GUÍA DE IMPLEMENTACIÓN DE

PROTECCIÓN DE DATOS Y USO RESPONSABLE

de **Inteligencia Artificial** en Bolivia

indico GLOBAL

Funded by the European Union

INTERNET BOLIVIA .ORG

PRIMERA EDICIÓN

Depósito legal:
4-1-3167-2025

ISBN:
978-9917-0-5297-5

La presente guía fue elaborada por la Fundación InternetBolivia.org en el marco del proyecto **"Fomento de la protección de datos y el uso responsable de la Inteligencia Artificial en Bolivia"** en colaboración del Consorcio InDiCo Global, con el financiamiento de la Unión Europea.

La Paz, Bolivia, 2025

PUBLICADO POR:
- Fundación InternetBolivia.org
- Consorcio InDiCo Global

FINANCIADO POR:
- Unión Europea

ELABORADO POR:
- Estefani Cabrera Rojas
- Nicole Angel Sánchez Rojas

EQUIPO DE COMUNICACIÓN:
- Lisette Balbachan
- Sabrina Lanza

DISEÑO Y DIAGRAMACIÓN:
- Marcelo Lazarte

COORDINACIÓN DEL PROYECTO:
- Cristian León Coronado
- Nicole Angel Sánchez Rojas

indico GLOBAL

Funded by the European Union

INTERNET BOLIVIA .ORG

GUÍA DE IMPLEMENTACIÓN DE

PROTECCIÓN DE DATOS Y USO RESPONSABLE

de **Inteligencia Artificial** en Bolivia

Contenido

Glosario de protección de datos y AI Act

Algoritmo: conjunto de reglas o instrucciones definidas para resolver un problema o realizar una tarea. En IA, los algoritmos procesan datos para tomar decisiones o hacer predicciones.

Anonimización: proceso mediante el cual se eliminan o transforman los elementos identificadores de los datos personales, de forma que no sea posible identificar al titular, directa ni indirectamente.

Consentimiento informado: manifestación de voluntad libre, específica, informada e inequívoca del titular de los datos mediante la cual acepta el tratamiento de sus datos personales.

Ética en el uso de IA: se refiere al conjunto de principios, valores y normas orientadas a guiar el desarrollo, implementación y uso responsable de sistemas de inteligencia artificial. Busca asegurar que las tecnologías basadas en IA respeten los Derechos Humanos, promuevan la equidad, eviten discriminaciones y daños, y garanticen la transparencia, la rendición de cuentas y la supervisión humana. La ética de la IA también implica considerar el impacto social, económico y ambiental de estas tecnologías, fomentando una innovación alineada con los principios del bien común.

Datos personales: información que puede identificar directa o indirectamente a una persona física, como nombres, direcciones, números de identificación, ubicaciones, datos genéticos, etc.

Datos sensibles personales: revelan información sobre aspectos más íntimos o privados de una persona. Datos sobre: salud, origen étnico o racial, creencias religiosas, opiniones políticas, orientación sexual, antecedentes penales, etc

Derechos digitales: los derechos digitales se refieren a cuestiones relativas a cómo se ejercen y protegen los mismos derechos que siempre han sido fundamentales para todos los seres humanos, como la libertad de expresión, la privacidad y el acceso a la información, en la era de Internet, las redes sociales y la tecnología.

Encargado del tratamiento: persona natural o jurídica, autoridad pública, agencia u otro organismo que trata datos personales por cuenta del responsable del tratamiento.

Inteligencia artificial (IA): conjunto de técnicas y sistemas informáticos que permiten simular procesos inteligentes como el aprendizaje, razonamiento o autocorrección.

Incidente de seguridad: evento adverso, confirmado o bajo sospecha, que compromete la confidencialidad, integridad o disponibilidad de los datos personales o de los sistemas que los almacenan, procesan o transmiten. Un incidente de seguridad puede incluir accesos no autorizados, pérdida o destrucción de información, fuga de datos, ataques informáticos, errores humanos o fallas técnicas que afecten la seguridad de los datos.

Privacidad por Diseño: principio que implica integrar medidas de protección de datos desde el inicio de la concepción de un producto, servicio o sistema.

Procesamiento de datos: cualquier operación o conjunto de operaciones que se realicen sobre datos personales, ya sea de forma automatizada o no, como la recopilación, almacenamiento, organización, estructuración, etc.

Responsable del tratamiento: persona natural o jurídica, autoridad pública, agencia u otro organismo que determina los fines y medios del tratamiento de datos personales.

Riesgo de seguridad: probabilidad de que una amenaza explote una vulnerabilidad en un sistema o proceso, ocasionando un impacto negativo sobre la confidencialidad, integridad o disponibilidad de los datos personales o de los sistemas de información que los gestionan.

Sociedad de la información: modelo social y económico caracterizado por la producción, circulación y acceso masivo a la información mediante el uso intensivo de las tecnologías de la información y la comunicación (TIC). Esta sociedad transforma las formas de interacción social, el ejercicio de los derechos fundamentales y los deberes de los Estados, generando nuevos retos en materia de privacidad, propiedad intelectual, ciberseguridad y acceso equitativo a la tecnología.

Tecnologías de la información y la comunicación (TIC): las Tecnologías de la Información y Comunicación (TIC) se refieren al conjunto de tecnologías, recursos y herramientas que se utilizan para gestionar, procesar, transmitir y almacenar información. Estas tecnologías abarcan tanto dispositivos físicos como software, redes de comunicación, sistemas electrónicos y medios digitales. Las TIC tienen un impacto profundo en la sociedad al facilitar la comunicación, el acceso a la información, la automatización de procesos y el intercambio de datos a nivel global. En el contexto del derecho informático, las TIC también plantean desafíos legales relacionados con la seguridad de la información, la privacidad y la regulación de actividades en línea.

Tratamiento de datos: cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por medios automatizados o no. Incluye acciones como la recolección, registro, organización, estructuración, conservación, modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión o destrucción de dichos datos. El tratamiento debe realizarse de conformidad con principios legales como la licitud, finalidad, proporcionalidad y responsabilidad, entre otros, garantizando siempre los derechos del titular de los datos.

Introducción

La presente **Guía de Implementación de protección de datos y Uso Responsable de inteligencia artificial** fue desarrolla por la **Fundación InternetBolivia.org** en base al proyecto "Fomento de la protección de datos y el uso responsable de la inteligencia artificial en Bolivia", gracias al apoyo del consorcio **InDiCo Global**, una iniciativa financiada por la Unión Europea y conformada por actores clave en el ecosistema digital europeo conformada por ETSI (European Telecommunications Standards Institute), CEN (European Committee for Standardization) y CENELEC (European Committee for Electrotechnical Standardization), quienes elaboran estándares europeos en diversos sectores industriales, incluyendo la ciberseguridad, protección de datos y ética de la IA. Estos organismos, junto con las ESOs (European Standardization Organizations), conforman la estructura del consorcio, cuyo enfoque es promover la cooperación digital global mediante la armonización de buenas prácticas y marcos regulatorios.

En Bolivia, aunque no existe una ley integral de protección de datos personales, el marco constitucional y normativas sectoriales reconocen el derecho a la privacidad, lo que refuerza la necesidad de avanzar hacia políticas institucionales de cumplimiento voluntario, con base en estándares internacionales.

El propósito de este documento es proporcionar a organizaciones públicas y privadas un marco de referencia para la adopción de medidas de seguridad y cumplimiento normativo en materia de protección de datos y ética en el uso de inteligencia artificial en Bolivia.

El presente documento busca brindar lineamientos generales a organizaciones tanto públicas como privadas sobre la protección de datos y el uso de IA de forma responsable, buscando la protección de los derechos digitales de las y los bolivianos, así como de extranjeros en territorio boliviano, siguiendo estándares internacionales como el Reglamento General de protección de datos (RGPD) y el AI Act, documentos desarrollados por la Unión Europea.

Así mismo de manera conexa, se recomienda a las organizaciones tomar medidas de seguridad de la información, entendiendo que esta se trabaja de manera conjunta a la protección de datos. El presente documento no busca llegar a lineamientos de certificación a nivel de una auditoría de seguridad, sin embargo, busca que las organizaciones cuenten con parámetros mínimos requeridos para el tratamiento de datos personales y el uso de inteligencia artificial de manera ética y responsable.

1. Bases para el desarrollo de la guía

1.1. Antecedentes

La protección de datos personales es un derecho fundamental que garantiza la privacidad y el control sobre la información que identifica a una persona. En Bolivia, este tema cobra especial relevancia debido a la creciente digitalización de los servicios públicos y privados, el uso de tecnologías emergentes y la ausencia de un marco normativo específico que regule la recopilación, almacenamiento y tratamiento de datos personales.

Se cuentan con normativas específicas, sin embargo, no son suficientes para el resguardo de derechos como la privacidad o intimidad de las personas. Hoy en día las ciudadanas y ciudadanos no cuentan con procesos efectivos a los cuales acudir en casos de vulneración de datos personales.

Hasta el año 2024 se observaron cuatro propuestas de ley de protección de datos personales en Bolivia, sin embargo, estos no fueron aprobadas, asimismo, se plantearon normativas para la sanción de ciberdelitos, comercio electrónico e inteligencia artificial, si bien estas normativas son necesarias para un desarrollo económico y tecnológico más seguro y accesible, cada una de las normas propuestas requiere de un marco regulatorio de protección de datos personales, porque algo que tiene en común el desarrollo de tecnología es la necesidad de datos personales para su funcionamiento.

Sólo en el primer trimestre de 2025, el Centro de Gestión de Incidentes Informáticos (CGII) atendió 197 casos de incidentes y vulnerabilidades informáticas de instituciones públicas, de los cuales el 50% obedecía al compromiso y obtención indebida de información[1]. En este sentido, contar con una política de protección de datos personales dentro cualquier tipo de organización resulta fundamental para prevenir, detectar o gestionar cualquier tipo de incidente de seguridad que comprometa información.

1 CGII, Informe de Gestión de Incidentes y Vulnerabilidades Informáticas, Primer Trimestre 2025, Recuperado de: https://cgii.gob.bo/sites/default/files/IGIV-trim_1_25-firmado-firmado-firmado_0.pdf

1.2. Objetivo de la guía

La presente guía tiene como objetivo proporcionar un marco conceptual, normativo y técnico sobre la protección de datos personales en Bolivia, considerando la ausencia de una legislación específica que regule esta materia. La guía busca:

- Concientiza a los ciudadanos, empresas y entidades públicas sobre la importancia de la protección de datos personales, destacando los riesgos asociados a su inadecuado tratamiento
- Proporcionar un marco de referencia basado en estándares internacionales, como el Reglamento General de protección de datos (RGPD) de la Unión Europea, para orientar a empresas y organismos públicos en la adopción de buenas prácticas
- Promover la implementación de medidas de seguridad en el tratamiento de datos personales, con el fin de minimizar riesgos de filtraciones, accesos no autorizados y vulneraciones a la privacidad
- Destacar las obligaciones y derechos relacionados con la protección de datos, tanto para los responsables del tratamiento como para los titulares de los datos, con base en normativas internacionales y en el marco constitucional boliviano

La falta de una normativa integral de protección de datos en Bolivia genera vacíos legales que pueden afectar la privacidad de las personas y el uso adecuado de la información personal. Por ello, esta guía busca servir como un documento de referencia para fomentar la adopción de políticas de privacidad y seguridad en la gestión de datos.

1.3. Principales razones que hacen necesaria una regulación en Bolivia:

1.3.1. Ausencia de una ley integral de protección de datos:

Actualmente, Bolivia no cuenta con una ley específica que regule el uso, protección y tratamiento de datos personales. Aunque existen disposiciones constitucionales y normativas sectoriales que reconocen el derecho a la privacidad (como la Constitución Política del Estado, Ley General de Telecomunicaciones, normativas financieras), no hay un marco legal que establezca principios, derechos y obligaciones claras en temas de protección de datos.

1.3.2. Vulneraciones y uso indebido de datos personales:

En la última década, la vulneración de datos personales y bases de datos aumentó de manera disruptiva, esto se ve representado con la comercialización de bases de datos a través de redes sociales, sin mecanismos efectivos para proteger la información de los ciudadanos, así mismo, se observa un descuidado uso de datos, como los datos de profesionales en áreas jurídicas, donde con sólo contar con el número de documento de identidad del profesional se accede a domicilio y universidad en la cual obtuvo el título profesional.

Durante la pandemia de COVID-19, se evidenciaron múltiples filtraciones de datos médicos de personas contagiadas, exponiendo su privacidad y generando discriminación. Lo cual demostró nuevamente que las y los ciudadanos no contaban con medidas o procesos a los cuales acudir para la protección de su privacidad e intimidad.

El uso de sistemas de identificación digital, como el Carnet de Identidad Digital y la Ciudadanía Digital, aumenta la necesidad de garantizar la protección de la información almacenada en estas plataformas, ya que no solamente se trata de implementar nuevas líneas de digitalización, sino también de brindar a las ciudadanas y los ciudadanos seguridad.

1.3.3. Desarrollo de gobierno electrónico sin garantías de privacidad:

El avance del e-Government en Bolivia promovió el uso de plataformas digitales para la prestación de servicios públicos, a través de procesos de digitalización, trámites que pueden iniciarse de manera virtual, lo cual busca reducir pasos dentro de la burocracia, pero sin contar con los resguardos normativos necesarios para la protección de datos y privacidad de quienes utilizan estas nuevas herramientas, las cuales, recolectan y almacenan datos, que en muchos casos se encuentran interconectados con diferentes instituciones, exponiendo a las personas a ser víctimas de diferentes tipos de vulneraciones y ciberdelitos, como se observó en los últimos meses, donde ciberdelincuentes suplantan la identidad de instituciones estatales y con los datos obtenidos en las plataformas cometen ciberestafas o el robo de cuentas.

1.3.4. Expansión y desarrollo de tecnología en diferentes sectores:

El crecimiento del comercio electrónico, el uso de redes sociales y el procesamiento automatizado de datos por parte de entidades públicas y privadas generó nuevas problemáticas relacionadas con la seguridad de la información.

El desarrollo de la sociedad de la mano de la convergencia tecnológica dio lugar a desarrollos como la inteligencia artificial (IA), el Big Data y el Internet de las Cosas (IoT), las cuales requieren un marco normativo que regule su uso en relación con la privacidad de los ciudadanos. En diferentes países como Brasil, Argentina o Colombia se comenzó a hablar de regulaciones referentes a Big Data o inteligencia artificial, sin embargo, las bases para el planteamiento de estas regulaciones son las normativas de protección de datos personales vigentes en estos países.

Asimismo, el crecimiento del uso de tecnología como la banca electrónica pueden exponer nuestros datos personales e información financiera, que resulta de tratamiento confidencial. Según datos de la Autoridad de Supervisión del Sistema Financiero, en el último año (2024) los ataques cibernéticos ocasionaron un daño de más de Bs. 3 millones, a través de ataques de suplantación de identidad (phishing).

En este contexto, es fundamental desarrollar políticas públicas y normativas que garanticen la protección de los datos personales, minimicen los riesgos de vulneraciones y aseguren el respeto a la privacidad en el entorno digital, buscando la protección de derechos digitales, así como el impulso a la innovación y economía de Bolivia.

1.4. El RGPD como referencia normativa

El Reglamento General de protección de datos (RGPD)[2] de la Unión Europea, en vigor desde mayo de 2018, se ha convertido en el estándar global más relevante en materia de protección de datos personales. Su aplicación trasciende las fronteras de la UE, ya que establece obligaciones para cualquier empresa o entidad que procese datos de ciudadanos europeos, independientemente de su ubicación. Varios países latinoamericanos tomaron como referencia esta normativa para la reforma o actualización de las normativas de protección de datos personales, así mismo, los lineamientos establecidos y la implementación de normativas que respeten los derechos de las personas sobre sus datos dio lugar a que países como Uruguay pudieran ser parte de estándares internacionales como el Convenio 108 de Estrasburgo, primera normativa que menciona la protección de las personas respecto al tratamiento automatizado de sus datos.

2 Parlamento Europeo y Consejo de la Unión Europea. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de protección de datos).
Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679

1.4.1. Principios fundamentales del RGPD

El Reglamento General de protección de datos (RGPD) cuenta con ciertos principios para su cumplimiento:

- **Licitud, lealtad y transparencia:** los datos deben ser tratados de manera legal, justa y transparente para el titular
- **Limitación de la finalidad:** sólo pueden recolectarse datos para fines específicos, explícitos y legítimos
- **Minimización de datos:** debe recopilar la menor cantidad de datos posible para cumplir con la finalidad establecida
- **Exactitud:** los datos deben mantenerse actualizados y corregidos cuando sea necesario
- **Limitación del almacenamiento:** no pueden conservarse por más tiempo del necesario
- **Integridad y confidencialidad:** deben implementarse medidas de seguridad adecuadas para proteger la información
- **Responsabilidad proactiva:** las organizaciones deben demostrar que cumplen con estas normas a través de políticas y procedimientos internos

1.4.2. Impacto del RGPD a nivel internacional y su aplicación en Bolivia:

Si bien Bolivia no está obligada a cumplir con el RGPD, este reglamento ha servido de modelo para la legislación de otros países en América Latina, como Brasil (Ley General de protección de datos – LGPD) y Argentina (Ley 25.326). La adopción de principios del RGPD en Bolivia permitiría:

- Establecer un marco normativo robusto que garantice la protección de los datos personales
- Generar confianza en el ecosistema digital boliviano, promoviendo la inversión y el comercio electrónico
- Brindar mayor seguridad jurídica a las empresas que procesan datos personales
- Facilitar la interoperabilidad con mercados internacionales que exigen estándares elevados en privacidad y seguridad

1.5. Beneficios de la implementación del RGPD para organizaciones

Las organizaciones bolivianas, tanto públicas como privadas, pueden beneficiarse significativamente al adoptar estándares de protección de datos basados en el RGPD. Entre los principales beneficios destacan:

- **Mayor confianza y reputación organizacional:** implementar buenas prácticas en protección de datos mejora la percepción de los consumidores y refuerza la confianza en la organización
- **Reducción del riesgo legal y financiero:** al adoptar estándares internacionales, las organizaciones minimizan el riesgo de sanciones y demandas por el mal uso de datos personales
- **Acceso a mercados internacionales:** la alineación con el RGPD facilita la colaboración con organizaciones y clientes de la Unión Europea, que exigen altos niveles de protección de datos
- **Mejora en la seguridad de la información:** la implementación de medidas de seguridad robustas reduce el riesgo de ciberataques y filtraciones de datos
- **Optimización de la gestión de datos:** aplicar principios como la minimización de datos y la limitación del almacenamiento permite un uso más eficiente de la información dentro de la organización

1.6. Contexto legal y ausencia de normativa en Bolivia (normas nacionales)

Actualmente, Bolivia no cuenta con una ley específica de protección de datos personales. Sin embargo, existen disposiciones normativas dispersas en diferentes cuerpos legales:

- **Constitución Política del Estado:** reconoce el derecho a la privacidad y a la protección de la imagen, honra y dignidad (Art. 21, 130 - 131)
- **Código Civil:** regula el derecho al nombre, imagen y honor (Arts. 12-19)
- **Ley 164 de Telecomunicaciones:** protege la privacidad y establece normas sobre el tratamiento de datos personales en el ámbito de las telecomunicaciones

Sin una legislación integral, la protección de datos en Bolivia sigue siendo insuficiente, lo que resalta la necesidad de adoptar un marco normativo robusto y alineado con estándares internacionales.

2. Principios fundamentales del RGPD y su aplicación en Bolivia

2.1. Principios de protección de datos

La protección de datos personales se basa en una serie de principios fundamentales que garantizan el tratamiento adecuado, seguro y legítimo de la información. Estos principios, recogidos en normativas internacionales como el Reglamento General de protección de datos (RGPD)[3] mencionado anteriormente, buscan equilibrar el uso de la información con la protección de los derechos individuales.

En concordancia con los principios previamente descritos como fundamentales dentro del RGPD, la presente Guía considera como marco de referencia los siguientes principios para el tratamiento de datos personales:

- Licitud, lealtad y transparencia
- Exactitud
- Limitación de la finalidad
- Limitación de plazo de conservación
- Minimización de datos
- Integridad y confidencialidad

El principio clave y común a las normas internacionales de protección de datos, es el principio de licitud, lealtad y transparencia, el cual establece que el tratamiento de datos debe realizarse de manera legal y ética, asegurando que los titulares de los datos sean plenamente informados sobre cómo se procesará su información y con qué finalidad. Esto implica que las empresas y organizaciones deben proporcionar políticas de privacidad claras y accesibles, así como obtener el consentimiento de los usuarios cuando sea necesario.

El principio de limitación de la finalidad señala que los datos personales deben ser recolectados únicamente para propósitos específicos, explícitos y legítimos, sin posibilidad de utilizarlos posteriormente para fines incompatibles con los originales. Esta restricción impide el uso indiscriminado de la información y refuerza la confianza de los titulares en el manejo de sus datos.

