

No se trata de “hackers”, sino de **empleados con acceso legítimo que rompen la ley**. Por eso el problema **no siempre está en la seguridad del sistema**, sino en la **ética y control del personal que manipula los datos**.

Historial crediticio: ¿se borra?

No. El historial crediticio **no se borra como tal**. Lo que sucede es que:

- Puedes **comenzar a construir nuevo historial positivo**, que con el tiempo **diluye el pasado negativo**.
- Pero los registros antiguos, en la mayoría de sistemas, **quedan guardados como históricos**.
- Lo que se puede hacer legalmente es **corregir errores** (por ejemplo, si ya pagaste y no fue actualizado).

Quienes acceden a tu historial:

- **Bancos y cajas municipales,**
- **Financieras, cooperativas, casas comerciales,**
- **Notarías** (para compra/venta de inmuebles),
- **Empresas que ofrecen créditos al consumo.**

Todo esto **está regulado por ley**, pero también es utilizado en **exceso o sin transparencia** por el mercado.

¿Y la ley protege al ciudadano?

La **Autoridad Nacional de Protección de Datos Personales** (del Ministerio de Justicia) es el órgano encargado de velar por el cumplimiento de esta ley. En su portal puedes:

- Descargar **formularios de denuncia**,
- Revocar tu consentimiento al tratamiento de datos,
- Solicitar que **no se te envíe más publicidad** (Ley de No Llamar),
- Presentar reclamos contra empresas u organizaciones que usen tus datos sin autorización.

Sin embargo:

- El trámite es **lento**, puede tardar entre **60 y 90 días hábiles**,
- No siempre hay respuesta oportuna,

- Y muchas veces el ciudadano **desiste por frustración** o desconocimiento del proceso.
-

¿Y qué pasa con los datos que usamos a diario?

Empresas como **Google, Meta (Facebook), TikTok, etc.**, ofrecen servicios gratuitos a cambio de tus datos. Esto es legal, porque **aceptaste los términos y condiciones**, incluso si **no los leíste**.

Pero si alguien ajeno (un compañero, empresa, vendedor informal) **usa tus datos sin tu consentimiento**, sí se configura una infracción.

Por eso es tan importante conocer los **Derechos ARCO**.

¿Qué son los Derechos ARCO?

Los Derechos ARCO son los **derechos fundamentales** que todo ciudadano tiene respecto al tratamiento de sus datos personales. Son:

1. Acceso

- Puedes saber **qué datos tuyos tienen**, dónde están, y para qué los usan.

2. Rectificación

- Puedes solicitar la **corrección de errores** o actualizaciones.

3. Cancelación

- Puedes pedir que **se eliminen tus datos** cuando ya no sean necesarios.

4. Oposición

- Puedes **negarte a que tus datos sean utilizados** para ciertos fines, como publicidad.
-

Conclusión: ¿protección o vulnerabilidad?

La **Ley N.º 29733** es un avance importante, pero aún está lejos de garantizar una protección real en la práctica. ¿Por qué?

- Hay **falta de fiscalización efectiva**,
- La ciudadanía **no conoce ni ejerce sus derechos**,
- Las empresas abusan de los formularios y de las letras pequeñas,

- Y el **mercado negro de datos personales sigue activo** en redes sociales y mensajería instantánea.

La única forma de equilibrar esto es con:

- **Educación digital** desde las escuelas,
- **Campañas de sensibilización masivas,**
- Y una **ciudadanía activa que denuncie y exija respeto por su privacidad.**

Entre lo privado y lo público: el ciudadano frente a su propia exposición

Una de las grandes paradojas de la era digital es que **mientras exigimos que nuestras instituciones protejan nuestros datos, nosotros mismos muchas veces los exponemos voluntariamente.**

Publicamos:

- Nuestra **dirección,**
- Nuestro **número de teléfono,**
- Nombres de nuestros **padres, hijos o pareja,**
- Fotografías de nuestro hogar, nuestras rutinas, incluso nuestra salud...

Y luego nos preguntamos:

“¿Cómo es que alguien tiene acceso a mi información personal?”

¿Dónde están mis datos? ¿Quién accede?

Los **Derechos ARCO** garantizan que toda persona puede:

- **Acceder** a saber dónde están sus datos y quién los utiliza,
- **Rectificarlos** si son incorrectos o están desactualizados,
- **Cancelar su uso** cuando ya no son necesarios,
- **Oponerse** a su tratamiento cuando afectan sus derechos.

Ejemplo práctico:

Al llenar una ficha socioeconómica en la universidad, entregas datos sensibles. Pero, ¿sabes quién puede acceder a ellos? ¿Solo el área de admisión o también cualquier docente, administrador o externo?

¿Y si la información fue usada con otra finalidad?

Si entregaste tus datos para un fin específico (como matricularte), y luego esa información **se usa para enviarte publicidad, compartirse con terceros, o aparecer en campañas de marketing sin tu permiso**, se está violando el principio de **finalidad y consentimiento informado**.

Incluso el **uso de tu imagen** sin autorización —como en fotografías institucionales, videos promocionales o redes sociales— debe ser regulado. Si no diste consentimiento:

- La imagen debe **ser censurada o difuminada**,
 - O debe existir una autorización firmada.
-

El dilema del consentimiento y la autocompartición

Cuando una persona **publica voluntariamente** sus datos o imágenes en redes sociales, **pierde parte del control** sobre su información. Si tú haces público:

- Tu ubicación,
- Tu número de teléfono,
- Tus rutinas o incluso tu estado de salud,

Entonces, difícilmente puedes exigir privacidad total sobre eso.

Ahí es donde entra la educación digital.

Conciencia ≠ culpa

El problema no es publicar, sino **no saber las consecuencias de lo que publicamos**.

¿Y qué pasa si una empresa o institución usa mal mis datos?

Toda empresa u organización que trata datos debe:

- Informar su **base de datos** ante la Autoridad Nacional de Protección de Datos Personales (ANPDP),
 - Solicitar **consentimiento informado**,
 - Permitir **ejercer los derechos ARCO**,
 - **No compartir datos con terceros** sin justificación legal.
-

¿Infracción o delito?

No todo uso indebido de datos es un delito penal. La ley distingue entre:

- **Infracción administrativa** (leve, grave o muy grave):
→ Se sanciona con **multas económicas** por la ANPDP.
- **Delito penal**:
→ Cuando hay **intención de dañar**, extorsionar, chantajear, lucrar o discriminar.
→ Se sanciona con **penas de cárcel**, según el Código Penal.

Ejemplo de infracción:

Una empresa usa tu número para enviar publicidad sin tu autorización.

Ejemplo de delito:

Alguien difunde tus datos personales (como dirección o número) en un grupo público para hostigarte o dañar tu reputación.

Infracciones, sanciones y el peso desigual de la ley

La **Ley N.º 29733** establece claramente que **las empresas e instituciones que tratan datos personales tienen responsabilidades legales**. Si incumplen la ley, incurren en **infracciones administrativas** que se clasifican en:

◆ **Leves**

- No informar adecuadamente al titular de los datos.
- Tratar datos sin medidas mínimas de seguridad.
- **Sanción:** Puede no incluir multa, o sanciones menores.

◆ **Graves**

- Impedir sistemáticamente que el titular ejerza sus derechos (ARCO).
- **No inscribir su base de datos** en el Registro Nacional de Protección de Datos Personales (RNPDP).
- No respetar el principio de confidencialidad.
- **Sanción:** Hasta **50 UIT** (aproximadamente S/ 257,500).

◆ **Muy graves**

- Crear, modificar o eliminar bases de datos sin autorización.
 - Proveer documentación falsa o incompleta a la Autoridad Nacional.
 - Usar datos personales a pesar de la negativa o retiro del consentimiento.
 - **Sanción:** Hasta **100 UIT** o el **10% de los ingresos brutos anuales**.
-

¿Quién infringe? ¿Y a quién se sanciona?

Estas infracciones se aplican a:

- **Empresas privadas** (bancos, operadoras, tiendas, hoteles, etc.),
- **Instituciones públicas** (ministerios, universidades, municipalidades).

Sin embargo, **la ley no está diseñada para sancionar al ciudadano común**, sino a quienes **almacenan, comparten, manipulan o comercializan bases de datos** sin el debido cumplimiento legal.

Pero aquí aparece el problema:

La ley existe. Las sanciones también. Pero el cumplimiento real es escaso.

¿Multas que duelen?

