Universidad de Buenos Aires
Facultad de Ciencias Económicas

Aspectos éticos, legales y sociales

en el uso de las tecnologías de la información:

El cumplimiento tecnológico

Aníbal M. Mazza Fraquelli

fraquelli@economicas.uba.ar

1 Moral, ética, deontología y responsabilidad social

1.1 Moral

La moral se refiere a los **principios, valores y normas que guían el comportamiento humano y determinan lo que es considerado correcto o incorrecto, bueno o malo**, desde el punto de vista ético. La moral **es un sistema de creencias y juicios que afecta nuestras decisiones y acciones** en la vida cotidiana.

La moral es **construida por la sociedad** y puede variar de una cultura a otra, así como a lo largo del tiempo. Está influenciada por factores como la religión, la filosofía, las tradiciones, las leyes y las normas sociales.

Importante: Lo que es moral para una sociedad en un determinado contexto y en una determinada época pueden no serlo para la misma sociedad en un contexto y época distinta.

La moral proporciona un **marco de referencia para evaluar la conducta y tomar decisiones éticas**. Ayuda a establecer **estándares de comportamiento aceptables** y a fomentar la convivencia y la cohesión social.

1.2 Ética

La ética y la deontología son dos conceptos relacionados pero distintos en el ámbito de la moral y la conducta humana.

La **ética** se refiere al estudio y la reflexión sobre los valores y principios morales que guían la conducta humana.

Se ocupa de analizar qué es moralmente correcto o incorrecto, y busca establecer pautas para la toma de decisiones éticas.

La ética se basa en la razón, la reflexión y los juicios personales sobre lo que se considera bueno o malo.

Una pregunta que todas las organizaciones deben interpretar es que los **aspectos legales** en los cuales se desempeña **pueden no ser éticos para la sociedad**.

1.3 Deontología

Por otro lado, la **deontología** se centra en los deberes y obligaciones morales que deben seguirse en la **práctica profesional** o en contextos específicos.

Se trata de un conjunto de reglas o normas que rigen la conducta de los individuos en **determinados roles o profesiones**, y se enfoca en el cumplimiento de los **deberes y responsabilidades**. Para los profesionales del CC.EE. es la ley 20.488.

La ética establece los fundamentos morales, mientras que la deontología proporciona directrices prácticas para la conducta ética en situaciones profesionales específicas.

1.4 Responsabilidad social

La responsabilidad social se refiere al **compromiso** de las organizaciones y las personas con el bienestar y el impacto que generan en la sociedad en general.

Implica que las **empresas, instituciones y particulares** asuman la responsabilidad de sus acciones y decisiones, considerando no solo sus intereses económicos, sino también los impactos sociales, ambientales y éticos que puedan tener.

Un caso especial es la Responsabilidad Social Empresarial (RSE) la que conlleva que las empresas actúen de manera ética y responsable, no solo cumpliendo con las leyes y regulaciones, sino también contribuyendo activamente al desarrollo sostenible y al bienestar de la comunidad en la que operan.

Esto puede incluir prácticas como respetar los derechos humanos, promover la igualdad de género, proteger el medio ambiente, el uso humanizado de las tecnologías, apoyar causas sociales y garantizar condiciones laborales justas, entre otros aspectos.

La responsabilidad social también puede aplicarse a nivel individual, donde las personas se comprometen a tomar decisiones éticas y contribuir al bienestar de la sociedad en su vida personal y profesional.

Esto puede incluir acciones como ser respetuoso con los demás, ser consciente del impacto ambiental, participar en actividades voluntarias o colaborar en proyectos sociales.

2 Aspectos éticos y sociales en el uso de la tecnología

Al considerar los aspectos éticos, sociales y deontológicos en el uso de la tecnología de la información, es importante tener en cuenta varios elementos. Estos elementos pueden incluir:

1. **Privacidad y protección de datos**: El uso de la tecnología de la información implica el manejo de datos personales y sensibles. Es fundamental respetar la privacidad de los individuos y garantizar la protección de sus datos, cumpliendo con las leyes y regulaciones aplicables. Es llamada “Habeas Data”

2. **Seguridad cibernética**: La seguridad de la información y la protección contra ataques cibernéticos son aspectos cruciales. Se deben implementar medidas adecuadas para proteger los sistemas y los datos de posibles amenazas, como el acceso no autorizado **(interno y externo)**, el robo de información **(interna y externa)** o el malware.

3. **Acceso equitativo y brecha digital:** Es importante considerar el acceso equitativo a la tecnología de la información, evitando la profundización de la brecha digital entre diferentes grupos socioeconómicos o regiones. Esto implica promover la inclusión digital y garantizar que todos tengan la oportunidad de beneficiarse de la tecnología.

4. **Impacto social**: El uso de la tecnología de la información puede tener un impacto significativo en la sociedad. Es necesario evaluar y considerar cómo se están utilizando las tecnologías en relación con aspectos como la equidad, la justicia social, la discriminación, la igualdad de oportunidades y la calidad de vida de las personas.

5. **Ética en la inteligencia artificial (IA):** La IA plantea desafíos éticos particulares, como la transparencia de los algoritmos, la toma de decisiones automatizadas y el sesgo algorítmico. Se deben establecer principios éticos sólidos para guiar el desarrollo y la implementación de la IA, asegurando que se utilice de manera responsable y respetando los valores humanos. **Este aspecto aún no se encuentra bien dimensionado.**

6. **Cumplimiento legal y normativo**: Es fundamental cumplir con las leyes, regulaciones y estándares aplicables en el uso de la tecnología de la información, lo que abarca los **derechos de autor, la propiedad intelectual, la protección de datos y la seguridad de la información**.

7. **Responsabilidad profesional**: Los profesionales de la tecnología de la información tienen la responsabilidad de actuar de manera ética y cumplir con los códigos de conducta profesional establecidos. Esto implica ser consciente de las implicaciones éticas de su trabajo y tomar decisiones éticas en beneficio de la sociedad, **nuevamente la deontología.**

3 Habeas Data

Habeas Data es un concepto legal que se refiere al derecho de las personas a acceder, conocer, actualizar y rectificar la información que sobre ellas se encuentra almacenada en bases de datos o archivos, tanto públicos como privados. El término "Habeas Data" proviene del latín y significa "tener los datos".

Aquí se plantean varias relaciones a considerar esto es 1) los individuos con las organizaciones, 2) los individuos con el estado, 3) los individuos entre sí, 4) los individuos que trabajan en las organizaciones y el estado, 5) las relaciones de las organizaciones con el estado y 6) las relaciones entre estados.

El Habeas Data busca **garantizar la protección de la privacidad y la autodeterminación informativa de las personas**.

