EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN EL CUMPLIMIENTO NORMATIVO: DESAFÍOS Y BUENAS PRÁCTICAS EN EL CONTEXTO EUROPEO E INTERNACIONAL

ALBERT SALVADOR LAFUENTE

La Inteligencia Artificial (IA) se ha convertido en una herramienta de alto impacto para reforzar los programas de cumplimiento normativo (*compliance*) en las organizaciones. En sectores altamente regulados, como el financiero, asegurador, sanitario o tecnológico, las empresas se enfrentan a un volumen y complejidad creciente de regulaciones que hacen cada vez más desafiante asegurar el pleno cumplimiento legal.

La IA ofrece soluciones innovadoras para gestionar estos retos: por ejemplo, algoritmos de *machine learning* pueden monitorizar transacciones y operaciones en tiempo real, ayudando a detectar anomalías asociadas al lavado de dinero o al fraude con mucha más rapidez y precisión que los métodos tradicionales. Según datos de la Autoridad Bancaria Europea, un 22% de los bancos europeos ya utilizan técnicas de IA en sus tareas de cumplimiento normativo, lo que refleja la rápida adopción de estas tecnologías. La IA también permite una gestión proactiva del riesgo: sistemas de alerta temprana inteligentes pueden señalar potenciales incumplimientos antes de que ocurran, reduciendo la probabilidad de sanciones y protegiendo la reputación empresarial.

No obstante, el uso de IA en *compliance* conlleva riesgos éticos y operativos que las organizaciones deben abordar cuidadosamente. Muchos algoritmos de IA funcionan como una "caja negra", dificultando explicar cómo se toman ciertas decisiones, lo cual puede minar la transparencia y generar desconfianza en los grupos de interés. Asimismo, si los modelos de IA se entrenan con datos históricos sesgados, podrían perpetuar o amplificar sesgos y discriminaciones, planteando riesgos éticos y legales graves. La gestión de grandes volúmenes de datos por la IA también suscita preocupaciones sobre privacidad y cumplimiento de la normativa de protección de datos, así como posibles vulnerabilidades de ciberseguridad. Otros retos incluyen la dificultad de asignar responsabilidades cuando la toma

de decisiones es automatizada, el posible uso malintencionado de la IA para manipular información, y el impacto en el empleo y la necesidad de adaptación del personal a nuevas funciones. En definitiva, integrar la inteligencia artificial en el cumplimiento normativo implica aprovechar su potencial para mejorar la eficiencia y anticiparse a los riesgos, sin descuidar la necesidad de salvaguardar los principios éticos y respetar estrictamente el marco regulatorio.

Este artículo aborda esa dualidad mediante un análisis integrado de dos aspectos complementarios. En primer lugar, se analiza el conjunto de normas europeas e internacionales que buscan orientar el desarrollo de una inteligencia artificial segura y de confianza. Este panorama incluye tanto marcos jurídicos obligatorios —como el Reglamento de IA de la Unión Europea— como herramientas de *soft law* y estándares internacionales, entre los que destacan los principios de la OCDE y la Recomendación de la UNESCO sobre la ética en la IA. En segundo lugar, se exploran las buenas prácticas empresariales para la implementación responsable de la IA en sistemas de *compliance*, destacando cómo las empresas pueden alinear sus usos de IA con estos marcos normativos y con los principios de buen gobierno corporativo. A lo largo de este artículo vamos a analizar los principales desafíos éticos y operativos vinculados al uso de IA en *compliance*, y se proponen recomendaciones prácticas para que las organizaciones aprovechen las ventajas de la IA sin comprometer la ética, la transparencia ni el cumplimiento de sus obligaciones legales. El propósito es ofrecer una perspectiva integral, con enfoque divulgativo y profesional, que ayude a empresas y responsables de cumplimiento normativo a orientarse en el cruce entre inteligencia artificial, regulación y ética empresarial.

MARCO REGULATORIO EUROPEO E INTERNACIONAL DE LA IA APLICADA A *COMPLIANCE*

El acelerado avance de la IA ha impulsado en los últimos años la elaboración de marcos regulatorios y éticos, tanto en Europa como a nivel internacional, orientados a promover una IA confiable y alineada con derechos fundamentales. Estos marcos buscan mitigar los riesgos inherentes a la IA a la vez que aprovechan sus beneficios, sentando principios y obligaciones que son especialmente relevantes para su uso en ámbitos sensibles como el cumplimiento normativo.