- A una **gran empresa**, pagar una multa de 50,000 soles puede ser insignificante.
- A una **pyme**, la misma multa puede significar el cierre del negocio.
- La ley contempla sanciones proporcionales (como el 10% de los ingresos brutos), pero rara vez se aplican en toda su magnitud.

Además, muchas veces las empresas:

- **No inscriben sus bases de datos,**
- **No tienen políticas de privacidad claras,**
- **No cumplen los procedimientos**
- ,
- **No cumplen los procedimientos** para atención de reclamos.

Y aun así, **no reciben sanción efectiva**, o simplemente **el proceso se diluye** entre trámites, apelaciones y lentitud administrativa.

Caso adicional: spam telefónico

En 2018 se emitió un **decreto legislativo** que modificó la **Ley de Protección y Defensa del Consumidor**, incluyendo el tema de **llamadas y mensajes no solicitados**.

Según la norma:

- Toda llamada publicitaria debe tener **consentimiento previo, expreso e informado**.
- El ciudadano tiene derecho a **revocar su consentimiento** en cualquier momento.

- Las empresas deben contar con un **registro de números excluidos** para no volver a llamar.

Pero... ¿se cumple?

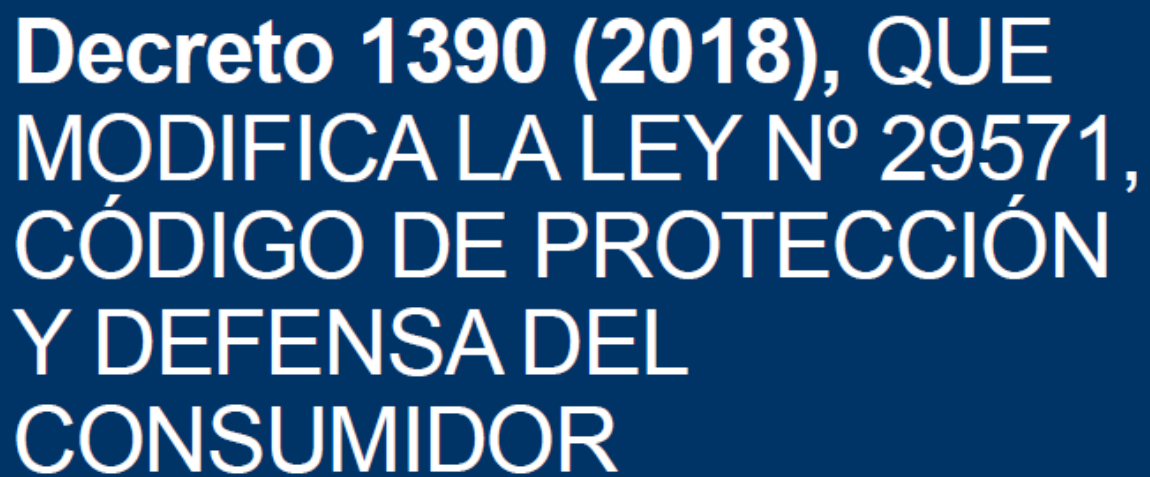
No.

La trampa está en que el ciudadano debe **hacer el reclamo primero ante la empresa infractora**.

Si no haces nada, **te seguirán llamando**.

Si no reclamas, **tu número seguirá circulando**.

Y aunque existe el servicio “**Registro ‘Gracias... no insista’**” del INDECOPI, **muy pocos ciudadanos saben cómo funciona**, y las empresas **pocas veces lo respetan**.



**Decreto 1390 (2018), QUE
MODIFICA LA LEY N° 29571,
CÓDIGO DE PROTECCIÓN
Y DEFENSA DEL
CONSUMIDOR**

**DECRETO LEGISLATIVO
QUE MODIFICA LA LEY N° 29571,
CÓDIGO DE PROTECCIÓN Y DEFENSA
DEL CONSUMIDOR**

Artículo 1.- Modificación del literal e) del numeral 58.1 del artículo 58, del artículo 106, del literal f) del segundo párrafo del artículo 108, del numeral 3 del tercer párrafo del artículo 112, del primer y segundo párrafo del artículo 125, del artículo 130, del numeral 131.1 del artículo 131 y del segundo párrafo del artículo 154 del Código de Protección y Defensa del Consumidor, aprobado por la Ley N° 29571.

Modifíquese el literal e) del numeral 58.1 del artículo 58, el artículo 106, el literal f) del segundo párrafo del artículo 108, el numeral 3 del tercer párrafo del artículo 112, el primer y segundo párrafo del artículo 125, el artículo 130, el numeral 131.1 del artículo 131 y el segundo párrafo del artículo 154 del Código de Protección y Defensa del Consumidor, aprobado por la Ley N° 29571, en los términos siguientes:

"Artículo 58.- Definición y alcances

58.1 El derecho de todo consumidor a la protección contra los métodos comerciales agresivos o engañosos implica que los proveedores no pueden llevar a cabo prácticas que mermen de forma significativa la libertad de elección del consumidor a través de figuras como el acoso, la coacción, la influencia indebida o el dolo.

En tal sentido, están prohibidas todas aquellas prácticas comerciales que importen:

(...)

e. Emplear centros de llamada (call centers), sistemas de llamado telefónico, envío de mensajes de texto a celular o de mensajes electrónicos masivos para promover productos y servicios, así como prestar el servicio de telemarketing, a todos aquellos números telefónicos y direcciones electrónicas de consumidores que no hayan brindado a los proveedores de dichos bienes y servicios su consentimiento previo, informado, expreso e inequívoco, para la utilización de esta práctica comercial. Este consentimiento puede ser revocado, en cualquier momento y conforme a la normativa que rige la protección de datos personales.

(...)"

<https://repositorio.indecopi.gob.pe/bitstream/handle/11724/6401/DL.1390.pdf?sequence=1&isAllowed=y>

**LEY QUE MODIFICA LA LEY 29571, CÓDIGO DE PROTECCIÓN Y DEFENSA DEL CONSUMIDOR,
RESPECTO A LA PROHIBICIÓN DE LAS LLAMADAS SPAM**

Artículo 1.- Modificación del literal e) del numeral 58.1 del artículo 58, del Código de Protección y Defensa del Consumidor, aprobado por la Ley 29571, modificado por el Decreto Legislativo N° 1390.

Se modifica el literal e) del numeral 58.1 del artículo 58, del Código de Protección y Defensa del Consumidor, aprobado por la Ley N° 29571, modificado por el Decreto Supremo N° 1390 en los términos siguientes:

"Artículo 58.- Definición y alcances

58.1 El derecho de todo consumidor a la protección contra los métodos comerciales agresivos o engañosos implica que los proveedores no pueden llevar a cabo prácticas que mermen de forma significativa la libertad de elección del consumidor a través de figuras como el acoso, la coacción, la influencia indebida o el dolo.

En tal sentido, están prohibidas todas aquellas prácticas comerciales que importen:

(...)

e) Que los proveedores puedan utilizar centros de llamada (Call Centers), sistemas de llamado telefónico, envío de mensajes de texto a celular o de mensajes electrónicos masivos para promover sus productos y servicios, así como prestar el servicio de telemarketing, a ningún consumidor. Sólo podrán enviar información y publicidad a los consumidores que se contacten directamente con el proveedor y soliciten, dando su consentimiento informado, expreso e inequívoco, que desean ser contactados. Sólo en ese caso, los proveedores podrán utilizar aquellos números telefónicos y direcciones electrónicas de consumidores que hayan brindado a los proveedores de dichos bienes y servicios su consentimiento, para la utilización de esta práctica comercial. Este consentimiento puede ser revocado, en cualquier momento y conforme a la normativa que rige la protección de datos personales. Recurrir a esta práctica sin contar con el consentimiento del consumidor, se considerará infracción muy grave y podrá ser sancionado por la Autoridad de Consumidor. Esto sin perjuicio de las competencias de la Autoridad de Datos para el inicio de un procedimiento fiscalizador. Se considerará un agravante que el proveedor se contacte con consumidores considerados vulnerables y la carga de la prueba, en un procedimiento administrativo sancionador, recaerá en el proveedor, quien deberá probar que cuenta con el consentimiento del consumidor. La Autoridad de Consumidor y la Autoridad de Datos efectuarán acciones educativas y fiscalizadoras conjuntas e informarán anualmente a la Comisión de Defensa del Consumidor y Organismos Reguladores de los Servicios Públicos, las acciones realizadas y sus resultados.