Asimismo, el principio de minimización de datos enfatiza que solo deben recopilarse los datos estrictamente necesarios para cumplir con el propósito del tratamiento. Este principio está alineado con las mejores prácticas de privacidad desde el diseño, reduciendo riesgos innecesarios asociados a la acumulación de información personal o a la recopilación de información automática y desmedida por parte de las organizaciones.

La exactitud de los datos es otro principio fundamental, ya que establece la obligación de mantener la información actualizada y corregir cualquier inexactitud en un plazo razonable. Este aspecto es especialmente relevante en sectores como el financiero o el de salud, donde el uso de información incorrecta puede generar graves consecuencias para los titulares.

Por otro lado, el principio de limitación del plazo de conservación exige que los datos personales no sean almacenados por un período superior al necesario para cumplir con la finalidad para la que fueron recopilados. Por lo tanto, las empresas deben definir plazos de retención adecuados y mecanismos de eliminación segura una vez que los datos dejen de ser necesarios.

En términos de seguridad, el principio de integridad y confidencialidad impone la obligación de implementar medidas de protección adecuadas para evitar accesos no autorizados, pérdidas, alteraciones o divulgaciones indebidas. Esto puede incluir el cifrado de datos, el control de acceso a la información y auditorías periódicas para evaluar vulnerabilidades.

3 Parlamento Europeo y Consejo de la Unión Europea. (2016). Reglamento General de protección de datos, Artículo 5. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679

2.2. Responsabilidad proactiva (accountability)

Si bien la responsabilidad proactiva se trata también de uno de los principios fundamentales de la protección de datos personales, establecido en el RGPD[4]. Este principio representa un cambio de enfoque en el tratamiento de datos personales, ya que transforma la protección de la privacidad en una obligación activa y continua, en lugar de un simple cumplimiento formal o reactivo ante incidentes o exigencias regulatorias[5].

Antes de la incorporación de este principio, la gestión de la privacidad se centraba en un modelo reactivo, en el cual las organizaciones cumplían con la regulación en la medida en que se les exigía o cuando surgía un problema, como una filtración de datos o una inspección por parte de la autoridad competente, con un objetivo predominante de cumplir con la normativa mínima necesaria. Con la introducción del principio de responsabilidad proactiva, se establece una nueva lógica que conmina a las organizaciones a asumir un papel activo en la gestión de la privacidad. Esto significa que las organizaciones deben integrar la protección de datos en su estructura organizativa, diseñar políticas internas adecuadas, implementar medidas de seguridad efectivas, capacitar a su personal y documentar todas sus acciones de cumplimiento.

El principio de responsabilidad proactiva se define como la obligación no sólo de cumplir con la normativa de protección de datos, sino también de demostrar de manera activa y continua que dicho cumplimiento se lleva a cabo de forma efectiva.

Este cambio de enfoque también representa un cambio en la cultura organizacional de cumplimiento, donde la seguridad de los datos se contempla desde el diseño mismo de los procesos institucionales, adoptando dentro de estos procesos: las evaluaciones de riesgos de manera continua, la adopción de medidas preventivas, la asignación de responsabilidades dentro de la organización y la generación de evidencia documentada de las medidas adoptadas. Todo lo anterior genera que estos procesos sean dinámicos, requiriendo adaptaciones y actualizaciones constantes.

2.3. Bases legales para el tratamiento de datos

El tratamiento de datos personales sólo es legítimo si se fundamenta en una de las bases legales reconocidas en la normativa aplicable. Estas bases establecen las condiciones bajo las cuales una organización puede procesar información personal de manera legítima y ética. De conformidad con el RGPD[6] las bases legales son:

Consentimiento del titular de los datos: El tratamiento de datos personales es lícito cuando el titular ha otorgado su consentimiento libre, informado, específico e inequívoco para uno o varios fines determinados. Para que el consentimiento sea válido:

- Debe ser otorgado de forma voluntaria, sin presiones ni condiciones para acceder a un servicio
- La información proporcionada al titular debe ser clara y accesible, sin términos ambiguos
- Debe ser posible revocar el consentimiento en cualquier momento y esta revocación debe ser tan sencilla como otorgarla

4 Parlamento Europeo y Consejo de la Unión Europea. (2016). Reglamento General de protección de datos, Artículo 24. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679

5 Instituto Nacional de Ciberseguridad Español (INCIBE). (2014). Ganar en competitividad cumpliendo el RGPD: guía de recomendaciones para empresas, p. 28 y ss. Recuperado de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-ganar-competitividad-cumpliendo-rgpd-2024.pdf

6 Parlamento Europeo y Consejo de la Unión Europea. (2016). Reglamento General de protección de datos, Artículo 6. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679

Ejecución de un contrato o medidas precontractuales: El tratamiento de datos personales es legítimo cuando es necesario para la ejecución de un contrato en el que el titular de los datos sea parte, o para la aplicación de medidas precontractuales solicitadas por el mismo.

Cumplimiento de una obligación legal: Cuando el tratamiento de datos es necesario para cumplir con una obligación legal a la que está sujeta la organización, no se requiere el consentimiento del titular. En estos casos, la normativa que establece la obligación debe ser clara y específica.

Protección de intereses vitales del titular o de otra persona física: El tratamiento es lícito cuando es necesario para proteger la vida o la integridad física del titular de los datos o de otra persona.

Cumplimiento de una misión de interés público o ejercicio de poderes públicos: Las autoridades o entidades públicas pueden tratar datos personales cuando el procesamiento sea necesario para el cumplimiento de una tarea realizada en interés público o en el ejercicio de poderes conferidos por la ley.

Interés legítimo del responsable del tratamiento o de un tercero: El tratamiento de datos puede ser legítimo cuando exista un interés legítimo por parte de la organización o de un tercero, siempre que dicho interés no prevalezca sobre los derechos y libertades del titular de los datos. Al momento de aplicar esta base legal se tendrá que determinar si el interés legítimo justifica el tratamiento.

2.3.1. Constitución Política del Estado

Bolivia cuenta actualmente con tres articulados referentes a privacidad en la Constitución Política del Estado[7].

En primer lugar, dentro de los derechos civiles y políticos, se encuentra el artículo 21:

ARTÍCULO 21: Las y los bolivianos tienen los siguientes derechos:

2) A la privacidad, intimidad, honra, honor, propia imagen y dignidad

6) A acceder a la información, interpretarla, analizarla y comunicarla libremente, de manera individual o colectiva.

El artículo 21 menciona la protección a la privacidad y acceder a la información y llega a tener una relación directa con el derecho europeo, donde se menciona que no solo se debe proteger o acceder a la información, sino que esta debe ser correcta y comprobable.

En segundo lugar, los artículos 130 y 131 referentes a la acción de protección de privacidad, establecen lo siguiente:

ARTÍCULO 130

I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad.

II. La Acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa.

ARTÍCULO 131

I. La Acción de Protección de Privacidad tendrá lugar de acuerdo con el procedimiento previsto para la acción de Amparo Constitucional.

II. Si el tribunal o juez competente declara procedente la acción, ordenará la revelación, eliminación o rectificación de los datos cuyo registro fue impugnado.

7 Estado Plurinacional de Bolivia. 2009. Constitución Política del Estado Boliviano.

III. La decisión se elevará, de oficio, en revisión ante el Tribunal Constitucional Plurinacional en el plazo de las veinticuatro horas siguientes a la emisión del fallo, sin que por ello se suspenda su ejecución.

IV. La decisión final que conceda la Acción de Protección de Privacidad será ejecutada inmediatamente y sin observación. En caso de resistencia se procederá de acuerdo con lo señalado en la Acción de Libertad. La autoridad judicial que no proceda conforme con lo dispuesto por este artículo quedará sujeta a las sanciones previstas por la ley.

Es en la constitución del año 2009 que, por segunda vez en Bolivia, se menciona en un texto constitucional la protección de la privacidad y protección de datos. La primera constitución en reconocerlo fue la del año 1967, reconociendo el habeas data.

Si bien actualmente se cuenta con estos tres articulados dentro de la norma boliviana no son suficientes para la protección de las y los ciudadanos y no brindan los parámetros internacionales de protección solicitados en la comunidad internacional para poder acceder a otros mercados.

2.3.2. Código Civil Boliviano

Dentro del Código Civil del año 1975[8], se establecen ciertos puntos para la protección de ciertos derechos inherentes a toda persona, que con el desarrollo de las tecnologías de información y comunicación evolucionaron, mencionando la protección del nombre, el derecho a la imagen, derecho al honor, derecho a la intimidad y el derecho a la inviolabilidad de las comunicaciones y papeles privados.

ARTÍCULO 12 (PROTECCIÓN DEL NOMBRE)

La persona a quien se discuta el derecho al nombre que lleva o sufra algún perjuicio por el uso indebido que de ese nombre haga otra persona, puede pedir judicialmente el reconocimiento de su derecho o la cesación del uso lesivo. El juez puede ordenar que la sentencia se publique por la prensa.

ARTÍCULO 16 (DERECHO A LA IMAGEN)

I. Cuando se comercia, publica, exhibe o expone la imagen de una persona lesionando su reputación o decoro, la parte interesada y, en su defecto, su cónyuge, descendientes o ascendientes pueden pedir, salvo los casos justificados por la ley, que el juez haga cesar el hecho lesivo. II. Se comprende en la regla anterior la reproducción de la voz de una persona.

ARTÍCULO 17 (DERECHO AL HONOR)

Toda persona tiene derecho a que sea respetado su buen nombre. La protección al honor se efectúa por este Código y demás leyes pertinentes.

ARTÍCULO 18 (DERECHO A LA INTIMIDAD)

Nadie puede perturbar ni divulgar la vida íntima de una persona. Se tendrá en cuenta la condición de ella. Se salvan los casos previstos por la ley.

ARTÍCULO 19 (INVIOLABILIDAD DE LAS COMUNICACIONES Y PAPELES PRIVADOS)

I. Las comunicaciones, la correspondencia epistolar y otros papeles privados son inviolables y no pueden ser ocupados sino en los casos previstos por las leyes y con orden escrita de la autoridad competente. II. No surten ningún efecto legal las cartas y otros papeles privados que han sido violados o sustraídos, ni las grabaciones clandestinas de conversaciones o comunicaciones privadas.

8 República de Bolivia. 1975. Código Civil, Artículos 12,16,17,18,19.

2.3.3. Ley 164 de telecomunicaciones y el decreto supremo 1391 reglamento general de la ley 164

La ley 164 de telecomunicaciones[9], si bien parece ser más específica y aislada, menciona de forma directa la protección de datos, así mismo establece los parámetros necesarios para la protección de privacidad de empleados, tomando en cuenta la inviolabilidad y secreto de las telecomunicaciones. Así mismo establece la protección de usuarios de comunicaciones comerciales publicitarias por correo o medios electrónicos, que en caso de no tener un consentimiento del usuario para recibir información y publicidad se incurriría en SPAM y vulneración de datos personales como correo electrónico, usuario o número de celular.

ARTÍCULO 56 (INVIOLABILIDAD Y SECRETO DE LAS COMUNICACIONES)

> En el marco de lo establecido en la constitución política del estado, los operadores de redes públicas y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación, deben garantizar la inviolabilidad y secreto de las comunicaciones, al igual que la protección de los datos personales y la intimidad de usuarias o usuarios, salvo los contemplados en guías telefónicas, facturas y otros establecidos por norma.

ARTÍCULO 91 (COMUNICACIONES COMERCIALES PUBLICITARIAS POR CORREO ELECTRÓNICO O MEDIOS ELECTRÓNICOS)

> Mediante reglamento se establecerán, las condiciones de las comunicaciones comerciales publicitarias realizadas por medio de correo electrónico o cualquier otro medio electrónico, sin perjuicio de la aplicación, en los casos que corresponda, de la normativa vigente en materia comercial sobre publicidad y protección a las usuarias o usuarios.

Por otro lado, el decreto supremo N° 1391 reglamento general de la ley 164, es la primera normativa que establece de manera detallada el proceso de tratamiento y protección de datos a partir del artículo 176:

ARTÍCULO 176 (PROTECCIÓN DE LOS DATOS PERSONALES)

I. El personal de operadores y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación, está obligado a guardar secreto de la existencia o contenido de las comunicaciones y a la protección de los datos personales y la intimidad de los usuarios.

II. Los operadores y proveedores de servicios están obligados a adoptar las medidas más idóneas para garantizar, preservar y mantener la confidencialidad y protección de los datos personales de los usuarios del servicio, salvo en los siguientes casos:

a) De existir una orden judicial específica;

b) Con consentimiento previo, expreso y por escrito del usuario titular;

c) En casos que la información sea necesaria para la emisión de guías telefónicas, facturas, detalle de llamadas al titular acreditado, o para la atención de reclamaciones, provisión de servicios de información y asistencia establecidos por el presente Reglamento, o para el cumplimiento de las obligaciones relacionadas con la interconexión de redes y servicios de apoyo.

III. El operador o proveedor de servicios deberá coadyuvar en la identificación de los presuntos responsables de vulneraciones a la inviolabilidad, secreto de las comunicaciones, protección de los datos personales y la intimidad de los usuarios, que su personal pudiera cometer en las instalaciones del operador o proveedor.

IV. La ATT aprobará los procedimientos y medidas utilizadas por los operadores y proveedores para salvaguardar la inviolabilidad y secreto de las comunicaciones y a la protección de los datos personales y la intimidad de los usuarios.

V. Queda prohibido que los operadores y proveedores de servicios permitan el acceso a registros o bases de datos de sus usuarios, ya sea de manera individual o a través de listas de usuarias, usuarios o números, con fines comerciales o de publicidad, salvo autorización previa, expresa y escrita de la usuaria o usuario que desee recibir dicha publicidad.

9 Estado Plurinacional de Bolivia. 2011. Ley de telecomunicaciones (Ley 164)

2.4. Derechos de los titulares de los datos

Los derechos de los titulares de los datos personales constituyen un elemento fundamental dentro del RGPD[10], ya que garantizan que las personas tengan control sobre su información personal y puedan ejercer facultades específicas sobre su tratamiento.

El RGPD reconoce una serie de derechos que deben ser respetados por todas las organizaciones que procesan datos personales. Para ello, se exige que las organizaciones faciliten mecanismos accesibles y transparentes que permitan a los titulares ejercer estos derechos de manera efectiva.

Los derechos de los titulares de datos reconocidos en el RGPD y que concuerdan con la protección otorgada para los titulares de datos en Bolivia[11] se pueden calificar en una protección ARCO+P[12]:

Derecho de acceso: El derecho de acceso otorga al titular de los datos la facultad de conocer si sus datos personales están siendo procesados por una organización. En caso afirmativo, puede solicitar información detallada sobre el tratamiento de sus datos, como los fines del procesamiento, las categorías de datos en cuestión, los destinatarios de los datos, y el período durante el cual se conservarán. Este derecho le permite a la persona ejercer control sobre la manera en que sus datos están siendo utilizados y verificar la exactitud de la información que una entidad tiene sobre ella. Además, se le debe proporcionar una copia de los datos personales que se están tratando de manera gratuita, salvo que se trate de solicitudes repetitivas o excesivas[13].

Derecho de rectificación: Este derecho permite al titular de los datos corregir cualquier inexactitud o error en los datos personales que le conciernen. En el caso de que los datos sean incompletos, el titular puede solicitar que se completen con información adicional. Este derecho tiene un impacto fundamental sobre la precisión de los datos que se procesan, garantizando que los responsables del tratamiento mantengan información actualizada y veraz, lo cual es crucial para la protección de la privacidad del individuo.

Derecho de cancelación (o supresión): El derecho de cancelación implica que el titular de los datos puede solicitar la eliminación de sus datos personales cuando ya no sean necesarios para los fines para los cuales fueron recolectados o tratados. También puede aplicarse en situaciones en las que el tratamiento sea ilícito o cuando el titular retire su consentimiento (si este es la base legal para el tratamiento), o cuando el titular se oponga al tratamiento y no exista otro interés legítimo que prevalezca. Este derecho contribuye al principio de minimización de datos, garantizando que solo se conserven aquellos que sean estrictamente necesarios.

Limitación del tratamiento: Los usuarios tienen derecho a solicitar la limitación del tratamiento de sus datos personales en ciertas circunstancias, por ejemplo, cuando cuestionan la exactitud de los datos o la legalidad del tratamiento. Esto con la finalidad que los usuarios puedan presentar una solicitud en caso de transferencia internacional de datos o ampliación de tratamiento de datos.

Consentimiento informado: Las organizaciones deben garantizar que los individuos otorguen su consentimiento de manera libre, específica, informada e inequívoca para el tratamiento de sus datos personales. Esto implica que los usuarios deben comprender qué datos se recopilan, cómo se utilizarán y con quién se compartirán. Esto no solamente con la finalidad de resguardar al usuario, sino también de proteger a la organización en caso de reclamos, ya que el usuario al momento de ser informado sobre el tratamiento de datos, conoce los alcances y limitaciones, para brindar su consentimiento.

10 Parlamento Europeo y Consejo de la Unión Europea. (2016). Reglamento General de protección de datos, Capítulo III. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679

11 Tal como se mencionó anteriormente, Bolivia no tiene una norma de protección de datos específica, la mención a estos derechos tampoco se encuentra reconocida expresamente en una norma, sin embargo, se puede considerar que la protección existente alcanza a estos derechos.

12 Agencia Española de protección de datos. (2018). Guía del Reglamento General de protección de datos para Responsables de Tratamiento, p. 8 y ss. Recuperado de https://www.aepd.es/guias/guia-rgpd-para-responsables-de-tratamiento.pdf

13 Organización de Estados Americanos. (2022). Principios Actualizados sobre la Privacidad y la protección de datos Personales, p. 59 y ss.

Derecho de oposición: El derecho de oposición permite que los titulares se opongan al tratamiento de sus datos personales en situaciones específicas, como cuando el tratamiento se basa en el interés legítimo del responsable del tratamiento o en la realización de tareas de interés público o ejercicio de la autoridad pública. Este derecho también es aplicable cuando los datos son procesados con fines de marketing directo, lo que permite a la persona oponerse al uso de sus datos para este tipo de actividades. El responsable del tratamiento debe cesar el tratamiento, salvo que pueda demostrar razones legítimas convincentes que prevalezcan sobre los intereses, derechos y libertades del titular.

Derecho a la portabilidad de los datos: El derecho a la portabilidad de los datos permite a los titulares obtener sus datos personales en un formato estructurado, de uso común y lectura mecánica, y transmitirlos a otro responsable del tratamiento sin que se interrumpa el servicio. Este derecho facilita la movilidad de los datos entre distintos proveedores de servicios, y refuerza la autonomía del titular, permitiéndole transferir sus datos a la plataforma o empresa de su elección. Se trata de un derecho que facilita la competencia y mejora la transparencia en el mercado.

Derecho al olvido: Permite solicitar la eliminación de datos personales cuando ya no sean necesarios o hayan sido tratados indebidamente. Este derecho surge como una acción para ejercer frente a los buscadores, bases de datos u otros sitios de almacenamiento de la información, partiendo de que dicha información es correcta, sin embargo, su almacenamiento ya no resulta necesario, relevante, útil y por tanto, el titular puede solicitar la supresión. En el sector financiero, este derecho se ha desarrollado mediante la modificación al Reglamento para el Registro de Directores, Miembros del Órgano Interno de Control, Ejecutivos y demás Funcionarios, en relación con los requisitos y procedimientos para la cancelación de antecedentes disciplinarios[14].

2.4.1. Otros derechos

Los derechos ARCO pueden considerarse la base de protección de los titulares de datos personales, sin embargo, vale la pena hacer referencia a otros y nuevos derechos que se reconocen en favor de los titulares, para garantizar una óptima protección de sus datos personales:

- **Derecho a la no discriminación por el tratamiento de datos:** prohíbe que el uso de datos personales genere trato desigual o perjudicial para el titular
- **Derecho a la impugnación automatizada:** permite a los titulares oponerse a decisiones basadas únicamente en tratamientos automatizados que afecten sus derechos
- **Derecho a la confidencialidad de los datos:** garantiza que los datos personales sean tratados con reserva y solo accedan a ellos quienes estén autorizados
- **Derecho a obtener una indemnización**
- **Derecho a revocar la autorización o consentimiento**

14 Resolución ASFI 156/2025 de 27 de febrero de 2025, Recuperado de https://servdmzw.asfi.gob.bo/circular/Circulares/ASFI_856.pdf

2.5. Evaluación de impacto en protección de datos (EIPD)

La EIPD es una herramienta reconocida por el RGPD[15] que permite a las organizaciones identificar, evaluar y mitigar los riesgos asociados con el tratamiento de datos personales. Esta evaluación resulta esencial cuando un tratamiento puede implicar un alto riesgo para los derechos y libertades de los titulares de los datos, especialmente en situaciones donde se empleen tecnologías nuevas o donde los datos sean procesados de manera extensa o sensible, su adopción permite que las organizaciones cumplan con el principio de responsabilidad proactiva.