Europa: el Reglamento de IA y la estrategia de IA confiable

La Unión Europea ha asumido un papel pionero al proponer la primera ley integral sobre IA, conocida como el Reglamento de IA de la UE (*Artificial Intelligence Act*). Aprobado en 2024, este Reglamento establece un enfoque regulatorio basado en los riesgos que plantea cada uso de IA. La regulación europea clasifica las aplicaciones de inteligencia artificial en cuatro categorías según su nivel de riesgo: inaceptable, alto, limitado y mínimo. A cada categoría le corresponde un conjunto de obligaciones proporcionales, que buscan proteger los derechos fundamentales sin frenar la innovación tecnológica. Este enfoque garantiza que las aplicaciones con mayor impacto sobre las personas estén sometidas a los estándares más rigurosos de transparencia, control y seguridad. El Reglamento europeo prohíbe aquellas aplicaciones de inteligencia artificial que atentan gravemente contra los valores fundamentales de la Unión Europea. Estas incluyen, por ejemplo:

- Sistemas de identificación biométrica masiva en espacios públicos, salvo excepciones muy restringidas aplicables a las fuerzas de seguridad.
- Puntuación social de personas ("*social scoring*"), similar al modelo de calificación ciudadana utilizado en algunos regímenes autoritarios.
- Vigilancia masiva indiscriminada, incompatible con los principios de proporcionalidad y respeto a la vida privada.
- Sistemas de manipulación del comportamiento humano que exploten vulnerabilidades, especialmente en personas

menores o en situación de vulnerabilidad.

- Uso de IA para *profiling* predictivo con fines policiales, cuando no existan garantías jurídicas sólidas.

Estas prohibiciones reflejan la preocupación central de la Unión Europea por impedir desarrollos tecnológicos que puedan socavar la dignidad humana, la democracia, la libertad individual o la protección de datos personales.

El núcleo del Reglamento se centra en los denominados sistemas de IA de alto riesgo, que abarcan aquellos usos de IA con potencial de causar daños significativos a la salud, la seguridad o los derechos fundamentales de las personas (por ejemplo, IA empleada en infraestructuras críticas, en evaluación de personas para acceso a empleo, educación, servicios financieros, en contextos de aplicación de la ley, control migratorio, administración de justicia, entre otros). Para estos sistemas de alto riesgo, el Reglamento impone estrictas obligaciones de cumplimiento: las entidades desarrolladoras o implantadoras deberán llevar a cabo evaluaciones de riesgos antes de la puesta en el mercado, adoptar medidas para mitigar riesgos identificados, mantener registros (*logs*) detallados del funcionamiento del sistema, garantizar niveles apropiados de precisión, robustez y ciberseguridad, asegurar la supervisión humana efectiva sobre las decisiones automatizadas, y proveer una transparencia adecuada (información a usuarios sobre que interactúan con una IA, explicaciones de decisiones cuando corresponda). Además, el Reglamento europeo no solo impone obligaciones técnicas, sino que reconoce derechos concretos para las personas afectadas por sistemas de inteligencia artificial de alto riesgo. En particular, consagra el derecho a presentar quejas y a recibir explicaciones claras y comprensibles cuando una decisión automatizada afecte sus derechos. Esto refuerza los principios fundamentales de responsabilidad (*accountability*), explicabilidad y control humano significativo.

Para los sistemas de riesgo limitado o mínimo, el Reglamento no establece exigencias estrictas. No obstante, incentiva fuertemente la autorregulación, promoviendo la adopción voluntaria de códigos de conducta alineados con los principios éticos aplicables a los sistemas de mayor riesgo. Este enfoque equilibrado busca fomentar una cultura de ética tecnológica y confianza en la IA, sin desincentivar la innovación.

De esta forma, la UE busca elevar el estándar general de las aplicaciones de IA promoviendo la autorregulación responsable incluso más allá de lo legalmente exigido.

Más detalles es: https://www.europarl.europa.eu/topics/es/article/20230601STO93804/ley-de-ia-de-la-ue-primera-normativa-sobre-inteligencia-artificial

Principios internacionales: OCDE y UNESCO

Más allá de Europa, destacan dos referencias clave en la gobernanza ética de la inteligencia artificial: los Principios de IA de la OCDE y la Recomendación de la UNESCO sobre la ética de la IA. Ambos documentos ofrecen un marco internacional para orientar a gobiernos y empresas en el desarrollo responsable de estas tecnologías.

La OCDE fue pionera en 2019 al adoptar la primera norma intergubernamental sobre IA. Sus principios promueven una IA confiable, alineada con derechos humanos y valores democráticos. Entre ellos destacan: crecimiento inclusivo, respeto a los derechos y diversidad, transparencia, seguridad técnica y rendición de cuentas. Estos principios han sido adoptados por el G20 y han influido en políticas nacionales, sirviendo también de guía práctica para las empresas al integrar equidad, transparencia y seguridad en sus proyectos de IA.

Por su parte, la Recomendación de la UNESCO, aprobada en 2021 por 193 Estados, constituye el primer marco normativo global en ética de la IA. Pone énfasis en la protección de la dignidad humana y los derechos fundamentales, e introduce principios detallados como: uso necesario y proporcional de la IA, equidad, no discriminación, privacidad durante todo el ciclo de vida, supervisión humana final y evaluación

FIGURA 1
LOS SIETE PILARES DE IA RESPONSABLE EN COMPLIANCE

Fuente: Elaboración propia

de impacto social y ambiental. También promueve la transparencia, la educación pública, y el desarrollo de marcos de auditoría y gobernanza inclusiva. Aunque no es vinculante, esta recomendación ya ha influido en regulaciones nacionales y es vista como referencia para implementar buenas prácticas en IA con legitimidad social.

