Cumplimiento corporativo e inteligencia artificial: Aportes y controles en la gestión de riesgos

Liliana Vaudo*
Siro Tagliaferro**
Catherina Gallardo***
RVDM, Nro. 13, 2024, pp. 67-86

Resumen: La gestión de riesgos organizacionales destinada a hacer efectivo el cumplimiento corporativo exige un alto nivel de efectividad, de manera que los nuevos aportes tecnológicos, en especial la inteligencia artificial, constituyen herramientas que permiten optimizar esos procesos, tales como el monitoreo de actividades sospechosas, procesamiento de denuncias, diseño de indicadores de gestión. Para ello, este artículo propone un acercamiento al empleo de la inteligencia artificial en la elaboración, seguimiento, mitigación y corrección de las políticas y procedimientos en el *compliance* corporativo, así como las medidas que debe asumir para el uso correcto de la herramienta.

Palabras clave: Cumplimiento corporativo; Inteligencia artificial; Límites.

Corporate compliance and artificial intelligence: Contributions and controls in risk management

Abstract: *The management of organizational risks aimed at making corporate compliance effective requires a high level of effectiveness, so that new technological contributions, especially artificial intelligence, are tools that allow optimizing these processes, such as monitoring suspicious activities, processing complaints, designing management indicators. To this end, this article proposes an approach to the use of artificial intelligence in the elaboration, monitoring, mitigation and correction of corporate compliance policies and procedures, as well as the measures that must be taken for the correct use of the tool.*

Keywords: *Corporate compliance, Artificial intelligence; Limits.*

Recibido: 20/10/2024
Aprobado: 28/11/2024

* Abogada, Universidad Central de Venezuela. Doctora en Ciencias mención Derecho. Universidad Central de Venezuela. Especialista en Derecho Procesal. Universidad Central de Venezuela. Especialista en Ciencias Penales y Criminológicas. Universidad Central de Venezuela. Diplomado en educación virtual (Unimet). Bootcamps en competencias digitales (Unimet). Profesor Titular de la Universidad Metropolitana y Profesor Investigador. Orcid 0000-0002-6008-2066, Correo institucional lvaudo@unimet.edu.ve, . Afiliación Universidad Metropolitana, Venezuela.

** Ingeniero de Producción Universidad Metropolitana, Magister en Administración de Empresas (IESA) y Magister en Ciencia de Datos (Unimet). Profesor Asociado en Ingeniería Industrial (Unimet)Venezuela, Consultor Técnico del Observatorio de Derecho Corporativo y Buenas Prácticas Empresariales (Unimet). correo institucional staglaferro@unimet.edu.ve Afiliación Universidad Metropolitana, Venezuela.

*** Abogado. Universidad Central de Venezuela, con estudios en las especializaciones de Derecho Constitucional y Derecho Administrativo, Universidad Central de Venezuela; profesora tiempo parcial en las asignaturas: Derecho Constitucional, Sistema de Justicia Constitucional y Derecho Administrativo, Universidad Metropolitana, Venezuela, Diplomado en Urbanismo Universidad Central de Venezuela, correo institucional cgallardo@unimet.edu.ve. Afiliación Universidad Metropolitana, Venezuela.

Cumplimiento corporativo e inteligencia artificial: Aportes y controles en la gestión de riesgos

Liliana Vaudo*
Siro Tagliaferro**
Catherina Gallardo***
RVDM, Nro. 13, 2024, pp. 67-86

SUMARIO:

INTRODUCCIÓN

Cada vez resulta más frecuente e imperioso acudir a los avances de la tecnología para poder llevar a cabo los diferentes procesos dentro de las empresas; estos avances se convierten en necesarios y facilitan el desarrollo de las diferentes actividades, requiriendo la supervisión de personal capacitado y competente para que dicha implementación en el ámbito operativo y legal resulten eficientes y garanticen resultados positivos.

Para el logro de resultados favorables se requiere, igualmente, la ciberresiliencia y adaptación a los procesos mediados por la Inteligencia Artificial, debiendo concebirse como una herramienta para el logro de los fines de la empresa, que puede utilizarse en el seguimiento y mitigación de riesgos en el cumplimiento organizacional, facilitando la optimización tecnológica; por lo cual es importante que en los sistemas de gestión de *compliance* se dé cumplimiento tanto al ordenamiento jurídico positivo -que sobre Inteligencia Artificial aún en Venezuela no se cuenta con normas positivas sobre el tema- y las recomendaciones derivadas de las normas de estandarización, especialmente las específicas y todas aquellas vinculadas a la protección de datos.

* Abogada, Universidad Central de Venezuela. Doctora en Ciencias mención Derecho. Universidad Central de Venezuela. Especialista en Derecho Procesal. Universidad Central de Venezuela. Especialista en Ciencias Penales y Criminológicas. Universidad Central de Venezuela. Diplomado en educación virtual (Unimet). Bootcamps en competencias digitales (Unimet). Profesor Titular de la Universidad Metropolitana y Profesor Investigador. Orcid 0000-0002-6008-2066, Correo institucional lvaudo@unimet.edu.ve, . Afiliación Universidad Metropolitana, Venezuela.

** Ingeniero de Producción Universidad Metropolitana, Magister en Administración de Empresas (IESA) y Magister en Ciencia de Datos (Unimet). Profesor Asociado en Ingeniería Industrial (Unimet)Venezuela, Consultor Técnico del Observatorio de Derecho Corporativo y Buenas Prácticas Empresariales (Unimet). correo institucional staglaferro@unimet.edu.ve Afiliación Universidad Metropolitana, Venezuela.

*** Abogado. Universidad Central de Venezuela, con estudios en las especializaciones de Derecho Constitucional y Derecho Administrativo, Universidad Central de Venezuela; profesora tiempo parcial en las asignaturas: Derecho Constitucional, Sistema de Justicia Constitucional y Derecho Administrativo, Universidad Metropolitana, Venezuela, Diplomado en Urbanismo Universidad Central de Venezuela, correo institucional cgallardo@unimet.edu.ve. Afiliación Universidad Metropolitana, Venezuela.

En este orden de ideas, se analizan algunas normas europeas que pueden orientar las buenas prácticas y la prevención de delitos, debido a que el territorio europeo se encuentra sujeto al control de organismos que cumplen funciones de seguridad como la Agencia Europea para la Ciberseguridad y Centro Europeo de Ciberdelincuencia (Europol); estableciendo cooperación con instituciones, organizaciones y Estados para garantizar la protección de las personas y gobiernos en la unión.

La inexistencia de disposiciones legales en el territorio venezolano, no pueden ser utilizadas como excusas para la no adopción voluntaria de medidas en los sistemas de gestión de cumplimiento, ya que, los daños que pueda ocasionar la vulneración de derechos por omisión o mal uso de la herramienta, perjudican la productividad y la imagen corporativa. [1] Ello, al margen de sectores en los cuales la existencia de ordenamientos jurídicos especiales pudiera incluir regulaciones indirectas a la inteligencia artificial, como sucede en el ámbito de telecomunicaciones. Por ejemplo, la Ley de Responsabilidad Social en Radio, Televisión y *Medios Electrónicos* pudiera aplicarse desde el punto de vista de los contenidos transmitidos por empresas que prestan servicios de internet y otras que operan en el sector.