ECONOMÍA

10 ENE 2023 | 15:21 h

**Congreso: Comisión aprueba
predictamen para prohibir las
llamadas spam**

Por unanimidad, los miembros de la Comisión de Defensa del Consumidor aprobaron la iniciativa que busca proteger los datos personales de los ciudadanos.



Congreso del Perú

@congresoperu · Seguir

#PlenoDelCongreso | Se sustentan los proyectos de ley 2942, 3131 y 3541 que proponen modificar la Ley 29571, Código de Protección y Defensa del Consumidor, a fin de ampliar la prohibición de las comunicaciones spam.

Detalles de la autógrafa

El texto modifica los literales d) y e) del numeral 58.1 del artículo 58, de la Ley 29571, Código de Protección y Defensa del Consumidor.

En esa línea, queda prohibida las visitas en persona al domicilio del consumidor o realizar proposiciones no solicitadas, por teléfono, fax, correo electrónico u otro medio, de manera persistente e impertinente, o ignorando la petición del consumidor para que cese este tipo de actividades.

Asimismo, en ningún caso las proposiciones solicitadas -si el consumidor lo solicita- podrán realizarse entre las 20:00 horas y las 7:00 horas, ni los días sábados, domingos ni feriados.

Ley 30096 – Ley de Delitos Informáticos

Ley 30096 – Ley de Delitos Informáticos

Timeline de la Ley de Delitos Informáticos



Delitos contra datos y sistemas informáticos

- ☐ Artículo 2. Acceso ilícito
- ☐ Artículo 3. Atentado a la integridad de datos informáticos
- ☐ Artículo 4. Atentado a la integridad de sistemas informáticos
- ☐ Artículo 5. Propositiones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos.
- ☐ Artículo 7. Interceptación de datos informáticos.
- ☐ Artículo 8. Fraude informático
- ☐ Artículo 10. Abuso de mecanismos y dispositivos informáticos

Incorporación del art. 12 a la Ley

Artículo 12. **Exención de responsabilidad penal**

- ☐ Está exento de responsabilidad penal el que realiza las conductas descritas en los artículos 2, 3, 4 y 10 con el propósito de llevar a cabo **pruebas autorizadas** u otros procedimientos autorizados destinados a **proteger sistemas informáticos**.

Penas

- ☐ Entre **1 y 8 años** de pena privativa de la libertad
- ☐ En **interceptación de datos**, la pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanía nacionales. Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos.
- ☐ Si el delito de **fraude informático** va en contra del patrimonio del Estado que va destinado a programas sociales se incrementa hasta **10 años** de pena privativa de la libertad.
- ☐ Ley 27269 – Firmas digitales (2000)
- ☐ Ley 28493 – Ley contra Spam (2005)
- ☐ Ley 30999 - Ley de Ciberdefensa (2019)
- ☐ Convenio de Budapest (Tratado Europeo 185, Decreto Supremo 010-2019-RE)

La Ley de Delitos Informáticos en el Perú: avances, vacíos y nuevas amenazas

En el Perú, la **Ley de Delitos Informáticos (Ley N.º 30096)** fue promulgada en el año **2013**, con una modificación posterior en **2014**. Esta legislación nació como respuesta al creciente uso de tecnologías digitales tanto en el Estado como en el sector privado, en un contexto en que:

- **No existía un marco legal específico** para castigar los delitos cometidos con medios informáticos,
- Los **hackeos a instituciones** y empresas comenzaron a masificarse,

- Y empezaron a aparecer **cursos y plataformas que enseñaban técnicas de intrusión**, sin regulación alguna.
-

¿Por qué fue necesaria esta ley?

Antes del 2013, si alguien accedía sin permiso a una red o modificaba datos digitales, **no se le podía procesar penalmente** con precisión. No había un artículo específico en el Código Penal para delitos como:

- Acceso no autorizado a un servidor,
 - Intercepción de comunicaciones digitales,
 - Alteración de información en bases de datos (por ejemplo, cambiar notas),
 - Suplantación de identidad digital,
 - Uso de malware o herramientas de escaneo masivo.
-

Delitos tipificados por la Ley 30096

Algunos de los delitos que contempla esta ley son:

1. Acceso ilícito a sistemas informáticos

- Entrar sin autorización a un sistema, red, servidor o cámara IP.
- Incluso si la contraseña por defecto no fue cambiada, **el acceso sin permiso es delito.**

2. Interferencia de datos

- Modificar, borrar o alterar información sin autorización (por ejemplo: **cambiar notas, editar archivos oficiales**, etc.).

3. Interferencia del funcionamiento del sistema

- Realizar ataques que impidan el funcionamiento normal de servicios o redes (ej. ataques de denegación de servicio, sabotajes digitales).

4. Suplantación de identidad digital

- Hacerse pasar por otra persona en redes, correos o plataformas, **con fines de daño, fraude o acoso.**

5. Uso de datos personales obtenidos ilícitamente

- Acceder o divulgar información privada (como fotos, datos bancarios, historial médico), **sin consentimiento del titular.**

Vacíos de la ley y desafíos reales

La ley, aunque importante, **se ha quedado corta frente a los desafíos actuales**:

- No contempla a fondo **el Internet de las Cosas (IoT)**, donde cámaras, sensores, routers, refrigeradoras, relojes, etc., están expuestos.
- No hay mecanismos ágiles para **rastrear atacantes extranjeros** o delitos transfronterizos.
- No considera las nuevas formas de fraude mediante **deepfakes, IA generativa o estafas por apps móviles**.

Ejemplo claro:

Muchas cámaras IP en hogares, empresas, jardines, incluso en dormitorios, han estado expuestas públicamente en Internet por configuración incorrecta o claves por defecto. ¿Qué pasa si alguien accede a una de ellas desde otro país? ¿A quién se sanciona? ¿Cómo?

¿Qué pasa si se modifica una nota sin autorización?

Modificar calificaciones, asistencia o cualquier información oficial sin permiso **es delito** bajo esta ley. Pero:

- Se necesita **probar quién lo hizo, cuándo y cómo**.
- Muchas veces, **la trazabilidad digital no está bien configurada**, lo que dificulta la investigación.
- **No basta con saber que algo fue alterado**; debe demostrarse técnicamente **la autoría y el daño**.

Reflexión final

La **Ley N.º 30096** fue un avance necesario, pero:

- **Está desactualizada** frente a los riesgos tecnológicos actuales,
- **Carece de mecanismos eficientes para persecución internacional de ciberdelitos**,
- Y muchas veces los atacantes **se escudan en la falta de pruebas técnicas sólidas**.

Además, el ciudadano común, sin saberlo, **puede cometer delitos informáticos** solo por "probar una herramienta" o seguir un tutorial. Por eso, es fundamental:

- **Educar en ética digital desde colegios y universidades**,
- Actualizar la ley con un enfoque técnico y preventivo,

- Y establecer canales rápidos para **denunciar, investigar y sancionar** con proporcionalidad.

Delitos informáticos en detalle: entre lo técnico y lo penal

◆ ¿Qué diferencia hay entre dañar datos y dañar sistemas?

En la **Ley de Delitos Informáticos**, existe una distinción importante:

- **Alteración de datos informáticos (Art. 3)**
Ejemplo: Modificar calificaciones en un sistema académico, cambiar saldos bancarios o borrar archivos de registros.
- **Alteración del sistema informático (Art. 4)**
Ejemplo: Cambiar el comportamiento del sistema, como programar que se duplique una acción, que se envíen copias a terceros, o instalar un malware que redirige tráfico.

👉 En resumen: si modificas el *contenido*, afecta los **datos**; si modificas el *comportamiento*, afecta el **sistema**.

◆ Exposición de menores y delitos sexuales

Si bien el artículo 5 de la ley contempla delitos como el **acoso, proposiciones sexuales o difusión de material indebido hacia menores** en redes sociales, **la práctica penal suele aplicar otros artículos del Código Penal** que tienen penas más severas.

Por eso, muchos casos **se investigan bajo delitos sexuales o acoso agravado**, usando la red social o app como **medio del delito**, pero no como su núcleo.

◆ Interceptación de datos (sniffing)

El **sniffing** es una técnica avanzada para **capturar comunicaciones en red**, pero es también **uno de los delitos más difíciles de detectar y probar** (Art. 7).

- ¿Cómo se prueba que alguien está “escuchando” una red local?
- ¿Cómo saber que interceptó credenciales o información sensible?

