Aspectos éticos, legales y sociales en el uso de las tecnologías de la información: El cumplimiento tecnológico

Área
ACTUALIZACION ACADEMICA

Autor
Aníbal Mario Mazza Fraquelli - fraquelli@economicas.uba.ar

Introducción

En la era digital actual, las tecnologías de la información (TI) se han convertido en un componente esencial de la vida cotidiana, tanto a nivel personal como empresarial. Estas herramientas han transformado la forma en que nos comunicamos, trabajamos, interactuamos y accedemos a la información. Sin embargo, el crecimiento acelerado de las TI ha planteado importantes desafíos legales y éticos que deben ser abordados por las organizaciones y las personas que trabajan en ellas.

En este artículo, exploraremos la importancia del cumplimiento de las regulaciones legales en el uso de las tecnologías de la información, y analizaremos los aspectos éticos, morales, sociales y deontológicos que subyacen en esta necesidad. Comprender y cumplir con estas regulaciones es fundamental para garantizar una conducta responsable en el ámbito digital y preservar los derechos y valores fundamentales de las personas.

En primer lugar, es fundamental destacar el aspecto ético de las tecnologías de la información. Estas herramientas ofrecen innumerables beneficios y oportunidades, pero también plantean dilemas éticos complejos. El uso inadecuado o irresponsable de las TI puede dar lugar a la violación de la privacidad, la manipulación de datos, el robo de información personal y otros problemas éticos de gran magnitud. Por lo tanto, las organizaciones y las personas que trabajan en ellas tienen la responsabilidad de garantizar que sus acciones en el ámbito digital sean éticas y respeten los derechos y valores fundamentales.

En segundo lugar, las consideraciones morales también entran en juego cuando se trata del uso de las TI. Las decisiones relacionadas con la implementación y el manejo de las tecnologías de la información pueden tener un impacto significativo en las personas y en la sociedad en general. Por ejemplo, el desarrollo de algoritmos de inteligencia artificial y la automatización de procesos laborales pueden generar desafíos éticos y morales, como el reemplazo de trabajadores humanos por máquinas, el sesgo algorítmico o la discriminación algorítmica. Cumplir con las regulaciones legales en este ámbito es una forma de asegurar que las decisiones tomadas sean justas, equitativas y moralmente aceptables.

En tercer lugar, el cumplimiento de las regulaciones legales en el uso de las TI tiene un impacto directo en el ámbito social. Las TI han generado cambios profundos en la forma en que las personas se relacionan entre sí y en cómo interactúan con las instituciones y las organizaciones. Estas tecnologías han permitido la creación de comunidades virtuales, el acceso a la información global y la conectividad instantánea. Sin embargo, también han surgido problemas como el acoso en línea, el ciberbullying, la desinformación y la polarización social. Cumplir con las regulaciones legales es esencial para fomentar un entorno digital seguro, inclusivo y respetuoso, donde se promueva la convivencia pacífica y se proteja la integridad de las personas.

Por último, el cumplimiento de regulaciones legales en el uso de las TI también tiene una base deontológica. La deontología se refiere al estudio de los deberes y obligaciones morales de los individuos y las organizaciones. En el contexto de las tecnologías de la información, esto implica que las organizaciones deben seguir principios éticos fundamentales, como la transparencia, la responsabilidad, la confidencialidad y la protección de datos. Las regulaciones legales proporcionan un marco jurídico para garantizar que se cumplan estos principios y se promueva una cultura de integridad y confianza en el uso de las TI.

En resumen, el cumplimiento de las regulaciones legales en el uso de las tecnologías de la información es crucial para abordar los desafíos éticos, morales, sociales y deontológicos que surgen en este ámbito. Las organizaciones y las personas que trabajan en ellas deben asumir la responsabilidad de garantizar un comportamiento ético, moralmente aceptable y socialmente responsable en el uso de las TI.

