

A portrait of Jose Francisco Rodríguez, a middle-aged man with grey hair, wearing green-rimmed glasses, a white shirt, and a dark blue blazer. He has his arms crossed and is smiling slightly. The background is blurred, showing what appears to be an office or indoor setting with warm lighting.

VERINT.
engage **24**
ESPAÑA

Como afecta el nuevo Reglamento de Inteligencia Artificial a los Contact Centers

Jose Francisco Rodríguez
Presidente asociación AEERC
Jose.francisco.rodriguez@aeerc.com

Rosewood villa magna

VERINT.

© 2024 Verint Systems Inc. All Rights Reserved Worldwide.
CONFIDENTIAL AND PROPRIETARY INFORMATION OF VERINT SYSTEMS INC.

¿Qué es el Reglamento de Inteligencia Artificial?

El Reglamento de IA tiene por objeto garantizar que los sistemas de inteligencia artificial (IA) se desarrollen y utilicen de manera responsable. Las normas imponen **obligaciones a los proveedores y los responsables del despliegue de tecnologías de IA** y regulan la autorización de los **sistemas de inteligencia artificial** en el mercado único de la UE.

El Reglamento aborda los **riesgos** relacionados con la IA, como los sesgos, la discriminación y las lagunas en la rendición de cuentas, promueve la **innovación** y fomenta la adopción de la IA.

Dado que se trata de la primera norma jurídica del mundo encaminada a regular la IA, las disposiciones del Reglamento de la UE podrían convertirse en un **referente a escala mundial** en materia de regulación de la IA, como lo es el Reglamento General de Protección de Datos (RGPD) en materia de privacidad de los datos, y promover una inteligencia artificial ética, segura y fiable en todo el mundo.

La Ley Europea de Inteligencia Artificial establece varias medidas específicas para garantizar la transparencia en el uso de IA, especialmente en la atención al cliente:

1. Informar a los usuarios: Las empresas deben notificar a los usuarios cuando están interactuando con un sistema de IA, ya sea a través de chatbots o llamadas telefónicas, para que sean conscientes de que no están tratando con una persona real.
2. Explicabilidad: Los sistemas de IA, especialmente los de alto riesgo, deben proporcionar información clara sobre sus capacidades y limitaciones. Esto permite a los usuarios entender cómo se toman las decisiones y tomar decisiones informadas.
3. Control humano: En aplicaciones de alto riesgo, debe haber mecanismos para que un ser humano supervise y controle las decisiones importantes tomadas por la IA, garantizando que no dependan exclusivamente del algoritmo.

Estas medidas buscan fomentar un uso ético y responsable de la IA, protegiendo los derechos de los usuarios y promoviendo su confianza en la tecnología.

Para asegurar que la personalización con IA sea ética y transparente, se deben seguir varios principios fundamentales:

1. **Transparencia:** Informar a los usuarios cuando interactúan con un sistema de IA, como chatbots o recomendaciones personalizadas, para que sepan que no están tratando con una persona real.
2. **Protección de datos:** Cumplir con las normativas de protección de datos, garantizando que la información personal utilizada para personalizar el servicio esté adecuadamente protegida y no se utilice sin consentimiento.
3. **Evitar sesgos y discriminación:** La IA debe ser diseñada y entrenada con datos diversos y de alta calidad para evitar sesgos que puedan resultar en discriminación o trato injusto hacia ciertos grupos de usuarios.
4. **Supervisión humana:** Mantener un control humano sobre las decisiones importantes tomadas por la IA, especialmente en casos donde las decisiones pueden afectar significativamente a los usuarios, como en temas de crédito o empleo.
5. **Explicabilidad:** Asegurar que los algoritmos sean explicables, es decir, que los usuarios puedan entender cómo y por qué se toman ciertas decisiones personalizadas, lo que fomenta la confianza en el sistema.