Solo se puede evidenciar:

1. **Accediendo al dispositivo sospechoso** (ej. su laptop, celular o servidor),
2. **Y revisando logs o capturas guardadas.**

Si no hay rastro forense, es casi imposible de demostrar legalmente.

◆ Fraude informático: ¿cómo funciona?

Hay fraudes informáticos que se camuflan dentro de sistemas normales. Por ejemplo:

- Automatizar **desvíos de céntimos** desde miles de cuentas hacia una cuenta propia.
- Usar una vulnerabilidad para **pagar menos** por pasajes aéreos, productos o servicios.
- Modificar **algoritmos de cálculo**, impuestos o descuentos.

En estos casos, el **fraude es digital**, pero el **impacto es financiero**, por lo que muchas veces se procesa como **fraude bancario o financiero**, según su impacto y no solo su origen informático.

◆ ¿Y el phishing?

El **phishing** es una técnica, no un delito aislado, y puede servir para:

- **Robar credenciales** (usuarios y contraseñas),
- **Instalar malware o troyanos**,
- **Suplantar identidades**.

¿Dónde entra el delito?

- Si alguien usa credenciales **válidas** que obtuvo por phishing, **el acceso en sí puede parecer legítimo**, pero no lo es. El reto es **probar que no era el titular quien accedía**, sino un tercero.
 - Esto puede investigarse como:
 - **Acceso ilícito** (Art. 2),
 - **Suplantación de identidad** (Art. 9),
 - O incluso **fraude informático**, si hubo beneficio económico.
-

◆ ¿Y si solo tengo datos personales, sin usarlos?

Solo **tener datos personales** no es delito por sí mismo.

El delito ocurre si:

- Se **utilizan sin consentimiento**,
- Se **difunden públicamente**,
- Se **comercializan o se usan para chantaje, fraude o suplantación**.

Ejemplo: si obtengo una lista con nombres, direcciones y números de teléfono, y la vendo sin permiso, **estoy cometiendo un delito de tráfico ilícito de datos** (Art. 10).

El abuso de mecanismos tecnológicos y el hacking ético: ¿dónde está el límite?

◆ Abuso de mecanismos legítimos

Muchos sistemas y protocolos de red tienen funcionalidades diseñadas para facilitar tareas administrativas o de gestión. Sin embargo, **cuando se abusa de estos mecanismos con fines maliciosos**, se puede incurrir en delito, incluso sin necesidad de malware.

Ejemplo:

- Protocolos activos por defecto en redes Windows Server (SMB, NetBIOS, RDP),
- Uso de PowerShell para exfiltración de datos,
- Automatización de ataques DDoS desde redes internas o dispositivos IoT (*botnets*, *zombies*).

⚠ Cuando se utiliza un mecanismo funcional del sistema para ejecutar un acto ilegal, ya no es una simple “configuración”, es **una acción criminal**.

◆ ¿Y si el atacante está en otro país?

La **naturaleza descentralizada y global de Internet** hace extremadamente difícil:

- Identificar al atacante,
- Atribuirle legalmente el acto,
- Y procesarlo penalmente si no existe un convenio internacional.

Por eso, en ciberseguridad se desarrolla un nuevo campo:

🎯 Cazadores de amenazas (Threat Hunters)

Equipos que trabajan en inteligencia ofensiva, rastrean atacantes, generan firmas digitales de ataques y colaboran con **fuerzas del orden internacionales**, como:

- INTERPOL,
 - Europol,
 - FBI (Cyber Division),
 - Policía Nacional con unidades de delitos informáticos.
-

◆ Caso real: el hacker de WannaCry

Un caso emblemático fue el arresto del joven **Marcus Hutchins**, también conocido como *MalwareTech*, quien ayudó a detener el **ransomware WannaCry** en 2017, pero luego fue **detenido en Estados Unidos en 2020** por actividades anteriores vinculadas al malware *Kronos*.

Este caso demostró:

- Que **aunque una persona contribuya al bien**, los delitos anteriores **no prescriben fácilmente**,
 - Y que **la colaboración internacional** puede activarse cuando una persona **viaja a un país con convenio judicial activo**.
-

◆ ¿Es delito hacer pruebas sin autorización?

Sí.

Antes de 2014, incluso hacer un escaneo de red o análisis de vulnerabilidades **sin permiso** era considerado delito, aun si se hacía con fines éticos o educativos.

Muchos cursos de **hacking ético** o **auditoría de sistemas** fueron suspendidos, ya que estaban **fuera del marco legal**.

Pero...

◆ Modificación de la ley en 2014: aparece el "pentesting autorizado"

Gracias a la modificación en 2014, se incluyó esta **cláusula de exención**:

No está penalmente sancionado quien realice pruebas de intrusión, escaneo, análisis o auditoría **con autorización expresa** del titular del sistema.

Esto abrió paso legal a:

- Auditorías de seguridad en empresas,
- Pruebas de penetración (pentesting),
- Simulacros de ciberataque (red team – blue team),
- Cacería de amenazas (threat hunting),
- **Formación académica en hacking ético.**

💡 Pero solo si están debidamente autorizadas.

Si no hay un documento que autorice la prueba, **se incurre en delito**, aunque sea “por buena intención”.

◆ ¿Qué distingue lo ético de lo ilegal?

La autorización.

No importa si no dañas, si no extraes datos o si crees que estás ayudando.

Si no tienes permiso del titular del sistema, estás violando la ley.

La ética no es una excusa.

Es una **intención correcta respaldada por una conducta legalmente válida.**

Epílogo: Entre la Ley, la Tecnología y la Realidad Nacional

◆ ¿Y las penas? ¿Qué tanto se castigan los delitos informáticos?

La Ley de Delitos Informáticos (Ley N.º 30096) contempla penas de:

- **8 a 10 años** si el delito compromete la **defensa nacional, soberanía o programas sociales** del Estado.
- Sin embargo, en la práctica judicial peruana, **si la pena no supera los 6 años**, puede ser:
 - **Suspendida** (no se va a prisión),
 - Conmutada por servicios comunitarios o restricciones.

Esto hace que muchos delitos informáticos **se traten judicialmente por su impacto real**, no por su tipificación digital.

Ejemplo: Si alguien hackea y roba una base de datos, **puede no ser procesado como ciberdelincuente**, sino como autor de **robo, fraude o suplantación**, que conllevan penas más severas.

Ley 27269 – Firmas digitales

17-Julio-2000



Ley de Firmas y Certificados Digitales

- ☐ **Artículo 1.-** Objeto de la ley La presente ley tiene por objeto regular la utilización de la firma electrónica **otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita** u otra análoga que conlleve manifestación de voluntad. Entiéndase por firma electrónica a cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita.
- ☐ **Artículo 3.-** Firma digital La firma digital es aquella firma electrónica **que utiliza una técnica de criptografía asimétrica**, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.

◆ ¿Y la firma digital? ¿Es legal?

Sí.

Desde el año **2000**, el Perú cuenta con una **Ley de Firma Digital (Ley N.º 27269)**, que establece que:

La firma digital tiene la **misma validez legal** que una firma manuscrita.

No hablamos de escanear tu firma en un PDF, sino de una **firma electrónica certificada y registrada** por entidades autorizadas (RENIEC, entidades de certificación digital, etc.).

✚ Pero recién con la pandemia (2020–2021) **empezó a usarse masivamente**, sobre todo en:

- Contratos,
 - Trámites del Estado,
 - Certificados académicos y laborales,
 - Procedimientos notariales virtuales.
-

◆ El spam: un problema tan viejo como Internet

Aunque se reguló legalmente en el Perú en **2005**, el **primer spam de la historia** fue en 1978, cuando ni siquiera existía la Web como la conocemos.

La ley establece que:

- Los correos publicitarios **deben identificarse como tal** en el asunto.
- Deben ofrecer al usuario una opción clara para **retirarse o desuscribirse**.

En la práctica, **muy pocos cumplen esto**. Seguimos recibiendo spam sin control ni fiscalización efectiva.

◆ Convenio de Budapest y ciberdefensa nacional

El Perú es firmante del **Convenio de Budapest sobre Ciberdelincuencia**, lo que implica compromisos en:

- Protección de infraestructuras críticas (electricidad, agua, salud, telecomunicaciones),
- Ciberdefensa nacional,
- Cooperación internacional en persecución de ciberdelitos.