Otros desarrollos internacionales y estándares

Además de la OCDE y la UNESCO, otros organismos internacionales han contribuido a establecer principios para una inteligencia artificial responsable. Naciones Unidas promueve un enfoque humanista; el G20, G7 y la OEI han respaldado principios éticos similares, incluyendo propuestas adaptadas al contexto latinoamericano. Paralelamente, se han desarrollado estándares técnicos para implementar estos principios. Destaca la norma ISO/IEC 42001:2023, primer estándar global de gestión de IA, que ayuda a las organizaciones a establecer un sistema estructurado que aborde riesgos éticos, de seguridad, transparencia y mejora continua.

Adoptar esta norma permite demostrar el uso responsable de la IA, fortalecer la confianza pública y facilitar el cumplimiento regulatorio. Aunque no es obligatoria, su adopción voluntaria puede posicionar a las empresas como líderes en gobernanza de IA, de forma análoga a la ISO 27001 en ciberseguridad. En conjunto, marcos como el Reglamento de IA de la UE, los principios de la OCDE, la Recomendación de la UNESCO y los estándares ISO forman una arquitectura normativa convergente. Todas estas iniciativas apuntan a una IA ética, transparente, segura y supervisada por humanos. Las empresas que integran IA en sus funciones de cumplimiento deben no solo respetar la normativa legal, sino también incorporar principios éticos internacionales en su cultura corporativa.

BUENAS PRÁCTICAS EMPRESARIALES PARA UNA IA RESPONSABLE EN SISTEMAS DE *COMPLIANCE*

Implementar la IA en las funciones de *compliance* corporativo no es simplemente una cuestión tecnológica, sino principalmente organizacional y de gobernanza. Las empresas líderes entienden que para aprovechar la IA en cumplimiento normativo –por ejemplo, en la automatización de controles, la auditoría interna continua, la detección de conductas irregulares o la gestión de riesgos regulatorios– es imprescindible establecer previamente una base sólida de políticas, procesos y cultura que orienten el uso de la IA de forma ética y alineada con las normas. A continuación (véase figura 1),

se presentan las principales buenas prácticas empresariales identificadas, fruto de la experiencia profesional y de numerosas guías especializadas, que sirven para integrar la IA de manera responsable en los sistemas de *compliance*.

Gobernanza y supervisión de la IA

Un primer bloque fundamental de buenas prácticas es crear una adecuada estructura de gobernanza para supervisar los sistemas de IA dentro de la organización. Esto implica definir claramente *quién* se encarga de qué respecto a la IA. Por una parte, numerosas organizaciones están creando comités éticos o equipos multidisciplinarios especializados en inteligencia artificial, responsables de evaluar y aprobar los usos más delicados de esta tecnología. Estos comités suelen incluir tanto expertos técnicos en IA como representantes del área legal y de cumplimiento, e incluso otras partes interesadas internas o externas según el caso. Su rol es evaluar los potenciales impactos éticos y legales de los algoritmos, y vigilar el cumplimiento de las políticas internas relativas a IA. Por otra parte, se aconseja definir con precisión los roles y responsabilidades vinculados al uso de la inteligencia artificial. Una buena práctica consiste en nombrar a un responsable interno de IA —similar a un 'AI *Compliance Officer*'— que supervise la gestión de riesgos, sirva de enlace entre los equipos técnicos y el área de cumplimiento, y asegure una coordinación eficaz. Asimismo, es fundamental establecer mecanismos claros de rendición de cuentas, de manera que la organización cuente con procedimientos para determinar responsabilidades en caso de que un sistema de IA genere daños o consecuencias no deseadas, evitando así vacíos de responsabilidad. Complementariamente, las organizaciones punteras realizan auditorías internas periódicas de sus sistemas de IA para verificar que siguen comportándose dentro de parámetros aceptables y cumpliendo tanto las normas externas como las políticas internas. Esta auditoría puede incluir revisar la calidad de los datos, re-evaluar sesgos en los modelos, probar la robustez frente a ataques adversariales, etc. En síntesis, una buena gobernanza de IA implica tratar los sistemas inteligentes con el mismo rigor (o más) que cualquier otro proceso crítico de la empresa: con políticas y protocolos claros, controles de supervisión independientes, y reportes regulares a la alta dirección y al órgano de gobierno sobre su desempeño y riesgos.