La EIPD debe llevarse a cabo antes de iniciar un tratamiento que pueda generar riesgos significativos para la protección de los datos personales. El RGPD establece que una organización deberá realizar esta evaluación cuando el tratamiento de datos sea "probablemente alto riesgo" y se base en tecnologías novedosas o cuando se trate de grandes volúmenes de datos sensibles.

El procedimiento para realizar una EIPD consiste en las siguientes etapas:

- **Planificación:** la organización debe definir el alcance de la EIPD, especificando los tratamientos que se evaluarán, los objetivos de la evaluación y las personas responsables de llevarla a cabo
- **Evaluación de los riesgos:** una vez identificado el tratamiento de datos, la organización evalúa los riesgos inherentes a dicho tratamiento. Esta evaluación incluye una consideración sobre el impacto de esos riesgos en los derechos y libertades de los titulares de los datos
- **Implementación de medidas:** tras identificar los riesgos, la organización debe poner en marcha medidas para mitigarlos, como el diseño de mecanismos para garantizar la seguridad de los datos o la adopción de medidas que protejan la privacidad desde el diseño y por defecto
- **Seguimiento y revisión:** una vez realizada la EIPD, la organización debe monitorear de manera continua el tratamiento de los datos personales para garantizar que se mantengan los controles adecuados y que no surjan nuevos riesgos. La evaluación no debe considerarse un proceso único, sino un ejercicio continuo de supervisión

En el caso de que la EIPD demuestre que existen riesgos que no pueden ser mitigados, el RGPD establece la obligación para la organización de consultar a la autoridad de protección de datos antes de proceder con el tratamiento. La consulta debe incluir una descripción de los riesgos residuales y las medidas propuestas para abordarlos.

En el caso boliviano, al no existir una autoridad específica para la materia de protección de datos personales, la consulta puede plantearse ante la autoridad sectorial competente, en el caso de que no se encuentre establecida como una obligación, podría considerarse un cumplimiento a la responsabilidad proactiva de la organización. Ver punto 3.2 sobre características específicas de ciertas organizaciones.

15 Parlamento Europeo y Consejo de la Unión Europea. (2016). Reglamento General de protección de datos, Artículo 35. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679

3. Análisis organizacional y evaluación inicial

Antes de implementar un sistema de cumplimiento en protección de datos y de adecuar las prácticas internas al RGPD, es importante que la organización realice un análisis exhaustivo de su contexto y situación actual. Esta etapa, que constituye la base de cualquier programa de cumplimiento, permite comprender la realidad operativa de la organización, identificar los procesos que implican el tratamiento de datos personales, y evaluar los riesgos específicos a los que está expuesta[16].

El análisis organizacional no solo debe centrarse en aspectos técnicos, sino que debe integrar una visión global que considere factores internos y externos que pueden influir en la forma en que la organización gestiona la privacidad de los datos. A partir de esta evaluación inicial, será posible diseñar un sistema de protección de datos alineado con la estructura, objetivos y recursos de la organización.

3.1. Contexto de la organización

El contexto de la organización es el marco que permite comprender cómo la misión, la naturaleza de las actividades, el tamaño y la estructura de la entidad influyen en la forma en que los datos personales son recopilados, utilizados y gestionados. Cada organización es única y, por tanto, las estrategias de cumplimiento en protección de datos deben adaptarse a su contexto específico.

En primer lugar, es necesario considerar la naturaleza de la actividad principal de la organización, ya que el nivel de riesgo y la complejidad de la gestión de datos varía significativamente según el sector en el que opere. Por ejemplo, una empresa de comercio electrónico que gestiona información financiera y comportamientos de consumo tendrá necesidades distintas a las de una institución educativa que procesa datos académicos y datos sensibles de estudiantes. De igual forma, una ONG que trabaja con poblaciones vulnerables maneja datos que, por su especial sensibilidad, requieren medidas de protección reforzadas.

El tamaño y la estructura organizacional también son factores determinantes. Una pequeña o mediana empresa con un equipo limitado puede requerir una estrategia de cumplimiento más simplificada, pero igualmente efectiva, mientras que una organización con múltiples unidades de negocio o presencia internacional deberá abordar la protección de datos desde una perspectiva más compleja y descentralizada. La existencia de departamentos específicos como tecnología de la información (TI), recursos humanos, marketing o atención al cliente influirá en la manera en que los datos son recolectados, almacenados y procesados.

El análisis del contexto debe contemplar los canales a través de los cuales la organización interactúa con los titulares de los datos. Esto incluye la identificación de si la recolección de datos se realiza a través de medios físicos, digitales, aplicaciones móviles, redes sociales, videovigilancia u otras tecnologías emergentes. Cada canal plantea desafíos particulares en términos de protección de datos y debe ser evaluado en función de su nivel de exposición a riesgos.

Por último, el análisis del contexto debe incluir una evaluación del grado de madurez organizacional en materia de protección de datos. Esto supone revisar si la organización ya cuenta con políticas internas formales, responsables designados, procedimientos de seguridad, canales para la atención de los derechos de los titulares, o si, por el contrario, se encuentra en una fase inicial en la que será necesario desarrollar desde cero los pilares de su sistema de cumplimiento.

16 Instituto Nacional de Ciberseguridad Española (INCIBE). (2017). Guía de gestión de riesgos: Una aproximación para el empresario, p. 6. Recuperado de https://www.incibe.es/empresas/guias/gestion-riesgos-guia-empresario

3.2. Características específicas de ciertas organizaciones

Existen sectores regulados cuya normativa establece determinadas obligaciones a cumplir con respecto a los datos personales de sus consumidores / clientes / usuarios.

En el caso de sectores cuya regulación no establece características específicas, se debe considerar factores como las relaciones comerciales que puedan mantener con entidades de otros países, ya que, si bien Bolivia aún no cuenta con una normativa integral de protección de datos personales, muchas organizaciones locales deben cumplir con obligaciones contractuales o regulatorias internacionales al operar con entidades de países que sí están sujetos al RGPD o a otras normativas similares. Este factor internacional también incide en la adopción de buenas prácticas y estándares globales.

3.2.1. Normativa del sector financiero

La Ley 393 de Servicios Financieros establece el derecho a la reserva y confidencialidad de la información[17], obligando a guardar la confidencialidad de los asuntos y operaciones de servicio financiero, así como la información de sus clientes, a los siguientes responsables y delegados:

- Entidades de intermediación financiera
- Empresas de servicios financieros complementarios
- Empresas de auditoría externa
- Empresas calificadoras de riesgo
- Sociedades controladoras de grupos financieros
- Empresas vinculadas patrimonialmente a empresas de intermediación financiera
- Autoridades, ejecutivos y funcionarios de instituciones del sector público

El Reglamento de Seguridad de la Información que se encuentra en la Recopilación de Normas del Sistema Financiero[18] establece medidas de seguridad y almacenamiento de información que alcanzan a proteger los derechos de los usuarios del Sistema Financiero.

Este Reglamento contiene una serie de disposiciones específicas para la seguridad de la información, considerándolo la medida de protección más alta en cuanto a una regulación vigente en nuestro ordenamiento jurídico. Estas disposiciones regulan:

- Planificación estratégica, estructura y organización de los recursos de tecnología de la información
- Administración de la seguridad de la información
- Administración del control de accesos
- Desarrollo, mantenimiento e implementación de sistemas de información
- Gestión de operaciones de tecnologías de información
- Gestión de seguridad en redes y comunicaciones
- Gestión de seguridad en transferencias y transacciones electrónicas

17 Ley 393 de servicios financieros, artículo 472 y siguientes.

18 Requisitos mínimos de seguridad, capítulo II, reglamento de seguridad de la información para los servicios financieros, recuperado de https://servdmzw.asfi.gob.bo/circular/Textos/L03T07.pdf

- Gestión de incidentes de seguridad de la información
- Continuidad del negocio
- Administración de servicios y contratos con terceros relacionados con tecnología de información
- Auditoría interna

Esta normativa alcanza aspectos relevantes para la protección de datos personales, como ser la protección de los derechos e información de los usuarios, la seguridad que deben tener sus sistemas, la contratación de servicios y productos de terceros y las medidas que estos terceros deben tomar para garantizar el nivel de seguridad adecuado, las medidas en caso de incidentes de seguridad, así como los controles periódicos y las auditorías internas.

Siguiendo el desarrollo del Análisis de Estado Inicial detallado en el punto 3.3 y siguientes, la prestación de servicios financieros deberá acompañar la implementación de la presente guía con el Reglamento de Seguridad de la Información, ya que en este se establecen obligaciones puntuales como ser, seguridad de sistemas informáticos, implementación de políticas y procedimientos adecuados, administración de sus bases de datos, implementación de planes de contingencia para asegurar la continuidad del negocio, gestión de incidentes, la administración de servicios y contratos con terceros, entre otros que también son detallados como buenas prácticas en el mencionado punto 3.3. y siguientes. Por lo tanto, en el caso de Servicios Financieros, la correcta adopción de esta guía debe acompañarse de la revisión y cumplimiento del Reglamento de Seguridad de la Información.

3.2.2. Normativa de sector de telecomunicaciones

Con respecto a las telecomunicaciones, la norma establece un tratamiento de confidencialidad para las comunicaciones privadas, correspondencia, papeles y cualquier soporte en el que se encuentren las manifestaciones privadas.

La referencia a esta definición se encuentra en la Constitución Política del Estado:

> **Artículo 25. I.** Toda persona tiene derecho a la inviolabilidad de su domicilio y al secreto de las comunicaciones privadas en todas sus formas, salvo autorización judicial. II. Son inviolables la correspondencia, los papeles privados y las manifestaciones privadas contenidas en cualquier soporte, éstos no podrán ser incautados salvo en los casos determinados por la ley para la investigación penal, en virtud de orden escrita y motivada de autoridad judicial competente. III. Ni la autoridad pública, ni persona u organismo alguno podrán interceptar conversaciones o comunicaciones privadas mediante instalación que las controle o centralice. IV. La información y prueba obtenidas con violación de correspondencia y comunicaciones en cualquiera de sus formas no producirán efecto legal.

Por otra parte, la Ley de Telecomunicaciones y sus reglamentos establecen:

- La inviolabilidad y secreto de las comunicaciones como un principio rector en el sector de telecomunicaciones y tecnologías de la información y comunicación[19]. Esta norma también se refiere a la protección de datos personales y protección de la intimidad de los usuarios. El detalle de los artículos se encuentra en el punto 2.3.3
- El reconocimiento de la confidencialidad de los datos de los usuarios, así como el derecho que estos tienen para comprobar, corregir y suprimir sus datos[20]
- Obligación del proveedor de brindar protección a los datos personales frente a publicidad no autorizada por el usuario[21]

19 Ley 164 de telecomunicaciones, Artículo 5 inc. 5).

20 Ley 164 de telecomunicaciones, Artículo 54 inc. 6) y 9).

21 Decreto supremo 1391 (reglamento de la ley de telecomunicaciones), Artículo 174 y siguientes. Específicamente el artículo 176 inc. V. se refiere a la prohibición de acceder o permitir el acceso a las bases de datos de sus usuarios con fines comerciales o de publicidad, sin autorización.

3.2.3. Normativa niñez y adolescencia

El Código Niña, Niño y Adolescente, reconoce el derecho que los menores de edad tienen a la privacidad e intimidad familiar, indicando que estos deben ser garantizados con prioridad por la familia, el Estado en todos sus niveles, la sociedad y los medios de comunicación[22]. En concordancia con la Convención sobre los Derechos del Niño de la cual Bolivia es parte.

Asimismo, los niños, niñas y adolescentes tienen derecho al respeto de su propia imagen, teniendo las autoridades y servidores públicos, así como las instituciones privadas, la obligación de mantener reserva y resguardar la identidad de los menores de edad en cualquier tipo de proceso en el que se vean involucrados, así como restringir el acceso a la documentación de los mismos.

Cuando se difundan o transmitan noticias que involucren a menores de edad, los medios de comunicación también están obligados a preservar su identificación y la del entorno familiar del menor de edad.

3.2.4. Normativa del sector salud

La protección de datos en temas médicos y aplicable para el Sector Salud, incluyendo la seguridad social a corto plazo, cuenta con líneas de procesamiento especial y las medidas de seguridad deberían ser aún más amplias, ya que se tratan datos sensibles personales, una brecha de seguridad en el sector médico es una vulneración a la imagen, honor, reputación de una persona, por lo cual la implementación de medidas específicas de gestión de datos y bases de datos es fundamental, esto no quiere decir que los datos no sean utilizado, ya que con fines estadísticos o de investigación, pueden ser empleados, simplemente esto se debe hacer con la encriptación de las bases de datos o la anonimización o seudonimización de datos.

Para esto se deben tomar en cuenta las siguientes normas y cumplir con lo establecido.

Ley 3131: Ley del Ejercicio Profesional Médico

Artículo 13. (Derechos del Paciente). Todo paciente tiene derecho a:

c) La confidencialidad

d) Secreto médico

i) Respeto a su intimidad

Ley 3729: Ley para la Prevención del VIH/SIDA, Protección de los Derechos Humanos y la Asistencia Integral Multidisciplinaria para las Personas que Viven con VIH/SIDA

Artículo 5 (Derechos y Garantías). Todas las personas que viven con el VIH/SIDA y con la garantía del Estado, tienen los siguientes derechos:

d. A que se respete su privacidad, manteniendo la confidencialidad de su estado serológico y prohibiendo las pruebas obligatorias, siempre que no este afectando a terceras personas. Excepto en los casos especificados en la presente Ley.

22 Ley 548, código niña, niño y adolescente, artículos 143 y siguientes.

3.2.5. Normativa del sector público

En muchos países con marcos normativos avanzados, como el RGPD, se establecen reglas específicas para el sector público, incluyendo la obligación de designar un Delegado de protección de datos en instituciones que procesan grandes volúmenes de información o que manejan datos sensibles. Asimismo, se exige la realización de Evaluaciones de Impacto en protección de datos cuando el tratamiento pueda afectar significativamente los derechos de los ciudadanos.

En el contexto boliviano, idealmente las instituciones públicas deberían adoptar medidas para garantizar la seguridad de los datos, implementar mecanismos de anonimización cuando sea posible y establecer políticas claras de acceso y rectificación de información, especialmente en sectores sensibles como el sector salud, financiero y registros administrativos.

Normativa específica para considerar en el Sector Público:

- Ley del Estatuto del Funcionario Público
- Ley de Procedimiento Administrativo
- Código Tributario
- Ley de Inscripción en Derechos Reales
- Ley de Registro Civil
- Código Electoral
- Ley del Sistema Nacional de Información Estadística

El Reglamento para el Desarrollo de Tecnologías de la Información y Comunicación, aprobado mediante Decreto Supremo 1793 del 13 de noviembre de 2013 establece una política tecnológica que se reconoce como pauta para el uso e implementación de nuevas tecnologías en este sector.

Es por ello que, pese a que no existe normativa específica que se refiera a protección de datos personales en el sector público, al referirnos al al almacenamiento y tratamiento de la información, los Lineamientos de software libre y estándares abiertos establecen consideraciones para los “datos y contenidos públicos” y “datos y contenidos no públicos”, señalando que dichos datos “no públicos” deben ser almacenados dentro de la infraestructura tecnológica de las entidades públicas o mediante servicios en la nube operados por el Estado, siempre dentro del territorio nacional[23].

23 Plan de Implementación de Software Libre y Estándares Abiertos (PISLEA) 2025-2030. Capítulo IV. Directrices Técnicas en el marco de la Soberanía Tecnológica.

Este PISLEA se elabora en función al mandato establecido en el Decreto Supremo 1793.

3.3. Análisis de estado inicial

El análisis de estado inicial es una fase estratégica dentro de la evaluación organizacional previa a la implementación de un sistema de cumplimiento en protección de datos personales. Su finalidad es obtener una visión clara y objetiva del punto de partida en el que se encuentra la organización en relación con el cumplimiento de los principios y obligaciones establecidos por el Reglamento General de Protección de Datos (RGPD).

El estado inicial no solo debe centrarse en aspectos formales, como la existencia de políticas de privacidad o registros de actividades, sino que debe abarcar un enfoque integral que contemple los procedimientos reales que se desarrollan en la organización y que involucran el tratamiento de datos personales[24].

Los objetivos del análisis de estado inicial son:

- Identificar si la organización cuenta con documentación y protocolos formales en materia de protección de datos
- Revisar las prácticas reales de recolección, uso, almacenamiento y eliminación de datos personales en todas las áreas funcionales
- Verificar la existencia y el grado de madurez de mecanismos internos de control, como políticas de seguridad, planes de contingencia o procedimientos para la atención de los derechos de los titulares
- Detectar riesgos específicos y posibles incumplimientos con respecto a las obligaciones previstas en el RGPD
- Evaluar el nivel de conocimiento y concienciación del personal sobre la normativa de protección de datos
- Revisar si existen relaciones con encargados del tratamiento y si dichas relaciones están reguladas contractualmente bajo los términos exigidos por el RGPD

Por otra parte, para realizar levantar correctamente esta información se debe analizar:

- **Normativa interna:** se analiza la existencia de documentos como políticas de privacidad, políticas de retención y eliminación de datos, reglamentos de uso de tecnologías, y códigos de conducta que guíen la actuación de los empleados en el tratamiento de la información
- **Procedimientos operativos:** se estudian las prácticas cotidianas de las distintas áreas para verificar cómo se aplican (o no) las políticas internas. Aquí se detectan posibles brechas entre la normativa formal y las prácticas reales
- **Infraestructura tecnológica:** se revisan los sistemas informáticos y plataformas que gestionan datos personales, verificando si cuentan con medidas de seguridad adecuadas (cifrado, control de accesos, segmentación de redes, etc.) y si las bases de datos están debidamente protegidas
- **Gestión de derechos de los titulares:** se examina si existen procedimientos claros para la atención de solicitudes de acceso, rectificación, supresión, oposición, limitación o portabilidad por parte de los titulares, y si dichos procedimientos cumplen con los plazos legales
- **Gestión de incidentes de seguridad:** se evalúa la existencia (o ausencia) de protocolos internos para responder a violaciones de datos personales, incluyendo la capacidad de notificar a la autoridad de control y a los titulares afectados en los casos previstos por la normativa[25]

Este diagnóstico inicial también materializa el principio de responsabilidad proactiva, ya que evidencia que la organización ha realizado una evaluación consciente de su situación antes de diseñar y poner en marcha un sistema de cumplimiento.

24 Instituto Nacional de Ciberseguridad Española (INCIBE). (2017). Guía de gestión de riesgos: Una aproximación para el empresario, p. 11 y ss. Recuperado de https://www.incibe.es/empresas/guias/gestion-riesgos-guia-empresario

25 Agencia Española de protección de datos (AEPD). (2021). Gestión de Riesgos y evaluación de impacto en tratamientos de datos personales, p. 49. Recuperado de https://www.aepd.es/guias/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

3.4. Identificación de tipos de datos e información

La identificación de los tipos de datos e información tratada es la tarea fundamental para garantizar que el tratamiento de datos se realice de acuerdo a los principios de minimización, licitud y limitación de finalidad previstos en el RGPD.

El RGPD establece que no todos los datos personales son iguales. Existen datos de uso cotidiano, como nombres y direcciones, y datos que se consideran especialmente sensibles, como información sobre salud, origen étnico o creencias religiosas. Por ello, conocer qué datos se manejan en cada proceso o actividad organizacional es imprescindible para adoptar medidas de seguridad proporcionales al nivel de riesgo que conlleva su tratamiento.

Algunas categorías de datos que pueden utilizarse para su identificación son:

1. **Datos de identificación personal:** son aquellos que permiten la identificación directa de la persona, como nombre completo, documento de identidad, dirección postal, correo electrónico, número de teléfono o fotografía

2. **Datos profesionales:** se refieren a la información relacionada con la vida laboral o profesional de una persona, como cargo, historial de empleo, información académica o desempeño laboral

3. **Datos financieros o patrimoniales:** incluyen información bancaria, números de cuenta, datos de tarjetas de crédito, salarios, bienes o deudas, y cualquier otra información financiera vinculada al titular

4. **Datos sensibles o de categorías especiales:** son aquellos que, según el RGPD, requieren un nivel más alto de protección debido a que su tratamiento podría generar un impacto significativo sobre los derechos y libertades de los titulares. Entre ellos se encuentran los datos de salud, datos biométricos, datos genéticos, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas y orientación sexual

5. **Datos de navegación o comportamiento digital:** se refieren a la información derivada de la interacción de los usuarios con entornos digitales, como cookies, direcciones IP, historial de navegación, datos de geolocalización o preferencias de consumo

6. **Datos de menores:** cuando la organización trata datos de menores de edad, estos adquieren una protección especial según lo previsto en el RGPD, exigiendo medidas reforzadas para garantizar su confidencialidad y seguridad

La identificación de tipos de datos debe realizarse también desde una perspectiva funcional, es decir, analizando las actividades y procesos específicos de cada área de la organización para determinar qué datos son tratados y con qué finalidad. Este análisis debe completarse con una revisión de los soportes o entornos en los que se almacenan los datos (archivos físicos, bases de datos locales, servicios en la nube, entre otros) y con la identificación de si los datos se transfieren a terceros, nacional o internacionalmente[26].