1. *La Inteligencia Artificial como herramienta de optimización de procesos dentro de la empresa*

Es conocido, que el *compliance* organizacional está conformado por una cultura de cumplimiento tanto normativo como ético, legal, social y de convivencia corporativa, que persigue tanto prevenir como contrarrestar los riesgos operativos y legales tanto en la prevención como en la mitigación de situaciones que puedan generar daño o pongan en peligro la tutela del medio ambiente, los derechos humanos y la reputación, productividad y rendimiento de los negocios.

En tal sentido, los avances tecnológicos son bienvenidos para facilitar la implementación, seguimiento y mitigación de riesgos, siendo la inteligencia artificial un instrumento cuyo uso ético y correcto puede aportar de manera positiva en la optimización de estos procesos. Por ejemplo, empleando inteligencia artificial se pueden automatizar procesos de seguimiento en el ámbito de la debida diligencia, lo cual aumenta la productividad y puede incluso reducir tiempo y costos operativos.

El *compliance* está llamado a cumplir con el ordenamiento jurídico positivo y las recomendaciones de los órganos y normas de estandarización en materia de protección de datos, como ocurre por ejemplo con el Reglamento General de Datos que orienta las exigencias en la materia en la Unión Europea. Lo anterior viene a reforzar todo lo atinente a gestión de datos personales, su acceso, rectificación y supresión (En Venezuela a través de la acción de *habeas data***,** prevista en la Constitución, artículo 28, existe el derecho a acceder al contenido sobre la propia información que curse ante un organismo y pedir su

[1] Actualmente se discute en la Asamblea Nacional venezolana, la Ley para Regular el uso de la Inteligencia Artificial, el cual fue aprobado en su primera discusión, en sesión del 19 de noviembre de 2024. Cuya finalidad, conforme a su artículo 2, numeral 1° será la de garantizar que los sistemas que utilicen IA sean seguros, transparentes, trazables, no discriminatorios y respetuosos de la Constitución, en aras de la seguridad jurídica, la innovación y mejoras de la gestión pública y privada con base a sus numerales 3° y 4°.

corrección y destrucción. Por ejemplo, en España, el contenido del Reglamento ha sido desarrollado a través de la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales.

Por ejemplo, se puede citar el caso a que hace referencia la sentencia del 5 de febrero de 2020, dictada por el Tribunal de Distrito de La Haya, el cual suspendió por razones de protección de derechos humanos, un sistema de detección de fraudes de asistencia social, el cual era utilizado por el gobierno en los Países Bajos, el cual llevaba por nombre "System Risk Indication" (SyRI), al excluir a personas que pertenecían a barrios pobres; de manera que se generaron limitaciones al uso de la inteligencia artificial. En tal sentido, las consideraciones de nulidad van referidas a la protección de datos.

Respecto a la protección de datos, Gamero (CincoDías, 12/04/2021) refiere la existencia de dos documentos emitidos por la Agencia Española de Protección de Datos (AEPD) en los cuales se establece el deber de preservar el derecho a la protección con la "Adecuación al RGPD de tratamientos que incorporan inteligencia artificial (2020)' así como respecto de los "Requisitos para auditorías de tratamientos que incluyan inteligencia artificial (2021)" cuyo incumplimiento puede conllevar la aplicación de sanciones, ya que, los algoritmos empleados no son claros y comprensibles (Ej. Los llamados algoritmos de caja negra).[2]

También cabe destacar su impacto en el sector financiero en el cual el Gen IA o inteligencia artificial generativa, puede transformar, agilizar y producir eficiencia respecto de los servicios que presta la entidad y los productos que ofrece. Así lo reseña la firma KPMG, quien luego de una encuesta realizada a un grupo de empresarios, reveló que los bancos han comenzado a ver a la inteligencia artificial generativa como una capacidad real. En ese orden de ideas, la mitad de los encuestados opinó que, para finales de 2024, entre 1% - 5% de las tareas diarias podrán ser realizadas por Inteligencia Artificial y de esta mitad, el 37% consideró un porcentaje mayor que pudiera llegar al 20% de sus actividades. [3]

En la referida encuesta, destaca, además que las instituciones financieras encuestadas han incorporado soluciones de inteligencia artificial generativa en su parte operativa, especialmente en las siguientes:

- Ciberseguridad, el 67% de los entrevistados;
- Prevención de fraude, el 51% de los encuestados
- *Compliance* y Riesgos, el 41%.
- Servicio al cliente 42%

La encuesta elaborada por KPMG, indica, sin embargo, la importancia de actuar de manera cautelosa, incorporando medidas de prevención y mitigación de eventuales impactos que pueda generar la inteligencia artificial generativa en el ámbito operativo,

[2] Gamero, Eduardo (2021) La *necesidad del compliance en la inteligencia artificial.* CincoDías, 12/04/2021. https://artificial cincodias.elpais.com/cincodias/2021/04/09/legal/1617964412_071507.html
[3]KPMG (2024) *Future-proofing banking: The Enterprise transformation imperative* *https://kpmg.com/us/en/articles/2024/2024-us-banking-industry-outlook-survey.html*

debiendo implementar los correspondientes programas de adiestramiento y formación, sobre el uso ético de la herramienta.[4]

Para Vaudo, las empresas deben implementar políticas "para la protección y seguridad de la información, a través de las cuales se establezcan lineamientos basados en estándares nacionales e internacionales, de cómo se almacenan y transmiten datos a través de diferentes mecanismos"[5].

De igual manera adquiere relevancia la recomendación dictada por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (en adelante UNESCO) denominada: "Recomendación sobre la Ética de la Inteligencia Artificial" (2022) basada en la tutela de derechos fundamentales de los ciudadanos en la protección de su dignidad y la transparencia en el uso de la inteligencia artificial. En dicha recomendación, la UNESCO considera que la ética es la "base dinámica para la evaluación y la orientación normativas de las tecnologías de la IA, tomando como referencia la dignidad humana, el bienestar y la prevención de daños y apoyándose en la ética de la ciencia y la tecnología", indicando además que debe considerarse a la ética de la inteligencia artificial como;

> una reflexión normativa sistemática, basada en un marco integral, global, multicultural y evolutivo de valores, principios y acciones interdependientes, que puede guiar a las sociedades a la hora de afrontar de manera responsable los efectos conocidos y desconocidos de las tecnologías de la IA en los seres humanos, las sociedades y el medio ambiente y los ecosistemas, y les ofrece una base para aceptar o rechazar las tecnologías de la IA. [6]

2. *Ley de Inteligencia Artificial de la Unión Europea*

Según refiere Beltrán[7], la Unión Europea se ha preocupado por los problemas que pueden surgir en esa comunidad de naciones, derivadas de la implementación de la Inteligencia Artificial, por lo que ha indicado:

> La Unión Europea (UE), en el marco de su estrategia digital, está tramitando una Ley de Inteligencia Artificial (IA) que, entre otros propósitos, aspira contener los efectos de esta amenaza Esta norma pretende establecer obligaciones para proveedores y usuarios en función del nivel de riesgo de la IA, estando a la espera de la redacción definitiva.