Les otorga el derecho de 1) conocer y controlar la información que se recopila y almacena sobre ellas, 2) solicitar su corrección o eliminación, 3) pedir la actualización o 4) si se obtuvo de forma ilegítima.

Este derecho permite a las personas tomar decisiones informadas sobre el uso de sus datos personales y mantener el control sobre su información. Además, brinda una herramienta legal para protegerse contra el uso indebido, la divulgación no autorizada o el tratamiento ilegal de sus datos.

El Habeas Data se encuentra reconocido en diversas legislaciones y marcos normativos de protección de datos personales en diferentes países.

Estos marcos legales establecen los derechos y las obligaciones tanto de los individuos como de las organizaciones que recopilan y procesan datos personales, con el objetivo de garantizar un uso responsable y respetuoso de la información personal.

Es un problema frecuente para las organizaciones que no tienen políticas o sectores destinados a tal efecto responder a solicitudes de habeas data.

3.1 Habeas data en Argentina, ley 25.326 – El "hoy"

La Ley de Habeas Data 25.326 de Argentina, también conocida como Ley de Protección de Datos Personales, es la normativa nacional que regula la protección de los datos personales de los ciudadanos argentinos. Debe considerarse que fue sancionada luego de la reforma constitucional del año 1994 que incluyó dentro del apartado nuevas declaraciones de derechos y garantías el **artículo 43** que en su tercer párrafo se enfoca específicamente en la protección de los datos personales.

1. **Ámbito de aplicación**: La ley se aplica a toda persona física o jurídica que realice el tratamiento (recolección, uso, almacenamiento, etc.) de datos personales en Argentina, ya sea en forma total o parcialmente automatizada, o en archivos o registros físicos.

2. **Definiciones**: La ley establece una serie de definiciones importantes, como **datos personales** (cualquier información que identifique o haga identificable a una persona), **datos sensibles** (un tipo muy particular de datos personales) tales como la religión, tendencias políticas u orientación sexual entre otros porque pueden derivar en una discriminación directa o inversa, **tratamiento de datos** (cualquier operación que se realice sobre los datos personales), y **responsable del archivo, registro o banco de datos** (la persona o entidad que decide sobre la finalidad y los medios del tratamiento de los datos).

3. **Principios rectores**: La ley establece los principios fundamentales que deben regir el tratamiento de los datos personales. Estos principios incluyen el **consentimiento informado** del titular de los datos, la finalidad específica y legítima del tratamiento, la calidad y veracidad de los datos, la proporcionalidad en el tratamiento, la seguridad de los datos y la confidencialidad.

4. **Derechos de los titulares de los datos**: La ley reconoce a los titulares de los datos una serie de derechos que pueden ejercer frente a los responsables del tratamiento. Estos derechos incluyen el acceso a los datos personales, la rectificación, actualización o supresión de los datos inexactos o desactualizados, la oposición al tratamiento para ciertos fines y la posibilidad de presentar denuncias ante la autoridad de control. **En organizaciones privadas no está "claro" quien lo hace, de hecho, puede que no forme parte de las tareas de la descripción de trabajo de los sectores/áreas del organigrama.**

5. **Obligaciones de los responsables del tratamiento**: Los responsables del tratamiento de datos personales tienen la obligación de cumplir con ciertos requisitos legales. Entre estos requisitos se encuentran la obtención del consentimiento del titular de los datos, la adopción de medidas de seguridad para proteger los datos, la notificación de las violaciones de seguridad, la conservación de los datos durante períodos razonables (período de retención) y la facilitación del ejercicio de los derechos de los titulares.

El período de retención no está claro para las organizaciones: ¿2, 3, 5, 10 años? ¿Si es un archivo digital, implica 2, 3, 5, 10 años de acceso operativo? Cuando se cumpla el plazo, ¿cómo debe realizarse la destrucción de los datos?

6. **Autoridad de control**: La ley establece la creación de una autoridad de control, actualmente la Agencia de Acceso a la Información Pública (AAIP), encargada de supervisar y fiscalizar el cumplimiento de la normativa de protección de datos en Argentina. Esta autoridad tiene poderes de investigación, sanción y asesoramiento.

7. **Transferencia internacional de datos**: La ley regula la transferencia de datos personales fuera del territorio argentino, exigiendo que el país receptor ofrezca un nivel adecuado de protección de datos o que existan garantías suficientes para la transferencia, como cláusulas contractuales o certificaciones reconocidas.

8. **Sanciones**: La ley establece un régimen de sanciones para quienes infrinjan sus disposiciones. Las sanciones pueden incluir amonestaciones, multas, clausura del archivo, registro o banco de datos, y la inhabilitación para el ejercicio de la actividad relacionada con el tratamiento de datos personales. Las sanciones son según formas tradicionales del principio de “no dañar” y suelen estructurarse en 1) multa con más 2) indemnizar, con más 3) cesar en la conducta y 4) desistir de continuar la acción que provoca el daño.

3.1.1 DNPDP

La Dirección Nacional de Protección de Datos Personales (DNPDP) de Argentina es el organismo encargado de promover y garantizar el derecho a la protección de datos personales en el país. Sus funciones principales incluyen:

1. Registro de bases de datos: La DNPDP mantiene el Registro Nacional de Bases de Datos, donde las organizaciones deben inscribir y mantener actualizada la información sobre las bases de datos que contienen datos personales. Esto permite tener un registro de las entidades que tratan datos personales y facilita el ejercicio de los derechos de los titulares de datos.

2. Fiscalización y control: La DNPDP realiza fiscalizaciones y controles para verificar el cumplimiento de la normativa de protección de datos personales. Esto faculta a evaluar las medidas de seguridad, privacidad y consentimiento utilizadas por las organizaciones que manejan datos personales, y tomar acciones en caso de detectar incumplimientos.

3. Recepción y gestión de denuncias: La DNPDP recibe y gestiona denuncias de los titulares de datos personales sobre posibles infracciones a la normativa de protección de datos. Realiza investigaciones y toma medidas para garantizar el cumplimiento de los derechos de privacidad y protección de datos.

4. Asesoramiento y capacitación: La DNPDP brinda asesoramiento a las organizaciones y al público en general sobre cuestiones relacionadas con la protección de datos personales. También desarrolla programas de capacitación y divulgación para promover buenas prácticas y conciencia sobre la importancia de la privacidad y la protección de datos.

5. Normativa y regulación: La DNPDP emite normativas y reglamentaciones relacionadas con la protección de datos personales en Argentina. Estas normativas establecen los principios y requisitos para el tratamiento de datos personales, así como los derechos de los titulares de datos.