Transparencia y explicabilidad de los sistemas

La transparencia es uno de los principios centrales para la IA responsable y en el contexto empresarial se traduce en varias prácticas concretas. Una es mantener una documentación completa y accesible de los sistemas de IA: desde la descripción del algoritmo y su finalidad, hasta los datos utilizados para entrenarlo, los criterios de validación y los resultados de evaluaciones de desempeño. Esta documentación permite que, ante cualquier cuestión de *compliance* (por ejemplo, una pregunta de un auditor externo o un requerimiento de un regulador), la empresa pueda demostrar cómo funciona su IA y qué medidas tomó para controlarla. Otra práctica es proveer explicaciones comprensibles a los usuarios finales o a los afectados por decisiones automatizadas. Por ejemplo, si se usa IA para filtrar transacciones sospechosas, los oficiales de cumplimiento deben contar con interfaces que les muestren de forma clara las razones o factores que la IA consideró para marcar una operación (p.ej., patrones detectados, umbrales excedidos), en un lenguaje entendible y no solo con métricas opacas. Esto facilita que el personal de cumplimiento confíe en la herramienta y pueda validar o refutar sus hallazgos con criterio humano. Adicionalmente, la transparencia hacia terceros es importante: las organizaciones deberían comunicar a sus clientes, empleados o *stakeholders* relevantes cuando interacciones o decisiones están siendo asistidas por IA, especialmente si esto pudiera afectar derechos. En ciertos casos, podría requerirse por normativa informar a interesados cómo solicitar revisiones humanas o cómo disputar decisiones tomadas por IA. La consigna es que la IA no debe introducir *opacidad* en *com-*

pliance, sino al contrario, debe reforzar la trazabilidad de las acciones. Para ello, además de explicabilidad, se aconseja habilitar logs y registros detallados de las operaciones de la IA (datos procesados, resultados generados, alertas emitidas, etc.), los cuales no solo ayudan a supervisar su desempeño sino que servirán de evidencia objetiva de las diligencias realizadas en caso de inspecciones o auditorías.

Protección de datos personales y ciberseguridad

Dado que muchos sistemas de IA para *compliance* procesan volúmenes masivos de datos, incluidas potencialmente categorías de datos personales sensibles, se debe prestar especial atención a cumplir con las normativas de privacidad y seguridad de la información. Una buena práctica es aplicar el principio de minimización y anonimización de datos: siempre que sea posible, entrenar y operar las IA con datos anónimos o pseudonimizados, para reducir riesgos de violaciones de privacidad. Asimismo, obtener siempre los consentimientos informados necesarios cuando se recojan datos personales para usos de IA, explicando claramente a los titulares la finalidad y posibles implicaciones del tratamiento. Las empresas deben realizar evaluaciones de impacto en protección de datos (PIA/DPIA) antes de desplegar IA que trate datos personales a gran escala, identificando riesgos para la privacidad y aplicando salvaguardas apropiadas. Desde el punto de vista de ciberseguridad, es crucial recordar que un sistema de IA es tan seguro como el entorno tecnológico donde se ejecuta. Por ende, deben implementarse sólidas medidas de seguridad: cifrado de datos en reposo y en tránsito, autenticación multifactor para acceder a las plataformas de IA, monitoreo continuo de accesos y actividades anómalas, entre otras. Algunos algoritmos de IA incluso pueden usarse para reforzar la ciberseguridad (por ejemplo, detección inteligente de intrusiones), pero aun así se debe proteger la propia IA de ataques (como intentos de manipular sus resultados mediante entradas adversarias). El cumplimiento con marcos como el RGPD (GDPR) en Europa es ineludible: toda aplicación de IA debe diseñarse bajo los principios de *Privacy by Design* y *Security by Design*, demostrando que la empresa mantiene el control sobre los datos y respeta los derechos ARCO (Acceso, Rectificación, Cancelación, Oposición) de los individuos. En resumen, una IA en *compliance* que vulnerase la privacidad de las personas o fuera fácilmente hackeable caería en una contradicción fatal, por lo que la protección de datos y la seguridad deben integrarse desde el inicio en cualquier proyecto de IA.

Cumplimiento normativo integral (legal y ético)

Por definición, un departamento de *compliance* velará porque cualquier herramienta o proceso que implemente cumpla con las leyes y regulaciones vigentes. Tratándose de IA, esto significa en primer lugar prepararse para el nuevo marco legal específico de IA. En la UE, aunque el Reglamento de IA concederá previsiblemente un período de transición hasta su aplicabilidad plena (posiblemente hasta 2026, según los borradores actuales), las empresas responsables ya están anticipando sus obligaciones para no verse rezagadas. Es aconsejable contar con asesoría legal especializada sobre el uso de IA, identificando qué sistemas de IA de la organización podrían ser clasificados como "alto riesgo" bajo la ley y qué requerimientos conllevarán. Igualmente, hay que mapear otras normativas sectoriales o generales que aunque no mencionen explícitamente IA, resultan aplicables: por ejemplo, las leyes anti-discriminación en decisiones laborales (si se usa IA en selección de personal), la normativa financiera (si se usa IA en calificación crediticia o detección de blanqueo), las obligaciones de auditoría en entornos SOX, etc. Una buena práctica es desarrollar políticas internas claras sobre el uso de IA, que sinteticen las reglas legales y éticas esperadas y las traduzcan a directrices para empleados y equipos técnicos. Estas políticas internas deben difundirse y acompañarse de capacitación específica (ver más adelante) para asegurar su cumplimiento efectivo. En muchos sentidos, adoptar un enfoque de *"cumplimien-*