El mencionado autor, en su trabajo, ha igualmente manifestado:

> En términos estrictamente jurídicos, al menos, obliga a plantearse si el concepto de acto propio y voluntario queda en entredicho. Y, de forma derivada, si también

[4] KPMG (2024) *Future-proofing banking: The Enterprise transformation imperative* https://kpmg.com/us/en/articles/2024/2024-us-banking-industry-outlook-survey.html

[5] Vaudo, Liliana (2023) *Integración normativa para la gestión de riesgos sobre sistemas de información empresarial* Revista Venezolana de Legislación y Jurisprudencia. Nro 21. Diciembre 2023. Ps: 151-174. https:// rvlj.com.ve/?page_id=3142

[6] Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (2022): "Recomendación sobre la Ética de la Inteligencia Artificial" https:// www.unesco.org/es/articles/recomendacion-sobre-la-etica-de-la-inteligencia-artificial

[7] Beltrán, Ignasi (2023) *Algoritmos y condicionamiento por debajo del nivel consciente: un análisis crítico de, la propuesta de ley de Inteligencia Artificial de la Unión Europea*, Revista de la Facultad de Derecho de México,Número 286. DOI: https://doi.org/10.22201/fder.24488933e.2023.286.86406

> impacta en el de culpa y responsabilidad. Si, realmente, estamos hablando de herramientas efectivas que trascienden la conciencia es posible que necesitemos un marco jurídico que (paradójicamente) nos dé amparo frente a nosotros mismos y, obviamente también, frente a quienes quieran aprovecharse de nuestros actos por debajo de dicho umbral [8]

Estos argumentos, llevan a plantear nuevas formas de responsabilidad frente a posibles conductas o ciberataques generados a través del empleo de la Inteligencia Artificial y cuyas consecuencias pongan en peligro o lesiones los derechos de los ciudadanos y puedan llegar a afectar el propio sistema económico.

2.1. Parámetros de seguridad de los sistemas de inteligencia artificial según la Ley de la Unión Europea

La ley establece los diferentes niveles de seguridad para los sistemas que utilizan inteligencia artificial en sus procesos. En tal sentido, realiza una clasificación de los sistemas según su riesgo, estableciendo al efecto cuatro categorías, tomando en cuenta su riesgo potencial para las personas y la sociedad:

- Sistemas de IA de riesgo bajo: Estos sistemas son los que tienen un riesgo bajo de causar daño. No están sujetos a ninguna norma específica, pero deben cumplir con los principios generales de la Ley de IA.
- Sistemas de IA de riesgo moderado: Estos sistemas son los que tienen un riesgo moderado de causar daño. Están sujetos a una serie de requisitos específicos, como la realización de una evaluación de riesgos, la implementación de medidas de seguridad y la designación de un responsable de la IA.
- Sistemas de IA de riesgo alto: Estos sistemas son los que tienen un riesgo alto de causar daño. Están sujetos a requisitos aún más estrictos, como la realización de una evaluación de riesgos exhaustiva, la implementación de medidas de seguridad adicionales y la supervisión por parte de una autoridad independiente.

Es importante señalar, que la referida norma contiene una serie de prohibiciones: respecto al uso de sistemas de inteligencia artificial para fines específicos, tales como:

- La puntuación de personas o grupos de personas.
- El uso de datos biométricos para identificar a personas sin su consentimiento.
- La manipulación de las emociones de las personas.

Por otra parte, la Ley europea de Inteligencia Artificial establece una serie de principios generales que deben respetarse en el desarrollo, el uso y la aplicación de la inteligencia artificial. Estos principios incluyen:

- Seguridad: Los sistemas de IA deben ser diseñados y desarrollados de manera que se minimice el riesgo de daño para las personas y la sociedad.
- Transparencia: Los sistemas de IA deben ser transparentes en su funcionamiento y en sus resultados.

[8] Beltrán, Ignasi (2023). Op cit. P. 6.

- Trazabilidad: Los sistemas de IA deben ser trazables, de modo que se pueda identificar y comprender su origen y funcionamiento.
- No discriminación: Los sistemas de IA no deben discriminar a personas o grupos de personas por motivos de raza, género, orientación sexual, religión, etc.
- Respeto a los derechos humanos: Los sistemas de IA deben respetar los derechos humanos, como el derecho a la privacidad, el derecho a la igualdad y el derecho a la no discriminación.

2.2. Otras regulaciones europeas

El marco legal que utiliza la Unión Europea para imponer sanciones por ciberataques se basa en varias herramientas:

- Reglamento (UE) 2019/796: Este reglamento establece el marco amplio para la aplicación de medidas restrictivas (sanciones) en respuesta a ciberataques que supongan una amenaza para la Unión Europea o cualquiera de sus estados miembros. Permite a la Unión Europea imponer una serie de sanciones, como restricciones de viaje y congelación de actividades y cuentas a personas y organizaciones, incluyendo empresas, involucradas en ataques cibernéticos.
- Directiva NIS2: Esta normativa está destinada a impulsar la resiliencia de la Unión Europea y sus estados, frente a los posibles ciberataques. Esta Directiva NIS2, contempla una serie de requisitos más rigurosos en materia de ciberseguridad para los proveedores de servicios digitales y los operadores de servicios esenciales, estableciendo regulaciones respecto a gestión de riesgos, por lo cual no se centra específicamente en la parte sancionatoria.
- Política Exterior y de Seguridad Común (PESC): Esta política de seguridad común a los estados miembros de la unión, proporciona un marco más amplio con relación a la acción exterior de la Unión Europea, que va a incluir la imposición de sanciones.

Algunas de las sanciones que podrá imponer la Unión Europea, frente a la producción de ciberataques podrán consistir en:

- Congelación de activos: Relacionadas con actividades ejecutadas por individuos y organizaciones -incluyendo empresas- que resulten implicadas en ciberataques, pudiendo la unión congelar sus cuentas y afectar sus transacciones financieras.
- Restricciones de viaje: Por ejemplo, para evitar que personas que puedan encontrarse enfermas o poseen alguna prohibición de acceder a la Unión Europea, viajen a territorio de sus estados miembros.
- Prohibiciones dirigidas contra la realización de negocios: Siendo posible imponer limitaciones a la capacidad de las empresas pertenecientes a la Unión Europea, para realizar negocios con personas y organizaciones que se encuentren sancionadas.
- Embargos de armas: En situaciones graves que puedan involucrar la comisión de delitos de tráfico, armas para grupos o actividades terroristas que pongan en peligro la estabilidad de la Unión Europea, ésta tendrá derecho a impulsar embargos de armas de los países involucrados en los ataques o conspiraciones..

2.2.1. Normas vinculadas con la Ciberresilencia

Los ciberataques y la ciberdelincuencia están incrementándose en todo el territorio de la Unión Europea, siendo cada vez más sofisticados; siendo que esta tendencia seguirá agravándose en el futuro, más cuando se espera que para el próximo año una cifra superior a 40.000 dispositivos telefónicos esté conectados sólo en la unión, En tal sentido, cabe recordar que las ciberamenazas más comunes son:

- Los Malware: Cualquier software malicioso diseñado para infiltrarse en sistemas y causar daño, como virus, gusanos, troyanos y los que pueden hurtar datos, espiar a los usuarios o dañar el hardware.
- El Phishing: Que son ataques destinados a engañar a las personas para que revelen información confidencial, como contraseñas o datos financieros, a través de correos electrónicos falsos, mensajes de texto o sitios web fraudulentos.
- La Ingeniería social: Son ataques que explotan la confianza y la interacción humana para obtener acceso a sistemas o información de modo fraudulento.
- Los ataques a las cadenas de suministro; Sobre los proveedores o socios de una organización para acceder a sus sistemas y datos.
- Desinformación y propaganda: La difusión intencional de información falsa o engañosa con el objetivo de manipular la opinión pública o causar daño
- Criptohacking: El uso no autorizado de dispositivos para minar criptomonedas, ralentizando los sistemas y aumentando los costos de energía.