En resumen, a través de sus funciones de registro, fiscalización, recepción de denuncias, asesoramiento y regulación, busca asegurar que las organizaciones cumplan con los estándares de privacidad y seguridad establecidos por la normativa de protección de datos.

3.2 Habeas data en Argentina, ley 25.326 – El "futuro"

A través de la Resolución 119/2022, la Agencia de Acceso a la Información Pública (AAIP) abrió el procedimiento de elaboración participativa de normas con relación al Anteproyecto de Ley de Protección de Datos Personales, que tiene como fin reformar y actualizar la ley vigente en la temática.

Lo que se busca **es armonizar con los estándares regionales e internacionales** en materia de protección de datos personales para fortalecer una estrategia global de regulación, desde un enfoque de derechos humanos. **La armonización es reactiva, no proactiva.**

Además, se enfatiza que la actualización normativa de la Ley se realice en el marco de un proceso de debate participativo, abierto y transparente con el fin de producir una nueva legislación integral que garantice el ejercicio del derecho fundamental de las personas a la protección de sus datos personales y a la privacidad.

Por todo ello, se invita a toda persona física o jurídica, pública o privada, que invoque un derecho o interés simple, difuso o de incidencia colectiva para que presente sus propuestas y opiniones sobre el Anteproyecto.

Dicho anteproyecto cuenta con once capítulos:

- Capítulo 1 – Disposiciones Generales
- Capítulo 2 – Tratamiento de Datos Personales
- Capítulo 3 – Transferencias Internacionales

- Capítulo 4 – Derecho de los Titulares de los Datos
- Capítulo 5 – Obligaciones de los Responsables y Encargados del Tratamiento
- Capítulo 6 – Protección de Datos de Información Crediticia
- Capítulo 7 – Autoridad de Aplicación
- Capítulo 8 – Procedimientos y Sanciones
- Capítulo 9 – Acción de Habeas Data
- Capítulo 10 – Disposiciones Transitorias
- Capítulo 11 – Disposiciones Finales.

3.2.1 Cambios y adaptaciones del anteproyecto

- Ampliación de la definición de datos sensibles, es decir aquellos que se refieran a la esfera íntima o que puedan generar discriminación o riesgo grave para el/la titular. Bajo este paraguas se incorporan los datos genéticos y los biométricos.
- Además, se refuerzan las características que debe tener el consentimiento (debe ser previo, libre, específico, informado e inequívoco); y se amplía el ámbito de aplicación de la ley, ya que se exige el respeto de los derechos de los ciudadanos argentinos frente a organizaciones extranjeras que, aunque pueden no tener domicilio legal en el país, recolectan sus datos personales.
- El proyecto también exige mayor transparencia en la explicación de las decisiones que se adoptan mediante mecanismos como la inteligencia artificial; y hasta incluye el derecho a solicitar la revisión por una persona humana de las decisiones tomadas sobre la base del tratamiento automatizado o semiautomatizado.
- En relación a la seguridad de los datos, la iniciativa establece la obligación de notificar a la autoridad de control y a los titulares de los datos en casos de incidentes de seguridad, como hackeos; y también aumenta el monto económico de las sanciones.

Sin embargo, no aborda directamente:

- Un organismo de control capaz de garantizar la seguridad efectiva de los datos, que sea una autoridad de aplicación lo suficientemente autónoma del poder estatal y privado
- No se especifica cual es la capacidad funcional ni el presupuesto acorde a la misión que tiene la institución como órgano garante de un derecho de la ciudadanía.
- En relación al aspecto de la seguridad de los datos, no se delimitan los estándares de seguridad que deben aplicar quienes administran los datos personales y cómo la autoridad de aplicación puede evaluar su cumplimiento.
- Los controles preventivos que debería poder realizar el organismo de control no están claros, de modo tal que su accionar no se limite a responder frente a hackeos u otros usos indebidos de los datos personales.

- Se introducen figuras “obligatorias” que toda organización debería tener, similares al oficial de cumplimiento y responsable del control, pero no especifica a qué nivel jerárquico reportan.

4 Habeas data a nivel internacional

El cumplimiento legal en el uso de tecnologías de la información a nivel internacional implica considerar una serie de aspectos clave. A continuación, se enumeran algunos de los aspectos más relevantes:

1. **Legislación de protección de datos**: Las leyes de protección de datos varían en diferentes países y regiones. Es importante comprender y cumplir con las leyes y regulaciones específicas en cada jurisdicción donde se opera o se recopilan datos personales.

2. **Transferencia internacional de datos**: Si se realiza la transferencia de datos personales fuera del país de origen, es fundamental cumplir con los requisitos legales aplicables a la transferencia internacional de datos, como asegurarse de que el país de destino ofrezca un nivel adecuado de protección de datos o implementar medidas de seguridad y salvaguardias apropiadas.

3. **Cumplimiento normativo sectorial**: Además de las leyes de protección de datos, existen regulaciones específicas en diferentes sectores, como el **financiero**, de la **salud** o de las **telecomunicaciones**. Es importante cumplir con las regulaciones sectoriales relevantes al utilizar tecnologías de la información en esos sectores.

4. **Derechos de autor y propiedad intelectual**: Las tecnologías de la información están sujetas a leyes de derechos de autor y propiedad intelectual. Es necesario cumplir con las leyes y regulaciones relacionadas con la protección de los derechos de autor y los derechos de propiedad intelectual al crear, distribuir o utilizar contenido y software.

5. **Seguridad cibernética**: La seguridad de la información es fundamental en el entorno de las tecnologías de la información. Cumplir con las leyes y regulaciones de seguridad cibernética es esencial para proteger los sistemas y datos contra amenazas y ataques cibernéticos.

6. **Comercio electrónico y protección al consumidor**: Si se realizan transacciones comerciales en línea, es necesario cumplir con las leyes y regulaciones relacionadas con el comercio electrónico y la protección al consumidor. Esto puede incluir información clara sobre precios, términos y condiciones, protección de datos de los clientes y solución de disputas.

7. **Cumplimiento con regulaciones específicas de países**: Además de los aspectos mencionados anteriormente, es importante tener en cuenta las regulaciones específicas de cada país en el que se opera o se ofrecen servicios. Esto puede incluir regulaciones relacionadas con la publicidad en línea, la privacidad, la seguridad de datos, el almacenamiento de datos y otros aspectos específicos de la tecnología de la información.

4.1 En algunos países y territorios

4.1.1 Estados Unidos:

En Estados Unidos, no existe una legislación federal específica denominada "habeas data". Sin embargo, hay leyes y regulaciones que protegen la privacidad y los derechos de los individuos en relación con el manejo de sus datos personales. Por ejemplo, la Ley de Privacidad de las Comunicaciones Electrónicas (ECPA) y la Ley de Protección al Consumidor de Información Crediticia (FCRA) son ejemplos de legislaciones que protegen ciertos aspectos de la privacidad y la seguridad de los datos personales en el país.