to por diseño" en IA significa considerar desde la fase de diseño todos los requisitos normativos y valores éticos relevantes, tal como se hace con la privacidad por diseño. Así, por ejemplo, si se va a implementar un sistema de IA para monitorear comunicaciones internas en busca de indicios de fraude o malas prácticas (caso de uso de *compliance*), se debería desde el diseño incorporar: restricciones para no invadir comunicaciones personales protegidas, criterios de retención y borrado de datos que cumplan la ley, umbrales de detección que equilibren eficacia con evitar falsos positivos que afecten injustamente la reputación de empleados, procedimientos de doble verificación humana antes de sanciones, etc. Todo ello derivado de analizar qué leyes aplican (laborales, privacidad, derecho penal, etc.) y qué principios éticos están en juego (justicia, presunción de inocencia, dignidad, etc.). En suma, las mejores prácticas de *compliance* con IA implican unificar el cumplimiento legal con el cumplimiento ético, entendiendo que la legitimidad social es tan importante como la legalidad. Muchas compañías líderes van más allá de la mera observancia legal y asumen compromisos públicos de autorregulación, adhiriendo a códigos de conducta voluntarios sobre IA responsable. Esto se alinea con las recomendaciones regulatorias de incentivar la autorregulación: el Reglamento de IA de la UE alienta explícitamente a los proveedores de sistemas no cubiertos por la regulación estricta a desarrollar códigos de conducta voluntarios inspirados en sus requisitos y en las directrices éticas de la Unión. Adoptar tales códigos sectoriales o propios puede ayudar a estructurar internamente las prácticas éticas y demostrar ante terceros el compromiso con un cumplimiento "360 grados", que incluye la dimensión legal y la ética corporativa.

Prevención de sesgos y promoción de la equidad

Como se mencionó, uno de los riesgos más señalados de la IA es la posible discriminación algorítmica. Por ello, un componente esencial de las buenas prácticas es establecer medidas para evitar el sesgo injusto en los sistemas de IA. En la práctica esto comienza por los datos: se deben utilizar datos de entrenamiento lo más diversos, representativos y de calidad posible, procurando que incluyan distintos grupos demográficos relevantes para la aplicación. Por ejemplo, si se entrena una IA para detectar transacciones sospechosas, los datos deberían reflejar múltiples perfiles de clientes y no sobre-representar únicamente ciertos países o etnias que podrían inducir sesgos étnicos. Además de la selección de datos, las empresas están llevando a cabo pruebas de equidad (*fairness testing*) en sus modelos, que implican medir las tasas de error o decisiones por subgrupos para identificar posibles disparidades. Es recomendable realizar auditorías independientes de sesgo periódicamente; existen herramientas técnicas para ello, pero también puede implicar contratar terceros que evalúen objetivamente si un modelo de IA (por ejemplo, uno que puntúa riesgos de clientes) está penalizando sistemáticamente a un grupo protegido sin justificación. Si se detecta un sesgo, se deben tomar acciones correctivas: ajustar el algoritmo, re-entrenar con datos balanceados, o incluso descartar el modelo si no puede garantizar resultados equitativos. Otra buena práctica es fomentar la diversidad en los equipos de desarrollo de IA. La experiencia muestra que equipos multidisciplinarios y diversos (en género, origen, formación) tienden a identificar más fácilmente sesgos ocultos y a diseñar soluciones más inclusivas, en contraste con equipos homogéneos donde ciertos supuestos no se cuestionan. En resumen, la equidad algorítmica no ocurre por azar: debe gestionarse activamente. Para una función de *compliance*, esto es crítico pues una IA sesgada no solo es injusta sino que puede derivar en incumplimientos legales (por ejemplo, violación de normativas anti-discriminación) y en severos daños reputacionales. Las empresas comprometidas con la RSC (Responsabilidad Social Corporativa) incorporan la no discriminación como principio rector en sus proyectos de IA, evaluando el impacto social de sus algoritmos como parte del proceso de desarrollo.