Motivado a estas y otras conductas perjudiciales a los sistemas, en el mes de octubre de 2020, la Unión Europea solicitó mejoras para su capacidad de control, con el fin de

- Proporcionar un entorno de comunicación seguro, a través de la encriptación cuántica;
- Protegerse contra ciberamenazas
- Garantizar el acceso a los datos para efectos judiciales**.**

Por cuanto la ciberseguridad incluye las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de dichos sistemas y de otras personas afectadas por las ciberamenazas, el Consejo de Europa adoptó en marzo de 2022, las denominadas Conclusiones sobre la Estrategia de Ciberseguridad. En estas conclusiones, el Consejo destacó que la ciberseguridad es esencial para construir una Europa resiliente, ecológica y digitalmente, por lo cual se estableció como fin el de lograr la autonomía estratégica preservando la economía abierta a través de la adopción de decisiones autónomas en el ámbito de la ciberseguridad.

Con base en lo anteriormente expuesto, ya se encontraba en vigor desde 2019, el Reglamento sobre la Ciberseguridad de la Unión Europea, el cual había establecido un mandato de la Agencia de la Unión Europea para la Ciberseguridad y algunas medidas sobre certificación y seguridad, tales como:

- Certificación de productos y servicios: Implementa un esquema europeo de certificación de la ciberseguridad para garantizar la calidad y fiabilidad de los productos y servicios digitales.

- Incidentes de ciberseguridad: Establece mecanismos de notificación y respuesta a incidentes de ciberseguridad, para una detección temprana y una gestión eficaz de las crisis.
- Cooperación entre los Estados miembros: Fomenta la cooperación entre los Estados miembros y las instituciones de la UE para compartir información y coordinar acciones en materia de ciberseguridad.
- Sensibilización y formación: Promueve la concienciación y la formación en ciberseguridad para todos los ciudadanos y profesionales.

Lo que más destaca de la creación de reglamentos en esta materia, radica en:

- Busca proteger la infraestructura crítica de sistemas esenciales como la energía, el transporte y las comunicaciones
- Persigue minimizar el impacto de incidentes negativos que generen pérdidas económicas y reputacionales.
- Se busca aumentar la confianza en el entorno digital.
- El fomento de la innovación hacia nuevas tecnologías y soluciones digitales.

Por otra parte, es aplicable a todos los productos que están conectados directa o indirectamente a otro dispositivo o red, también vehículos autodirigidos. Para lograr un sistema de gestión de riesgos seguros a partir de los reglamentos y estándares, se debe atender a:

- Una evaluación de riesgos que persiga identificar, evaluar y mitigar las amenazas y vulnerabilidades a las que está expuesta la empresa.
- Implementar medidas de seguridad para proteger los sistemas y datos.
- Contar con planes de respuesta a incidentes para recuperarse de incidentes a través de ciberseguridad.
- Formación continua y concientización del personal
- Fomentar la cooperación entre las organizaciones públicas y privadas.

Asimismo, con fundamento en la Ley de Ciberresilencia de la Unión Europea (2024)[9], la cual aún no está vigente, la ciberresilencia tiene como objetivo el de proteger a las personas y a las empresas que compran o de cualquier forma adquieren o utilizan productos y software, contentivos de componentes digitales. Esta norma contiene una serie de requisitos obligatorios de ciberseguridad, que abarcan tanto a los fabricantes como a los minoristas de dichos productos. De la Ley se infiere que las características de seguridad insuficientes se convertirían en cosa del pasado; debido a que la protección que se exige actualmente se extiende a todo el ciclo de vida del producto. Si bien se trata de un reglamento que aún no ha entrado en vigor, según la norma se persigue garantizar:

- Normas armonizadas a la hora de comercializar productos o programas informáticos con un componente digital;
- Marco de requisitos de ciberseguridad que rijan la planificación, el diseño, el desarrollo y el mantenimiento de dichos productos, con obligaciones que deben cumplirse en todas las fases de la cadena de valor;
- Obligación de garantizar el deber de diligencia durante todo el ciclo de vida de dichos productos.[10]

[9] Comisión Europea (2024) Ley de Ciberresiliencia de la Unión Europea. https:///digital-strategy.ec.europa.eu/es/policies/cyber-resilience-act
[10] Comisión Europea (2024) Op cit.

Cuando la norma entre en vigor, los programas informáticos y los productos conectados a internet llevarán el marcado CE para indicar que cumplen las nuevas normas. Por otra parte, al exigir a los fabricantes y minoristas que prioricen la ciberseguridad, los clientes y las empresas estarían facultados para tomar decisiones mejor informadas, seguros de las credenciales de ciberseguridad de los productos con el marcado CE.

En tal sentido, se identifican siete etapas de un ciclo de vida, dirigidas a mejorar la ciberresiliencia; a saber:

- Etapa 1 - Estrategia: estructura, capacidad de detección y ciber gobierno para anticipar y abordar eventos empresariales o cibernéticos adversos.
- Etapa 2: Resistir: un marco de ciberdefensa adaptable y de misión preservada que pueda resistir las amenazas a la empresa.
- Etapa 3: Proteger: Protegerse contra ciberataques disruptivos utilizando una inmunidad digital fuerte y autorreparable, así como una ciberdefensa activa.
- Etapa 4 - Inspección: Cibervisibilidad de amenazas en tiempo real a través de detección añadida por máquinas, caza automatizada y conocimiento avanzado de la situación.
- Etapa 5: Observar: Confianza en la automatización, el aprendizaje automático y la detección adaptativa de ciberamenazas para hacer frente a futuras amenazas para la empresa.
- Etapa 6 - Recuperación: la capacidad de restaurar y adaptar rápidamente las plataformas digitales, los sistemas de misión crítica y evitar interrupciones de la actividad empresarial.
- Etapa 7 - Adaptación: Evaluar y medir continuamente el estado del rendimiento cibernético para apoyar a la empresa.

2.2.2. Lucha de la Unión Europea contra la ciberdelincuencia

La Unión Europea también ha emitido una Directiva destinada a frenar la ciberdelincuencia, buscando que la unión sea tecnológicamente neutral. La Directiva abarca tanto los pagos tradicionales como transferencias bancarias, cheques, nuevas formas de pago tal como el dinero electrónico, pagos móviles y monedas virtuales. La norma busca armonizar definiciones como lo que se entiende por delitos en línea, el establecimiento de normas estandarizadas para las penas corporales, prestación de asistencia y apoyo a las víctimas y alcance de las competencias para combatir el fraude transfronterizo de manera eficaz.