4.1.2 México:

En México, el habeas data se encuentra establecido en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP). Esta ley establece los derechos de acceso, rectificación, cancelación y oposición (ARCO) que tienen los individuos sobre sus datos personales. Además, se establece la obligación de las organizaciones de proteger los datos personales y obtener el consentimiento informado para su tratamiento.

4.1.3 Europa en general y Reino Unido:

En Europa, el habeas data se aborda a través del Reglamento General de Protección de Datos (GDPR), que es aplicable en todos los países miembros de la Unión Europea (UE). El GDPR establece los derechos de los individuos sobre sus datos personales, así como las obligaciones de las organizaciones en relación con el tratamiento y la protección de los datos. Además, se establece la Autoridad de Protección de Datos en cada país miembro como el órgano encargado de supervisar y aplicar la normativa de protección de datos. En cuanto al Reino Unido, no hay aún expectativas de cambio regulatorio post Brexit.

4.1.4 Brasil:

En Brasil, el habeas data se encuentra consagrado en la Constitución Federal y en la Ley General de Protección de Datos Personales (LGPD). La LGPD establece los derechos de los individuos sobre sus datos personales y las obligaciones de las organizaciones en cuanto al tratamiento y la protección de los datos. Además, se crea la Autoridad Nacional de Protección de Datos (ANPD) como el órgano encargado de supervisar y aplicar la ley.

4.1.5 Chile:

En Chile, el habeas data se encuentra consagrado en la Constitución Política y en la Ley N° 19.628 sobre Protección de la Vida Privada. Esta ley establece los derechos de los individuos sobre sus datos personales y las

obligaciones de las organizaciones en relación con su recolección, uso y tratamiento. Además, se encuentra la Agencia de Protección de Datos Personales (APDP) como el organismo encargado de supervisar y hacer cumplir la ley en Chile.

4.1.6 Uruguay:

En Uruguay, el habeas data está protegido por la Constitución de la República y por la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data. Esta ley establece los derechos de los individuos sobre sus datos personales, así como las obligaciones de las organizaciones en cuanto a su recolección, almacenamiento, uso y divulgación. La Agencia de Protección de Datos Personales (URCDP) es el organismo encargado de supervisar y hacer cumplir la ley en Uruguay.

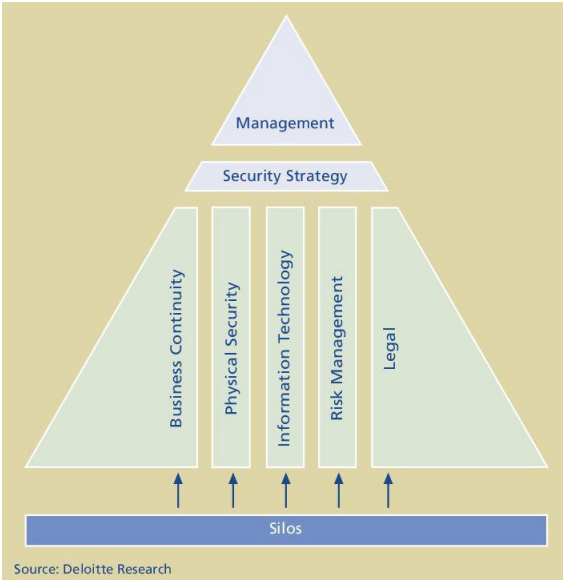
4.1.7 Paraguay:

En Paraguay, el habeas data se encuentra consagrado en la Constitución Nacional y en la Ley N° 1682/01 de Protección de Datos Personales. Esta ley establece los derechos de los individuos sobre sus datos personales y las obligaciones de las organizaciones en relación con su recolección, uso y tratamiento. La Dirección Nacional de Protección de Datos Personales (DNPDP) es el organismo encargado de supervisar y hacer cumplir la ley en Paraguay.

5 El ”Compliance” Tecnológico

El compliance tecnológico, también conocido como cumplimiento tecnológico, se refiere a la implementación y cumplimiento de políticas, procedimientos y normativas relacionadas con el uso ético, legal y seguro de la tecnología en una organización.

El objetivo del compliance tecnológico es garantizar que las actividades tecnológicas de una empresa se realicen de manera responsable y de acuerdo con las leyes, regulaciones y estándares aplicables.



El compliance tecnológico abarca una amplia gama de áreas, entre las que se incluyen:

1. **Protección de datos**: Incluye el cumplimiento de las leyes y regulaciones de protección de datos, como el acceso, uso, almacenamiento y divulgación adecuados de la información personal de los clientes y empleados. Esto implica garantizar la privacidad de los datos, obtener el consentimiento adecuado, implementar medidas de seguridad y gestionar adecuadamente las solicitudes de los titulares de los datos.

2. **Seguridad cibernética**: Implica establecer medidas de seguridad técnicas y organizativas para proteger los sistemas y datos de la organización contra amenazas cibernéticas, como ataques de hackers, malware y robo de datos. Esto puede incluir la implementación de firewalls, sistemas de detección de intrusos, encriptación de datos, políticas de contraseñas seguras y capacitación en seguridad para los empleados.

3. **Cumplimiento normativo**: Se refiere al cumplimiento de las leyes y regulaciones aplicables a la tecnología, como las leyes de propiedad intelectual, las regulaciones sectoriales específicas, las leyes de comercio electrónico, las leyes de seguridad de la información y otras normativas relevantes. Esto implica mantenerse actualizado con los cambios legales, evaluar el impacto de las regulaciones en las operaciones tecnológicas y garantizar que se cumplan los requisitos legales aplicables.

4. **Ética y responsabilidad social**: Incluye asegurar que el uso de la tecnología sea ético y responsable. Esto puede abarcar aspectos como evitar la discriminación algoritmos, respetar la privacidad de los usuarios, evitar el uso indebido de datos personales, promover la igualdad y la diversidad, y considerar el impacto social y ambiental de las tecnologías utilizadas.

5. **Gestión de riesgos**: Implica identificar, evaluar y mitigar los riesgos asociados con el uso de la tecnología en la organización. Esto puede incluir riesgos de seguridad cibernética, riesgos legales y regulatorios, riesgos de privacidad, riesgos reputacionales y otros riesgos relacionados con el uso de la tecnología.

El compliance tecnológico se ha vuelto cada vez más importante debido al creciente papel de la tecnología en las operaciones empresariales y la necesidad de garantizar la confianza de los clientes, proteger los datos y cumplir con las regulaciones aplicables. Las organizaciones suelen contar con equipos o roles especializados en compliance tecnológico para asegurarse de que se cumplan los estándares y requisitos relevantes.