Enfoque ético y valores corporativos en IA

Más allá de controles técnicos, una empresa debe definir el marco ético en el que quiere utilizar la IA, de forma coherente con sus valores corporativos y con las expectativas de la sociedad. Una buena práctica es elaborar un código ético o directrices internas específicas para IA, que articulen principios y valores a respetar en todas las fases del ciclo de vida de los sistemas inteligentes. Dicho marco suele incluir componentes como la justicia, transparencia, privacidad, responsabilidad y sostenibilidad, entre otros, en consonancia con las grandes referencias (OCDE, UNESCO, UE) pero adaptados al contexto y lenguaje de la empresa. Es importante que en la formulación de este código participen diferentes áreas y visiones: no solo el departamento técnico y legal, sino también expertos en ética (si es posible colaborando con academia), representantes de empleados, incluso consultas a clientes o comunidades relevantes. Incluir a diversas partes interesadas en la creación de las directrices éticas de IA enriquece la perspectiva y facilita la aceptación y legitimidad de las mismas. Una vez establecido el marco ético, la empresa debe implementar mecanismos para hacerlo cumplir efectivamente. Esto puede incluir, por ejemplo, evaluaciones éticas previas a lanzar una nueva herramienta de IA (similares a un *comité de bioética* pero en tecnología), *checklists* de verificación ética que los equipos deben completar, canales para que empleados u otros alerten sobre posibles dilemas éticos ("*whistleblowing*" ético), y las ya mencionadas auditorías y comités de ética supervisores. El objetivo es pasar de palabras a hechos, integrando la ética en la toma de decisiones diaria sobre IA. Cuando surja un conflicto entre el beneficio empresarial y un principio ético, la organización debe estar preparada para ponderar cuidadosamente y, idealmente, priorizar sus valores fundamentales, manteniendo un equilibrio con la sostenibilidad del negocio. De esta manera, la IA se convierte en una extensión más de la cultura de integridad de la empresa. Aquellas compañías con un fuerte compromiso de buen gobierno corporativo verán la IA no como un terreno exento, sino como un área más donde demostrar su ética corporativa en acción.

Formación y capacitación del personal

Ninguna de las políticas o procesos anteriores será efectiva sin un elemento esencial: las personas que los llevan a cabo. La introducción de IA en *compliance* exige invertir en la formación y sensibilización de todos los niveles de la organización. En primer lugar, los equipos de cumplimiento y legales necesitan adquirir nociones básicas de IA (¿qué es un modelo de *machine learning*, qué limitaciones y sesgos puede tener, cómo interpretar sus salidas?) para poder supervisar competentemente estos sistemas. A la vez, los equipos técnicos deben formarse en materias de cumplimiento, ética y regulación, para entender el contexto y las implicaciones de las herramientas que desarrollan. Muchas empresas están ofreciendo programas de capacitación periódica en temas técnicos, éticos y legales de IA, abiertos a empleados de diversas áreas. Por ejemplo, talleres sobre "IA y privacidad" para desarrolladores, o cursos sobre "conceptos básicos de IA" para auditores internos. Asimismo, a nivel directivo conviene realizar sesiones específicas para que la alta gerencia y los miembros del Consejo de Administración comprendan los riesgos y oportunidades de la IA en su sector, habilitándolos para hacer las preguntas correctas y tomar decisiones informadas. Esta promoción de una cultura de la IA responsable debe permear la empresa. Se debe comunicar claramente que el uso de IA conlleva una responsabilidad compartida y que todos –desde los científicos de datos hasta los analistas de cumplimiento– tienen un rol en asegurar su uso ético. Integrar los principios de IA responsable en la misión y valores corporativos ayuda a reforzar este mensaje. Un ejemplo de madurez cultural es cuando los propios empleados, en su trabajo diario, identifican potenciales riesgos o mejoras en los sistemas de IA y los comunican proactivamente, o cuando se incluye la consideración de "¿es este uso de IA consistente con nuestros valores?" como parte de los criterios en proyectos nuevos. En definitiva, la capacitación continua y la concienciación son la columna vertebral para que todas las demás buenas prácticas cobren vida, creando un personal empode-

rado para colaborar hombre-máquina de forma segura y eficaz.

En resumen, las empresas que encaran la implementación de IA en *compliance* con un enfoque proactivo están combinando políticas robustas y controles internos con una cultura organizativa atenta a la ética. Estas buenas prácticas permiten minimizar muchos de los riesgos señalados previamente (opacidad, sesgo, descontrol) y potenciar los beneficios de la IA de forma sostenible. Un sistema de cumplimiento apoyado por IA, cuando se gestiona correctamente, mejora la transparencia y la confianza tanto internamente como de cara a reguladores y terceros. Además, las organizaciones que logran integrar la IA de manera responsable pueden posicionarse como líderes en ética y responsabilidad corporativa, obteniendo incluso ventajas reputacionales en entornos donde demostrar un cumplimiento sólido es un diferenciador clave. Ahora bien, implementar todas estas prácticas no está exento de desafíos. En la siguiente sección, profundizamos en los principales desafíos éticos y operativos que persisten en el uso de IA para *compliance*, incluso siguiendo buenas prácticas, y cómo enfrentarlos.

DESAFÍOS ÉTICOS Y OPERATIVOS EN EL USO DE IA PARA EL CUMPLIMIENTO

A pesar de contar con marcos normativos claros y guías de buenas prácticas, las organizaciones enfrentan en la realidad cotidiana múltiples desafíos al intentar incorporar IA en sus sistemas de cumplimiento. Estos retos pueden ser de índole ética (dilemas morales o impactos sobre valores) u operativa (dificultades prácticas de implementación y gestión). Identificar y entender estos desafíos es crucial para poder mitigarlos adecuadamente.