Cada categoría de datos debe estar vinculada a una finalidad concreta y legítima que justifique su tratamiento, de conformidad con el principio de limitación de la finalidad establecido en el RGPD. Asimismo, es necesario documentar cuál es la base legal que sustenta cada tratamiento, ya sea consentimiento, ejecución de un contrato, obligación legal, interés legítimo, entre otros.

Este paso permite a la organización detectar posibles situaciones de tratamiento excesivo o de acumulación de datos innecesarios, permitiendo ajustar sus procesos a los principios de minimización y proporcionalidad.

26 Agencia Española de protección de datos (AEPD). (2021). Gestión de Riesgos y evaluación de impacto en tratamientos de datos personales, p. 30. Recuperado de https://www.aepd.es/guias/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

3.5. Bases de datos y almacenamiento de información

El análisis de esta área permite a la organización identificar no solo dónde y cómo se almacenan los datos, sino también evaluar la seguridad de los entornos y tecnologías utilizadas, así como la trazabilidad y control sobre los datos procesados[27].

Las bases de datos constituyen el soporte sobre el cual se almacena la información personal de titulares, ya sean clientes, empleados, usuarios, proveedores u otros grupos de interés. Estas pueden estar estructuradas de distintas maneras según el tamaño y la actividad de la organización, abarcando desde simples hojas de cálculo o archivos físicos hasta sistemas más complejos, como servidores locales, plataformas en la nube o bases de datos distribuidas.

El análisis inicial debe partir de la identificación y clasificación de todas las bases de datos que la organización utiliza para almacenar datos personales. Esto incluye tanto bases de datos internas como aquellas gestionadas por terceros, a través de encargados del tratamiento o proveedores de servicios (por ejemplo, plataformas CRM, ERP o sistemas de almacenamiento en la nube).

Es importante distinguir entre bases de datos que contienen datos estructurados, tales como registros en sistemas administrativos, contables o de recursos humanos, y aquellas que almacenan datos no estructurados, como correos electrónicos, documentos escaneados, imágenes, grabaciones de audio o video y datos provenientes de redes sociales o aplicaciones móviles.

La organización también debe identificar la ubicación física o virtual de estas bases de datos. En el contexto actual, es cada vez más frecuente que las organizaciones utilicen servicios de almacenamiento en la nube, lo que puede implicar la transferencia internacional de datos. Este factor, en el RGPD, tiene implicaciones jurídicas importantes, ya que la organización debe asegurarse de que cualquier transferencia cumpla con los requisitos de seguridad y legalidad.

3.5.1. Seguridad y acceso

La protección de las bases de datos implica no solo garantizar la confidencialidad de la información, sino también su integridad y disponibilidad. Para ello, la organización debe evaluar las medidas de seguridad técnicas y organizativas implementadas para evitar accesos no autorizados, pérdidas accidentales, alteraciones indebidas o divulgaciones no autorizadas.

Entre estas medidas se encuentran los sistemas de control de acceso que permitan que solo las personas autorizadas puedan visualizar, modificar o eliminar los datos, la implementación de cifrado tanto en reposo como en tránsito, la segmentación de redes internas, la gestión segura de contraseñas y la realización periódica de copias de seguridad que garanticen la recuperación de la información en caso de incidentes.

La gestión de accesos debe ser proporcional al nivel de riesgo y a la sensibilidad de los datos almacenados. Por ejemplo, los datos personales sensibles o de categorías especiales deben contar con medidas de seguridad reforzadas y con registros detallados que permitan auditar quién accede a dicha información, cuándo y con qué finalidad[28].

27 Instituto Nacional de Transparencia, Acceso a la Información y protección de datos Personales (INAI). (2015). Guía para implementar un Sistema de Gestión de Seguridad de datos Personales (SGSDP), p.19. Recuperado de https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Guía_Implementación_SGSDP%28Junio2015%29.pdf

28 Instituto Nacional de Transparencia, Acceso a la Información y protección de datos Personales (INAI). (2023). Mejores Prácticas protección de datos Personales, p. 8. Recuperado de https://home.inai.org.mx/wp-content/uploads/Guía_Mejores-prácticas_SP.pdf

3.5.2. Ciclo de vida de la información y conservación

El ciclo de vida de los datos personales hace referencia a todas las etapas que atraviesa la información personal dentro de una organización, desde el momento en que es recopilada por primera vez hasta su eventual supresión o anonimización. El principio de limitación del plazo de conservación previsto en el RGPD exige que los datos personales solo se almacenen durante el tiempo necesario para cumplir con las finalidades para las cuales fueron recogidos. Una vez cumplida la finalidad, la organización debe proceder a la eliminación segura o anonimización de los datos.

En este sentido, la organización debe definir en su política interna criterios claros sobre los plazos de retención de los datos y los procedimientos para la eliminación segura, especialmente cuando se trate de dispositivos físicos o servicios de almacenamiento en la nube administrados por terceros.

3.5.2. Seguridad de los servidores externos

El almacenamiento de información en servidores externos también deberá considerar los mecanismos de seguridad propios de la organización que está encargada del almacenamiento. Este punto representa una obligación dentro del Reglamento de Seguridad de la Información del Sistema Financiero contempla que *las Entidades Supervisadas deben efectuar copias de seguridad de todos los datos e información, necesarios para el continuo funcionamiento de la institución, considerando mínimamente*[29]:

- Contar con políticas y procedimientos que aseguren la realización de copias de seguridad
- La información respaldada debe poseer un nivel adecuado de protección lógica, física y ambiental, en función a la criticidad de la misma
- Los medios de respaldo deben probarse periódicamente
- El ambiente físico destinado al resguardo de la información crítica debe contar con condiciones físicas y ambientales suficientes
- El sitio externo de respaldo debe mantener al menos 10 años de información crítica de la entidad supervisada
- Cualquier traslado físico de los medios digitales de respaldo debe realizarse con controles de seguridad adecuados
- Debe existir un etiquetado de los medios de respaldo y un inventario actualizado de los mismos

Continuando con la normativa para los servicios financieros, en caso de que dicho almacenamiento en servidores externos se realice a través de contratación de servicios de nube, el Reglamento de Seguridad de la Información establece la obligación de solicitar una NO OBJECIÓN emitida por la autoridad competente, adjuntando su “Proyecto de implementación del servicio de computación en la nube”, además de demostrar que se garantizará (i) el derecho a la reserva y confidencialidad; (ii) el proveedor deberá cumplir con los requisitos de seguridad de la información vigentes; (iii) el proveedor deberá garantizar la posibilidad de realizar auditorías por la autoridad competente, entre otros[30].

29 Reglamento de Seguridad de la Información, Sección 6: Gestión de operaciones de Tecnología de Información, Artículo 3 y siguientes.

30 Reglamento de Seguridad de la Información, Sección 11: Administración de servicios y contratos con terceros, Artículo 10.

3.6. Manejo de datos por áreas de la organización

Dado que las actividades de tratamiento no se desarrollan de manera homogénea en toda la organización, es necesario mapear y documentar de manera detallada la manera en que cada área recopila, utiliza, almacena, comparte y elimina la información personal.

Cada unidad funcional, según su naturaleza y sus funciones, realiza tratamientos con finalidades específicas y con distintos niveles de riesgo asociados. Por ejemplo, el departamento de recursos humanos tratará datos de trabajadores, incluyendo categorías sensibles como información de salud o antecedentes penales, mientras que el área de marketing se centrará en la gestión de datos de clientes y potenciales clientes, con fines de comunicación comercial o perfilado.

Para identificar el manejo de datos por áreas, se deberá considerar:

- Qué tipos de datos se tratan en cada área
- Cuál es la base legal que justifica el tratamiento
- Qué herramientas, plataformas o bases de datos son utilizadas
- Quiénes son los responsables internos de cada proceso
- Cómo se transfieren los datos entre áreas internas o hacia terceros

El identificar correctamente el tratamiento de datos que realice cada departamento de la organización permitirá adecuar las medidas o políticas internas que se establezcan en referencia a la privacidad, protección de datos o seguridad de la información. Siguiendo el ejemplo anterior, el departamento de recursos humanos que realiza un tratamiento de datos sensibles de los trabajadores, podrá tener una política interna de manejo de información y documentación más estricta cuando se trate de expedientes de los trabajadores, con procedimientos específicos para el almacenamiento y control de accesos, a diferencia de otros departamentos cuya información y datos manejados no tengan la misma calidad.

3.6.1. Monitoreo de mails - correspondencia o correos electrónicos

La Ley 164 de Telecomunicaciones, establece el secreto de las telecomunicaciones, limitaciones y alcances de monitoreo de correos electrónicos laborales y personales. Lo cual da lugar a que la organización solamente podrá realizar un control o tendrá acceso a las telecomunicaciones cuando el correo electrónico sea corporativo. El correo electrónico personal no podrá ser revisado o monitoreado por la organización.

La organización deberá establecer en su normativa interna y de ser necesario en el contrato la gestión de datos e información de la organización, estableciendo si se contará con cuentas empresariales y la restricción de uso de cuentas personales para fines laborales.

ARTÍCULO 89 (CORREO ELECTRÓNICO PERSONAL)

A los efectos de esta Ley el correo electrónico personal se equipara a la correspondencia postal, estando dentro del alcance de la inviolabilidad establecida en la Constitución Política del Estado. La protección del correo electrónico personal abarca su creación, transmisión, recepción y almacenamiento.

ARTÍCULO 90 (CORREO ELECTRÓNICO LABORAL)

Cuando una cuenta de correo electrónico sea provista por la entidad empleadora al dependiente como medio de comunicación, en función de una relación laboral, se entenderá que la titularidad de la misma corresponde al empleador independientemente del nombre de usuario y clave de acceso que sean necesarias para su uso, debiendo comunicarse expresamente las condiciones de uso y acceso del correo electrónico laboral a la empleada o empleado.

3.7. Identificación de posibles vulnerabilidades

Una vez realizado el análisis de estado inicial, la siguiente etapa consiste en la identificación de posibles vulnerabilidades que podrían afectar la seguridad, integridad y confidencialidad de la información, así como exponer a la organización a incumplimientos del RGPD.

Las vulnerabilidades pueden encontrarse tanto en los aspectos técnicos como en las prácticas organizativas. En el plano técnico, las amenazas más comunes incluyen:

- La falta de cifrado de datos sensibles
- La deficiente gestión de contraseñas
- La ausencia de controles de acceso adecuados
- El uso de sistemas obsoletos o sin parches de seguridad
- La falta de respaldo periódico de las bases de datos, entre otros

En el plano organizativo y procedimental, las vulnerabilidades suelen estar relacionadas con la falta de políticas claras, la escasa capacitación del personal en materia de protección de datos, la recolección excesiva de información, o la omisión en la gestión de solicitudes de derechos por parte de los titulares. Asimismo, la falta de trazabilidad sobre quién accede o modifica los datos personales es otra debilidad frecuente que puede incrementar el riesgo de accesos no autorizados o de filtraciones internas.

La correcta detección de estas vulnerabilidades es indispensable para priorizar acciones y recursos. Las debilidades que afecten datos sensibles o datos de grandes volúmenes de personas deben ser consideradas de alto riesgo, lo que obligará a la organización a implementar medidas correctivas inmediatas o incluso a realizar una Evaluación de Impacto en protección de datos (EIPD) cuando corresponda.

Este diagnóstico de vulnerabilidades debe ser dinámico y revisarse periódicamente, dado que los riesgos evolucionan con la incorporación de nuevas tecnologías, el crecimiento de la organización o los cambios en la normativa aplicable.

4. Seguridad de la información, protección de datos y gestión de riesgos

La seguridad de la información es fundamental para la protección de activos digitales, continuidad operativa y mitigación de riesgos en cualquier organización. Más allá de la protección de datos personales, se requiere una estrategia robusta para proteger infraestructura crítica, sistemas de información, propiedad intelectual y operaciones empresariales contra amenazas internas y externas.

La misión de la seguridad de la información dentro del marco de gobierno de las TI es asegurar una adecuada gestión del riesgo. Debemos entender por ello que las organizaciones deben gestionar el riesgo que, en un momento dado, pueda afectar e impactar negativamente en sus actividades o procesos y que podría comprometer el cumplimiento de sus objetivos. Estos impactos pueden ser cuantificados en términos de daños sobre las dimensiones confidencialidad, integridad o disponibilidad, atendiendo al modelo de negocio propio de la organización y de las consecuencias que puede tener, para ellos, un incidente que altere estas dimensiones de seguridad.

El rol de la seguridad de la información es garantizar una adecuada protección de los activos y asegurar la continuidad de negocio en el supuesto de que se produzca una contingencia o desastre.

Puntos a ser analizados al auditar una organización:

- **Confidencialidad:** ¿qué consecuencias tendría para la organización que cierta información (la vinculada al área de gestión del entrevistado) fuera conocida o accesible por personal no autorizado interno o externo a la organización?
- **Integridad:** ¿qué consecuencias tendría para la organización que cierta información (la vinculada al área de gestión del entrevistado) fuera manipulada, de forma deliberada o accidental, por parte de personal no autorizado, interno o externo a la organización?
- **Disponibilidad:** ¿qué consecuencias tendría para la organización que cierta información (la vinculada al área de gestión del entrevistado) no pudiera ser accedida o consultada por personal interno o externo a la organización?

De las tres dimensiones de la seguridad de la información, la disponibilidad presenta una particularidad especial debido, principalmente, a que el daño suele ser proporcional a la duración del incidente.

Principales riesgos a los que se expone la información:

- Borrado o pérdida de los documentos o sus archivadores
- Contingencias, como fuego o inundación en las dependencias físicas donde residen los sistemas de información
- Deslealtad de los empleados en el tratamiento de la información
- Error o falla del equipamiento informático
- Errores de los administradores de sistemas o desarrolladores de aplicaciones
- Caídas de los servicios de telecomunicaciones que interconectan la organización
- Hacking de los servicios electrónicos que son alcanzables desde Internet
- Malware sobre los ficheros electrónicos

Se considera como amenaza a cualquier afectación al flujo normal de la información, existen diferentes tipos de incidentes:

- **Interrupción:** no poder acceder a la información cuando es vital y necesaria para la toma de decisiones, por inoperatividad de las infraestructuras tecnológicas (por ejemplo, debido a caída de servicios de telecomunicaciones, avería de los equipos informáticos, contingencias como el fuego en salas de CPD, etc.)
- **Interceptación:** información accedida por personas no autorizadas (por ejemplo, acciones de hacking en servidores con fuga de información, espionaje de las telecomunicaciones, robo de datos, etc.)
- **Modificación:** alteración de la información, de forma intencionada o por error, al no existir, en ninguno de los dos casos, controles (por ejemplo, debido a malware que altere ficheros, interceptación y modificación de documentos electrónicos, alteración de información en bases de datos, etc.)
- **Fabricación:** falta de confianza en las transacciones electrónicas con terceros, al no existir mecanismos de autenticidad y repudio (por ejemplo, suplantación de identidad digital o de páginas web mediante phishing, etc.)

Sin embargo, a nivel internacional se tiene una concepción errónea, ya que se busca simplemente el cumplimiento de seguridad de la información sin contar con un correcto proceso de protección de datos personales. La protección de datos se enfoca en la protección del usuario y la seguridad de la información tiene un enfoque más empresarial, que al aplicarse de manera aislada podría vulnerar el derecho de usuarios sobre sus datos, como por ejemplo con el derecho de acceso.

PRIVACIDAD DE DATOS

VS

SEGURIDAD DE LA INFORMACIÓN

La privacidad se trata más sobre el "derecho de elección''. Un individuo debe saber cómo se procesa (recopila, comparte, usa, etc.) su información personal.

La seguridad de la información se enfoca en la protección de datos confidenciales / sensibles / PII y activos, mediante controles como firewalls, cifrado, sistemas de prevención de intrusiones (IPS) o controles físicos.

OBJETIVO:
Salvaguardar la privacidad y los derechos-de los individuos en relación con el manejo y procesamiento de sus datos personales.

OBJETIVO:
Mantener la confidencialidad integridad y disponibilidad (CIA) de los datos dentro de una organización.

Cumplimiento con leyes de protección de datos dependiendo de la región e industria.

Normativas y regulaciones específicas de la industria suelen ser los principales impulsores de la seguridad de la información.

Protección de la información personal de los individuos manejada por organizaciones.

Protección de información sensible, propiedad intelectual y datos propietarios.

Generalmente, equipos de cumplimiento, legales y oficiales de protección de datos son quienes impulsan las iniciativas de privacidad de datos.

Generalmente, las iniciativas de seguridad de la información son lideradas por CISO y equipos de TI.

Mitigación de riesgos por incumplimiento de regulaciones de protección de. datos, manejo inadecuado de información y violaciones de privacidad.

Enfocado en la mitigación de riesgos como accesos no autorizados, filtraciones de datos y fugas de información.

SUPERPOSICIÓN Y COLABORACIÓN

La seguridad de la información y la privacidad de datos suelen colaborar para fortalecer las medidas de protección en general. Por ejemplo, las medidas de ciberseguridad protegen los datos contra brechas, lo que también garantiza la privacidad de los datos y mantiene la seguridad de la información.

4.1. Medidas técnicas y organizativas para la protección de datos y de la información

Para garantizar la seguridad de los datos personales, las organizaciones deben implementar una combinación de medidas técnicas y organizativas basadas en los principios del Privacy by Design y Privacy by Default, establecidos en el RGPD. Además de estos puntos es necesario tomar en cuenta estándares internacionales como los sistemas de gestión de seguridad de la información (ISO/IEC 27001)[31].

El PIA (Privacy impact assessment) o la evaluación de impacto de la protección de datos constituye una parte integral de tomar un enfoque de diseño de privacidad, un PIA debe permitir a las organizaciones identificar y corregir problemas en una etapa temprana, lo que reduce los costes asociados y los daños a la reputación que, de otro modo, podría ocurrir al no gestionar de forma adecuada los riesgos vinculados a la privacidad.

Un PIA debe entenderse como un proceso que ayuda a las organizaciones a identificar y minimizar los riesgos de privacidad de los nuevos proyectos o sistemas. La realización de un PIA implica trabajar con personas dentro de la organización, con terceros y con las personas afectadas para identificar y reducir los riesgos en materia de privacidad.

Medidas técnicas:

Seguridad en la infraestructura tecnológica

- Protección de infraestructura física, cloud y datos empresariales)
- Implementación de firewalls, IDS/IPS (Prevention Systems) sistemas de monitoreo.
- Sistemas de Detección y Prevención de Intrusiones (IDS/IPS) para identificar ataques.
- Aplicación de cifrado de datos en reposo y en tránsito
- Uso de herramientas de prevención de pérdida de datos, para evitar filtraciones

Protección en el almacenamiento y transmisión de datos

- Aplicación de cifrado de bases de datos y medidas de anonimización/pseudonimización
- Implementación de protocolos seguros para la transmisión de datos (HTTPS, SFTP, VPN)
- Determinar periodos de conservación de datos

Respaldo y recuperación de datos

- Implementación de políticas de backup periódico y restauración
- Uso de la regla 3-2-1 de copias de seguridad (3 copias, 2 formatos distintos, 1 fuera del sitio)

Medidas organizativas:

Políticas de seguridad y concienciación

- Creación de una Política de protección de datos
- Implementación de matrices de cumplimiento de seguridad de la información
- Capacitación continua en seguridad para todo el personal
- Simulaciones de ataques de phishing y sesiones de entrenamiento en ciberseguridad
- Aplicación de un modelo de gestión de cambio organizacional para adoptar buenas prácticas
- Creación de una Política de Clasificación y Manejo de la Información

Roles y responsabilidades

- Designación de un Responsable de protección de datos (DPO)
- Designación o entrenamiento de un responsable de Seguridad de la Información (CISO)
- Definición de responsabilidades claras en la gestión de datos personales en cada área

31 Organización Internacional de Normalización. (2013). ISO/IEC 27001:2013 - Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos. Recuperado de https://www.iso.org/standard/54534.html

4.2. Gestión de incidentes y respuesta ante brechas de seguridad

Un incidente de seguridad puede exponer datos personales, vulnerar la seguridad de la información y generar sanciones legales, daños reputacionales, así como pérdida de confianza. La organización debe contar con un plan de respuesta ante incidentes alineado con la ISO/IEC 27001, ISO/IEC 27035[32] y los mecanismos de respuesta ante vulneración de datos personales, tomando en este caso como base el Reglamento General de protección de datos (RGPD). Las organizaciones deben anticiparse y reaccionar eficazmente ante incidentes de seguridad, con Plan de Respuesta a Incidentes (IRP).

La gestión de incidentes varía en cada área, comenzando con la detección de phishing hasta llegar a un ataque DDOS o de denegación de servicio, por lo cual no todas las áreas de una organización cuentan con los mismos lineamientos de gestión de incidentes.