5.1 Compliance tecnológico en Argentina 2023

5.1.1 Banco Central de la República Argentina

El Banco Central de la República Argentina (BCRA) es la autoridad monetaria y financiera de Argentina. En relación al cumplimiento tecnológico, el BCRA tiene varias responsabilidades y acciones, entre las cuales se destacan las siguientes:

1. **Regulación y normativas**: El BCRA emite regulaciones y normativas relacionadas con el uso de tecnología en el sector financiero. Estas normativas abarcan aspectos como la seguridad de la información, la protección de datos personales, la infraestructura tecnológica y la ciberseguridad. El objetivo es establecer estándares y requisitos para garantizar la integridad, confidencialidad y disponibilidad de la información financiera.

2. **Autorización y supervisión de entidades financieras**: El BCRA es responsable de autorizar y supervisar a las entidades financieras en el país, como bancos y otras instituciones financieras. En este proceso, se evalúa el cumplimiento de las normativas tecnológicas, incluyendo la infraestructura tecnológica utilizada, los sistemas informáticos, las políticas de seguridad, los procedimientos de respaldo y recuperación, entre otros aspectos.

3. **Gestión de incidentes y seguridad informática**: El BCRA establece medidas para la gestión de incidentes y la seguridad informática en el sistema financiero. Esto implica la implementación de sistemas de detección y

respuesta a incidentes, así como la coordinación de acciones para mitigar y gestionar posibles amenazas cibernéticas. También promueve la colaboración con otras entidades y organismos para fortalecer la ciberseguridad a nivel del sistema financiero.

4. **Establecimiento de estándares tecnológicos**: El BCRA establece estándares tecnológicos para el desarrollo e implementación de sistemas financieros y servicios digitales. Estos estándares buscan asegurar la interoperabilidad, la compatibilidad y la confiabilidad de los sistemas utilizados en el sector financiero, promoviendo la innovación tecnológica y la protección de los usuarios.

5. **Monitoreo y evaluación de riesgos tecnológicos**: El BCRA monitorea y evalúa los riesgos tecnológicos asociados al sector financiero. Esto incluye el análisis de amenazas cibernéticas, la identificación de vulnerabilidades y la adopción de medidas para mitigar los riesgos. También promueve la educación y concientización sobre la importancia de la seguridad informática en el sector financiero.

El Banco Central de la República Argentina (BCRA) ha establecido varias normas relacionadas con el cumplimiento tecnológico en el sector financiero. A continuación, mencionaré algunas de las normas más relevantes:

1. **Comunicación "A" 4609**: Establece los requisitos para la implementación de políticas de seguridad de la información y ciberseguridad en las entidades financieras. Estos requisitos incluyen la designación de responsables de seguridad, la implementación de controles y procedimientos de seguridad, la realización de auditorías y la notificación de incidentes de seguridad.

2. **Comunicación "A" 5623**: Establece los requisitos de seguridad y continuidad operativa que deben cumplir las entidades financieras para garantizar la disponibilidad y funcionamiento de sus sistemas informáticos. Esta norma incluye aspectos como la realización de pruebas de continuidad operativa, la implementación de planes de contingencia y la protección de la infraestructura tecnológica.

3. **Comunicación "A" 6770**: Establece los requisitos para la implementación de un marco de gestión de riesgos tecnológicos en las entidades financieras. Estos requisitos incluyen la identificación y evaluación de los riesgos tecnológicos, la implementación de controles adecuados, la adopción de políticas de seguridad y la realización de pruebas de vulnerabilidad.

4. **Comunicación "A" 7030**: Establece los requisitos de seguridad para los servicios financieros electrónicos, como las transferencias electrónicas de fondos y los pagos electrónicos. Esta norma establece medidas de seguridad que deben implementarse en los sistemas de pago y en la protección de la información de los usuarios.

5. **Comunicación "A" 7109**: Establece los requisitos para la adopción de tecnologías de autenticación fuerte en las operaciones de banca electrónica y servicios financieros remotos. La norma define los estándares de seguridad que deben cumplir los mecanismos de autenticación utilizados por las entidades financieras.

6. **Comunicación "A" 7724**: Establece la obligación a instituciones financieras de definir un proceso que establezca responsabilidades, políticas, y procedimientos para la gestión de activos de información que brindan apoyo al negocio y a los servicios de la entidad, tanto propios, como delegados a terceras partes. Se trata de una actualización de la Comunicación "A" 4609, en la que se tiene en cuenta el contexto actual en función de las nuevas tecnologías.

Es por esto que, en esta nueva comunicación, se incluyen reglamentaciones vinculadas a los activos de Tecnología Informática lo que plantea requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información y deben adoptar un modelo de gestión compatible con las mejores prácticas en materia de control de los riesgos de tecnología y seguridad de la información. Esto impacta aspectos como:

- Resiliencia tecnológica.
- Obsolescencia de la tecnología y los sistemas.
- Gestión de las relaciones con terceras partes en el desarrollo y utilización de algoritmos de inteligencia artificial o aprendizaje automático.
- Protección de datos personales en el uso de tecnologías asociadas a blockchain.
- Gestión de escenarios de ciber incidentes relacionados a datos personales de los clientes y gestión de datos y activos informáticos.

Para cumplir con la regulación establecida las instituciones financieras deben realizar las siguientes tareas:

- Definir un proceso de gestión de activos de información que establezca responsabilidades, políticas y procedimientos para la gestión de los activos de información propios y delegados en terceras partes.
- Establecer criterios para la toma de decisiones relativas a la gestión de activos.
- Mantener, utilizar y actualizar los activos de información, considerando su obsolescencia, vulnerabilidades y necesidades de actualización o reemplazo.
- Cumplir con estándares internos de configuración y seguridad.
- Mantener un inventario detallado y actualizado de los activos de información propios y delegados en terceras partes.
- Clasificar los activos de información en concordancia con la clasificación de los datos requerida en la regulación.
- Definir un proceso para la revisión y actualización de la clasificación de los activos de información.

5.1.2 Conozca a su cliente – Know Your Customer

Las políticas administrativas de una organización relacionadas con el concepto de "conozca a su cliente" (KYC, por sus siglas en inglés) son aquellas que se establecen para verificar y recopilar información sobre los clientes con el fin de mitigar riesgos, prevenir actividades ilegales y asegurar el cumplimiento de las regulaciones aplicables. Estas políticas suelen incluir los siguientes elementos:

1. **Identificación del cliente**: Establece los procedimientos para recopilar y verificar la identidad de los clientes. Esto puede incluir la solicitud de documentos de identificación válidos, como pasaportes, licencias de conducir o tarjetas de identificación, y la verificación de su autenticidad.