También se tiene que en el mes de diciembre de 2020 entró en vigor el Código Europeo de las Comunicaciones Electrónicas (CECE), el cual introdujo una nueva definición de servicios de comunicaciones electrónicas que incluye los «servicios de comunicaciones interpersonales independientes de la numeración», de los que forman parte los servicios de mensajería. En tal sentido, algunos de los proveedores de servicios de comunicaciones interpersonales independientes de la numeración, han empleado tecnologías específicas para encontrar material de abuso sexual de menores en sus servicios, motivo por el cual se han visto en la necesidad de tomar medidas eficaces para prevenir y mitigar estos riesgos, tales como el retiro del material y la denuncia ante las autoridades.

2.3. Organismos de la Unión Europea para la Ciberseguridad

2.3.1. La Agencia de la Unión Europea para la Ciberseguridad

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) es una organización creada para garantizar un alto nivel común de ciberseguridad en toda Europa. Actúa como un centro de excelencia en ciberseguridad, proporcionando asistencia técnica y operativa a los Estados miembros, a las instituciones de la UE y a los ciudadanos europeos.

ENISA realiza diversas actividades para cumplir su misión, entre las que destacan:

- Análisis de amenazas: Identifica y analiza las últimas tendencias en ciberamenazas para anticipar los riesgos futuros.
- Desarrollo de directrices: Elabora directrices y recomendaciones para mejorar la ciberseguridad en diferentes sectores.
- Organización de actividades de formación: Ofrece formación y capacitación a profesionales de la ciberseguridad.
- Cooperación internacional: Colabora con organizaciones internacionales para abordar los desafíos cibernéticos a nivel global.

Dentro de las funciones mas relevantes de la ENISA son las siguientes :

- Contribuir a la política de seguridad cibernética de la UE: ENISA trabaja en estrecha colaboración con las instituciones europeas para desarrollar y aplicar políticas de ciberseguridad efectivas.
- Mejorar la confianza en los productos y servicios digitales: A través de programas de certificación de la ciberseguridad, ENISA ayuda a garantizar la fiabilidad de los productos y servicios digitales que utilizamos a diario.
- Cooperar con los Estados miembros: Facilita el intercambio de información y la cooperación entre los Estados miembros en materia de ciberseguridad, para una respuesta más coordinada ante las amenazas.
- Preparar a Europa para los desafíos futuros: Anticipa las nuevas amenazas cibernéticas y desarrolla estrategias para hacer frente a los desafíos emergentes.

Una de las legislaciones mas importas de la ENISA fue la creación de la Directiva SRI NIS2, la cual entró en vigor el 16 de enero de 2023, la cual presenta un hito importante en la lucha contra las ciberamenazas.

2.3.2. El Centro Europeo de Ciberdelincuencia (Europol)

El Centro Europeo de Ciberdelincuencia (EC3) es una unidad especializada de la Europol, la agencia de la Unión Europea que supervisa la cooperación policial. Esta oficina tiene como objeto coordinar la lucha contra la ciberdelincuencia a escala europea, protegiendo a ciudadanos, empresas y gobiernos contra las amenazas digitales.

Algunas de las principales actividades que lleva a cabo el EC3 son las siguientes:

- La recopilación y el análisis de información: El EC3 actúa como un órgano de inteligencia, recopilando datos sobre las últimas tendencias en ciberdelincuencia, identificación de autores de delitos
- Coopera con los Estados miembros de la Unión Europea para combatir el crimen organizado digital.
- Se encarga de dar apoyo operativo y técnico a las investigaciones en la materia.
- Imparte formación para sensibilizar a los agentes de los estados encargados del sistema de justicia; en áreas como: Ataques a infraestructuras críticas; explotación sexual infantil; delitos financieros en línea y ataques a empresas y gobiernos.

Muchos de los casos investigados por el Centro Europeo contra la Ciberdelincuencia, no se publica dado que se trata de:

- Algunas operaciones que aún están en curso y podría comprometerse la operación.
- Para proteger a las víctimas, especialmente cuando se trata de explotación sexual, pornografía infantil o trata de personas.
- Para descubrir las tácticas empleadas por los cibercriminales

En todo caso, la prolífera normativa europea puede servir de ejemplo para la adopción en Venezuela de normas y mecanismos que garanticen la seguridad en el uso de la Inteligencia Artificial.

3. Los aspectos clave de los estándares contenidos en las normas de la serie ISO 27000 e ISO 42001

Las ISO 27001 (2019)[11] y 27002 (2022)[12], establecen una serie de principios generales para la gestión de la seguridad de la información, en tanto que la Ley de Inteligencia Artificial de la Unión Europea refuerza algunos de estos principios, como la transparencia, la trazabilidad y la no discriminación. Las organizaciones deben tener en cuenta estos principios a la hora de implementar su Sistema de Gestión de Seguridad de la Información que incluye la identificación de riesgos y los procedimientos para mitigar y corregir posibles errores.

En general, la Ley de Inteligencia Artificial de la Unión Europea puede ayudar a las organizaciones a implementar un Sistema de Gestión de Seguridad de la Información -en adelante SGSI- más completo y eficaz, en tanto que aquellas que ya han implementado un SGSI pueden revisarlo para asegurarse de que cumple con los requisitos de la ley. Un buen programa debe contener las siguientes fases:

- Planeación
- Implementación
- Comprobación
- Actuación

[11] Organización Internacional de Normalización.(2019). Norma ISO 27001 sobre la Seguridad de la Información.. “On Information Security”. Disponible en: https://www.iso.org/standard/82875.htm,
[12] Organización Internacional de Normalización 2022. (2022). Norma ISO 27002 sobre la Seguridad de la Información.. “On Information Security”. Disponible en: https://www.iso.org/standard/82875.htm,

Además, está la Norma ISO 27015, también de la Organización Internacional de Normalización, que determina la orientación de las organizaciones que llevan a cabo una prestación de servicios financieros o Fintech, con el objetivo de servir de mejorar la gestión de seguridad de la información de sus activos, bases de datos, clientes, entre otros.

Las empresas del sector financiero se están centrando tanto en redes más abiertas como en prestar servicios de banco electrónico y móvil, lo que quiere decir que en este momento se enfrentan a unos retos nuevos sobre las amenazas de seguridad de la información como el *malware*, ataques cibernéticos y *phising*.

Con la aplicación de la ISO 27015-2014 [13] las empresas financieras:

- Mejorar la seguridad de la información: reduce los riesgos e impactos a los datos financieros y de los clientes.
- Fortalece la confianza de los clientes: demuestra el compromiso de la empresa con la seguridad de la información.
- Aumenta la eficiencia operativa: optimiza los procesos de gestión de la seguridad de la información.
- Facilita el cumplimiento legal: ayuda a cumplir con las regulaciones de protección de datos.
- Promueve la mejora continua: establece un marco para la revisión y mejora continua del sistema de gestión de la seguridad de la información.

3.1. Modo en el cual la serie ISO 27000 puede contribuir con el cumplimiento normativo

Una organización que utiliza un sistema de inteligencia artificial de riesgo moderado que debe tomar decisiones sobre sus trabajadores, deberá realizar una evaluación del mismo para identificar los niveles de peligro relacionados con el uso de este sistema. La organización debe implementar medidas de seguridad para mitigar estos riesgos, como la transparencia, la ética, la debida diligencia, el respeto de los derechos de quienes acceden y la trazabilidad de las decisiones tomadas por el sistema.