¿Quién lidera la ciberdefensa en el Perú?

Según el marco legal vigente, **la ciberdefensa recae en las Fuerzas Armadas**, a través del Comando Conjunto y unidades especializadas en:

- Ciberinteligencia,
- Ciberdefensa ofensiva y defensiva,

- Ciberseguridad crítica nacional.
-

◆ ¿Qué son las infraestructuras críticas?

Se consideran **infraestructuras críticas** aquellas cuya afectación podría causar un colapso social o económico. Ejemplo:

- Sistema eléctrico nacional (COES),
- Redes de agua potable,
- Servicios de salud (hospitales públicos),
- Telecomunicaciones (Red dorsal de fibra óptica),
- Transporte y energía (OLEODUCTO, gasoductos, puertos).

🔒 Si un ciberataque afecta alguna de estas infraestructuras, **no es solo un delito informático**, es **una amenaza a la seguridad nacional**.

Apéndice: Firma Digital en el Perú – Aplicación real y legalidad

◆ ¿Qué es la firma digital?

La **firma digital** es un mecanismo criptográfico que:

- Garantiza la **autenticidad** del firmante,
- Asegura la **integridad** del documento firmado,
- Tiene **validez legal equivalente** a una firma manuscrita (*Ley N.º 27269, año 2000*).

⚠ Escanear una firma NO es firma digital.

Solo es válida si utiliza un **certificado digital emitido por una entidad acreditada** (RENIEC, SUNAT, etc.).

◆ ¿Cómo se aplica en la práctica?

Para firmar documentos digitalmente se necesita:

1. **Certificado digital:** Puede estar contenido en:
 - El **DNLe (DNI electrónico)**,
 - Un **token USB** criptográfico,
 - Una **plataforma integrada de firma** (como PIDE, SIGNNET, etc.).

2. **Software compatible:** Como Adobe Acrobat, Firma Digital de RENIEC, etc.
 3. **Identidad validada:** El firmante debe tener un rol reconocido (persona natural o jurídica).
-

◆ Ejemplo real: Firma institucional en universidades

Un profesor o autoridad puede firmar documentos (sílabos, actas, resoluciones, etc.):

- Usando su **token USB** con certificado digital,
- Firmando con el rol de “Director de Escuela” (firma jurídica),
- La firma se integra en el PDF como **firma visible** o **firma invisible**.

✚ La firma visible muestra un ícono o imagen.

Pero lo **legalmente vinculante** es la **validación del certificado digital** en el archivo.

◆ ¿Cómo se valida una firma digital?

El sistema o receptor del documento debe verificar:

- Que el certificado digital **no ha caducado**,
 - Que el certificado fue emitido por una entidad **autorizada y vigente**,
 - Que el documento **no ha sido modificado** tras la firma.
-

◆ Validez legal

Según la ley peruana:

“La firma digital tiene la misma validez y eficacia jurídica que una firma manuscrita.”
(Ley N.º 27269 – Artículo 2)

Esto aplica para:

- Documentos académicos,
- Contratos,
- Resoluciones internas,
- Trámites administrativos con el Estado.

Firma Digital, Certificados y Validez Jurídica

En cuanto a la firma digital, es importante tener en cuenta ciertos detalles técnicos y jurídicos.

Por ejemplo, cuando se genera un archivo firmado digitalmente, puede aparecer un mensaje que indique: **“La validez de la firma es desconocida”**. Esto no significa necesariamente que la firma sea inválida, sino que el **certificado digital aún no ha sido reconocido por el software que estás utilizando**, como Adobe Acrobat.

Esto ocurre porque la **RENIEC**, aunque es una autoridad certificadora oficial en el Perú, **no está incluida por defecto** en las bases de confianza de algunos programas. Por ello, es necesario **agregar manualmente el certificado de RENIEC** al repositorio de confianza del software. Este procedimiento es similar al de los navegadores web, donde también se debe confiar manualmente en ciertos certificados cuando no son reconocidos de forma automática.

Por ejemplo, en Adobe puedes ir a la opción de “Agregar certificado” y cargar el archivo correspondiente para que el sistema lo reconozca como confiable. Una vez hecho esto, el software validará correctamente la firma y mostrará que el documento ha sido firmado por una entidad certificadora reconocida.

En este caso particular, el certificado fue emitido por RENIEC, clase C, y tiene vigencia hasta octubre de 2025. Esto significa que el certificado es válido y funcional hasta esa fecha, momento en el cual deberá ser renovado.

¿Qué pasa si imprimo un documento firmado digitalmente?

Al imprimir el archivo, **la firma digital pierde validez legal**, ya que el papel no contiene la encriptación ni los datos del certificado. La validez jurídica **solo se mantiene dentro del archivo digital original firmado**. Por tanto, aunque se vea una imagen con una “firma” en el papel, **solo la versión digital garantiza autenticidad, integridad y no repudio**.

Otros datos importantes

Además de RENIEC, existen **otras entidades certificadoras autorizadas**, muchas de las cuales proveen certificados digitales a pequeñas empresas (pymes) para firmar documentos como facturas electrónicas, declaraciones juradas o contratos.

En muchos casos, los sistemas de facturación electrónica que ofrecen estas empresas **ya vienen integrados con firmas digitales**, lo que facilita su uso para comercios, restaurantes o negocios independientes.

Entidades certificadoras

En suma, el **ROPS (TSL)**:

1. Actúa como un **directorio para los PSCs** (entidades públicas y empresas acreditadas).
2. **Posibilita a las partes interesadas la verificación del ROPS** respecto de las organizaciones que están **ofreciendo servicios**, el **tipo** de servicios que se encuentran disponibles y el **estado** en que se **encuentran**.
3. **Es una forma de seguridad adicional para las terceras partes** cuando reciben algún tipo de documento **electrónico firmado** por una parte a la que no conocen.

ENTIDADES DEBIDAMENTE ACREDITADAS:

Nº	EMPRESA/ENTIDAD PÚBLICA	SERVICIO O PRODUCTO ACREDITADO
1.	ABC Identidad Digital S.A.C. (RUC Nro. 20506453800)	- Entidad de Registro o Verificación (🔗) Consulte por la Venta de certificado digital de la empresa Liana.Pa S.A. (🔗)
2.	ACJ Soluciones S.A.C. (RUC Nro. 20504097551)	- Software de Firma Digital (Librería de Firma Digital ACJ Signature versión 1.0) - Entidad de Certificación y Entidad de Certificación nivel subsiguiente - Entidad de Registro o Verificación (🔗) Consulte por la Venta de Certificados Digitales
3.	Accepta Perú S.A.C. (RUC Nro. 20502899711)	🔗 - Prestador de Servicio Añadido (Sellado de Tiempo) - Software de Firma Digital (Librería Firmador Accepta versión 1.2)
4.	Auraportal Perú S.A.C. (RUC Nro. 20500340043)	- Software de Firma Firma Digital (BPM AuraPortal Hellum compilado 20140313)
5.	Alejandro Mario Orihuela Romero (persona natural)	- Software de Firma Digital (RunSigner versión 1.0)

**+70 entidades
acreditadas**

<https://www.indecopi.gob.pe/web/firmas-digitales/lista-de-Servicios-de-confianza-trusted-services-list-tsl->

Ley 27291 – modif. Cod. Civil.

LEY N° 27291

EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

El Congreso de la República

ha dado la Ley siguiente:

EL CONGRESO DE LA REPÚBLICA;

Ha dado la Ley siguiente:

LEY QUE MODIFICA EL CÓDIGO CIVIL PERMITIENDO LA UTILIZACIÓN DE LOS MEDIOS ELECTRÓNICOS PARA LA COMUNICACIÓN DE LA MANIFESTACIÓN DE VOLUNTAD Y LA UTILIZACIÓN DE LA FIRMA ELECTRÓNICA

Artículo 1.- Modificación del Código Civil

Modifícanse los Artículos 141 y 1374 del Código Civil, con los siguientes textos:

“Artículo 141.- Manifestación de voluntad

La manifestación de voluntad puede ser expresa o tácita. Es expresa cuando se realiza en forma oral o escrita, a través de cualquier medio directo, manual, mecánico, electrónico u otro análogo. Es tácita cuando la voluntad se infiere indubitadamente de una actitud o de circunstancias de comportamiento que revelan su existencia.