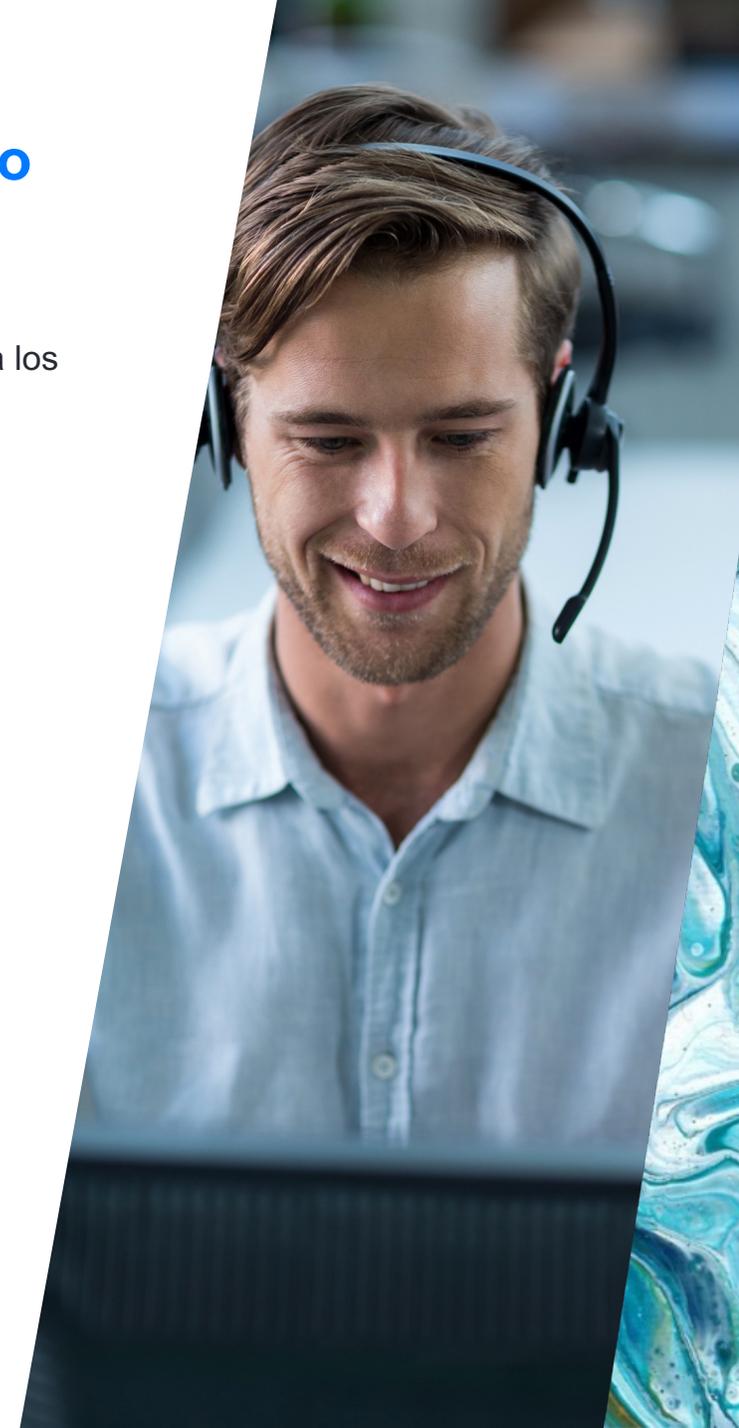
Siguiendo estos principios, las empresas pueden garantizar que el uso de la IA en la personalización sea ético, transparente y respetuoso con los derechos de los clientes.



La normativa europea clasifica los sistemas de inteligencia artificial (IA) en cuatro categorías de riesgo, según el impacto que puedan tener sobre los derechos fundamentales y la seguridad de las personas:

1. **Riesgo inaceptable:** Estos sistemas están prohibidos porque representan una amenaza significativa para los derechos fundamentales. Ejemplos incluyen IA que manipula el comportamiento humano, explota vulnerabilidades o utiliza técnicas subliminales, y sistemas de puntuación social.
2. **Riesgo alto:** Son sistemas que pueden afectar gravemente la seguridad o los derechos de las personas. Incluyen aplicaciones en infraestructuras críticas, sanidad, educación, contratación laboral, y servicios esenciales. Estos sistemas están sujetos a estrictos requisitos de transparencia, documentación y supervisión humana.
3. **Riesgo limitado:** Estos sistemas requieren obligaciones específicas de transparencia, como notificar a los usuarios que están interactuando con IA (por ejemplo, chatbots). Aunque no presentan un riesgo grave, deben garantizar la supervisión humana cuando sea necesario.
4. **Riesgo mínimo:** La mayoría de los sistemas de IA entran en esta categoría. No plantean riesgos significativos y no están sujetos a regulaciones estrictas. Ejemplos incluyen filtros de correo basura o videojuegos basados en IA.

Este enfoque basado en el riesgo permite regular la IA de manera proporcional a su impacto potencial, garantizando la seguridad y protección de los derechos fundamentales sin frenar la innovación.



En la industria de atención al cliente y contact centers, los riesgos asociados a la implementación de la Ley de Inteligencia Artificial (IA) pueden vincularse con los siguientes puntos clave destacados en la imagen:

1. Prohibiciones aplicables: Algunas aplicaciones de IA podrían estar prohibidas si se considera que vulneran derechos fundamentales, como el uso de IA para manipular el comportamiento del cliente o tomar decisiones automatizadas sin supervisión humana en temas críticos.
2. Documentación (gestión documentada de riesgos): Los contact centers deberán documentar cómo gestionan los riesgos asociados al uso de IA, especialmente en áreas como la automatización de quejas o consultas, garantizando que los sistemas sean seguros y respeten la privacidad.
3. Transparencia: Es crucial informar a los clientes cuando interactúan con sistemas automatizados, como chatbots o asistentes virtuales, para cumplir con las normativas de transparencia y evitar confusiones.
4. Robotización: El aumento del uso de IA en tareas repetitivas, como la gestión de consultas simples, puede mejorar la eficiencia, pero también plantea el desafío de equilibrar la automatización con la intervención humana en casos más complejos.
5. Resolución automatizada de quejas, consultas y reclamaciones: La IA puede resolver automáticamente problemas comunes, pero es necesario garantizar que estas soluciones no perjudiquen a los clientes ni generen respuestas inadecuadas.
6. Estandarización: Los contact centers deberán seguir estándares establecidos por la normativa para asegurar que sus sistemas de IA operen dentro de los límites legales y éticos, evitando sesgos o discriminación en las decisiones automatizadas.