2. **Verificación del origen de los fondos**: Se refiere a la necesidad de conocer la fuente de los fondos que un cliente utiliza en sus transacciones. Esto implica solicitar información sobre la procedencia de los fondos y realizar una debida diligencia para asegurarse de que no provengan de actividades ilegales, como el lavado de dinero o la financiación del terrorismo.

3. **Evaluación del riesgo**: Consiste en realizar una evaluación del riesgo asociado con cada cliente y sus transacciones. Esto implica categorizar a los clientes en función de su nivel de riesgo, considerando factores como el tipo de producto o servicio que solicitan, su ubicación geográfica, el volumen de transacciones y otros factores relevantes. Con base en esta evaluación, se pueden aplicar controles adicionales o medidas de monitoreo más rigurosas.

4. **Actualización de la información**: Establece la necesidad de mantener la información del cliente actualizada. Las políticas pueden exigir la verificación periódica de la información proporcionada por el cliente y la solicitud de actualizaciones en caso de cambios relevantes, como cambios de domicilio, cambios en la estructura organizativa o cambios en la propiedad de la empresa.

5. **Conservación de registros**: Establece los requisitos para la retención y conservación de registros relacionados con la información recopilada del cliente. Esto implica mantener los registros de manera segura y accesible durante un período de tiempo determinado, de acuerdo con las regulaciones aplicables y las políticas internas de la organización.

6. **Capacitación y concientización**: Establece la necesidad de capacitar y sensibilizar a los empleados sobre las políticas y procedimientos de KYC, así como sobre la importancia de cumplir con ellos. Esto ayuda a garantizar que todos los miembros del personal comprendan sus responsabilidades y los riesgos asociados con la falta de cumplimiento.

5.1.3 Botón de Arrepentimiento

El concepto de "botón de arrepentimiento" se refiere a una función o política que permite a los consumidores cancelar o deshacer una transacción realizada en línea dentro de un período de tiempo determinado, brindándoles la opción de retractarse de su compra. Aunque esta política puede variar en función de la empresa y la jurisdicción, a continuación se presentan algunas políticas administrativas comunes relacionadas con el botón de arrepentimiento:

1. **Periodo de arrepentimiento**: Esta política establece un período de tiempo durante el cual los consumidores pueden ejercer su derecho de arrepentimiento. Por ejemplo, puede ser de 7 días, 14 días o incluso más, dependiendo de las regulaciones y las políticas internas de la organización.

2. **Proceso de cancelación**: Se establecen los procedimientos para que los consumidores ejerzan su derecho de arrepentimiento. Esto puede incluir la necesidad de completar un formulario en línea, enviar una solicitud por correo electrónico o comunicarse con el servicio de atención al cliente de la empresa.

3. **Reembolso y devolución**: Se especifican las condiciones y los términos para el reembolso y la devolución de los productos o servicios. Esto puede incluir el reembolso total o parcial del monto pagado por el consumidor y las instrucciones para devolver los productos en caso de ser necesario.

4. **Excepciones**: Algunos productos o servicios pueden estar excluidos por razones de higiene, como productos alimentarios o productos personalizados.

5. **Comunicación y notificación**: Se establece cómo se debe comunicar y notificar a los consumidores sobre su derecho de arrepentimiento. Esto puede incluir la inclusión de información clara y visible en el sitio web de la empresa, en los correos electrónicos de confirmación de compra y en los recibos de pago.

6. **Responsabilidad de envío y costos**: Se establece quién es responsable de los costos de envío en caso de devolución de productos y si la empresa proporcionará una etiqueta de envío prepagada o si el consumidor debe asumir los gastos de envío de devolución.

Es importante tener en cuenta que estas políticas pueden variar según la jurisdicción y las regulaciones aplicables. Además, algunas empresas pueden optar por implementar políticas más flexibles que brinden a los consumidores un mayor período de tiempo o condiciones más favorables para ejercer su derecho de arrepentimiento. Por lo tanto, es recomendable revisar las políticas específicas de cada empresa para obtener información precisa y actualizada sobre su botón de arrepentimiento.

5.1.4 Retención y destrucción de datos

5.1.4.1 Retención

Los periodos de retención de datos se refieren al tiempo durante el cual una organización o entidad guarda y almacena información personal o datos en sus sistemas o archivos. Estos periodos están determinados por diferentes factores, como la legislación vigente, los requisitos regulatorios, las políticas internas de la organización y la finalidad para la cual se recopilaron los datos.

El periodo de retención puede variar significativamente según la naturaleza de los datos y la jurisdicción en la que se encuentre la organización. Algunos tipos de datos pueden tener requerimientos específicos de retención establecidos por la ley, mientras que otros pueden tener criterios más flexibles.

Es importante mencionar que, en muchos casos, las organizaciones están obligadas a cumplir con ciertos plazos de retención de datos establecidos por la legislación vigente. Estos plazos pueden variar según el tipo de datos y la finalidad para la cual se recopilaron. Además, algunas leyes pueden requerir la destrucción o eliminación segura de los datos una vez que el periodo de retención ha expirado.

En general, los periodos de retención de datos están diseñados para equilibrar la necesidad de mantener los datos durante un tiempo adecuado para cumplir con sus finalidades legítimas (como registros contables, obligaciones fiscales, demandas legales, entre otros) y el respeto a la privacidad de los individuos, evitando la retención innecesaria o excesiva de datos personales.

Es importante que las organizaciones establezcan políticas claras y procedimientos de retención de datos que estén alineados con la legislación aplicable y las mejores prácticas en materia de privacidad y protección de datos. Además, deben contar con mecanismos para asegurar la eliminación segura de los datos una vez que hayan cumplido su periodo de retención.

5.1.4.2 Destrucción

Para eliminar datos pasados su periodo de retención, es recomendable seguir ciertas políticas y procedimientos que garanticen una eliminación segura y adecuada de la información. Algunas de las políticas a considerar son las siguientes:

1. **Política de retención de datos**: Es importante contar con una política clara y documentada que especifique los periodos de retención aplicables a los diferentes tipos de datos y la forma en que se debe llevar a cabo su eliminación una vez que hayan expirado. Esta política debe estar alineada con la legislación y regulaciones aplicables.

2. **Proceso de revisión periódica**: Es recomendable realizar revisiones periódicas de los datos almacenados para identificar aquellos que hayan superado su periodo de retención. Esto implica realizar una evaluación de la necesidad continua de retener los datos y, en caso de que no sean necesarios, proceder a su eliminación.