Una organización que utiliza un sistema de IA de alto riesgo para procesar datos personales debe designar un responsable de la IA., con la formación y competencia requeridas, a fin de garantizar que el sistema se utilice de manera ética y responsable. Del mismo modo, debe puntuar a los usuarios para asegurarse de que el sistema no discrimina a las personas por motivos de raza, género, orientación sexual, religión o cultura.

Relacionado con la protección de datos tecnológicos, Vaudo, en una investigación relacionada a las empresas Fintech del sector bancario venezolano, adopta algunos criterios generales que aplican también a cualquier empresa que utilice tecnología que incluye el empleo de la Inteligencia artificial, considerando que debe asegurarse la protección de los datos de la empresa y sus clientes, por lo cual se indican algunos aspectos que se deben observar, destacando:

[13] Organización Internacional de Normalización 2014. Norma ISO 27015 sobre la Seguridad de la Información.. “On Information Security”. Disponible en: https://www.iso.org/standard/82875.htm,

• Preservación de la información y documentos por un lapso de por lo menos cinco años
• La exactitud de los datos que revelen la verdadera situación de la empresa o de los operarios y clientes
• Integración de las diferentes fuentes de información
• Confidencialidad
• Protección y seguridad, para prevenir la posible alteración fraudulenta de los datos,
• Canales de denuncia e investigación frente a posibles desvíos, adulteración o mal uso de la información
• Realizar copias de seguridad, ante posible intrusión de hackers a través de diferentes mecanismos como firewalls, antivirus, navegación privada
• Respuesta oportuna ante errores producidos por fallas tecnológicas
• Encriptación de información para proteger los datos almacenados y su ulterior bloqueadores de ventanas emergentes
• Uso de plataformas tecnológicas privadas (VPN)
• Reportar la ocurrencia de posibles actividades sospechosas ante el Oficial de cumplimiento.
• Incorporar los reconocimientos faciales, códigos de barra y QR, sistemas de blockchain para garantizar efectividad en la prevención (2024, p. 9).

Algo importante que hay que destacar, es que la tecnología es el mejor recurso para establecer un canal de denuncia eficaz para la empresa. Si bien pueden establecerse canales de denuncia a través de un buzón o por vía telefónica, es mucho más seguro y efectivo el uso de correos electrónicos de los que se encargue el órgano de investigaciones internas, los cuales deben estar protegidos y separados del resto de la información que manejan otros órganos dentro de la sociedad mercantil.

También pudiera establecerse una aplicación a través de la web o un formulario que utilice tecnología de la información para gestionar un canal de denuncia, debiendo ofrecer seguridad a los informantes para garantizar su empleo. Todos los grupos de interés internos deben ser puestos en conocimiento de este mecanismo de información y de la seguridad que ofrece el canal de denuncia, a fin de garantizar que se realicen las investigaciones internas correspondientes frente a una situación que pudiera considerarse una actividad sospechosa que pueda afectar a la empresa, al entorno o a la colectividad y posiblemente constituya un ilícito administrativo, e incluso, un delito.

En todo caso, se deberá elaborar dentro de la normativa un protocolo de actuación, indicando a quién corresponde gestionar las denuncias. Similar al canal interno, se puede establecer un canal externo con características comunes, a través del cual los *stakeholders* externos puedan interponer quejas o denuncias que ameritan ser investigadas.

Las empresas que utilicen este tipo de tecnología, aparte de los órganos de supervisión como los oficiales de cumplimiento, deben contar con un equipo tecnológico que adiestre al personal y operarios del sistema, debiendo establecerse mecanismos de seguridad suficientes para garantizar la fiabilidad y cualquier modalidad de fraude.

3.2. Contenido de la Norma ISO 42001-2023

En lo que se refiere a los de Sistemas de Gestión de Inteligencia Artificial, la Norma ISO 42001-2023 [14], se constituye en un mecanismo de apoyo dirigido al uso debido de la inteligencia artificial, apoyando la gestión previa de los riesgos potenciales y su impacto social.

En este orden de ideas se debe comprender que la Inteligencia Artificial puede ser utilizada en la actividad laboral empresarial fortaleciendo la productividad y eficiencia, mejorando la seguridad digital y también la física (cuando se emplea, por ejemplo, en medicina robótica) lo cual se traduce en mejoras de servicios al cliente, fortaleciendo sectores como la industria, agricultura, medicina, energía, favoreciendo la toma de decisiones.

Como contrapartida, sin embargo, su desarrollo permite que disminuya el costo de los ataques cibernéticos y estos se lleven a cabo con mayor facilidad, especialmente contra los usuarios, afectando su privacidad y haciéndolos víctima de conductas delictivas, mediante ataque de equipos de emergencia médica, en las cadenas de alimentos, tránsito terrestre, actividades financieras, circulación de información falsa y hurto de información privilegiada.

Por los motivos anteriores, es importante que se elaboren matrices de riesgo para clasificar el nivel de riesgo desde los riesgos inaceptables, como por ejemplo los que amenacen derechos humanos como la discriminación, las amenazas a los medios de subsistencia; riesgos altos como los que pueden afectar al sistema financiero; riesgos limitados como los vinculados con calidad de productos, falsificaciones; y, los riesgos menores o mínimos que se identifican con spam, video juegos o propaganda no deseada.

La norma ISO 42001, aplica a todo tipo de empresa, contribuyendo a la obtención de certificación, previa comprobación a través de los mecanismos que la norma establece y de los que se desprenda el buen uso ético y transparente que hace la empresa de la inteligencia artificial.

Esta norma se relaciona con la Norma ISO/IEC 23053: la cual desarrolla el marco de aprendizaje de la inteligencia artificial y sobre el aprendizaje automático. También se vincula con la Norma ISO/IEC 23894: que brinda apoyo sobre la correcta gestión de riesgos operativos y legales.

La Norma ISO/IEC 42001 tiene como fin el de garantizar el desarrollo y uso responsable de la inteligencia artificial, por lo cual se recomienda que los órganos de cumplimiento que deben desarrollar las políticas de cumplimiento y seguimiento de su aplicación tengan pericia en esta materia.

[14] Organización Internacional de Normalización (2023) ISO/IEC 42001. Information technology — Artificial intelligence — Management system www.iso.org/es/contents/data/standard/08/12/81230.html

El seguimiento de esta norma trae aportes en pro de la organización, clientes y proveedores, tales como:[15]

- Establece un marco regulatorio, para la debida gestión de un ambiente que emplee la inteligencia artificial
- Mejorar la competitividad, confianza del sistema y gobernanza empresarial, al demostrar su uso consciente y responsable
- Marco para la gestión de riesgos legales y operativos
- Ahorro de costos y aumento de la eficiencia
- Trazabilidad
- Reducción de los riesgos asociados con el uso de la inteligencia artificial.
- Beneficios para proveedores de la ISO/IEC 42001:2023
- Confiabilidad de los productos y servicios de IA.
- Fortalece la reputación de la empresa
- Mejora la productividad al evitar la repetición de los errores, reduciendo costos
- Permite un uso más eficaz de los recursos y la inversión en IA.