No puede considerarse que existe manifestación tácita cuando la ley exige declaración expresa o cuando el agente formula reserva o declaración en contrario. (*)

24 de junio de 2000

**Ley 28493 – Ley
contra Spam**

2005

Ley N° 28493

Archivo

12 de febrero de 2021

Ley N° 28493, Ley que regula el uso del Correo Electrónico Comercial no solicitado (SPAM), de fecha 11 de abril de 2005.

Artículo 5.- Correo electrónico comercial no solicitado

Todo correo electrónico comercial, promocional o publicitario no solicitado, originado en el país, debe contener:

- a) La palabra "PUBLICIDAD", en el campo del "asunto" (o subject) del mensaje.
- b) Nombre o denominación social, domicilio completo y dirección de correo electrónico de la persona natural o jurídica que emite el mensaje.

"Artículo 6.- Correo electrónico comercial no solicitado considerado ilegal

El correo electrónico comercial no solicitado será considerado ilegal en los siguientes casos:

- a) Cuando no cumpla con alguno de los requisitos establecidos en el artículo 5 de la presente Ley.

CONCORDANCIAS: [D.S. N° 031-2005-MTC, Art. 16](#)

- b) Contenga nombre falso o información falsa que se oriente a no identificar a la persona natural o jurídica que transmite el mensaje.

CONCORDANCIAS: [D.S. N° 031-2005-MTC, Arts. 9, y 16](#)

- c) Contenga información falsa o engañosa en el campo del "asunto" (o subject), que no coincida con el contenido del mensaje.

CONCORDANCIAS: [D.S. N° 031-2005-MTC, Art. 16](#)

- d) Se envíe o transmita a un receptor que haya formulado el pedido para que no se envíe dicha publicidad, luego del plazo de dos (2) días.

"Artículo 8.- Derecho a compensación pecuniaria

El receptor de correo electrónico ilegal podrá accionar por la vía del proceso sumarísimo contra la persona que lo haya enviado, a fin de obtener una compensación pecuniaria, la cual será equivalente al uno por ciento (1%) de la Unidad Impositiva Tributaria por cada uno de los mensajes de correo electrónico transmitidos en contravención de la presente Ley, con un máximo de tres (3) Unidades Impositivas Tributarias. Para tales efectos, el usuario afectado deberá adjuntar a su demanda copia certificada de la resolución firme o consentida emitida por el órgano competente del INDECOPI, donde se establezca la ilegalidad de la conducta del remitente del correo electrónico recibido. Mientras no se expida resolución firme sobre dicha infracción se suspende el plazo de prescripción para efectos de reclamar el derecho a la compensación pecuniaria."

Artículo 9.- Autoridad competente

El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - (INDECOPI), a través de la Comisión de Protección al Consumidor y de la Comisión de Represión de la Competencia Desleal, será la autoridad competente para conocer las infracciones contempladas en el artículo 6 de la presente Ley; cuyas multas se fijarán de acuerdo a lo establecido en el Decreto Legislativo N° 716, Ley de Protección al Consumidor, o en el Decreto Legislativo N° 691, Normas de la Publicidad en Defensa del Consumidor, según corresponda.

Medios electrónicos y spam

La Ley de Firmas y Certificados Digitales también se complementa con normativas sobre el **uso de medios electrónicos para fines comerciales**, como el envío de correos electrónicos.

Legalmente, todo mensaje promocional o publicitario enviado por correo debe indicar claramente en el asunto que se trata de **“Publicidad”**. Sin embargo, en la práctica, muchas empresas no cumplen con esta disposición, y los correos suelen llegar directamente a la bandeja de spam o son descartados por los usuarios sin ser leídos.

Aunque existe una ley, **la regulación es débil y las sanciones casi inexistentes**, especialmente porque la carga del reclamo recae sobre el usuario. La mayoría de personas opta por no hacer trámites o denuncias, y eso permite que la práctica continúe sin control.

Impacto económico y denuncias

En casos graves, **sí es posible denunciar un mal uso de los datos personales o el envío masivo de mensajes no solicitados**, pero se requiere demostrar **el impacto económico o personal** generado por esa acción. Aquí surgen preguntas como:

- ¿Cómo te afectó?
- ¿Qué consecuencias económicas o psicológicas hubo?

Y es justo ahí donde muchas denuncias pierden fuerza, porque no hay una justificación clara o evidencia suficiente del daño ocasionado.

Ley 30999 - Ley de Ciberdefensa

2019

Ley 30999 - Ley de Ciberdefensa 2019

Artículo 2. Finalidad

Defender y proteger la soberanía, los intereses nacionales, los activos críticos nacionales y recursos claves para mantener las capacidades nacionales frente a amenazas o ataques en y mediante el ciberespacio, cuando estos afecten la seguridad nacional.

Artículo 4. Definición

Entiéndase por ciberdefensa a la capacidad militar que permite actuar frente a amenazas o ataques realizados en y mediante el ciberespacio cuando estos afecten la seguridad nacional.

Artículo 5. Órganos ejecutores

Las Fuerzas Armadas, que están constituidas por el Ejército, la Marina de Guerra y la Fuerza Aérea, y el Comando Conjunto de las Fuerzas Armadas son instituciones con calidad de órganos ejecutores del Ministerio de Defensa.

TERCERA. Recursos críticos de Internet

Se reconoce a las entidades que gestionen recursos críticos de Internet (nombres de dominio, números IP y protocolos) en su naturaleza de entidades vinculadas a la ciberdefensa, debiendo mantener mecanismos de comunicación de incidentes que pudieran afectar la capacidad de ciberdefensa nacional.

Ciberdefensa y soberanía digital

Desde 2019, el Perú ha reconocido oficialmente la importancia de la **ciberdefensa como parte de la defensa nacional**. Esto incluye la protección de la soberanía en el **ciberespacio**, es decir, en todo el entorno digital e internet.

La ciberdefensa no solo protege infraestructuras críticas, sino también sistemas estatales, redes gubernamentales y plataformas que forman parte de la seguridad y estabilidad del país frente a ciberataques o amenazas internacionales.

Infraestructura Crítica, Confianza Digital y Normas Técnicas en el Perú

Cuando hablamos de **infraestructura crítica**, nos referimos principalmente a los **flujos esenciales de internet y telecomunicaciones**, como redes eléctricas, de agua, transporte, petróleo, salud, entre otras. Un ciberataque a estos sistemas podría tener consecuencias devastadoras, razón por la cual han surgido diversas normas y estrategias nacionales de **ciberdefensa y transformación digital**.

Confianza digital y transformación institucional

En el año **2020** se aprobó un **Decreto Supremo** sobre la **Confianza Digital**, el cual establece la **designación obligatoria de un “Oficial de Transformación Digital y Confianza Digital”** en todas las entidades del Estado, incluidas las universidades públicas.

Sin embargo, aquí surge una crítica importante:

¿Quién ocupa ese cargo en su institución?

¿Saben cuál es su nombre o su perfil profesional?

En muchos casos, la persona designada **no tiene formación en sistemas ni experiencia en tecnologías de la información**. Se trata de personal administrativo o de otras áreas como contabilidad, designado simplemente para **cumplir con el requerimiento legal**, sin una verdadera implicancia operativa.

La universidad, en efecto, "cumple" con la norma, pero **no se ejecutan acciones concretas ni se observan resultados reales** en materia de transformación digital.



Otros

DECRETO DE URGENCIA N° 007-2020
DECRETO DE URGENCIA QUE APRUEBA EL MARCO DE CONFIANZA DIGITAL Y
DISPONE MEDIDAS PARA SU FORTALECIMIENTO

CAPÍTULO III
MEDIDAS PARA FORTALECER
LA CONFIANZA DIGITAL

Artículo 8. Registro Nacional de Incidentes de Seguridad Digital

8.1 Créase el Registro Nacional de Incidentes de Seguridad Digital que tiene por objetivo recibir, consolidar y mantener datos e información sobre los incidentes de seguridad digital reportados por los proveedores de servicios digitales en el ámbito nacional que puedan servir de evidencia o insumo para su análisis, investigación y solución.

8.2 El Registro Nacional de Incidentes de Seguridad Digital y la información contenida en el mismo tiene carácter confidencial, se soporta en una plataforma digital administrada por la Secretaría de Gobierno Digital, quien es responsable de su disponibilidad, confidencialidad e integridad.

9.3 Las entidades de la administración pública deben implementar un Sistema de Gestión de Seguridad de la Información (SGSI), un Equipo de Respuestas ante Incidentes de Seguridad Digital cuando corresponda y cumplir con la regulación emitida por la Secretaría de Gobierno Digital.