3. **Procedimientos de eliminación**: Se deben establecer procedimientos claros y seguros para llevar a cabo la eliminación de los datos. Esto puede incluir la utilización de técnicas de borrado seguro, eliminación de respaldos, destrucción física de medios de almacenamiento, entre otros métodos, dependiendo de la naturaleza de los datos y los requisitos de seguridad.

4. **Registro y documentación**: Es importante llevar un registro de las acciones de eliminación de datos realizadas, incluyendo detalles como la fecha, los datos eliminados, los responsables y el método utilizado. Esta documentación ayuda a demostrar el cumplimiento de las políticas y los requisitos legales en caso de auditorías o investigaciones.

5. **Capacitación y concientización**: Todos los empleados y personal involucrado en el manejo de datos deben recibir capacitación y concientización sobre la importancia de cumplir con los periodos de retención y seguir los procedimientos de eliminación. Esto incluye la comprensión de las implicancias legales, los riesgos de retener datos innecesariamente y la responsabilidad de proteger la privacidad de los individuos.

6. **Auditoría y monitoreo**: Es recomendable realizar auditorías periódicas y monitorear el cumplimiento de las políticas de eliminación de datos. Esto puede incluir la revisión de registros de eliminación, verificación del cumplimiento de los periodos de retención y la identificación de áreas de mejora.

Al seguir estas políticas, las organizaciones pueden asegurarse de que los datos sean eliminados de manera adecuada y en cumplimiento de los requisitos legales y de privacidad. Además, contribuyen a minimizar los riesgos asociados con la retención innecesaria de datos personales.

5.1.4.3 Concientización de tratamiento

La concientización en el tratamiento de datos se refiere a educar y sensibilizar a las personas sobre la importancia de manejar y proteger los datos personales de manera adecuada, respetando la privacidad y cumpliendo con las leyes y regulaciones aplicables.

Implica informar y educar a las personas sobre los riesgos y desafíos asociados con el manejo incorrecto de los datos personales, así como sobre los derechos y responsabilidades que tienen como usuarios y custodios de esa información.

Algunos aspectos clave de la concientización en el tratamiento de datos incluyen:

1. **Privacidad y confidencialidad**: Se informa a las personas sobre la importancia de la privacidad y la confidencialidad de los datos personales, explicando cómo pueden ser utilizados y protegidos de manera segura.

2. **Derechos de los individuos**: Se explican los derechos que tienen los individuos sobre sus datos personales, como el derecho a acceder, rectificar, limitar o eliminar su información, y cómo pueden ejercer esos derechos.

3. **Consentimiento informado**: Se promueve el entendimiento de la importancia del consentimiento informado para el manejo de datos personales, asegurando que las personas comprendan y otorguen su consentimiento de manera consciente y voluntaria.

4. **Riesgos y amenazas**: Se educa sobre los riesgos y amenazas relacionados con el manejo inadecuado de datos personales, como el robo de identidad, el fraude, el phishing, el malware y otras prácticas maliciosas.

5. **Buenas prácticas**: Se fomenta el conocimiento y la adopción de buenas prácticas en el tratamiento de datos personales, como el uso de contraseñas seguras, el cifrado de datos, la protección de dispositivos y la actualización de software, entre otros.

La concientización en el tratamiento de datos puede ser realizada a través de campañas de comunicación, capacitaciones, materiales educativos y políticas internas dentro de las organizaciones. El objetivo principal es promover una cultura de privacidad y seguridad de los datos, en la que las personas estén informadas y sean responsables en el manejo de la información personal.

5.1.4.4 Políticas administrativas en general

Las políticas administrativas relacionadas con el tratamiento de datos con tecnología de la información se refieren a las directrices y normas establecidas por una organización para regular y asegurar un manejo adecuado de los datos utilizando las herramientas tecnológicas disponibles. Algunas de estas políticas pueden incluir:

1. **Política de privacidad**: Establece los principios y procedimientos para el manejo de datos personales, incluyendo la recopilación, uso, almacenamiento, transferencia y eliminación de dichos datos. También puede abordar aspectos como el consentimiento, la confidencialidad y los derechos de los individuos.

2. **Política de seguridad de la información**: Establece medidas y controles de seguridad para proteger los datos contra accesos no autorizados, pérdidas, alteraciones o divulgaciones indebidas. Puede incluir aspectos como el uso de contraseñas seguras, el cifrado de datos, el control de accesos, la gestión de parches y actualizaciones, y la protección contra malware y ataques cibernéticos.

3. **Política de retención de datos**: Define los periodos de retención de los datos y los procedimientos para su eliminación segura una vez que han cumplido su propósito o los plazos legales establecidos. Esta política también puede incluir consideraciones sobre la destrucción física de medios de almacenamiento, en caso de que sea necesario.

4. **Política de gestión de consentimiento**: Establece los criterios y procedimientos para obtener y gestionar el consentimiento de los individuos para el tratamiento de sus datos personales. Puede abordar aspectos como el consentimiento explícito, el consentimiento informado y la documentación del consentimiento obtenido.

5. **Política de acceso y control de datos**: Define los niveles de acceso y los controles de seguridad que se aplican a los datos, asegurando que solo las personas autorizadas puedan acceder y manipular la información. Puede incluir aspectos como la asignación de roles y responsabilidades, la autenticación de usuarios y la monitorización de actividades de acceso.

6. **Política de educación y concientización**: Establece la importancia de la capacitación y concientización de los empleados sobre las mejores prácticas en el manejo de datos y el cumplimiento de las políticas establecidas. Esto puede incluir programas de formación, comunicaciones regulares y pruebas de conocimientos.

Estas son solo algunas de las políticas administrativas que pueden estar relacionadas con el tratamiento de datos utilizando tecnología de la información. Es importante que cada organización adapte y desarrolle sus políticas según sus necesidades y el marco legal y normativo aplicable a su sector y ubicación geográfica.

5.1.5 Sarbanes-Oxley

La Ley Sarbanes-Oxley (Sarbanes-Oxley Act o SOX) es una legislación estadounidense que se promulgó en 2002 en respuesta a los escándalos financieros corporativos, como el caso Enron, con el objetivo de mejorar la transparencia, la responsabilidad y la gobernanza corporativa en las empresas.

Aunque la Ley Sarbanes-Oxley es una legislación de Estados Unidos, sus requisitos y principios se han convertido en referentes internacionales en materia de gobernanza corporativa y gestión de riesgos. Muchas organizaciones fuera de los Estados Unidos adoptan prácticas similares a las establecidas por la ley SOX como una forma de mejorar sus estándares y ganar confianza en los mercados globales.