Etapas clave en la gestión de incidentes:

Identificación y detección:

- Monitoreo constante con herramientas SIEM (Security Information and Event Management)
- Implementación de alertas ante accesos no autorizados o tráfico inusual

Contención:

- Aislamiento del sistema afectado para evitar propagación
- Bloqueo de cuentas comprometidas y cambios de credenciales

Erradicación y mitigación:

- Eliminación del malware, cierre de vulnerabilidades y restauración de sistemas
- Evaluación del impacto en los datos personales

Notificación y comunicación:

- De acuerdo con el RGPD, las brechas de seguridad deben notificarse a la autoridad competente en un plazo máximo de 72 horas, estos plazos cuentan con cierta estandarización a nivel internacional, en países sin una autoridad se solicita la notificación a usuarios sobre la brecha existente
- Comunicación con usuarios afectados en caso de alto riesgo

Lecciones aprendidas y mejora continua:

- Revisión de incidentes para prevenir futuras vulnerabilidades
- Actualización de políticas de seguridad

32 Organización Internacional de Normalización. (2013). ISO/IEC 27035:2013 - Tecnología de la información - Técnicas de seguridad - Gestión de incidentes de seguridad de la información. Recuperado de https://www.iso.org/standard/44379.html

4.3. Cifrado, anonimización y seudonimización

El cifrado, la anonimización y la seudonimización son técnicas fundamentales para la protección de datos personales, alineadas con los principios de Privacy by Design, aplicado como técnica para tratar datos sin vulnerar la intimidad, imagen o identidad de una persona.

Este tipo de herramientas de seguridad se emplean para la protección de información o datos sensibles o confidenciales, contando con lineamientos de identificación del valor y la sensibilidad. Sin embargo, no es necesario que se emplee de manera continua ya que en algunos casos podría hacer que algunos procesos sean más lentos y es aquí donde la clasificación de tipos de datos e información juega un papel fundamental. Así mismo, la organización no necesita capacitar a todo su personal, ya que puede asignarse la tarea a un área específica para este proceso. Por ejemplo, en casos de manejo de información sensible o confidencial, por lo cual no todo el personal debe conocer de procesos de cifrado de datos, pero sí debe considerarse que información o datos contarán con cifrado para su protección.

Aplicación de anonimización y pseudonimización en procesos empresariales:

- **Anonimización:** enmascaramiento de datos, generalización, supresión de atributos
- **Pseudonimización:** reemplazo de datos por identificadores reversibles bajo control estricto

Casos de uso en seguridad de la información:

- Anonimización de logs y registros en auditorías de seguridad
- Pseudonimización de datos en pruebas de desarrollo para evitar acceso a datos reales

Cifrado de datos

- **En tránsito:** uso de TLS 1.3, VPN y SSH para proteger la comunicación de datos
- **En reposo:** implementación de AES-256 o RSA-4096 en bases de datos, discos y backups

Anonimización de datos

- Proceso que impide identificar a una persona
- **Técnicas:** enmascaramiento de datos, generalización y agregación. Ejemplo: Sustitución de nombres por valores aleatorios

Pseudonimización de datos

- Sustitución de datos identificativos por seudónimos, permitiendo su reversión bajo ciertas condiciones. Ejemplo: Codificación de nombres con un identificador único en vez de información real

4.4. Control de accesos y autenticación

Una estrategia de Gestión de Identidad y Accesos robusta es esencial para evitar accesos no autorizados.

Principios de control de acceso:

- **Principio de Mínimo Privilegio (PoLP):** los empleados sólo deben acceder a la información necesaria para su trabajo
- **Segregación de funciones (SoD):** evita que un solo usuario tenga control total sobre procesos críticos
- Control de Accesos Basado en Roles (RBAC) y en Atributos (ABAC)
- Monitorización de accesos y alertas en tiempo real

Sistemas de autenticación segura:

- Autenticación basada en biometría (huella digital, reconocimiento facial) (Mecanismos seguros de recolección y almacenamiento de datos biométricos)
- Autenticación robusta: Implementación de MFA (autenticación multifactor) y contraseñas seguras
- Uso de hardware tokens y certificados digitales para reforzar autenticación

Técnicas de seguridad en acceso a datos:

- Autenticación biométrica (reconocimiento facial, huella digital)
- Single Sign-On (SSO) para evitar contraseñas múltiples y débiles

4.5. Análisis continuo y evaluación de nuevos riesgos

La seguridad de la información, así como la protección de datos no son procesos estáticos, requiere un monitoreo constante y una evaluación de riesgos proactiva.

- Identificación de activos y amenazas
- Evaluación del impacto y probabilidad
- Implementación de controles y monitoreo continuo

Evaluaciones periódicas de seguridad (se analizará más a detalle en el punto 6 de la presente Guía)

- Pruebas de penetración (Pentesting)
- Simulaciones de ataques
- Monitoreo con inteligencia de amenazas (Threat Intelligence)
- Evaluaciones de impacto en protección de datos (DIA/PIA)

Adaptación a normativas emergentes

- Cumplimiento de RGPD, ISO/IEC 27001
- Análisis de riesgos en sistemas de inteligencia artificial según el AI Act

5. Implementación del RGPD en la organización

La implementación del RGPD en una organización supone la adopción de un enfoque integral que debe trascender a todas las actividades relacionadas con el tratamiento de datos personales. Esta implementación va más allá de un simple cumplimiento formal con las regulaciones, en su lugar, invoca la construcción de una cultura organizacional donde la protección de datos se trata como un asunto estructural que se puede encontrar en cada nivel y departamento. Las organizaciones deben transformar la gestión de la privacidad en un proceso sistemático y estructurado que garantice la seguridad jurídica, la confianza de los usuarios y la prevención de riesgos[33].

Al igual que se detalla en los aspectos a considerar para la elaboración de Políticas de Privacidad, la implementación de un Reglamento de protección de datos Personales debe elaborarse de forma específica y con las características particulares de cada organización, por lo que no existe un "modelo" que aplique a todas las organizaciones. No obstante, los puntos esenciales que deben tratarse en este documento se han colocado como Anexo 1.

La aplicación efectiva del RGPD se articula mediante diversas medidas que incluyen la delimitación interna de roles y responsabilidades, la documentación de políticas, la documentación de procedimientos y el registro de respuestas a solicitudes de interesados. Estas medidas comprenden:

5.1. Nombramiento del responsable de protección de datos (DPO)

El responsable de protección de datos, conocido como Data Protection Officer (DPO), es una figura clave en la estructura de cumplimiento del RGPD[34]. Su rol es garantizar que la organización aplique y conozca correctamente la normativa de protección de datos, supervise la adecuación de los procesos internos a los principios del RGPD y actúe como enlace con la autoridad competente.

El DPO debe poseer un conocimiento profundo de la normativa de protección de datos y habilidades suficientes para evaluar riesgos, asesorar a la organización y fomentar la cultura de cumplimiento. El RGPD establece que su nombramiento es obligatorio en determinados supuestos, especialmente en organizaciones que realizan tratamientos a gran escala de datos sensibles o que monitorizan de forma sistemática y regular a personas físicas. Esta figura también ha sido incorporada en los Proyectos de Ley de Protección Datos Personales que se han presentado en la Asamblea Legislativa en Bolivia.

El DPO debe participar activamente en la planificación de nuevos proyectos o iniciativas que impliquen la recolección y uso de datos personales, asegurando que la protección de la privacidad esté integrada desde la fase inicial del diseño de cualquier producto, servicio o proceso (lo que se conoce como "privacidad desde el diseño" o "privacy by design").

Además de sus tareas de supervisión, el DPO actúa como punto de contacto para los titulares de los datos que deseen ejercer sus derechos o plantear consultas relacionadas con la privacidad. La independencia funcional y facultades de ejecución del DPO dentro de la organización son un aspecto crucial[35], ya que debe actuar de manera autónoma y sin recibir instrucciones directas sobre cómo desempeñar sus funciones. La presencia de un DPO asegura que la organización cuente con una figura especializada que impulse la implementación efectiva del RGPD, que promueva la cultura de la privacidad y que garantice la rendición de cuentas ante autoridades y titulares de los datos.

33 Guía del Reglamento General de protección de datos para Responsables de Tratamiento, Agencia Española de protección de datos. Recuperado de https://www.aepd.es/guias/guia-rgpd-para-responsables-de-tratamiento.pdf

34 Parlamento Europeo y Consejo de la Unión Europea. (2016). Reglamento General de protección de datos, Artículos 37-39. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679

35 Sobre la independencia y posición del DPO dentro de una organización se recomienda: El Manual del DPD (Delegado de protección de datos) Elaborado por Douwe Korff & Marie Georges para el proyecto T4DATA (2019), financiado por la Unión Europea. Recuperado de https://www.aepd.es/documento/el-manual-del-dpd-korffgeorges-esp.pdf

5.1.1. Proceso de selección de un DPO

En primer lugar, la organización deberá considerar que, no siempre es necesario realizar una nueva contratación de personal para asumir el cargo específico de Responsable de protección de datos. En el día a día, muchas organizaciones optan por capacitar a un funcionario de un cargo existente para asumir esta función, para tomar esta decisión la organización deberá evaluar la criticidad de los datos personales que se encuentran en tratamiento, el tratamiento a gran escala y sistemático, así como el nivel de riesgo y exposición de los datos personales.

En caso de tratarse de una pequeña o mediana organización cuyo tratamiento de datos no requiere de la contratación de un perfil específico en calidad de DPO, es posible cubrir dichas funciones con un funcionario del departamento legal o del departamento técnico informático[36]. En cuyo caso será importante que la persona cumpla con una serie de capacitaciones que le permitan ejercer la supervisión y cumplimiento debido.

Por otra parte, en caso de contratación de un DPO, en términos generales deberá contar con conocimientos en (i) derecho de protección de datos, (ii) seguridad de la información, y (iii) gestión de cumplimiento. Asimismo, este deberá poseer el suficiente conocimiento técnico y legal aplicable para las características particulares de la organización.

Adicionalmente, resulta recomendable que el perfil de DPO cuente con certificaciones internacionales en protección de datos y privacidad, como la CIPP/E (aplicable para el RGPD), CIPM y/o ISO 27001.

5.2. Creación de un programa de cumplimiento

La creación de un programa de cumplimiento en protección de datos es esencial para estructurar y consolidar las acciones que la organización llevará a cabo para cumplir con el RGPD. Este programa debe ser una herramienta dinámica que guíe a la organización en la gestión del ciclo de vida de los datos personales, desde la recopilación hasta su eliminación.

El programa de cumplimiento actúa como una herramienta de gestión de la privacidad, que orienta las acciones de la organización hacia un enfoque estructurado y sistemático. Su correcta implementación requiere que la protección de datos se incorpore desde las primeras fases de cualquier proyecto, proceso o actividad que implique la recolección o tratamiento de información personal, en línea con los principios de privacidad desde el diseño y por defecto.

El programa debe comenzar con un diagnóstico de la situación actual de la organización, que incluya la identificación de flujos de datos, los responsables de cada proceso y los riesgos asociados. A partir de este análisis inicial, se deben establecer los procedimientos y controles internos necesarios para garantizar la conformidad con la normativa. Lo anterior se refiere a la creación de un sistema de supervisión interna que permita verificar, de manera continua, que las políticas y procedimientos de protección de datos están siendo correctamente aplicados en la práctica. Este sistema debe incluir la programación de auditorías internas periódicas, dirigidas a evaluar el nivel de cumplimiento de la normativa y la eficacia de las medidas implementadas.

Un programa de cumplimiento efectivo debe estar alineado con los principios de responsabilidad proactiva y protección de datos desde el diseño, asegurando que la privacidad sea considerada en todas las decisiones estratégicas de la organización.

Finalmente, será importante considerar que la efectividad de cualquier programa de cumplimiento depende en gran medida del nivel de conocimiento y compromiso del personal de la organización. Por ello, el programa debe incluir un plan de formación continua para todo el personal que interviene en el tratamiento de datos personales.

36 Microsoft. (2023). RGPD simplificado: Una guía para su pequeña empresa.
Disponible en https://learn.microsoft.com/es-es/microsoft-365/admin/security-and-compliance/gdpr-compliance?view=o365-worldwide

5.3. Registro de actividades de tratamiento

El Registro de Actividades de Tratamiento es una herramienta documental que permite a las organizaciones tener un control exhaustivo sobre los tratamientos de datos personales que realizan y, al mismo tiempo, constituye una prueba material de la aplicación del principio de responsabilidad proactiva (accountability).

El RGPD[37] establece la obligación de llevar este Registro de Actividades de Tratamiento para las organizaciones que emplean a más de 250 personas, que realicen tratamiento sistemático o incluya categorías especiales de datos personales, como ser datos de salud, religión u origen étnico o racial.

Este Registro se constituye en una herramienta estratégica para la gestión de la privacidad, ya que proporciona una visión integral de todos los flujos de datos dentro de la organización, identificando los procesos, actores y riesgos asociados a cada actividad de tratamiento. Esta herramienta debe contemplar:

- La identidad y datos de contacto del responsable del tratamiento y, en su caso, del delegado de protección de datos (DPO) y de los encargados del tratamiento
- Las finalidades específicas del tratamiento, es decir, para qué se utilizan los datos personales dentro de la organización (por ejemplo: gestión de recursos humanos, atención al cliente, marketing, seguridad física, entre otros)
- Descripción de las categorías de interesados y de las categorías de datos personales tratados. En este punto se detallan los colectivos cuyos datos son gestionados (clientes, empleados, proveedores, etc.) y los tipos de datos que se recogen (datos de contacto, datos bancarios, datos de salud, etc.)
- Los destinatarios o categorías de destinatarios a quienes se comunicarán los datos, incluyendo transferencias a terceros países u organizaciones internacionales, si corresponde
- Los plazos previstos para la supresión de las distintas categorías de datos, lo que implica definir las políticas de conservación y eliminación que se aplican a cada proceso
- Descripción general de las medidas técnicas y organizativas de seguridad que garantizan la protección de los datos personales frente a accesos no autorizados, pérdida, alteración o divulgación

Los registros deben mantenerse actualizados y disponibles para consulta, ya que su valor recae en la función operativa, al tratarse de un mapa detallado que permite a la organización identificar sus procesos, tratamientos innecesarios, evaluar los riesgos y priorizar la implementación de medidas correctivas o de seguridad necesarias.

El correcto mapeo y levantamiento de la información para los registros, dependerá de la cultura organizacional e involucramiento de todas las áreas correspondientes, mismas que deberán reflejar la realidad operativa de la organización, revisar y periódicamente los reportes, garantizando así el cumplimiento de la responsabilidad proactiva.

5.4. Políticas de privacidad y avisos legales

Las Políticas de Privacidad y los avisos legales son instrumentos esenciales dentro del sistema de cumplimiento del RGPD y constituyen uno de los principales mecanismos para garantizar la transparencia en el tratamiento de datos personales[38]. Su función no se limita a cumplir una obligación formal, sino que representan el primer punto de contacto entre la organización y los titulares de los datos, generando confianza y demostrando el compromiso institucional con la protección de la información.

Estas herramientas permiten informar de manera clara, precisa y accesible a los individuos sobre cómo se recopilan, utilizan, almacenan y protegen sus datos personales, facilitando la comprensión de sus derechos y de las garantías que ofrece la organización para el resguardo de su privacidad. La redacción de estos documentos debe estar alineada con el principio de transparencia y lealtad, que obliga a las organizaciones a comunicar de manera clara y comprensible toda la información relacionada con el tratamiento de datos personales.

37 Parlamento Europeo y Consejo de la Unión Europea. (2016). Reglamento General de protección de datos, Artículo 30. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679

38 Instituto Nacional de Transparencia, Acceso a la Información y protección de datos Personales (INAI). (2011). Guía para el Aviso de Privacidad, p. 24 y ss. Recuperado de https://inicio.inai.org.mx/CalendarioCapacitacion/ManualAvisoPrivacidad.pdf

La adecuación de las políticas de privacidad y avisos legales al tipo de organización es un aspecto crítico para garantizar la efectividad de la gestión de la privacidad y la conformidad con el RGPD. No existe una política de privacidad universal o un aviso legal estándar que pueda ser aplicado indistintamente a cualquier organización. Cada entidad, ya sea una empresa privada, una universidad, una ONG o una institución pública, posee características particulares que determinan cómo y para qué finalidades trata los datos personales.

En este contexto, una política de privacidad genérica o un aviso legal estandarizado no será capaz de reflejar fielmente cómo se procesan los datos, lo cual puede derivar en falta de transparencia, incumplimiento normativo y pérdida de confianza por parte de los usuarios. La personalización de estos documentos permite explicar con precisión qué se hace con los datos y qué garantías ofrece la organización frente a los riesgos asociados[39].

Asimismo, dado que las actividades de tratamiento de datos pueden evolucionar con el tiempo —ya sea por la introducción de nuevos servicios, la adopción de tecnologías emergentes o cambios regulatorios— tanto la política de privacidad como los avisos legales deben ser revisados y actualizados de manera periódica. Cualquier modificación sustancial en la finalidad del tratamiento, en las bases legales o en los derechos de los titulares debe ser informada de manera clara a los usuarios, garantizando el cumplimiento continuo del principio de transparencia.

5.4.1. Elementos de una política de privacidad

La política de privacidad es el documento central que establece de manera integral cómo una organización gestiona la información personal que recopila en el ejercicio de sus actividades. No debe concebirse como un documento genérico, sino como una política específica adaptada al contexto particular de cada organización, considerando las características de los tratamientos de datos que realiza y los sectores en los que opera.

Elementos esenciales de una política de privacidad:

- La identificación clara del responsable del tratamiento y sus datos de contacto
- Las finalidades concretas para las cuales se recogen los datos personales, diferenciando entre tratamientos necesarios para la ejecución de un contrato, cumplimiento de obligaciones legales, intereses legítimos o aquellos que requieren consentimiento
- Las bases legales que legitiman cada tratamiento de datos
- La descripción de las categorías de datos personales tratados
- La identificación de los destinatarios o categorías de destinatarios a quienes se comunicarán los datos, incluyendo transferencias internacionales, si las hubiera
- El plazo durante el cual los datos serán conservados, o los criterios utilizados para determinar dicho plazo.
- Una explicación clara de los derechos que asisten a los titulares (acceso, rectificación, supresión, limitación, portabilidad, oposición, entre otros)
- Los procedimientos establecidos para ejercer estos derechos, incluyendo los canales de contacto y los plazos de respuesta
- Información sobre la existencia de decisiones automatizadas o elaboración de perfiles, si procede
- La referencia a la autoridad de control competente ante la cual los titulares pueden presentar reclamaciones

El lenguaje utilizado debe ser claro, accesible y libre de tecnicismos jurídicos o ambigüedades. De este modo, se garantiza que cualquier persona, independientemente de su formación o conocimientos previos, pueda comprender de forma sencilla cómo se tratarán sus datos personales.

Para mayor referencia sobre los aspectos esenciales que debería contemplar una Política de Privacidad, se ha colocado un MODELO en el Anexo 2.

39 Instituto Nacional de Transparencia, Acceso a la Información y protección de datos Personales (INAI). (2011). Guía para el Aviso de Privacidad, p. 7 y ss. Recuperado de https://inicio.inai.org.mx/CalendarioCapacitacion/ManualAvisoPrivacidad.pdf

5.4.2. Avisos legales

Los avisos legales o cláusulas informativas son textos más breves que deben presentarse en todos aquellos puntos en los que la organización recolecte datos personales, ya sea a través de formularios físicos, portales web, aplicaciones móviles o cualquier otro canal de recolección.

El aviso legal debe proporcionar la información básica sobre la finalidad del tratamiento, la identidad del responsable y los derechos que asisten al titular. Aunque de menor extensión que la política de privacidad, el aviso legal debe incluir los elementos esenciales que permitan al usuario comprender de manera inmediata el destino que tendrán sus datos personales antes de que estos sean recabados.

En el ámbito digital, estos avisos suelen integrarse directamente en los formularios de registro o contacto, acompañados de una casilla de aceptación expresa que confirma que el titular ha leído y acepta la política de privacidad y las condiciones asociadas al tratamiento.

En los casos en los que los datos se recojan para varias finalidades diferenciadas (por ejemplo, gestión de la relación contractual y envío de comunicaciones comerciales), el aviso legal debe permitir que el titular pueda otorgar su consentimiento de manera granular, es decir, aceptar una finalidad y rechazar otra.

5.5. Gestión del consentimiento y derechos de los titulares

La gestión del consentimiento y de los derechos de los titulares de los datos constituye no solo son la materialización práctica de los principios de licitud, lealtad y transparencia, sino que también reflejan el respeto efectivo por la autonomía y la dignidad de las personas en el uso de su información personal.