Se vincula también con la Norma ISO/IEC 25059 sobre la calidad de producto sobre el uso del software de Inteligencia Artificial, ya que su adaptabilidad puede fomentar la precisión sobre información de datos, pudiendo el usuario intervenir de manera correcta y oportuna en su operación para mitigar los riesgos; construyendo un sistema seguro y fiable. Debiendo relacionarla con la Norma ISO/IEC 8000-2019, contentiva de recomendaciones sobre calidad e ingeniería de datos y vocabulario relacionado con gestión de datos maestros e ingeniería de datos.

4. Otras regulaciones de interés que deben ser tenidas en consideración y ser cumplidas

Finalmente cabe referir que en Venezuela, no existe en este momento regulación expresa sobre el tema, ya que, sobre un proyecto que reposa en la Asamblea Nacional, se conoce, además de lo que reseña la Cadena Venezolana de Noticias [16], sobre este proyecto de ley para el uso de la Inteligencia Artificial, que el mismo está a cargo de la Subcomisión de Innovación, Modernización del Estado y Escalamiento de Sectores Estratégicos de la Asamblea Nacional (AN), que busca potenciar el aporte de las nuevas tecnologías disruptivas a fin de competir en los mercados internacionales y promover el desarrollo cultural.

Esta circunstancia, no impide que las empresas, basadas en las buenas prácticas que derivan de la autorregulación, elaboren sistemas de gestión de riesgos robustos, que le permitan aprovechar los beneficios de la herramienta, contando con personas capacitadas que lleven a cabo la labor de seguimiento y mitigación de posibles daños.

El proyecto, aprobado recientemente en su primera discusión, resalta por establecer el principio de autoridad humana (2024, art.5) y el deber de registrar ante el Ministerio

[15] Organización Internacional de Normalización 2023. Norma ISO 42001-2023 Information technology — Artificial intelligence — Management system www.iso.org/es/contents/data/standard/08/12/81230.html
[16] López, Alexis 2023. Cadena Venezolana de Noticias 2023. Asamblea Nacional propone ley para el uso de la inteligencia artificial Cadena Venezolana de Noticias https://cvn.com.ve/2023/06/08/asamblea-nacional-propone-ley-para-el-uso-de-la-inteligencia-artificial/

del Poder Popular para la Ciencia y la Tecnología, las actividades comerciales vinculadas con proveer, comercializar y distribuir el Servicio de Inteligencia Artificial (2024, art.9). También establece como áreas de uso prioritario en materia de políticas públicas las vinculadas a cambio climático, salud, crecimiento inclusivo, protección de los derechos de propiedad intelectual, el uso de datos, entre otros, regulando, asimismo, temas relacionados con la gestión de riesgos, estableciendo criterios que incluyen aquellos considerados inaceptables y por ende, prohibidos.

Asimismo, a pesar de no existir normas específicas en materia de inteligencia artificial, ello no obsta para que la regulación en materia penal no sea un límite en torno a las conductas que puedan considerarse delictivas y que pasen a ser perpetradas a través del uso de la inteligencia artificial, como puede ocurrir, por ejemplo, en temas de estafas (art. 462 y siguientes del Código Penal), adulteración y falsificación de documentos o aprovechamiento de los mismos (arts. 321 y siguientes Código Penal), adulteración o falsificación de signos distintivos, modelos industriales, marcas; o el uso de dichas falsificaciones (art. 337 Código Penal), difamación e injurias (art. 442 y siguientes Código Penal), por sólo mencionar aquellos delitos que pueden tener incidencia en el área empresarial. Incluso, hoy día se habla hasta del uso de la inteligencia artificial para ataques bélicos, como ha sucedido en la guerra entre Rusia y Ucrania[17][18], que de materializarse supuestos similares en el país, pudiera conllevar a la comisión de algunos de los delitos contra la independencia y seguridad de la Nación, previstos en los artículos 128 y siguientes del Código Penal.

Del mismo modo, la Ley Especial Contra los Delitos Informáticos sanciona el acceso y la interferencia en sistemas que utilicen tecnología de la información (art. 6) o modifiquen las datas e informaciones de dichos sistemas (art. 7), el espionaje informático (art. 11), falsificación de documentos (art. 12), fraude (art. 14), apoderamiento, utilización, modificación o eliminación de data (art. 20), violación a la privacidad de las comunicaciones (art. 21), revelación indebida de data (art. 22), copia, reproducción, modificación, divulgación o distribución de software y obras de intelecto (art. 25), entre otros.

La violación a derechos de propiedad intelectual y derechos de autor, a través del plagio, uso indebido o adulteración, mediante el uso de creaciones protegidas por propiedad intelectual, también es sancionable en virtud de los daños y perjuicios materializados, por la vía de la responsabilidad civil prevista en el Código Civil venezolano y demás normativa legal vigente.

Por otra parte, también en materia de telecomunicaciones, el uso indebido de la inteligencia artificial, cuando sea realizado mediante medios electrónicos, resulta sancionable conforme a la Ley de Responsabilidad Social en Radio, Televisión y Medios

[17]Vasco Cotovio, Clare Sebastian, Allegra Goodwin (2024) CNN *Drones ucranianos con inteligencia artificial intentan alterar la industria energética de Rusia. Hasta ahora, está funcionand*o https://cnnespanol.cnn.com/2024/04/02/drones-ucranianos-ia-inteligencia-artificial-alterar-industria-energetica-rusia-hasta-ahora-funcionando-trax

[18] Pardo de Santayana, José. 2024.La inteligencia artificial y la guerra de Ucrania. https://dialnet.unirioja.es/descarga/articulo/9666375.pdf Se habla de que Ucrania ha logrado enfrentarse seriamente a Rusia y contraatacar gracias al empleo de drones, designación de objetivos con IA e inteligencia de imágenes.

Electrónicos, cuando promueva el odio y la intolerancia, realice propaganda de guerra, cause zozobra, promueva alteraciones al orden público, promueva violaciones al ordenamiento jurídico, entre otras, dispuestas en el artículo 27 de dicha norma.

De igual manera, en materia de protección del consumidor, en especial cuando se está en presencia de la figura de sectores fuertemente regulados, como sucede en materia de banca, seguros, Fintech, etc., existen parámetros de protección de datos de los usuarios y de debida atención de los derechos de los mismos, que no pueden ser dejados de lado por el uso indebido o el mal funcionamiento de los sistemas de inteligencia artificial, siendo que dichos derechos van más allá de la protección de datos, sino que abarcan, por ejemplo, la idoneidad de las respuestas que puedan ser dadas a los clientes frente a consultas, solicitudes y reclamos, cuando estas respuestas no devengan de seres humanos sino que sean generadas a través del uso de la inteligencia artificial (por ejemplo, si conducen a error, dan información falsa sobre productos o servicios, etc.).

Sin pretensiones de ser futuristas, y teniendo presente los últimos avances en materia de ciencia y medicina, por ejemplo, que incluso involucran el uso de la inteligencia artificial a nivel médico, se debe tener presente (y ello debe replicarse en las diversas áreas del ejercicio económico), que cuando se hagan uso de estas tecnologías, igualmente deben cumplirse todas las normativas aplicables en materia de salud (igual que sucedería en cualquier otro sector de la vida económica), ya que el uso de inteligencia artificial no debe entenderse como una exclusión del ordenamiento jurídico ordinario, el cual es el primer llamado a regular cada una de las situaciones que acontezcan en la vida diaria, y que a su vez, en estos casos específicos, será complementado, más nunca sustituido, por las normas en materia de inteligencia artificial, siendo que ante la inexistencia de éstas, el primero siempre resultará aplicable.