Complejidad técnica vs. exigencia de explicabilidad

Los modelos de IA más avanzados, como redes neuronales o generativos, funcionan como "cajas negras" difíciles de explicar. En *compliance*, donde se deben justificar decisiones, esto representa un problema. Técnicas como XAI ofrecen explicaciones aproximadas, pero no siempre suficientes. Además, los equipos de cumplimiento suelen carecer de formación técnica, lo que obliga a usar herramientas adicionales o apoyo externo. También existe el riesgo de creer que se entiende un sistema solo por su interfaz, cuando en realidad su lógica interna no ha sido validada. Se requiere inversión en algoritmos más comprensibles y capacitación en lectura crítica de resultados de IA.

Sesgos y equidad

Eliminar del todo los sesgos algorítmicos es difícil. Los datos reflejan desigualdades sociales previas que pueden trasladarse a la IA. A veces, reducir el sesgo para un grupo genera más errores en otro, lo que plantea dilemas éticos. No hay una única definición de equidad, y las organizaciones deben auditar y ajustar constantemente sus modelos. También deben consultar a grupos afectados, y estar dispuestas a descartar modelos técnicamente precisos si no cumplen con criterios éticos.

Integración con sistemas legados y calidad de datos

Muchos datos relevantes para *compliance* están en sistemas antiguos o formatos no estructurados. La IA exige limpiar e integrar estos datos, lo cual puede ser costoso y requerir expertos en datos. Sin una buena calidad, los resultados de IA son poco fiables. Además, si el sistema no se integra bien con las herramientas diarias del equipo de cumplimiento, es probable que no se use. Esto implica rediseñar procesos y capacitar al personal.

Resistencia cultural y dilemas internos

La IA puede generar temores entre los empleados, como pérdida de funciones o valor profesional. Si un sistema detecta errores pasados no advertidos por el equipo humano, puede crear tensiones. Es clave que las

decisiones finales sigan siendo humanas y que se comunique que la IA es un apoyo. Involucrar a los equipos en su implementación y adaptar indicadores de desempeño ayuda a superar resistencias.

Evolución normativa

El marco legal sobre IA cambia rápidamente. Lo que hoy es voluntario puede ser obligatorio mañana. Las empresas deben adaptar sus sistemas ante nuevas exigencias legales o sectoriales, lo cual implica ajustes técnicos y documentación adicional. Regulaciones futuras podrían exigir certificaciones antes de usar ciertos sistemas, lo que añade carga operativa. Cumplir con normas sobre herramientas de cumplimiento es ya un reto en sí mismo.

Responsabilidad legal y riesgos

Si un sistema de IA falla y causa una sanción, la empresa sigue siendo legalmente responsable. Internamente, esto puede generar tensiones sobre quién tiene la culpa. Se deben definir responsabilidades claras, revisar contratos con proveedores de IA y evaluar coberturas ante fallos. Además, si terceros son afectados por decisiones erróneas de la IA, puede haber consecuencias legales. Hasta que haya jurisprudencia clara, debe mantenerse supervisión humana sobre las decisiones críticas.

Superar estos desafíos exige una visión estratégica, un compromiso con la mejora continua y la capacidad de adaptarse de forma ágil a un entorno en constante evolución. Las empresas deben seguir de cerca los avances tecnológicos y las expectativas sociales, manteniendo una implementación ética, transparente y responsable de la IA en sus procesos de cumplimiento.

RECOMENDACIONES PARA UNA IMPLEMENTACIÓN ALINEADA CON EL BUEN GOBIERNO CORPORATIVO

Implementar IA en *compliance* requiere más que soluciones técnicas: debe enmarcarse dentro del buen gobierno corporativo. Integrar la gobernanza de la IA a la estructura de gobierno de la empresa refuerza pilares como la transparencia, la rendición de cuentas y la sostenibilidad. A continuación, se exponen siete recomendaciones para una implementación alineada con el buen gobierno corporativo:

1. **Liderazgo del Consejo de Administración**: el Consejo debe supervisar estratégicamente la adopción de IA, como lo hace con riesgos financieros o normativos. Debe recibir informes periódicos, aprobar políticas de IA y velar por su alineación con los valores corporativos. Involucrarlo garantiza un "tono desde arriba" claro y facilita integrar la IA en la visión de largo plazo, asegurando su uso responsable.

2. **Integración con la estrategia de *compliance***: la IA debe formar parte del plan estratégico general. Es recomendable elaborar un plan de inteligencia artificial alineado con los objetivos estratégicos del negocio y las prioridades del área de compliance. Asimismo, resulta esencial actualizar las políticas internas para incorporar explícitamente el uso de IA, definiendo su función dentro de los procesos de control y otorgándole legitimidad dentro del marco de gobernanza corporativa

3. **Políticas internas y protocolos de IA**: es fundamental establecer una política corporativa de IA que recoja principios éticos y normativos (como los de la OCDE y la UNESCO), y protocolos operativos para su gestión. Estos incluyen gobernanza de modelos, calidad de datos, y respuesta a incidentes. Formalizar estos elementos permite evidenciar el control sobre la IA ante auditores y reguladores.