Tanto el consentimiento como la capacidad de ejercer derechos otorgan a los individuos un control efectivo sobre sus datos personales, permitiéndoles decidir cuándo, cómo y para qué sus datos serán tratados[40]. Una gestión adecuada de estos aspectos fortalece la confianza de los titulares en la organización y garantiza que el tratamiento de datos se desarrolle dentro del marco de la legalidad y la ética.

La gestión efectiva de estos derechos implica que la organización debe contar con procedimientos claros y accesibles para la recepción, tramitación y resolución de las solicitudes que presenten los titulares. Estos procedimientos deben garantizar la atención de las solicitudes en los plazos establecidos y deben prever mecanismos para autenticar la identidad del solicitante, asegurando que la respuesta solo se entregue a la persona legitimada.

Además de establecer canales de comunicación (como formularios en línea, direcciones de correo electrónico o atención presencial), la organización debe disponer de un equipo responsable —que puede ser el DPO o un comité interno de privacidad— encargado de evaluar la procedencia de cada solicitud y de coordinar la respuesta en conformidad con la normativa.

El ejercicio de estos derechos no puede estar sujeto a barreras indebidas, como formularios excesivamente complejos o solicitudes de información no justificada. Asimismo, las organizaciones deben ofrecer información clara y sencilla sobre los procedimientos para ejercer estos derechos, tanto en la política de privacidad como en cualquier comunicación dirigida a los titulares.

40 Agencia Española de protección de datos (AEPD). (2018). Guía para el cumplimiento del deber de informar, p. 6, Recuperado de https://www.aepd.es/sites/default/files/2019-09/guia-modelo-clausula-informativa.pdf

6. Evaluación continua y mejora del cumplimiento

La seguridad de la información y la protección de datos no son procesos estáticos, sino que requieren evaluaciones continuas para garantizar la conformidad con estándares internacionales, normativas y mejores prácticas. En este contexto, tanto el Reglamento General de protección de datos (RGPD) como la norma ISO/IEC 27001 son fundamentales y se complementan entre sí. El RGPD establece un marco legal obligatorio para la protección de los datos personales dentro de la Unión Europea, definiendo principios, derechos y obligaciones para responsables y encargados del tratamiento. Por otro lado, la ISO/IEC 27001 proporciona un enfoque sistemático para la gestión de la seguridad de la información mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), aplicable a cualquier organización, independientemente de su sector o ubicación. La combinación de ambas normativas es esencial: mientras la ISO 27001 garantiza la implementación de controles técnicos y organizativos sólidos, el RGPD refuerza la obligación de proteger los datos personales bajo un marco normativo exigente. Este capítulo establece un marco para la evaluación y mejora del cumplimiento, alineado con ambos estándares, permitiendo una protección integral de la información y la reducción de riesgos asociados a su tratamiento.

6.1. Líneas de evaluación de cumplimiento

La evaluación de cumplimiento debe seguir un enfoque estructurado y sistemático, integrando indicadores clave de desempeño (KPIs) y métricas de seguridad para medir la efectividad de las políticas y controles implementados.

Las auditorías desempeñan un papel fundamental en la validación de la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) y la protección de datos personales. Estas permiten identificar vulnerabilidades, evaluar la aplicación de controles de seguridad y garantizar el cumplimiento de normativas nacionales e internacionales.

Un SGSI bien estructurado debe contar con auditorías periódicas que abarquen aspectos técnicos, organizativos y normativos. La correcta implementación de estas auditorías permite prevenir incidentes de seguridad, mitigar riesgos y asegurar la confianza de clientes, socios y entidades regulatorias.

Revisión de cumplimiento en protección de datos (RGPD):

Principios clave a evaluar:

- Licitud, lealtad y transparencia en el tratamiento de datos
- Limitación de finalidad y minimización de datos
- Exactitud y almacenamiento limitado
- Integridad, confidencialidad y responsabilidad proactiva

Evaluaciones clave:

- Registro de Actividades de Tratamiento (RAT) actualizado conforme al Art. 30 del RGPD
- Evaluaciones de Impacto en la protección de datos (DPIA) en proyectos de alto riesgo
- Gestión de Consentimiento: ¿Se está recopilando y documentando adecuadamente?

Evaluación del cumplimiento en seguridad de la información (ISO/IEC 27001):

Revisión de la Declaración de Aplicabilidad (SoA): Identificación de los controles implementados de la norma.

Evaluación del SGSI (Sistema de Gestión de Seguridad de la Información):

- Cumplimiento con Anejo A de la ISO 27001 (Controles de Seguridad)
- Análisis de la efectividad de medidas como gestión de accesos, cifrado, respuesta a incidentes y continuidad del negocio

Herramientas y métodos para la evaluación de cumplimiento:

- Cuadros de Mando de Cumplimiento con métricas de seguridad y protección de datos
- Benchmarking con estándares internacionales y organizaciones del sector
- Pruebas de madurez organizacional mediante modelos como CMMI (Capability Maturity Model Integration)

6.2. Auditorías internas y externas

Las auditorías son fundamentales para validar la eficacia del SGSI[41] y la protección de datos, brindan los mecanismos de prevención y gestión de riesgos necesarios para responder a incidentes de seguridad, cumpliendo con estándares y parámetros internacionales en temas normativos y de seguridad.

Las auditorías internas son revisiones sistemáticas y documentadas que permiten identificar brechas de seguridad y oportunidades de mejora dentro de una organización. Se realizan con base en estándares internacionales como ISO/IEC 27001[42], el Reglamento General de protección de datos (RGPD) y el NIST 800-53, y pueden ser llevadas a cabo por equipos internos o consultores especializados.

Las auditorías internas ayudan en el proceso de reconocimiento de riesgos y vulnerabilidades, a través de auditorías externas, las organizaciones tienen la posibilidad a certificaciones de cumplimiento.

6.2.1. Auditorías Internas (ISO 27001, RGPD, NIST 800-53)

1) Objetivos de las auditorías internas:

- Identificar brechas de seguridad y riesgos legales
- Evaluar la aplicación de políticas y procedimientos internos
- Detectar vulnerabilidades en la infraestructura tecnológica
- Analizar la efectividad de los controles de seguridad implementados
- Proveer recomendaciones para la mejora continua del SGSI

41 Organización Internacional de Normalización. (2013). ISO/IEC 27001:2013 - Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos. Recuperado de https://www.iso.org/standard/54534.html

42 ISO/IEC 27001:2022 - Sistemas de Gestión de Seguridad de la Información Organización Internacional de Normalización (ISO). Recuperado de: https://www.iso.org/standard/54534.html

2) Frecuencia de las auditorías internas

La ISO/IEC 27001 recomienda que las auditorías internas se realicen al menos una vez al año o cuando haya cambios significativos en la infraestructura tecnológica, procesos o requisitos legales de la organización. En el RGPD[43], se sugiere que los responsables del tratamiento de datos personales realicen auditorías periódicas para verificar el cumplimiento de las obligaciones normativas.

3) Aspectos clave a evaluar:

- **Políticas y procedimientos documentados:** revisión de políticas de seguridad de la información, normativas internas y procesos de gestión de datos personales
- **Aplicación de controles de seguridad:** evaluación de la eficacia de mecanismos de acceso, cifrado, autenticación y seguridad perimetral
- **Gestión de incidentes de seguridad:** revisión de procedimientos para detección, respuesta y recuperación ante incidentes de ciberseguridad
- **Registro de accesos y logs:** verificación de registros de eventos de seguridad, trazabilidad de accesos y monitoreo de actividades críticas
- **protección de datos y Cumplimiento Normativo:** evaluación de medidas de protección de datos conforme a regulaciones como la ISO/IEC 27701, el RGPD y la Ley de protección de datos Personales en cada jurisdicción

6.2.2. Auditorías externas (certificación y cumplimiento normativo):

Las auditorías externas tienen un enfoque certificatorio o de evaluación de conformidad con normativas internacionales y regulatorias. Son realizadas por organismos independientes acreditados y suelen ser requeridas en contextos empresariales que involucran regulaciones estrictas o cuando una empresa busca certificaciones de seguridad.

Casos en los que son necesarias:

- Obtención de certificaciones de seguridad como ISO/IEC 27001, ISO/IEC 27701 (para privacidad), SOC 2 (para proveedores de tecnología en EE.UU.) y NIST 800-53 en entornos gubernamentales
- Cumplimiento del Reglamento General de protección de datos (RGPD) si la empresa procesa datos de ciudadanos europeos
- Verificación de proveedores externos (Due Diligence) en contratos B2B para evaluar su nivel de cumplimiento en seguridad y protección de datos
- Requerimientos contractuales o de clientes en sectores como finanzas, salud, tecnología y telecomunicaciones, donde el cumplimiento de estándares de seguridad es obligatorio

Entidades certificadoras y reguladoras

- **ISO/IEC 27001:** certificación otorgada por organismos acreditados como ANAB (Estados Unidos), UKAS (Reino Unido) y ENAC (España). **En el caso de Bolivia, esta certificación puede realizarse a través de IBNORCA[44]**
- **RGPD:** supervisado por las Autoridades de protección de datos (DPA's) en la UE, como la Agencia Española de protección de datos (AEPD) o la CNIL en Francia
- **NIST[45] 800-53[46]:** conjunto de controles de seguridad y privacidad recomendados para sistemas de información y organizaciones federales para ayudar a cumplir con los requisitos de la Ley Federal de Gestión de Seguridad de la Información, evaluados por auditores de seguridad acreditados en EE.UU

43 Reglamento General de protección de datos (RGPD) - Unión Europea Parlamento Europeo y Consejo de la Unión Europea. Recuperado de: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679

44 El Instituto Boliviano de Normalización y Calidad (IBNORCA), es una asociación privada sin fines de lucro, creada mediante Decreto Supremo N° 23489 del 29 de abril de 1993 y fundada el 5 de mayo de 1993. Extraído de: https://www.ibnorca.org/

45 Framework for Improving Critical Infrastructure Cybersecurity National Institute of Standards and Technology (NIST). Recuperado de: https://www.nist.gov/cyberframework

46 NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations National Institute of Standards and Technology (NIST). Recuperado de: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Metodología de una auditoría externa

- **Revisión documental:** análisis de políticas, procedimientos y reportes de auditorías internas
- **Evaluación de infraestructura tecnológica:** pruebas de seguridad sobre redes, servidores y dispositivos
- **Análisis de gestión de riesgos:** evaluación de planes de respuesta ante incidentes, continuidad del negocio y gestión de vulnerabilidades
- **Entrevistas y pruebas operativas:** verificación del conocimiento y aplicación de protocolos de seguridad dentro de la organización

6.3. Monitoreo de cambios en normativas internacionales y nacionales

Las regulaciones en ciberseguridad y protección de datos están en constante evolución, por lo que las organizaciones deben adoptar un enfoque de cumplimiento dinámico. Este tipo de monitoreos reconocen nuevos riesgos a los que la empresa se expone, el impacto y los procesos necesarios para garantizar la continuidad del negocio o de las actividades que desarrolla la organización.

Las revisiones se pueden realizar a través de diferentes mecanismos o estándares, los más comunes son, en temas de protección de datos cumplir con estándares de los RGPD[47], certificación en la ISO/IEC 27001 de sistemas de gestión de seguridad de la información o temas de seguridad informática y ciberseguridad con estándares CISO, NIST o COBIT.

Principales normativas y estándares a monitorear:

1. **RGPD y su evolución (Revisiones por parte del Comité Europeo de protección de datos - EDPB)**
2. **Directiva NIS2 (Seguridad de redes y sistemas de información en la UE)**
3. **Ley de IA de la UE (AI Act): Evaluación de riesgos en sistemas de inteligencia artificial**
4. **Normativas sectoriales**
   ISO/IEC 42001 (Norma de Gestión de IA) para riesgos en sistemas de IA

Mecanismos para el seguimiento normativo:

1. Membresía en organizaciones de seguridad y privacidad (IAPP, ISACA, CISO)
2. Participación en foros y eventos internacionales de protección de datos
3. Implementación de herramientas de LegalTech para monitoreo normativo automatizado

47 Parlamento Europeo y Consejo de la Unión Europea. (2016). Reglamento General de protección de datos, Artículo 35. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679

6.4. Formación y sensibilización del personal

El factor humano es una de las principales vulnerabilidades en seguridad de la información. Se debe implementar un programa de capacitación continuo, estas capacitaciones contarán con procesos específicos según las necesidades de la organización[48].

Las capacitaciones a desarrollarse deben contar con dos etapas, una capacitación general de protección de datos, gestión de riesgos y detección de vulnerabilidades y una capacitación específica por área, tomando en cuenta los riesgos específicos y capacidades de gestión aplicables en cada área de la organización.

Programas de formación en seguridad y protección de datos:

1. **Formación obligatoria para todos los empleados:**
- Seguridad en el uso de dispositivos y redes
- Buenas prácticas en gestión de contraseñas y phishing
- Concienciación sobre manejo seguro de datos personales

2. **Capacitación específica por áreas:**
- **Equipos de TI y Seguridad:** análisis forense, respuesta a incidentes, cumplimiento normativo
- **Recursos Humanos:** protección de datos en gestión de empleados
- **Marketing y Comercial:** tratamiento de datos en campañas, cookies y consentimiento

3. **Métodos y Herramientas de Sensibilización:**
- Simulaciones de phishing y red teaming
- Gamificación y entrenamientos interactivos (Hack The Box, CyberRange)
- Evaluaciones periódicas con certificación interna

48 Agencia Española de protección de datos. (2019). Guía para la gestión del cumplimiento normativo y los riesgos en tratamientos de datos personales. Recuperado de https://www.aepd.es/sites/default/files/2020-05/guia-gestion-cumplimiento-riesgos.pdf

7. Transferencias internacionales y relaciones con terceros

Las organizaciones con frecuencia deben transferir datos personales a entidades ubicadas en otros países, ya sea por razones operativas, comerciales o tecnológicas. Estas transferencias pueden incluir el uso de servicios en la nube, la contratación de proveedores internacionales, la gestión de datos de clientes o empleados en diferentes jurisdicciones o la integración con plataformas tecnológicas extranjeras.

Es importante que, para la transferencia internacional de datos, puedan adoptarse las mejores prácticas reconocidas a nivel global, dentro de dichas prácticas se deben considerar los siguientes puntos:

7.1. Condiciones para transferencias de datos fuera de Bolivia

Dado que Bolivia aún no cuenta con una legislación específica en materia de protección de datos personales que aplique a todo tipo de organizaciones, quienes operan con datos en el ámbito internacional deben adoptar estándares y mejores prácticas reconocidas a nivel global, como las establecidas en el RGPD.

Según el RGPD, una transferencia de datos a un país tercero solo puede realizarse si se cumplen ciertas condiciones:

- **Decisión de adecuación:** si el país de destino cuenta con un reconocimiento oficial de la Comisión Europea o de una autoridad reguladora equivalente, se considera que ofrece un nivel de protección adecuado, y las transferencias pueden realizarse sin restricciones adicionales
- **Cláusulas contractuales estándar:** en ausencia de una decisión de adecuación, las organizaciones deben utilizar contratos que incluyan disposiciones específicas de protección de datos, asegurando que el receptor de los datos cumpla con principios equivalentes a los exigidos por el RGPD
- **Normas corporativas vinculantes:** grandes organizaciones y grupos multinacionales pueden implementar normas internas que regulen la transferencia de datos entre sus entidades en diferentes países
- **Consentimiento explícito del titular:** en algunos casos, la transferencia puede justificarse si el titular ha otorgado su consentimiento informado y específico para que sus datos sean enviados a un país sin garantías adecuadas de protección

Además de evaluar la base legal de la transferencia, las organizaciones deben considerar factores como la seguridad de la infraestructura tecnológica utilizada, la existencia de acuerdos de confidencialidad y la posibilidad de que los datos sean accesibles por autoridades extranjeras bajo normativas locales.

7.2. Cláusulas contractuales estándar

Las cláusulas contractuales estándar (Standard Contractual Clauses - SCCs) son una de las herramientas más utilizadas para garantizar que la información seguirá estando protegida en su destino.

Las SCCs son modelos de contrato desarrollados por la Comisión Europea y otros organismos internacionales que establecen obligaciones contractuales claras para ambas partes involucradas en la transferencia de datos. Estas cláusulas garantizan que el destinatario de los datos mantendrá niveles adecuados de seguridad, confidencialidad y respeto por los derechos de los titulares, aun cuando no esté sujeto a la normativa del país de origen.

El uso de este tipo de cláusulas estará sujeto a los países intervinientes dentro de la transferencia internacional de datos, ya que cada país o región ha desarrollado su propio modelo de cláusulas[49]. No obstante, los modelos normalmente contemplan los siguientes puntos:

- **Limitación en el uso de los datos:** el receptor solo podrá procesar la información con la finalidad específica para la que se transfirieron los datos
- **Medidas de seguridad:** el destinatario debe adoptar medidas técnicas y organizativas adecuadas para evitar accesos no autorizados, pérdida o alteración de los datos

49 En el siguiente enlace se puede encontrar la referencia a las cláusulas de diferentes países y regiones, como ser la Región Europea, Asiática y de países como Argentina, Nueva Zelanda y Reino Unido. Comisión Europea: Cláusulas contractuales estándar (CCE). Disponible en: https://commission-europa-eu.translate.goog/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

- **Obligación de notificación:** si el receptor sufre una brecha de seguridad, deberá informar de inmediato al remitente de los datos
- **Derechos de los titulares:** el destinatario debe garantizar que los titulares de los datos puedan ejercer sus derechos de acceso, rectificación, supresión y oposición
- **Supervisión y auditoría:** la organización que transfiere los datos tiene derecho a realizar auditorías o solicitar información sobre el cumplimiento de las medidas de protección

Las cláusulas contractuales estándar pueden integrarse dentro de contratos comerciales más amplios o establecerse como anexos específicos para regular la transferencia de datos.

7.3. Evaluación de proveedores y contratos con terceros

Las relaciones y contratación con proveedores y terceros debe resultar un aspecto importante para las organizaciones con respecto al tratamiento de sus datos personales, ya que no es posible garantizar la protección de datos personales si es que no se ha realizado una correcta valoración del tratamiento que puedan realizar los proveedores o terceros.

En ese sentido, la implementación de un proceso de evaluación y selección que garantice que los proveedores cumplen con estándares adecuados de protección de datos, disminuiría el riesgo que el tratamiento de datos puede representar.

7.3.1. Proceso de evaluación

Antes de contratar a un proveedor que realice tratamiento de datos personales que están bajo su responsabilidad, la organización debe evaluar:

- **Políticas de privacidad y seguridad:** revisar si el proveedor cuenta con protocolos internos de protección de datos y seguridad de la información
- **Cumplimiento normativo:** verificar si el proveedor cumple con regulaciones internacionales reconocidas, como el RGPD, la ISO 27001 (seguridad de la información) o certificaciones equivalentes
- **Ubicación y jurisdicción:** analizar si el proveedor está sujeto a normativas de protección de datos o si existe riesgo de acceso indebido por parte de autoridades extranjeras
- **Historial de incidentes:** identificar si el proveedor ha sufrido brechas de seguridad o sanciones por incumplimientos previos
- **Capacidad de respuesta:** evaluar los tiempos y mecanismos de atención a incidentes de seguridad o solicitudes de los titulares de los datos

7.3.2. Contratación con proveedores y terceros

Una vez cumplido el proceso de evaluación, se deben contemplar cláusulas específicas en el contrato que regulen el tratamiento de datos personales. Dependiendo del tipo de tratamiento que el proveedor o tercero vaya a realizar, se deberán considerar aspectos como:

- Finalidad del tratamiento y terceros intervinientes
- Medidas de seguridad exigidas
- Obligaciones de confidencialidad
- Procedimientos en caso de incidentes
- Devolución o eliminación de datos

El seguimiento y auditoría que se pueda realizar a los proveedores terceros intervinientes en el tratamiento resultará también en una forma de cumplimiento de la responsabilidad proactiva que debe tener la obligación[50]. Este es un aspecto que complementa a la firma de un contrato, ya que el seguimiento continuo es el que permitirá minimizar los riesgos asociados al tratamiento de datos personales.

50 Agencia Española de protección de datos. (2018). Directrices para la elaboración de contratos entre Responsables y Encargados del Tratamiento. Recuperado de https://www.aepd.es/guias/guia-directrices-contratos.pdf

8. Regulación de la inteligencia artificial y protección de datos

La inteligencia artificial (IA) representa una de las transformaciones tecnológicas más disruptivas de nuestro tiempo. Su acelerada expansión marca el inicio de una nueva etapa en la cuarta revolución industrial, impulsando cambios profundos en la forma en que se producen, gestionan y consumen bienes y servicios. Si bien sus aplicaciones prometen mejorar significativamente el bienestar social, optimizar procesos y enfrentar desafíos globales, su desarrollo no está exento de riesgos complejos para los derechos fundamentales.

En este contexto, la Unión Europea ha adoptado el AI Act, un instrumento jurídico pionero que establece un marco regulatorio basado en un enfoque de gestión por riesgos. Este régimen clasifica los sistemas de IA según su nivel de impacto potencial y determina obligaciones diferenciadas de cumplimiento, sentando precedentes regulatorios para otras jurisdicciones.