9.4 Toda actividad crítica debe estar soportada en una infraestructura segura, disponible, escalable e interoperable.

CAPÍTULO IV
USO ÉTICO DE LAS TECNOLOGÍAS
DIGITALES Y DE LOS DATOS

Artículo 12. Datos como activos estratégicos

12.1 Las entidades públicas y las organizaciones del sector privado administran los datos, en especial los datos personales, biométricos y espaciales, como activos estratégicos, garantizando que estos se generen, compartan, procesen, accedan, publiquen, almacenen, conserven y pongan a disposición durante el tiempo que sea necesario y cuando sea apropiado, considerando las necesidades de información, uso ético, transparencia, riesgos y el estricto cumplimiento de la normatividad en materia de protección de datos personales, gobierno digital y seguridad digital.

12.2 Las entidades públicas y las organizaciones del sector privado promueven y aseguran el uso ético de tecnologías digitales, el uso intensivo de datos, como internet de las cosas, inteligencia artificial, ciencia de datos, analítica y procesamiento de grandes volúmenes de datos.

12.3 El tratamiento de datos personales debe cumplir la legislación de la materia emitida por la Autoridad Nacional de Protección de Datos Personales.

09 de enero del 2020

Resolución Fiscalía de la Nación 1503-2020

Archivo

12 de febrero de 2021

Resolución Fiscalía de la Nación 1503-2020 mediante la cual se crea la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con competencia nacional, publicada con fecha 01 de enero de 2021.

Artículo Primero.- Crear la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con competencia nacional, la misma que dependerá administrativamente y funcionalmente de la Fiscalía de la Nación.

Artículo Segundo.- Asignar de manera temporal una (01) plaza de Fiscal Superior y dos (02) plazas de Fiscales Adjuntos Superiores, a nivel nacional, con carácter transitorio, creadas mediante Resolución de la Junta de Fiscales Supremos N° 009-2020-MP-FN-JFS, de fecha 24 de febrero de 2020, a la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con competencia nacional, a partir de la fecha y hasta el 31 de marzo de 2021, en mérito a lo dispuesto por la Resolución de la Junta de Fiscales Supremos N° 084-2020-MP-FN-JFS, de fecha 15 de diciembre de 2020.

☐ Convenio de Budapest (Tratado Europeo 185, Decreto Supremo 010-2019-RE)

☐ Resolución N° 0791-2015/CDA-INDECOPI (Uso legal de software)

Fiscalías especializadas en ciberdelincuencia

En el ámbito judicial, también existen grandes deficiencias en el tratamiento de **delitos informáticos**. La falta de preparación técnica, tanto en el **Ministerio Público como en el sistema judicial**, limita la capacidad de respuesta frente a la ciberdelincuencia.

Por ello, en **enero de 2021** se implementó la **Fiscalía Especializada en Ciberdelincuencia**, con sede inicial en Lima. Aunque se han creado algunas plazas y trasladado fiscales para su organización, **el avance ha sido lento** y en muchos casos **sólo ha quedado como proyecto piloto**.

Marco legal internacional: Convenio de Budapest

Como parte del proceso de integración y cooperación internacional en ciberseguridad, el Perú forma parte del **Convenio de Budapest**, el cual establece principios y lineamientos sobre delitos cibernéticos, protección de datos y cooperación transfronteriza.

Este convenio ha motivado la **actualización de normativas nacionales**, como las leyes sobre delitos informáticos y protección de datos.



- ☐ ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems - Requirements. **Certificable.**
- ☐ ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection - Information security controls .
- ☐ ISO/IEC 27003:2017. Information technology – Security techniques - Information security management systems - Guidance. (Guía de diseño)
- ☐ ISO/IEC 27004:2016. Information technology – Security techniques - Information security management - Monitoring, measurement, analysis and evaluation.
- ☐ ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection - Guidance on managing information security risks.

ISO/IEC 27001:2022

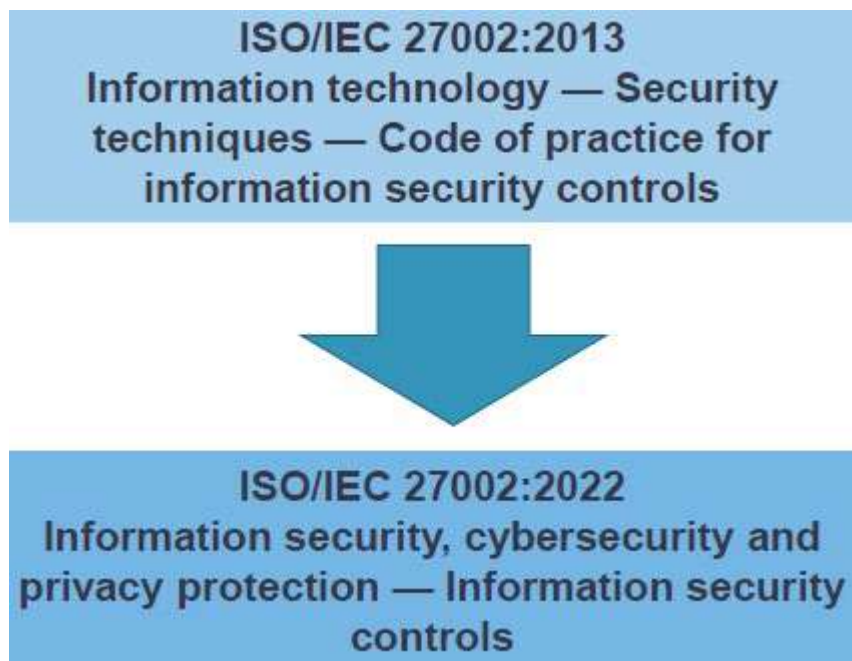
ISO/IEC 27002:2022



Videos de referencia:

<https://www.youtube.com/watch?v=bED5EhgbUyI>

https://www.youtube.com/watch?v=MatJR6p_lxU



Hay 93 controles en 4 grupos o tipos de controles en comparación con los 114 controles en 14 cláusulas en la versión de 2013. Se definen 11 nuevos controles, los cuales corresponden a:

- ☐ 5.7 Inteligencia de Amenazas
- ☐ 5.23 Seguridad de la información para el uso de servicios en la nube
- ☐ 5.30 Preparación de las TIC para la continuidad del negocio
- ☐ 7.4 Monitoreo de la seguridad física
- ☐ 8.9 Gestión de la configuración
- ☐ 8.10 Eliminación de la información
- ☐ 8.11 Enmascaramiento de datos
- ☐ 8.12 Prevención de la fuga de datos
- ☐ 8.16 Actividades de monitoreo
- ☐ 8.23 Filtrado Web
- ☐ 8.28 Codificación Segura

NTP-ISO/IEC 27001:2022

Seguridad de la información, ciberseguridad y protección de la privacidad. **Sistemas de gestión de la seguridad de la información.** Requisitos. 3ª Edición
Reemplaza a la NTP-ISO/IEC 27001:2014

NTP-ISO/IEC 27005:2022

Seguridad de la información, ciberseguridad y protección de la privacidad. **Orientación sobre la gestión de los riesgos de seguridad de la información.** 3ª Edición
Reemplaza a la NTP-ISO/IEC 27005:2018

NTP-ISO/IEC 27002:2022

Seguridad de la información, ciberseguridad y protección de la privacidad. **Controles de seguridad de la información.** 2ª Edición
Reemplaza a la NTP-ISO/IEC 27002:2017

NTP-ISO/IEC 27036-1:2022

Ciberseguridad. **Relación con proveedores.** Parte 1: Visión general y conceptos. 1ª Edición

Normas Técnicas Peruanas (NTP) y seguridad de la información

Un punto clave para la gestión de seguridad es el conocimiento y aplicación de las **Normas Técnicas Peruanas (NTP)**, especialmente las asociadas a seguridad informática, como la **NTP-ISO/IEC 27001:2022**.

¿Qué es una norma técnica peruana (NTP)?

Es un documento que establece especificaciones, requisitos y lineamientos técnicos consensuados, utilizados para garantizar calidad, seguridad y eficiencia en productos, servicios o procesos.

¿Quién las emite?

Las NTP son desarrolladas por el **Instituto Nacional de Calidad (INACAL)**, entidad adscrita al Ministerio de la Producción.