Por último, no se puede dejar de lado las regulaciones dictadas en materia de inteligencia artificial a nivel internacional, siendo que, si bien no existe ordenamiento jurídico interno, dichas normas resultan en un parámetro de actuación del uso que debe serle dado a la inteligencia artificial en el país.

Así, se busca llamar la atención en torno a la Resolución Nro. 78/265 aprobada por la Asamblea General de la Organización de las Naciones Unidas (ONU) en fecha 21 de marzo de 2024, denominada Aprovechar las Oportunidades de Sistemas Seguros y Fiables de Inteligencia Artificial para el Desarrollo Sostenible[19], la cual establece una serie de directrices en torno a los usos seguros de la IA y llama a todos los Estados, en primer lugar, a la promoción del uso de la inteligencia artificial, pero en forma “segura y fiable”, a emplearla como mecanismo para promover el desarrollo, a emplear en la misma mecanismos de gestión de riesgos y de protección de datos, a abstenerse de usar IA que pueda poner en riesgo los derechos humanos, entre otros aspectos de interés.

CONCLUSIONES

La inteligencia artificial es una herramienta útil en el diseño de las políticas de cumplimiento organizacional y gran parte de las empresas utiliza tecnología en el desarrollo de sus procesos productivos, la gestión de auditorías, la preservación de la data

[19] https://digitallibrary.un.org/record/4043244/files/A_RES_78_265-ES.pdf?ln=en

de los clientes y de los proveedores, los procesos operativos, el diseño de indicadores de gestión, implementación de criterios ESG e incluso, pagos al personal.

Es fundamental que exista, además, un sistema de gestión de riesgos informáticos, basado en estándares internacionales, especialmente las normas ISO de la serie 27000 y la Norma específica ISO/IEC 42001-2023, ambas de la Organización Internacional de Normalización, con el objeto de evitar manipulaciones en la data, ser objeto de ataques cibernéticos o conductas que comprometan la integridad y la confianza en la organización.

Si bien en Venezuela apenas ha superado la primera discusión un proyecto de ley en discusión en la Asamblea Nacional, las empresas no pueden esperar que ésta u otra norma entre en vigencia para aplicar medidas en el sistema de gestión de riesgos, que garanticen la seguridad en el uso de la Inteligencia Artificial. En todo caso, se puede acudir a la normativa existente en el derecho positivo en el ámbito sancionatorio y desde el ámbito preventivo, evitar, a toda costa, incurrir en cualquier conducta que pueda generarle responsabilidad a la empresa.

Los criterios que sirvan de base a la implementación de la inteligencia artificial deben ser éticos y evitar discriminaciones u otros daños que afecten las relaciones de la empresa con sus proveedores y demás grupos de interés.

Para ello, deben incluirse regulaciones tanto a nivel del derecho positivo, especialmente para el caso venezolano, de la mano de normas de debida diligencia y autorregulación organizacional, supervisión por parte de personal calificado en los entes de cumplimiento interno, así como una permanente vigilancia sobre su implementación, para lo cual se deberá contar con la asesoría de personal calificado para ello.

BIBLIOGRAFÍA

Asamblea Nacional (2024) *Proyecto de Ley para regular el uso de la Inteligencia Artificial.* Comisión Especial del Futuro de la AN.

Beltrán, Ignasi (2023) *Algoritmos y condicionamiento por debajo del nivel consciente: un análisis crítico de, la propuesta de ley de Inteligencia Artificial de la Unión Europea*, Revista de la Facultad de Derecho de México,Número 286. DOI: https://doi.org/10.22201/fder.24488933e.2023.286.86406

Comisión Europea (2024) Ley de Ciberresiliencia de la Unión Europea. https:///digital-strategy.ec.europa.eu/es/policies/cyber-resilience-act

Constitución de la República Bolivariana de Venezuela Gaceta Oficial N° 36.860 del 30/12/1999.

Gamero, Eduardo (2021) La *necesidad del compliance en la inteligencia artificial.* CincoDías, 12/04/2021. https:// artificial cincodias.elpais.com/cincodias/2021/04/09/legal/1617964412_071507.html

KPMG (2024) *Future-proofing banking: The Enterprise transformation imperative* *https://kpmg.com/us/en/articles/2024/2024-us-banking-industry-outlook-survey.html*

Ley del Sistema Venezolano para la Calidad Gaceta Oficial 37.555 del 23 de octubre de 2002

Ley Especial contra los delitos informáticos. Gaceta Oficial N° 37.313, del 30/10/2001.

Decreto 1204 con Rango y Fuerza de Mensajes de Datos y Firmas Electrónicas Gaceta Oficial N° 37.148 del 28/02/2001.

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura UNESCO (2022) *Recomendación sobre la ética de la inteligencia artificial*.https://www.unesco.org/es/articles/recomendacion-sobre-la-etica-de-la-inteligencia-artificial

Organización Internacional de Normalización.(2019). Norma ISO 27001 sobre la Seguridad de la Información... https://www.iso.org/standard/82875.htm,

_____. (2022). Norma ISO 27002 sobre la Seguridad de la Información... https://www.iso.org/standard/82875.htm,

_____. (2014). Norma ISO 27015-2022 sobre la Seguridad de la Información en empresas Fintech.. : https://www.iso.org/standard/82875.htm,

_____(2023). ISO/IEC 25059:2023 - Requisitos de calidad de software para sistemas de inteligencia artificial (IA) https:// www.iso.org/standard/80655.html

_____ (2019). ISO/IEC 8000-2019 - Gestión de riesgos de la seguridad de la información https://iso8000.es/normas-iso-8000

_____ (2023) ISO/IEC 42001. Information technology — Artificial intelligence — Management system www.iso.org/es/contents/data/standard/08/12/81230.html

Pardo, José. (2024) .*La inteligencia artificial y la guerra de Ucrania.* Capítulo Cuarto. https://dialnet.unirioja.es/descarga/articulo/9666375.pdf

Vasco Cotovio, Clare Sebastian, Allegra Goodwin (2024) CNN *Drones ucranianos con inteligencia artificial intentan alterar la industria energética de Rusia. Hasta ahora, está funcionand*o https://cnnespanol.cnn.com/2024/04/02/drones-ucranianos-ia-inteligencia-artificial-alterar-industria-energetica-rusia-hasta-ahora-funcionando-trax

Vaudo, Liliana (2023) *Integración normativa para la gestión de riesgos sobre sistemas de información empresarial* Revista Venezolana de Legislación y Jurisprudencia. Nro 21. Diciembre 2023. Ps: 151-174. https:// rvlj.com.ve/?page_id=3142

Vaudo, Liliana (2024) *Criterios de Buen Gobierno Corporativo en Empresas Fintech Venezolanas*. Especial Referencia al Sistema Financiero. Revista Internacional de Ciencias Sociales Interdisciplinares. ISSN: 2474–6029 (versión impresa), ISSN: 2254–7207 (versión electrónica) Volumen 12, Número 1, 2024 https://doi.org/10.18848/2474-6029/CGP/v12i01/1-22.