En contraste, Bolivia aún no cuenta con una normativa específica en materia de protección de datos personales ni de derechos digitales, situación que se replica en el ámbito de la inteligencia artificial. La ausencia de marcos regulatorios impide establecer criterios mínimos para el desarrollo ético, seguro y transparente de tecnologías basadas en IA, generando vacíos que dificultan tanto la tutela de derechos como la promoción de buenas prácticas.

Aunque el potencial de la IA es indiscutible, también lo son los riesgos que conlleva su adopción indiscriminada. Entre los más relevantes se identifican:

- **Sesgos y discriminación algorítmica:** los modelos de IA, entrenados con datos que reflejan desigualdades estructurales, pueden amplificar estereotipos y generar decisiones discriminatorias en áreas críticas como el empleo, el sistema penal, el acceso a crédito o los servicios públicos, afectando especialmente a mujeres, personas racializadas y otros grupos históricamente excluidos
- **Vulneraciones a la privacidad:** la recopilación y procesamiento masivo de datos personales, muchas veces sin consentimiento adecuado ni mecanismos de control, incrementa el riesgo de exposición indebida de información sensible, afectando el derecho a la intimidad y a la autodeterminación informativa
- **Falta de transparencia y explicabilidad:** muchos sistemas de IA operan como “cajas negras”, dificultando el acceso a la lógica interna de las decisiones automatizadas. Esta opacidad impide a las personas comprender, cuestionar o impugnar decisiones que las afectan directamente, minando la rendición de cuentas y el acceso a la justicia

Estos riesgos se profundizan aún más en contextos de alta vulnerabilidad, donde el impacto de la IA puede intensificar las desigualdades existentes. Niñas, niños y adolescentes, personas con discapacidad, comunidades indígenas, personas mayores, sectores empobrecidos y grupos de diversidad sexual y de género enfrentan una mayor exposición a los efectos adversos de sistemas que no han sido diseñados ni supervisados con criterios de equidad e inclusión.

Los lineamientos establecidos en esta guía buscan brindar lineamientos para la adopción y desarrollo responsable de este y otro tipo de tecnologías.

8.1. Principios del AI Act de la Unión Europea y su aplicación en Bolivia

El AI Act define una serie de principios rectores para el desarrollo y uso de sistemas de inteligencia artificial, asegurando que su aplicación sea ética y respetuosa con los Derechos Humanos.

1. Transparencia y explicabilidad de los sistemas de IA

- Obligación de informar a los usuarios cuando interactúan con IA (chatbots, asistentes virtuales)
- Explicabilidad de decisiones automatizadas (ej. rechazo de crédito, selección laboral)

2. Principio de minimización de datos en la IA

- La IA solo debe procesar los datos estrictamente necesarios para su propósito
- Evitar la recopilación excesiva o innecesaria de datos personales

3. Evaluaciones de impacto en protección de datos y sesgos algorítmicos

- Evaluaciones de Impacto en protección de datos (DPIA) obligatorias para sistemas de alto riesgo
- Mitigación de sesgos en IA que afectan a grupos vulnerables

4. Derechos de los titulares sobre decisiones automatizadas

- Derecho a no ser sujeto a decisiones automatizadas sin intervención humana en temas sensibles (empleo, salud, justicia)
- Derecho a solicitar una explicación de la decisión tomada por un algoritmo

8.2. Clasificación de los sistemas de IA según el AI Act

El Reglamento de inteligencia artificial (AI Act) de la Unión Europea divide los sistemas de IA en tres niveles de riesgo, dependiendo del impacto que tienen en los Derechos Humanos y las libertades fundamentales. Esta clasificación es una base que puede ser tomada en cuenta para la implementación responsable de IA en organizaciones en Bolivia, especialmente para aquellas que operan en mercados internacionales o desean adoptar estándares éticos globales.

Actualmente no existe una regulación específica sobre IA, pero las organizaciones que implementen estos sistemas deben seguir estándares internacionales para evitar riesgos legales y éticos.

Las empresas que exportan servicios o productos a la UE pueden estar sujetas a regulaciones extraterritoriales.

8.2.1. IA de alto riesgo

Los sistemas de IA de alto riesgo[51] tienen un impacto significativo en los derechos fundamentales de las personas y pueden afectar áreas críticas como el empleo, la salud, la seguridad y la justicia. Debido a este potencial daño, están sujetos a regulaciones estrictas y requieren controles específicos antes de su implementación.

Ejemplos de IA de alto riesgo:

- **Reconocimiento facial en espacios públicos:** utilizado por gobiernos o empresas para la vigilancia masiva
- **Algoritmos de selección y contratación de empleados:** IA que filtra candidatos o toma decisiones sobre contratación
- **Sistemas de diagnóstico médico o tratamiento automatizado:** IA que determina enfermedades o prescribe tratamientos sin intervención humana
- **IA en justicia penal:** algoritmos utilizados para predecir delitos o recomendar sentencias judiciales

51 Parlamento Europeo y Consejo de la Unión Europea. (2024). Reglamento de inteligencia artificial (AI Act), texto consolidado. Recuperado de https://digital-strategy.ec.europa.eu/en/policies/regulation-artificial-intelligence

Medidas necesarias para su implementación:

a. Evaluación de Impacto en protección de datos (DPIA)
- Es obligatoria antes de desplegar la IA
- Debe evaluar los riesgos para la privacidad y los derechos de las personas

b. Supervisión humana en decisiones críticas
- Un ser humano debe tener control y capacidad de intervenir en decisiones automatizadas
- Ejemplo: Un médico debe revisar las decisiones de un sistema de IA antes de aplicarlas en un paciente

c. Registro y trazabilidad del sistema de IA
- Mantener registros detallados sobre cómo se entrenó la IA, con qué datos y bajo qué criterios toma decisiones
- Permite auditorías y revisiones de seguridad

d. Pruebas rigurosas antes de su despliegue
- Se deben realizar pruebas para evaluar sesgos y errores en el sistema antes de su uso real
- Obligación de transparencia y explicabilidad
- La IA debe poder justificar sus decisiones para que los afectados puedan impugnarlas si es necesario

8.2.2. IA de riesgo limitado

Los sistemas de riesgo limitado[52] pueden influir en las decisiones de los usuarios, pero no tienen un impacto directo en sus derechos fundamentales. Sin embargo, se requiere transparencia para que las personas comprendan que están interactuando con IA.

A medida que más empresas bolivianas adoptan IA en atención al cliente y personalización de servicios, es importante aplicar principios de transparencia y accesibilidad.

No hay obligaciones legales específicas en Bolivia, pero seguir estándares como el AI Act puede mejorar la confianza de los usuarios.

Ejemplos de IA de riesgo limitado:

- **Chatbots y asistentes virtuales:** atención al cliente en bancos, empresas de telecomunicaciones, comercios electrónicos, etc
- **Sistemas de recomendación:** plataformas como Netflix, YouTube o Spotify que sugieren contenido con base en el comportamiento del usuario
- **Moderadores automatizados de contenido:** IA que filtra comentarios ofensivos en redes sociales o foros en línea

Medidas necesarias para su implementación:

a. Informar a los usuarios
- Las personas deben saber que están interactuando con una IA y no con un humano
- Ejemplo: Un chatbot debe indicar claramente que es un asistente virtual

b. Permitir opciones de salida
- Los usuarios deben poder optar por hablar con un operador humano si lo desean
- Ejemplo: En una plataforma bancaria, la IA puede gestionar preguntas básicas, pero el cliente debe tener la opción de contactar a un asesor

c. Evitar sesgos en los algoritmos
- Aunque no sean de alto riesgo, los sistemas deben ser monitoreados para evitar discriminación en recomendaciones y respuestas automatizadas

52 Parlamento Europeo y Consejo de la Unión Europea. (2024). Reglamento de inteligencia artificial (AI Act), texto consolidado. Recuperado de https://digital-strategy.ec.europa.eu/en/policies/regulation-artificial-intelligence

8.2.3. IA de riesgo inaceptable:

Son sistemas de IA que vulneran los Derechos Humanos y están explícitamente prohibidos o de riesgo inaceptable[53] por el AI Act. Estos sistemas representan un riesgo extremo porque pueden manipular el comportamiento de las personas, violar su privacidad o discriminar de manera injusta.

Aunque el país no cuenta con una regulación específica, las organizaciones que operan internacionalmente deben evitar el uso de IA prohibida para no enfrentarse a sanciones o restricciones en mercados como la UE.

Ejemplos de IA Prohibida:

a. Manipulación subliminal: IA que influye en las decisiones de las personas sin su conocimiento
- Ejemplo: algoritmos que analizan emociones para manipular el voto en elecciones

b. Sistemas de puntuación social (Social Scoring): Modelos como los usados en China, donde el comportamiento de los ciudadanos es evaluado para otorgar o restringir beneficios
- Reconocimiento emocional en entornos laborales y educativos: IA que analiza expresiones faciales de empleados o estudiantes para evaluar desempeño o emociones sin consentimiento explícito

c. IA que explota la vulnerabilidad de grupos específicos: Tecnologías diseñadas para manipular a niños, ancianos o personas con discapacidad
- Ejemplo: publicidad hiperpersonalizada que induce a niños a comprar productos sin que lo entiendan completamente

Medidas necesarias para su prevención:

a. Prohibición total en organizaciones responsables
- Empresas y entidades deben evitar el uso de este tipo de IA para no infringir Derechos Humanos

b. Análisis de riesgos y cumplimiento ético
- Antes de implementar cualquier sistema de IA, se debe verificar que no infringe derechos fundamentales

c. Evaluación de proveedores de IA
- Muchas empresas utilizan IA desarrollada por terceros; es fundamental asegurarse de que estos proveedores no implementen modelos prohibidos

8.3. Evaluación del uso de IA en las organizaciones

Las organizaciones deben realizar un análisis de riesgos antes de implementar sistemas de IA para evitar vulneraciones a la privacidad y derechos fundamentales.

- Identificación de usos de IA en la organización
- Identificar qué procesos utilizan IA (reclutamiento, marketing, seguridad, etc.)
- Determinar si los algoritmos afectan derechos fundamentales
- Análisis de impacto en privacidad y derechos fundamentales
- Realizar Evaluaciones de Impacto en protección de datos (DPIA) para IA de alto riesgo
- Evaluar posibles sesgos algorítmicos que afecten a grupos vulnerables
- Implementar auditorías periódicas de los modelos de IA
- Medidas de mitigación de riesgos para IA de alto riesgo
- Supervisión humana en decisiones sensibles (empleo, salud, crédito, justicia)
- Cifrado y anonimización de datos utilizados en el entrenamiento de modelos de IA
- Explicabilidad del algoritmo: Los usuarios deben poder entender cómo y por qué se toman decisiones

53 Parlamento Europeo y Consejo de la Unión Europea. (2024). Reglamento de inteligencia artificial (AI Act), texto consolidado. Recuperado de https://digital-strategy.ec.europa.eu/en/policies/regulation-artificial-intelligence

El AI Act establece un marco de seguridad y ética para la IA, asegurando que las organizaciones desarrollen e implementen estos sistemas de manera transparente y sin afectar derechos fundamentales.

Aunque Bolivia no cuente con una regulación local, las organizaciones pueden adoptar los principios del AI Act para garantizar la confianza del usuario y el cumplimiento de estándares internacionales.

8.4. Uso responsable de inteligencia artificial en organizaciones

El desarrollo y aplicación de sistemas basados en inteligencia artificial (IA) representa una oportunidad significativa para la mejora de procesos, eficiencia institucional y generación de conocimiento. Sin embargo, su integración en organizaciones públicas y privadas debe hacerse de forma responsable, garantizando la transparencia, la protección de los datos personales y la tutela efectiva de los derechos fundamentales.

8.4.1. Recomendaciones para una implementación adecuada

- **Incorporar la privacidad desde el diseño y por defecto:** adoptar un enfoque de privacy by design y privacy by default, asegurando que la protección de datos personales esté integrada en todas las fases del ciclo de vida del sistema, desde su concepción hasta su desactivación
- **Realizar evaluaciones de impacto en protección de datos (DPIA):** evaluar de manera anticipada los posibles efectos de la implementación de IA sobre los derechos de las personas, identificando riesgos y estableciendo medidas de mitigación proporcionales al nivel de exposición
- **Garantizar la transparencia y explicabilidad algorítmica:** establecer mecanismos que permitan a las personas comprender cómo operan los sistemas de IA, qué datos se procesan, con qué finalidad y cuál es la lógica aplicada en la toma de decisiones automatizadas
- **Aplicar el principio de minimización de datos:** asegurar que únicamente se recopilen y procesen aquellos datos estrictamente necesarios, evitando el tratamiento excesivo o desproporcionado que pueda generar vulneración a la privacidad
- **Implementar medidas de seguridad técnica y organizativa:** adoptar protocolos de seguridad robustos (cifrado, control de accesos, auditorías, protocolos de destrucción) para proteger la integridad, confidencialidad y disponibilidad de los datos personales procesados por los sistemas de IA
- **Conformar equipos de trabajo interdisciplinarios y diversos:** involucrar perfiles técnicos, jurídicos, éticos y sociales en el diseño, evaluación y supervisión de los sistemas de IA, promoviendo la inclusión y el análisis de riesgos desde múltiples perspectivas
- **Registrar y documentar el ciclo de vida del sistema:** garantizar la trazabilidad mediante el registro detallado de las decisiones, los modelos utilizados, las fuentes de datos y las evaluaciones realizadas en cada etapa del sistema
- **Permitir intervención humana significativa:** incluir mecanismos que permitan a las personas solicitar revisión de decisiones automatizadas, oponerse a las mismas y ejercer su derecho a una explicación comprensible
- **Respetar plazos de conservación y establecer finalidades específicas:** establecer y cumplir con políticas claras sobre conservación de datos, asegurando que no se almacenen más allá del tiempo necesario para la finalidad previamente determinada
- **Fomentar la formación, sensibilización y gobernanza interna:** capacitar continuamente a los equipos sobre ética de la IA, protección de datos y derechos digitales, promoviendo una cultura organizacional comprometida con el uso responsable de tecnologías emergentes

8.4.2. Prácticas que deben evitarse

- **Desplegar sistemas sin evaluación previa de riesgos:** omitir el análisis de impacto puede generar afectaciones significativas a derechos fundamentales y conducir a desarrollos inseguros o discriminatorios
- **Recolectar y utilizar datos personales sin base legal o sin consentimiento válido:** el tratamiento debe fundarse en una causa legítima conforme al marco normativo vigente, de lo contrario, constituye una vulneración al principio de licitud
- **Procesar datos de baja calidad, desactualizados o falsos:** los sistemas de IA entrenados con datos inadecuados generan resultados imprecisos o injustos, afectando derechos como la no discriminación y la igualdad
- **Mantener opacidad en la toma de decisiones algorítmicas:** utilizar modelos no explicables en contextos sensibles (como justicia, salud o crédito) impide ejercer el derecho a la revisión y limita la rendición de cuentas institucional
- **Aplicar vigilancia o perfilamiento sin conocimiento ni consentimiento:** implementar herramientas de IA para monitorear comportamientos o establecer perfiles debe estar debidamente informado, justificado y regulado
- **Conservar datos personales sin límite temporal o sin justificación:** la retención indefinida de información incrementa los riesgos de uso indebido, reidentificación y filtraciones de datos
- **Discriminar mediante sesgos algorítmicos no corregidos:** ignorar los sesgos en el diseño o entrenamiento de modelos puede reproducir desigualdades estructurales, especialmente contra grupos en situación de vulnerabilidad
- **Permitir que decisiones automatizadas afecten significativamente sin control humano:** las personas tienen derecho a no ser sometidas a decisiones que les afecten de manera significativa basadas únicamente en procesos automatizados
- **No contar con un responsable o estructura de gobernanza interna en IA:** la ausencia de una política clara, responsable designado y mecanismos de control limita la capacidad de una organización para garantizar un uso ético y legal de estas tecnologías
- **Subestimar la importancia del marco legal y de los estándares internacionales:** ignorar los principios éticos y jurídicos aplicables debilita la legitimidad de las aplicaciones de IA y pone en riesgo la confianza ciudadana y reputacional de la organización

9. Empresas y Derechos Humanos: cumplimiento y protección de datos

El cumplimiento de los Derechos Humanos en el ámbito empresarial se ha convertido en una exigencia global debido a la creciente presión de organismos internacionales, reguladores, consumidores y la sociedad civil. La protección de datos personales es un derecho fundamental, reconocido en instrumentos internacionales como la Declaración Universal de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos.

Las empresas y organizaciones que operan con datos personales deben asegurar su gestión ética y responsable, alineándose con los estándares internacionales en Derechos Humanos, privacidad y seguridad de la información. El marco de Naciones Unidas y otras normativas establecen principios para que las organizaciones s sean actores responsables, evitando vulneraciones a los derechos de sus clientes, empleados y usuarios.

¿Por qué es importante para las organizaciones?

- Evitar sanciones y responsabilidades legales
- Fortalecer la confianza de clientes e inversionistas
- Acceder a mercados internacionales que exigen cumplimiento en Derechos Humanos
- Minimizar riesgos reputacionales y financieros por malas prácticas en el uso de datos

9.1. Marco normativo internacional sobre empresas, organizaciones y Derechos Humanos

Las empresas y organizaciones tienen la responsabilidad de respetar los Derechos Humanos en todas sus operaciones. Esta obligación se basa en varios instrumentos internacionales, entre ellos:

Principios rectores sobre empresas y Derechos Humanos de la ONU (UNGPs, 2011)

- Establecen el deber del Estado de proteger los Derechos Humanos
- Reconocen la responsabilidad empresarial de respetar los Derechos Humanos
- Exigen mecanismos de reparación en caso de vulneraciones

Pacto global de las Naciones Unidas

- **Principio 1:** las empresas deben apoyar y respetar la protección de los Derechos Humanos reconocidos internacionalmente
- **Principio 2:** asegurar que sus actividades no contribuyan a violaciones de Derechos Humanos

Convenios de la OIT sobre derechos laborales y privacidad en el trabajo

- **Convenio 108 y Protocolo 181:** protección de datos personales en el ámbito laboral
- **Convenio 190:** eliminación de la violencia y el acoso en el trabajo, incluyendo la protección de datos sensibles de las víctimas

Directrices de la OCDE para organizaciones multinacionales

- Incluyen recomendaciones sobre debida diligencia en Derechos Humanos y protección de datos

9.2. Relación entre organizaciones, Derechos Humanos y protección de datos

El uso de datos personales por parte de organizaciones puede afectar derechos fundamentales, como la privacidad, la no discriminación y la libertad de expresión. Algunos puntos clave de intersección incluyen:

Protección de la privacidad como derecho humano fundamental

- La privacidad es reconocida en el Artículo 12 de la Declaración Universal de Derechos Humanos y el Artículo 17 del Pacto Internacional de Derechos Civiles y Políticos
- Las organizaciones deben adoptar medidas para garantizar el tratamiento legítimo de datos personales

Debida diligencia en Derechos Humanos y protección de datos

- Identificación de riesgos en el procesamiento de datos personales
- Evaluación del impacto en Derechos Humanos de tecnologías como vigilancia biométrica, reconocimiento facial e inteligencia artificial
- Implementación de controles para prevenir violaciones de Derechos Humanos

No discriminación y sesgos en el uso de datos

- Evitar el uso de datos personales para decisiones que resulten en discriminación por género, etnia, religión u orientación sexual
- Aplicar principios de ética y equidad en algoritmos de inteligencia artificial

Transparencia y consentimiento informado

- Las organizaciones deben garantizar que los usuarios comprendan cómo se usan sus datos y los posibles impactos en sus derechos
- Aplicación del principio de explicabilidad en decisiones automatizadas

9.3. Implementación de un marco de protección de Derechos Humanos en las organizaciones

Para alinear su actuación con los estándares internacionales, las organizaciones deben:

- Adoptar una política de Derechos Humanos y protección de datos
- Compromiso con estándares internacionales
- Integración con las políticas de privacidad
- Realizar Evaluaciones de Impacto en Derechos Humanos (HRIA) y protección de datos
- Identificación de riesgos en el procesamiento de datos
- Evaluación de impacto en grupos vulnerables
- Garantizar mecanismos de quejas y reparación
- Canales para denunciar violaciones a la privacidad y otros derechos
- Procedimientos internos para gestionar incidentes
- Capacitación y sensibilización en Derechos Humanos y protección de datos
- Formación continua en privacidad, IA ética y no discriminación
- Creación de una cultura de cumplimiento

9.4. Responsabilidad empresarial y litigios sobre protección de datos y Derechos Humanos

El incumplimiento de las normativas de protección de datos y Derechos Humanos puede acarrear graves consecuencias legales, económicas y reputacionales para las empresas. En un entorno cada vez más regulado y con un mayor escrutinio público, las organizaciones deben adoptar un enfoque proactivo para garantizar la conformidad con las normativas vigentes y minimizar los riesgos asociados. Entre las principales repercusiones del incumplimiento se encuentran:

a. Sanciones y multas internacionales

Los marcos regulatorios como el Reglamento General de protección de datos (RGPD) en Europa y el emergente AI Act imponen obligaciones estrictas a las empresas en relación con el tratamiento de datos personales y el uso de tecnologías como la inteligencia artificial. El incumplimiento puede derivar en sanciones económicas significativas, como multas de hasta el 4% de la facturación global anual o 20 millones de euros según el RGPD. Además, organismos reguladores nacionales e internacionales pueden imponer restricciones a las actividades comerciales de la empresa, afectando su capacidad operativa y su acceso a mercados estratégicos.

b. Demandas por violación de privacidad y discriminación algorítmica

Los ciudadanos y consumidores tienen cada vez más herramientas legales para exigir el cumplimiento de sus derechos digitales. La recopilación, procesamiento y transferencia indebida de datos pueden derivar en litigios colectivos y demandas individuales por violación de la privacidad. Asimismo, el uso de algoritmos y sistemas de inteligencia artificial sin los controles adecuados puede generar discriminación algorítmica, afectando negativamente a grupos vulnerables. Casos emblemáticos han demostrado que decisiones automatizadas pueden reforzar sesgos estructurales, lo que ha llevado a demandas por discriminación y exclusión, con consecuencias legales y financieras para las empresas involucradas.

c. Impacto reputacional negativo y pérdida de confianza de los usuarios

Más allá de las sanciones económicas y legales, las empresas enfrentan un daño reputacional significativo cuando se ven involucradas en casos de vulneración de datos personales o uso indebido de tecnologías. La pérdida de confianza de los usuarios puede traducirse en la disminución de la base de clientes, caída en el valor de mercado y restricciones en el acceso a inversiones. En un mundo donde la ética digital y la transparencia son factores determinantes para la competitividad, una mala gestión de la seguridad de la información y la privacidad puede comprometer seriamente la sostenibilidad de una organización.