4. **Competencias cruzadas en compliance y tecnología**: se recomienda crear equipos mixtos entre compliance, TI y legal, incorporar perfiles técnicos en compliance y capacitar a ambos lados en las competencias del otro. Esto facilita una visión conjunta de los riesgos de IA y su integración efectiva en el sistema de gestión de riesgos.

5. **Indicadores de desempeño y monitoreo**: es clave definir métricas para evaluar la eficacia de la IA en cumplimiento (alertas, reducción de errores, satisfacción interna, etc.) y establecer procesos de revisión continua ante desviaciones. El monitoreo debe ser constante, con roles claros y protocolos de respuesta si los sistemas fallan.

6. **Transparencia con stakeholders externos**: la empresa debe comunicar proactivamente el uso de IA, tanto en informes anuales como ante reguladores. También debe habilitar canales para reclamaciones o revisión de decisiones automatizadas, fortaleciendo la confianza externa y la gobernanza digital.

7. **Adaptar control interno y auditoría**: la auditoría interna debe incorporar entre sus funciones la revisión de los modelos de inteligencia artificial y sus procesos asociados. Por su parte, el área de compliance tiene la responsabilidad de asegurar que se cumplan las políticas internas sobre el uso de IA, mientras que los comités éticos deben contar con autoridad efectiva para supervisar y hacer cumplir dichas directrices. Todo el sistema de control debe completarse con mecanismos sólidos de retroalimentación y medidas correctivas que garanticen la mejora continua.

En suma, aplicar la inteligencia artificial en el ámbito del *compliance* conforme a los principios del buen gobierno corporativo permite conjugar innovación tecnológica con responsabilidad ética. Las organizaciones deben velar porque el uso de la IA no solo cumpla con las normas, sino que refuerce los valores corporativos y consolide la confianza de sus grupos de interés. Las recomendaciones aquí expuestas constituyen una hoja de ruta para avanzar hacia ese objetivo con rigor y equilibrio.

CONCLUSIONES

La incorporación de la inteligencia artificial en el ámbito del *compliance* supone un verdadero cambio de paradigma, con el potencial de revolucionar la forma en que se gestionan los riesgos legales y éticos. Gracias a esta tecnología, es posible detectar en tiempo real patrones sospechosos y adaptar los programas de formación al perfil específico de cada empleado, lo que convierte al cumplimiento en un proceso más eficiente, ágil y preventivo. Esta tecnología puede convertirse en un guardián constante de buenas prácticas, ayudando a las empresas a prevenir sanciones y fomentar una cultura más íntegra.

No obstante, su uso implica nuevas responsabilidades. La IA no es neutra ni infalible; puede amplificar errores o generar opacidad si no se gestiona adecuadamente. Por ello, requiere marcos claros de regulación, ética y gobernanza. En el contexto europeo, el Reglamento de IA establece un precedente normativo relevante, mientras que organismos como la OCDE y la UNESCO han formulado principios ampliamente reconocidos —como la equidad, la transparencia y la rendición de cuentas— que las empresas deben tomar como guía para el diseño e implementación de sus políticas internas en materia de inteligencia artificial.

La clave está en implementar un ecosistema de gobernanza alrededor de la IA: políticas claras, comités de ética, auditorías, formación especializada y controles efectivos. La supervisión humana debe mantenerse siempre presente. Algunas organizaciones ya utilizan IA para monitorear riesgos en tiempo real, documentando cada decisión para responder ante auditores y reguladores, pero siempre bajo la supervisión de equipos expertos.

Aunque persisten desafíos técnicos y culturales, es probable que surjan nuevas certificaciones, metodologías de auditoría y directrices sectoriales específicas. El *compliance officer* del futuro deberá combinar conocimientos legales, éticos y tecnológicos, y los Consejos de Administración deben asumir un rol activo, tratando la IA como un tema estratégico, no solo técnico.

En conclusión, la IA puede reforzar el buen gobierno si se implementa con ética, liderazgo y prevención. Las empresas deben

adaptar las recomendaciones propuestas a su realidad, asegurando que la IA complemente la inteligencia humana. Esa sinergia bien gestionada puede impulsar una función de cumplimiento más preventiva, justa y resiliente, en beneficio de toda la organización y la sociedad.

REFERENCIAS

Parlamento Europeo – *Artificial Intelligence Act: MEPs adopt landmark law* (2024).

OCDE – *OECD AI Principles* (2019).

UNESCO – *Recommendation on the Ethics of Artificial Intelligence* (2021).

Grupo Atico34 – *Buenas prácticas para el uso de la inteligencia artificial* (2023).

ISO – *ISO/IEC 42001:2023 AI Management System* (2023).

Diario La Ley – *IA y Buen Gobierno* (2025).

SOBRE EL AUTOR

Albert Salvador Lafuente es Cofundador y Secretario General Internacional en World Compliance Association