Cumplir con las regulaciones legales no solo es una obligación legal, sino también una forma de preservar los derechos y valores fundamentales de las personas en el entorno digital en constante evolución.

Conceptos Iniciales

En el ámbito académico y en la vida cotidiana, los términos moral, ética, deontología y responsabilidad social son conceptos que desempeñan un papel fundamental en la comprensión de la conducta humana, la toma de decisiones y la forma en que interactuamos en sociedad. Aunque estos términos están relacionados, cada uno tiene su propia dimensión y significado específico. Exploraremos brevemente cada uno de estos conceptos, destacando sus diferencias y su relevancia en el ámbito académico y profesional.

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.

Debe recordarse algo importante: Lo que es "moral" para una sociedad en un determinado contexto y en una determinada época, puede 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.

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. 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**.

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.

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.

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.**

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) saber si se obtuvo de forma ilegítima y enmendar el daño que pudiera haber causado.

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.

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.

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.

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[8]:

- 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.

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

[8] Al momento de la redacción de este trabajo, junio/2023, el anteproyecto de modificación de la ley 25.326 ha ingresado a la Honorable Cámara de Diputados de la Nación.

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**.

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. Desde el surgimiento de servicios internacionales de ***hosting*** y ***housing*** que utilizan las organizaciones para sus datos, que pueden estar alojados en equipos físicos o virtuales en cualquier lugar del mundo **también se plantea un problema respecto de estándares de calidad, almacenamiento y supervisión de ésos datos**. 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. Tal situación **cobra especial relevancia si se trata de una organización cuyas controlantes son casas matrices** están sujetas a regulaciones regionales o nacionales ajenas al derecho argentino donde debe evaluarse si existe o no la colisión entre las normativas.

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.

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 internacionales y algunas nacionales de primer orden, suelen contar con equipos o roles especializados en compliance tecnológico para asegurarse de que se cumplan los estándares y requisitos relevantes, sean de orden municipal, provincial, nacional, internacional o "*corporate*" para éstas.

Es necesario que una organización en su totalidad se involucre en el compliance tecnológico debido a varios motivos fundamentales que afectan tanto a la empresa como a sus partes interesadas. En un entorno empresarial cada vez más digitalizado, el cumplimiento de las regulaciones legales y éticas en el uso de la tecnología de la información se ha convertido en una prioridad estratégica para garantizar la integridad, la transparencia y la confianza en las operaciones empresariales. Además, la participación de toda la organización en el compliance tecnológico fomenta la innovación responsable.

La tecnología está en constante evolución y las organizaciones deben adaptarse rápidamente para mantenerse competitivas. Sin embargo, la adopción de nuevas tecnologías debe ser equilibrada con la responsabilidad ética y legal. La participación activa de todos los miembros de la organización en el cumplimiento tecnológico garantiza que las decisiones relacionadas con la adopción de tecnología se realicen de manera informada, evaluando los riesgos y considerando los impactos éticos, sociales y legales.

Esto permite que la organización se beneficie de la innovación de manera responsable y sostenible, evitando posibles consecuencias negativas. Al involucrar a todos los miembros de la organización, se establece un enfoque integral que abarca desde la alta dirección hasta los empleados de todos los niveles. Esto fortalece la posición de la organización frente a los riesgos legales y éticos, mejora la confianza de las partes interesadas y promueve un entorno empresarial ético, seguro y sostenible en la era digital. 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** [9]: 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

[9] Con los conocimientos y desarrollos tecnológicos que tenemos en este momento, también debería considerarse que la propia evolución tecnológica es ineludible y que debería existir algún mecanismo proactivo que se adapte automáticamente a los nuevos avances que la tecnología trae a organizaciones y a la sociedad.