Dado este panorama, es crucial que las empresas adopten un enfoque de cumplimiento integral, alineando sus políticas internas con estándares internacionales como la ISO/IEC 27001 y las regulaciones de protección de datos. La implementación de mecanismos de auditoría, evaluación de impacto en la privacidad (DPIA) y medidas de ciberseguridad robustas no solo reduce la exposición a riesgos legales, sino que también fortalece la confianza de clientes, socios comerciales y autoridades regulatorias.

ANEXO 1

Aspectos esenciales para la elaboración de un reglamento de protección de datos personales

1 Disposiciones generales

- Objetivo del reglamento
- Ámbito de aplicación (empleados, clientes, proveedores, terceros)
- Definiciones clave (datos personales, tratamiento, responsable, encargado, DPO, etc.)
- Principios de protección de datos (licitud, lealtad, transparencia, minimización, integridad, confidencialidad)

2 Responsables y encargados del tratamiento

- Funciones y responsabilidades del responsable del tratamiento
- Funciones y responsabilidades del encargado del tratamiento
- Designación y funciones del Delegado de Protección de Datos (DPO), si aplica

3 Categorías de datos tratados

- Datos identificativos (nombre, DNI, dirección, etc.)
- Datos sensibles (salud, biométricos, financieros, ideología, etc.)
- Datos de navegación y tecnología (cookies, IP, geolocalización, etc.)

4 Finalidades y bases legales del tratamiento

- Justificación del tratamiento de datos (contrato, obligación legal, consentimiento, interés legítimo)
- Uso de datos para marketing, seguridad, análisis, etc.
- Consentimiento: obtención, revocación y registro

5 Derechos de los titulares de datos

- Acceso, Rectificación, Cancelación y Oposición (ARCO)
- Derecho a la portabilidad, limitación del tratamiento y olvido
- Procedimientos internos para la gestión de solicitudes

6 Medidas de seguridad de la información

- Protocolos de acceso y control de datos
- Políticas de cifrado, almacenamiento y respaldo
- Gestión de incidentes de seguridad y brechas de datos
- Obligación de confidencialidad para empleados y terceros

7 Transferencia y comunicación de datos

- Condiciones para compartir datos con terceros
- Transferencias internacionales y garantías legales
- Cláusulas contractuales con proveedores de servicios

8 Retención y eliminación de datos

- Plazos de conservación de datos según su naturaleza
- Procedimientos de anonimización y destrucción segura de datos

9 Evaluaciones de impacto y auditorías

- Criterios para realizar Evaluaciones de Impacto en Protección de Datos (EIPD)
- Planificación de auditorías internas y externas
- Mecanismos de mejora continua y actualización del reglamento

10 Sanciones y tesponsabilidades internas

- Consecuencias del incumplimiento del reglamento para empleados y terceros
- Medidas disciplinarias y procedimientos sancionatorios

11 Modificación y vigencia del reglamento

- Procedimiento para actualizar el reglamento
- Fecha de entrada en vigor y revisiones periódicas

Aspectos esenciales para la elaboración de una política de privacidad

1 Introducción y alcance

- Objetivo de la política
- Ámbito de aplicación (usuarios, empleados, clientes, proveedores, etc.)
- Legislación aplicable

2 Responsable del tratamiento

- Nombre y datos de contacto de la organización o entidad responsable
- Datos del Delegado de Protección de Datos (DPO), si aplica

3 Datos personales recopilados

- Tipos de datos tratados (identificativos, financieros, de navegación, etc.)
- Métodos de recolección (formularios, cookies, registros, etc.)

4 Finalidades del tratamiento

- Justificación del uso de los datos (prestación de servicios, seguridad, marketing, etc.)
- Base legal del tratamiento (consentimiento, interés legítimo, cumplimiento contractual o legal)

5 Derechos de los titulares

- Acceso, rectificación, cancelación y oposición (ARCO)
- Derecho a la portabilidad, limitación del tratamiento y olvido
- Procedimiento para ejercer los derechos

6 Transferencias y compartición de datos

- Cesión de datos a terceros (proveedores, socios, entidades gubernamentales)
- Transferencias internacionales y mecanismos de protección

7 Seguridad de la información

- Medidas técnicas y organizativas para la protección de datos
- Políticas de retención y eliminación de información

8 Uso de cookies y tecnologías similares

- Tipos de cookies utilizadas
- Finalidad del uso (analítica, funcionalidad, publicidad)
- Opciones de configuración y rechazo

9 Modificaciones y vigencia de la política

- Procedimiento de actualización de la política
- Fecha de la última revisión

10 Contacto y consultas

- Canales de comunicación para dudas o reclamos

ANEXO 3
Tiempo de conservación de datos

PAÍS	TIEMPO DE RECOLECCIÓN DE DATOS	TIEMPO
PANAMÁ PAN	El tiempo de recolección de datos deberá ser establecido y comunicado de manera clara al momento de solicitar el consentimiento para el almacenamiento y tratamiento de datos. • Los datos deben ser eliminado cuando ya no sean necesarios. • **El plazo de conservación no debe exceder de lo 5 años tras la finalización de relación contractual o de servicios con el titular de los datos.** • Los datos que tengan fines legales o financieros serán almacenados según las normas laborales, financieras, tributarias estatales, según el área de tratamiento.	5 años
ESPAÑA ESP	Los datos personales deben almacenarse solo durante el tiempo necesario para cumplir los fines para los cuales fueron recolectados. Una vez que estos fines hayan dejado de ser relevantes, los datos deben ser eliminados o anonimizados. El almacenamiento también este sujeto a otros factores como el tiempo de almacenamiento establecido pro normas de diferentes áreas como en temas tributarios o laborales, que por lo general tienen un plazo **de 3 a 5 años tras la finalización del tratamiento de los datos.**	3 a 5 años
BOLIVIA BOL	En Bolivia los tiempos de almacenamiento de datos recolectados se basan en normativas conexas como la norma laboral o las normas tributarias que exigen a las **empresas la conservación de información y datos por tiempos específicos de 3, 5 o 10 años, por lo cual el almacenamiento de datos este sujeto al fin para el cual se recolectan los datos.**	
COLOMBIA COL	La ley colombiana establece que los datos personales deben almacenarse únicamente durante el tiempo que sea razonable y necesario para cumplir con los fines para los cuales fueron recopilados. Esto implica que: • Si existe una norma legal que disponga un plazo específico, este debe cumplirse. • Si no hay una disposición específica, el tiempo debe ser definido de acuerdo con los principios de necesidad y finalidad. • Una vez cumplido el propósito del tratamiento, los datos deben ser eliminados o anonimizados, salvo que exista una obligación legal o contractual que requiera su conservación. **Datos personales básicos: se recomienda un plazo de 5 a 10 años después de la finalización de la relación contractual o el propósito específico,** en concordancia con requisitos legales. **Datos sensibles:** deben eliminarse o anonimizarse lo antes posible una vez cumplido el propósito para el cual fueron tratados. **Este plazo puede ser menor (1-3 años).** **Datos relacionados con obligaciones legales:** si existen normativas fiscales, laborales u otras, los plazos deben cumplir con esas disposiciones **(5 a 10 años para documentos fiscales).** **Registros en bases de datos inactivas:** un plazo comúnmente aceptado es **entre 6 meses y 1 año tras la inactividad,** salvo obligaciones legales o auditorías.	Datos personales: 5 a 10 años Datos sensibles: de 1 a 3 años Datos sobre obligaciones legales: 5 a 10 años Registros en bases de datos inactivas: 6 meses a 1 año
ARGENTINA ARG	La ley de protección de datos de Argentina no establece un plazo específico para el almacenamiento de datos, pero sí exige que los datos personales se conserven solo mientras sean necesarios o pertinentes para los fines para los cuales fueron recolectados. Recomendaciones de plazos de almacenamiento de datos: • **Datos personales básicos: un plazo comúnmente aplicado es 5 años tras la finalización de la relación contractual o el cumplimiento del propósito,** coincidiendo con los plazos de prescripción legales en materias comerciales y civiles. • **Datos sensibles:** se recomienda eliminarlos o anonimizarlos inmediatamente después de que dejan de ser necesarios, con un plazo máximo de 1 a 3 años tras el fin de su propósito. • **Datos asociados a obligaciones legales:** cumplir con los plazos de conservación que dicten otras normativas **(10 años para obligaciones contables según el Código Civil y Comercial).**	Datos personales: 5 años Datos sensibles: 1 a 3 años Datos asociados a obligaciones legales: 10 años
PERÚ PER	La Ley N.º 29733 no establece un plazo específico para el almacenamiento de datos personales, pero se rige por el principio de **limitación temporal, Los datos personales deben conservarse únicamente durante el tiempo necesario para cumplir con la finalidad para la cual fueron recopilados, salvo disposición legal en contrario.** **Recomendaciones prácticas:** • **Datos personales: un plazo recomendado es 5 años** después de la finalización de la relación contractual o cumplimiento del propósito, en línea con los plazos de prescripción en materia civil y comercial. • **Imágenes y voces grabadas:** se pueden almacenar **de 30 a 60 días,** y luego **deben eliminarse en un plazo máximo de 2 días** • **Datos sensibles:** deben ser eliminados o anonimizados inmediatamente tras cumplir su finalidad, con un plazo práctico de **1 a 3 años.** • **Datos personales de videovigilancia: se pueden almacenar por 1 mes.** • **Datos asociados a obligaciones legales:** analizar normas específicas o regulaciones fiscales que establecen **un plazo de 6 a 10 años.**	Datos personales: 5 años Imágenes y voces grabadas de 30 a 60 días, eliminación en un plazo de 2 días Datos sensibles: 1 a 3 años Datos personales de videovigilancia 1 mes Datos asociados a obligaciones legales: 6 a 10 años

PAÍS	TIEMPO DE RECOLECCIÓN DE DATOS	TIEMPO
BRASIL BRA	La LGPD establece en su artículo 15 que los datos personales deben ser almacenados solo durante el tiempo necesario para cumplir con las finalidades específicas para las cuales fueron recopilados, o para cumplir con obligaciones legales o regulatorias. • **Datos personales: un plazo recomendado es 5 años** alineado a la prescripción de acciones civiles establecidas en el Código Civil brasileño. • **Datos sensibles:** deben conservarse solo mientras sean imprescindibles para su finalidad específica, con un plazo práctico recomendado de **1 a 3 años** tras el fin de su propósito. • **Datos asociados a obligaciones legales:** analizar normas específicas o regulaciones fiscales que establecen **un plazo de 5 a 10 años.** • **Datos de navegación o registro de usuarios de 6 a 24 meses.**	Datos personales: 5 años Datos sensibles: 1 a 3 años Datos asociados a obligaciones legales: 5 a 10 años Datos de navegación o registro de usuarios: 6 a 24 meses
MÉXICO MEX	El tiempo de almacenamiento de datos en México depende del tipo de dato y de la normativa que lo regule ya que en la ley de protección de datos no se establece un plazo específico para la conservación de datos, pero si pide que se cumplan con los plazos de almacenamiento establecidos por otras normativas: • **Datos personales laborales o de seguridad social:** se conservan durante 4 años. • **Datos de videovigilancia:** se conservan durante 1 mes. • **Datos contables y fiscales:** se conservan durante 6 años. • **Documentación comprobatoria de contabilidad:** se conserva durante 5 años, pero puede ampliarse a 15 años o más en caso de pérdidas fiscales. • **Datos históricos confidenciales:** se conservan durante 30 años, pero pueden ampliarse a 70 años si afectan a la esfera más íntima del titular.	Datos personales laborales 4 años Videovigilancia 1 mes Contables y fiscales: 6 años Contabilidad: 5 años a 15 años
CHILE CHI	La Ley de protección de datos chilena no especifica un plazo máximo para el almacenamiento de datos personales, pero establece que deben tratarse solo mientras sean necesarios para cumplir con las finalidades para las que fueron recopilados (artículo 9). • **Datos personales - laborales:** se conservan durante 4 años. • **Datos sensibles de 1 a 3 años** • **Documentación comprobatoria de contabilidad:** se conserva durante 5 a 10 años.	Datos personales - laborales 4 años. Datos sensibles de 1 a 3 años Documentación de contabilidad 5 a 10 años.
ECUADOR ECU	La LOPDP no especifica un plazo exacto para la conservación de datos personales. Sin embargo, se rige por el principio de limitación del período de conservación, que establece que los datos deben mantenerse únicamente durante el tiempo necesario para cumplir con las finalidades para las cuales fueron recopilados. • **Datos personales: un plazo recomendado es 5 años** alineado a la prescripción de acciones civiles establecidas en el Código Civil brasileño. • **Datos sensibles:** deben conservarse solo mientras sean imprescindibles para su finalidad específica, con un plazo práctico recomendado de 1 a 3 años tras el fin de su propósito. • **Datos asociados a obligaciones legales:** analizar normas específicas o regulaciones fiscales que establecen **un plazo de 5 a 10 años.** • **Datos de navegación o registro de usuarios de 6 a 24 meses.**	Datos personales: 5 años Datos sensibles: 1 a 3 años Datos asociados a obligaciones legales: 5 a 10 años Datos de navegación o registro de usuarios: 6 a 24 meses
URUGUAY URU	La Ley N.° 18.331 no especifica un plazo exacto para la conservación de datos personales. Sin embargo, se rige por el principio de limitación del período de conservación, que establece que los datos deben mantenerse únicamente durante el tiempo necesario para cumplir con las finalidades para las cuales fueron recopilados. En Uruguay, el plazo para conservar datos personales depende del tipo de información: • **Obligaciones comerciales:** se pueden conservar hasta cinco años si se ha cumplido con la obligación. • **Datos sensibles:** deben ser eliminados o anonimizados inmediatamente después de que dejan de ser necesarios para la finalidad específica para la cual fueron tratados. Un plazo práctico sería de 1 a 3 años tras el cumplimiento de su propósito. • **Obligaciones personales sin plazo de prescripción:** se pueden conservar hasta cinco años desde que se pueda exigir el cumplimiento de la obligación.	Conservación de 5 años Datos sensibles: 1 a 3 años
REPÚBLICA DOMINICANA REP	Los datos personales deben ser cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. • **Datos personales: un plazo recomendado es 5 años** alineado a la prescripción de acciones civiles establecidas en el Código Civil brasileño. • **Datos sensibles:** deben conservarse solo mientras sean imprescindibles para su finalidad específica, con un plazo práctico recomendado de **1 a 3 años** tras el fin de su propósito. • **Datos asociados a obligaciones legales:** analizar normas específicas o regulaciones fiscales que establecen **un plazo de 5 a 10 años.**	Datos personales: 5 años Datos sensibles: 1 a 3 años Datos asociados a obligaciones legales: 5 a 10 años

Diagrama de implementación

FASE 1

Análisis y diagnóstico inicial

- Conformar un equipo de cumplimiento (o designar responsables temporales en cada área).
- Identificar el contexto organizacional: naturaleza, tamaño, estructura y canales de tratamiento de datos.
- Realizar un diagnóstico de estado inicial:
  - Revisión de políticas existentes.
  - Análisis de prácticas reales de tratamiento de datos.
  - Identificación de brechas de cumplimiento o procesos en los que exista vulneración de datos.
- Mapear áreas que tratan datos personales y procesos asociados.

FASE 2

Identificación y clasificación de datos

- Categorizar los datos que se manejan en la organización: personales, sensibles, financieros, menores, etc.
- Identificar bases legales para el tratamiento de datos y análisis de políticas según el tipo de organización.
- Evaluar el ciclo de vida de los datos y de la información y definir tiempos de conservación.

FASE 3

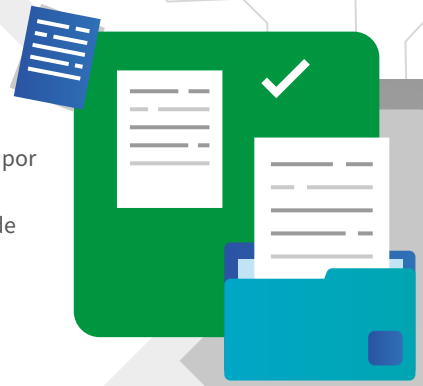
Diseño del programa de protección de datos

- Nombrar un Responsable de Protección de Datos (DPO) o un encargado por área para la gestión responsable de datos.
- Diseñar e implementar políticas internas:
  - Política de privacidad.
  - Política de retención y eliminación de datos.
  - Política de seguridad de la información.
- Implementar medidas técnicas y organizativas:
  - Cifrado, control de accesos, autenticación, backups.
  - Gestión de incidentes de seguridad.

FASE 4

Documentación y evaluaciones

- Registrar las actividades de tratamiento de datos por área/departamento.
- Realizar Evaluaciones de Impacto en Protección de Datos en tratamientos de alto riesgo.
- Evaluar la relación con terceros y proveedores:
  - Firmar cláusulas contractuales estándar.
  - Evaluar cumplimiento de proveedores.



FASE 6

Evaluación continua y mejora

- Monitorear el cumplimiento interno mediante auditorías periódicas.
- Actualizar políticas conforme a normativa nacional e internacional.
- Revisar contratos, transferencias internacionales y nuevas tecnologías.
- Documentar acciones como parte del principio de responsabilidad proactiva.

FASE 5

Implementación y ejecución

- Capacitar al personal en protección de datos y seguridad de la información.
- Asegurar el ejercicio de los derechos de los titulares:
  - Acceso, rectificación, oposición, cancelación, portabilidad, olvido.
- Establecer canales de atención a titulares y de notificación de incidentes.

PROCESO DE REVISIÓN:

- Yésica Quispe Arancibia, cofounder & CEO de NORA
- David Oliva, Cervieri Monsuarez
- ONG Programa de Coordinación en Salud Integral – PROCOSI
- Pamela Mendoza
- Valeria Paredes, Infocred Buró de Información S.A.

“Fostering data protection and responsible IA compliance in Bolivia” is one of the beneficiaries of a grant under the first Open Call under InDiCo-Global, which is a project funded as part of the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement No 101136022. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

En un país que aún carece de una legislación integral en materia de protección de datos personales e inteligencia artificial, esta guía se constituye en una vía fundamental para promover la adopción voluntaria de buenas prácticas, elevando los estándares de responsabilidad y ética digital en Bolivia.

Esta guía, elaborada por la Fundación InternetBolivia.org con el respaldo de InDiCo Global y la Unión Europea, proporciona a organizaciones públicas y privadas un marco práctico y adaptado a la realidad boliviana para la implementación de políticas de privacidad, gestión de datos y seguridad de la información.

Basada en estándares internacionales como el Reglamento General de Protección de Datos (RGPD) y el AI Act, esta publicación no sólo impulsa el desarrollo de una cultura de respeto a los derechos digitales en Bolivia, sino que también posiciona a las organizaciones en condiciones de competitividad internacional, facilitando su acceso a mercados globales y a marcos regulatorios internacionales cada vez más exigentes.

La guía busca ser una herramienta esencial para fortalecer el tratamiento responsable de los datos personales y garantizar un uso ético y seguro de la inteligencia artificial en Bolivia.