En resumen, las empresas deben implementar medidas para gestionar estos riesgos, asegurando el cumplimiento normativo mientras aprovechan los beneficios de la IA para mejorar la atención al cliente.

La inteligencia artificial (IA) puede mejorar la personalización del servicio al cliente de las siguientes maneras:

1. **Recomendaciones personalizadas:** Utilizando algoritmos de aprendizaje automático, la IA puede analizar el historial de compras y comportamiento de los clientes para sugerir productos o servicios que se ajusten a sus preferencias.
2. **Atención más rápida y eficiente:** Los chatbots impulsados por IA pueden ofrecer respuestas inmediatas y personalizadas a las consultas de los clientes, mejorando la velocidad y precisión del servicio.
3. **Experiencias únicas:** La IA permite crear experiencias personalizadas basadas en las interacciones previas, preferencias y necesidades específicas de cada cliente, lo que aumenta su satisfacción y lealtad.
4. **Segmentación de clientes:** La IA puede segmentar a los clientes en función de sus comportamientos y características, permitiendo campañas de marketing más efectivas y dirigidas.

En resumen, la IA permite a las empresas ofrecer un servicio más personalizado, eficiente y adaptado a las necesidades individuales de cada cliente, lo que mejora la experiencia general del usuario.



Calendario

6 meses después de la entrada en vigor:

- Prohibiciones de riesgo inaceptable AI. ([Artículo 113](#))

9 meses después de la entrada en vigor:

- Deben ultimarse los códigos de buenas prácticas para la IA de propósito general (GPAI). ([Artículo 113](#))
- 12 meses después de la entrada en vigor:

Se aplican las normas del GPAI. ([Artículo 113](#))

Nombramiento de las autoridades competentes de los Estados miembros. ([Artículo 70](#))

Revisión anual de la Comisión y posibles modificaciones de las prohibiciones. ([Artículo 112](#))

- 18 meses después de la entrada en vigor:

La Comisión publica actos de ejecución por los que se crea una plantilla para el plan de seguimiento poscomercialización de los proveedores de IA de alto riesgo. ([Artículo 6](#))

A los 24 meses de la entrada en vigor:

Ahora se aplican las obligaciones sobre los sistemas de IA de alto riesgo enumerados específicamente en el anexo III, que incluye los sistemas de IA en biometría, infraestructuras críticas, educación, empleo, acceso a servicios públicos esenciales, aplicación de la ley, inmigración y administración de justicia. ([Artículo 111](#))

Los Estados miembros deben haber aplicado normas sobre sanciones, incluidas multas administrativas. ([Artículo 57](#))

Las autoridades de los Estados miembros deben haber creado al menos un espacio aislado operativo para la regulación de la IA. ([Artículo 57](#))

Revisión por la Comisión, y posible modificación, de la lista de sistemas de IA de alto riesgo. ([Artículo 112](#))

- 36 meses después de la entrada en vigor:

Se aplican las obligaciones relativas a los sistemas de IA de alto riesgo [del anexo I](#). ([Artículo 113](#))

Obligaciones para los sistemas de IA de alto riesgo no prescritos en [el anexo III](#) pero destinados a utilizarse como componente de seguridad de un producto, o el IA es en sí mismo un producto, y el producto debe someterse a una evaluación de conformidad por terceros en virtud de la legislación específica vigente de la UE, por ejemplo, juguetes, equipos de radio, productos sanitarios para diagnóstico in vitro, seguridad de la aviación civil y vehículos agrícolas. ([Artículo 113](#))

A finales de 2030:

Las obligaciones entran en vigor para determinados sistemas de IA que son componentes de los sistemas informáticos a gran escala establecidos por la legislación de la UE en los ámbitos de libertad, seguridad y justicia, como el Sistema de Información de Schengen. ([Artículo 111](#))

La encuesta realizada por LHH Executive Search, refleja que se produce un empate técnico a la hora de crear o destruir puestos de trabajo.

- ✓ Más del 80% de los directivos españoles carece de guía para hacer un uso ético de la inteligencia artificial.
- ✓ Un 30% de los directivos declara que crearán nuevos puestos de trabajo para la gestión de proyectos de IA
- ✓ Un 29,62% sustituirán tareas desarrolladas por empleados por nuevas herramientas de IA

En cuanto a las prioridades estratégicas en 2024, destacan:

- ✓ Productividad y rendimiento de los trabajadores (56,54%)
- ✓ Transformación digital (44,42%)
- ✓ Conciliación y flexibilidad (29,42%)
- ✓ Sostenibilidad (24,42%)
- ✓ Salud mental de los equipos (23,27%)
- ✓ Igualdad e inclusión (19,23%)



Gracias



jose.francisco.rodriquez@aeerc.com

VERINT
engage **24**
ESPAÑA