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 cumplimiento tecnológico es un aspecto **que todavía no tiene un abordaje específico dentro de las organizaciones** dado que deben considerarse elementos que podrían referirse a la utilización de las tecnologías de la información en su **aspecto duro** (hardware, software, gestión de bases de datos, ciberseguridad y demás) y otro aspecto (que podríamos denominar blando) y es el que se ocupa de entender **cómo el uso adecuado o inadecuado de los datos** puede repercutir en decisiones que las personas toman (cuando están trabajando dentro de una organización, cuyos valores pueden no coincidir con los valores, moral y ética personal de esas personas) y el **potencial daño** que esas decisiones inadecuadas pueden provocar, "alguien" o a toda la sociedad en su conjunto.

Conclusión

En este artículo hemos explorado los conceptos de moral, ética, deontología, responsabilidad social y compliance tecnológico, destacando su importancia en el contexto actual. Hemos visto cómo estos conceptos se entrelazan y juegan un papel fundamental en la toma de decisiones y en la conducta de las organizaciones y las personas que trabajan en ellas.

La **moral**, como sistema de principios y valores internos, guía nuestras acciones diarias y nuestras percepciones de lo que es correcto o incorrecto. Es un componente intrínseco de nuestra naturaleza humana y está influenciada por diversos factores, como la cultura, la religión y la educación. Aunque la moralidad puede ser subjetiva y variar entre individuos,

o en diferentes épocas y contextos, es importante reflexionar sobre nuestras creencias y valores para tomar decisiones éticas y moralmente responsables.

La **ética**, por su parte, es el estudio sistemático de la moralidad. Nos proporciona un marco teórico y conceptual para analizar y justificar racionalmente nuestras acciones. La **ética busca establecer principios y normas que puedan aplicarse de manera más amplia, trascendiendo los juicios personales**. Es a través de la ética que podemos evaluar nuestras acciones en función de su impacto en los demás y en la sociedad en su conjunto.

La **deontología**, como rama de la ética, se **enfoca en los deberes y las obligaciones morales**. Se basa en la idea de que **hay principios universales que deben guiar nuestra conducta**, y que **existen reglas y normas morales que no deben ser transgredidas**. La deontología nos insta a actuar en consonancia con nuestros deberes y responsabilidades, que busca establecer límites y salvaguardar principios éticos fundamentales.

Asimismo, hemos abordado la **responsabilidad social**, que implica reconocer la obligación de actuar éticamente y contribuir al bienestar de la sociedad en su conjunto. Las organizaciones y las personas tienen un papel activo en la promoción de la justicia social, la sostenibilidad y el respeto a los derechos humanos. La responsabilidad social va más allá del cumplimiento de las leyes y regulaciones, buscando impactar positivamente en la sociedad y en el entorno en el que operamos.

En el contexto tecnológico, el compliance juega un papel fundamental. El **compliance tecnológico** se refiere al cumplimiento de las regulaciones legales y éticas en el uso de las tecnologías de la información. En un mundo cada vez más digitalizado, las organizaciones deben asegurarse de utilizar la tecnología de manera responsable y ética, protegiendo la privacidad y la seguridad de los datos, evitando el uso indebido de la información y garantizando la equidad y la transparencia en su aplicación. El compliance tecnológico no solo es una obligación legal, sino también una necesidad para preservar la confianza y la integridad en el ámbito digital.

Es importante destacar que estos **conceptos no son estáticos**, sino que evolucionan y se adaptan a medida que la sociedad y la tecnología avanzan. La ética, la deontología y la responsabilidad social deben ser consideradas de manera dinámica, teniendo en cuenta los cambios sociales, culturales y tecnológicos que influyen en nuestras vidas. En resumen, la moral, la ética, la deontología, la responsabilidad social y el compliance tecnológico son elementos clave para una conducta ética y responsable en el ámbito personal y empresarial. Estos conceptos nos invitan a reflexionar sobre nuestras acciones, a considerar el impacto de nuestras decisiones en los demás y a actuar de manera responsable y ética. Al integrar estos principios en nuestras vidas, en nuestra vida profesional y en las organizaciones en las que trabajamos, contribuimos a la construcción de un mundo más justo, equitativo y sostenible.