Antes, estas normas estaban a cargo de INDECOPI, pero fueron transferidas al INACAL para una gestión más especializada.

¿Sobre qué tratan?

Las NTP no solo abordan temas de seguridad informática. También existen normas sobre textiles, calzado, alimentos, puertos, telecomunicaciones, entre otros sectores.

Muchas de estas normas pueden ser adquiridas desde el portal de INACAL, aunque **no todas están disponibles gratuitamente**.

Normas Técnicas Peruanas y su Relación con Estándares Internacionales de Seguridad

Actualización de la ISO 27001 y su versión peruana

En el año **2022**, se publica la **nueva versión de la norma internacional ISO/IEC 27001**, que reemplaza a la anterior del **2013**. Paralelamente, en ese mismo año, el Perú adopta esta actualización mediante la **Norma Técnica Peruana (NTP)** correspondiente.

¿Cuál es la diferencia entre la ISO 27001 y la NTP ISO/IEC 27001?

La **NTP** no es una norma propia desarrollada desde cero, sino una **traducción oficial y validada al español** de la norma ISO, adaptada al marco legal y técnico peruano. En muchos casos, las normas técnicas peruanas **son traducciones literales** de estándares internacionales, pero si se introducen modificaciones sustanciales, se les asigna un **nuevo código y denominación** distinta.

¿Para qué se crean las Normas Técnicas Peruanas?

Las **Normas Técnicas Peruanas** (NTP) son esenciales en distintos sectores:

- En **ingeniería civil**, definen procesos para canalizaciones, instalaciones eléctricas, señalización, etc.
- En **tecnología**, especifican cómo implementar cableado estructurado, protocolos de ciberseguridad, normas de calidad y más.

El Estado y muchas licitaciones públicas **exigen** el cumplimiento de normas nacionales. Cuando no existe una norma local, se traduce y oficializa una norma internacional como NTP.

El rol de los comités de normalización

Yo participo activamente en un comité de normalización en telecomunicaciones. En nuestro caso, ya hemos logrado que **cinco normas técnicas peruanas sean aprobadas**, basadas en traducciones técnicas completas de normas internacionales. Este proceso incluye:

1. Traducción del contenido, gráficos y terminología técnica.
 2. Proceso de validación, revisión y consenso.
 3. Publicación como **NTP oficial** a través del **INACAL** (Instituto Nacional de Calidad).
-

Ejemplos de NTP relevantes en seguridad de la información

A continuación, algunos ejemplos clave:

- **NTP ISO/IEC 27001:2022** – Sistema de gestión de seguridad de la información.
 - **NTP ISO/IEC 27005:2018** – Gestión de riesgos de seguridad.
 - **NTP ISO/IEC 27036** – Seguridad en la relación con proveedores.
 - **NTP ISO/IEC 27035** – Gestión de incidentes de seguridad.
 - **NTP 29173 revisión 4** – Control de seguridad y privacidad de sistemas.
 - **PCI DSS (versión 4.0)** – Estándar de seguridad para datos de tarjetas de pago, con similitudes notables con ISO 27001 en cuanto a controles.
-

¿Qué tienen en común estas normas?

Pese a los diferentes nombres y orígenes, **todas convergen en el mismo propósito**: proteger la integridad, confidencialidad y disponibilidad de la información.

- ISO 27001 versión 2022 tiene ahora **93 controles**, organizados en **4 grandes temas**.
- PCI DSS pasó de **20 a 18 requisitos clave**, pero se desdoblan en múltiples controles específicos.
- CIS Benchmarks ofrece guías detalladas para la **configuración segura de sistemas**, como:
 - Windows Server 2012, 2016, 2019, 2022.
 - Linux (RHEL, Ubuntu, Debian).
 - Servidores en roles específicos (DNS, controlador de dominio, etc).

Estos documentos sirven como **listas de verificación (checklist)** que orientan en la implementación segura de sistemas y plataformas.

Gracias por compartir la transcripción tan completa. Veo que cubre una gran variedad de temas importantes sobre **normas, estándares y leyes en seguridad informática**, como:

- **ISO/IEC 27001:2022** y su versión como **Norma Técnica Peruana (NTP)** traducida y adaptada.
- **PCI DSS** para tarjetas de pago (Visa, MasterCard, etc.) y su aplicabilidad en pasarelas y entidades financieras.
- **Ley N° 29733 - Protección de Datos Personales** y sus principios, tipos de datos, derechos ARCO, consentimiento y sanciones.
- **Delitos informáticos** (Ley 30096) como acceso ilícito, interceptación, alteración de datos, fraude, y su evolución con nuevas tecnologías.
- **Firma digital y certificación digital**, incluyendo la RENIEC como entidad certificadora en Perú.
- **Ciberdefensa e infraestructura crítica**, con énfasis en las normativas post-pandemia.
- La diferencia entre infracciones y delitos, y los retos de implementación y cumplimiento de estas normas en la práctica real.
- Comparaciones con otras normas internacionales como HIPAA (salud en EE.UU.), SOX (sector financiero), GDPR, etc.

NIST 800-53 rev4

NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

NIST 800-61 rev2

Esta publicación ayuda a las organizaciones a establecer **capacidades de respuesta a incidentes de seguridad informática** y manejar incidentes de manera eficiente y efectiva



National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

Computer Security Incident Handling Guide

Recommendations of the National Institute
of Standards and Technology

Controls CIS
(*Center for Internet
Security*)



Controles CIS versión 8

CONTROL 01 Inventory and Control of Enterprise Assets 5 Safeguards: 101 2/5 102 4/5 103 5/5	CONTROL 02 Inventory and Control of Software Assets 7 Safeguards: 101 3/7 102 6/7 103 7/7	CONTROL 03 Data Protection 14 Safeguards: 101 6/14 102 12/14 103 14/14
CONTROL 04 Secure Configuration of Enterprise Assets and Software 12 Safeguards: 101 7/12 102 11/12 103 12/12	CONTROL 05 Account Management 6 Safeguards: 101 4/6 102 6/6 103 6/6	CONTROL 06 Access Control Management 8 Safeguards: 101 5/8 102 7/8 103 8/8
CONTROL 07 Continuous Vulnerability Management 7 Safeguards: 101 4/7 102 7/7 103 7/7	CONTROL 08 Audit Log Management 12 Safeguards: 101 3/12 102 11/12 103 12/12	CONTROL 09 Email and Web Browser Protections 7 Safeguards: 101 2/7 102 6/7 103 7/7
CONTROL 10 Malware Defenses 7 Safeguards: 101 3/7 102 7/7 103 7/7	CONTROL 11 Data Recovery 5 Safeguards: 101 4/5 102 5/5 103 5/5	CONTROL 12 Network Infrastructure Management 8 Safeguards: 101 1/8 102 7/8 103 8/8
CONTROL 13 Network Monitoring and Defense 11 Safeguards: 101 0/11 102 8/11 103 11/11	CONTROL 14 Security Awareness and Skills Training 9 Safeguards: 101 8/9 102 9/9 103 9/9	CONTROL 15 Service Provider Management 7 Safeguards: 101 1/7 102 4/7 103 7/7
CONTROL 16 Applications Software Security 14 Safeguards: 101 0/14 102 11/14 103 14/14	CONTROL 17 Incident Response Management 9 Safeguards: 101 3/9 102 8/9 103 9/9	CONTROL 18 Penetration Testing 5 Safeguards: 101 0/5 102 3/5 103 5/5

CIS Benchmarks

Referencias para mas de 100 plataformas y sistemas, entre los cuales destacan:

☐ Windows Server.

- ☐ Linux generic.
- ☐ Linux Ubuntu.
- ☐ Linux Debian.
- ☐ Linux Red Hat.
- ☐ Microsoft Office.
- ☐ Cisco IOS.

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	Account Policies		
1.1	Password Policy		
1.1.1	(L1) Ensure 'Enforce password history' is set to '24 or more password(s)' (Scored)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	(L1) Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (Scored)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	(L1) Ensure 'Minimum password age' is set to '1 or more day(s)' (Scored)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.4	(L1) Ensure 'Minimum password length' is set to '14 or more character(s)' (Scored)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.5	(L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled' (Scored)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.6	(L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (Scored)	<input type="checkbox"/>	<input type="checkbox"/>
1.2	Account Lockout Policy		
1.2.1	(L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)' (Scored)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	(L1) Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' (Scored)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Microsoft Windows Server 2012 R2 Benchmark

v2.3.0 - 03-30-2018