Aunque las organizaciones fuera de los Estados Unidos no están directamente sujetas a la ley SOX, pueden verse afectadas por ella de las siguientes maneras:

1. **Empresas con sede en los Estados Unidos**: Las organizaciones con sede en los Estados Unidos deben cumplir con la ley SOX, independientemente de su presencia en otros países. Esto implica que las subsidiarias o divisiones de estas empresas en otros países también deben seguir los requisitos de la ley SOX.

2. **Cotización en bolsas de valores estadounidenses**: Las organizaciones con sede en otros países que buscan cotizar en bolsas de valores de los Estados Unidos, como el NASDAQ o el NYSE, deben cumplir con los requisitos de la ley SOX para mantener su listado. Esto puede incluir la implementación de controles internos sólidos, la auditoría de informes financieros y la divulgación de información relevante.

3. **Presión regulatoria y mejores prácticas**: Aunque no haya una obligación legal directa, los reguladores y las autoridades en muchos países han adoptado principios similares a los establecidos por la ley SOX. También existen marcos internacionales, como el informe COSO (Committee of Sponsoring Organizations of the Treadway Commission), que proporcionan directrices para el establecimiento de sistemas de control interno y gestión de riesgos.

4. **Ventajas competitivas**: Adoptar prácticas y controles similares a los establecidos por la ley SOX puede ayudar a las organizaciones fuera de los Estados Unidos a mejorar su gobernanza corporativa, fortalecer su gestión de riesgos y ganar la confianza de los inversores y otras partes interesadas.

Es importante destacar que las implicaciones y el alcance de la ley SOX pueden variar según la jurisdicción y las regulaciones locales. Cada país puede tener sus propias leyes y normativas específicas en materia de gobernanza corporativa y controles internos. Por lo tanto, es recomendable consultar a expertos legales y contables para obtener asesoramiento adecuado sobre cómo aplicar los principios de la ley SOX en organizaciones fuera de los Estados Unidos.

5.1.6 Normas de la Unidad de Información Financiera

La Unidad de Información Financiera (UIF) de Argentina es un organismo especializado en la prevención y represión de los delitos de lavado de activos y financiamiento del terrorismo. Su objetivo principal es contribuir a la integridad y transparencia del sistema financiero y económico del país.

Las principales funciones de la UIF de Argentina son las siguientes:

1. **Análisis de información**: La UIF recibe, recopila y analiza información relacionada con transacciones sospechosas de lavado de activos y financiamiento del terrorismo. Recibe reportes de entidades obligadas, como bancos, casas de cambio, aseguradoras y otros sujetos obligados, así como también información proveniente de otras fuentes, como organismos de control y denuncias ciudadanas.

2. **Generación de inteligencia financiera**: La UIF genera inteligencia financiera a partir del análisis de la información recibida. Esto implica identificar patrones, tendencias y redes relacionadas con el lavado de activos y el financiamiento del terrorismo, con el fin de contribuir a la detección y prevención de estos delitos.

3. **Colaboración con organismos nacionales e internacionales**: La UIF colabora con otros organismos nacionales, como el Poder Judicial, el Ministerio Público Fiscal y las fuerzas de seguridad, brindando información y asistencia técnica en investigaciones relacionadas con lavado de activos y financiamiento del terrorismo. Además, mantiene relaciones de cooperación con organismos internacionales, como el Grupo de Acción

Financiera Internacional (GAFI), para intercambiar información y mejorar los estándares de prevención y represión a nivel global.

4. **Capacitación y concientización**: La UIF promueve la capacitación y la concientización sobre los delitos de lavado de activos y financiamiento del terrorismo. Organiza programas de formación dirigidos a profesionales de distintos sectores, como el financiero, legal y contable, con el objetivo de fomentar la adopción de buenas prácticas y fortalecer la prevención en estas áreas.

5. **Supervisión y control**: La UIF supervisa y controla el cumplimiento de las obligaciones establecidas por la ley de prevención de lavado de activos y financiamiento del terrorismo. Verifica que las entidades obligadas implementen medidas adecuadas de prevención y detección, y realiza inspecciones y auditorías para evaluar su cumplimiento.

En resumen, la UIF de Argentina desempeña un papel fundamental en la lucha contra el lavado de activos y el financiamiento del terrorismo. A través de sus funciones de análisis, generación de inteligencia, colaboración y supervisión, contribuye a fortalecer la integridad del sistema financiero y económico del país.

5.1.7 Superintendencia de Seguros

La Superintendencia de Seguros de Argentina (SSN) es el organismo encargado de regular y supervisar la actividad aseguradora en el país. En términos de cumplimiento tecnológico, la SSN tiene la responsabilidad de establecer normativas y exigencias relacionadas con el uso de tecnología por parte de las compañías de seguros. Algunas de las acciones que realiza la SSN en esta materia son las siguientes:

1. **Establecimiento de regulaciones y normativas**: La SSN emite normativas y reglamentaciones que establecen los requisitos técnicos y de seguridad que las compañías de seguros deben cumplir en relación con el uso de tecnología. Estas regulaciones pueden abarcar aspectos como la protección de datos personales, la ciberseguridad, la infraestructura tecnológica, entre otros.

2. **Evaluación y autorización de sistemas informáticos**: La SSN evalúa y autoriza los sistemas informáticos utilizados por las compañías de seguros para el procesamiento y almacenamiento de datos relacionados con la actividad aseguradora. Esto implica revisar la infraestructura tecnológica, los protocolos de seguridad, los procesos de respaldo y recuperación, entre otros aspectos.

3. **Supervisión y control**: La SSN realiza supervisiones y auditorías periódicas a las compañías de seguros para verificar el cumplimiento de las normativas en materia de cumplimiento tecnológico. Esto incluye la revisión de los sistemas informáticos, la seguridad de la información y el cumplimiento de las políticas y procedimientos establecidos.

4. **Recepción y gestión de denuncias**: La SSN recibe y gestiona denuncias relacionadas con incumplimientos o incidentes de seguridad tecnológica por parte de las compañías de seguros. Puede investigar y tomar medidas correctivas en caso de detectar infracciones o vulnerabilidades en el cumplimiento tecnológico.

5. **Asesoramiento y divulgación**: La SSN brinda asesoramiento y promueve la divulgación de buenas prácticas en materia de cumplimiento tecnológico. Puede emitir guías, circulares o recomendaciones para que las compañías de seguros adopten medidas adecuadas en el uso de tecnología y seguridad de la información.

En general, la Superintendencia de Seguros de Argentina se encarga de velar por el cumplimiento normativo y la seguridad tecnológica en el sector asegurador. A través de su rol regulador y supervisor, busca garantizar que las compañías de seguros utilicen la tecnología de manera segura, protejan la información de los asegurados y cumplan con los estándares establecidos en la normativa aplicable.