MAGAZINE Nº9
#INTELIGENCIAARTIFICIAL

# Gobernanza de la Inteligencia Artificial en Ciberseguridad

El Magazine de ISMS Forum - International Information Security Community



**MARZO 2024**
www.ismsforum.es

**EDITA**
**ISMS Forum**

**CONSEJO EDITORIAL, DISEÑO Y MAQUETACIÓN**
**Cynthia Rica Gómez**

**EQUIPO**

**MANAGING DIRECTOR**
**Daniel García Sánchez**

**DEPUTY DIRECTOR OF EVENTS**
**Leire Ruiz Díaz-Rullo**

**DEPUTY DIRECTOR OF PROJECTS, TRAINING AND CERTIFICATION**
**Beatriz García**

**CORPORATE COMMUNICATION MANAGER**
**Cynthia Rica Gómez**

**EVENT MANAGER**
**Andrea Gallego**

**CERTIFICATION MANAGER**
**Wasim Escribano**

**FINANCIAL CONTROLLER**
**Mayte Alonso**

**SALES SUPPORT AND ADMINISTRATION**
**Virginia Terrasa**

**TRAINING AND PROJECTS TECHNICIAN**
**Raquel de Saá**

**TRAINING TECHNICIAN**
**Óscar Hernández**

**PÁGINA WEB**
**www.ismsforum.es**

# JUNTA DIRECTIVA

**PRESIDENTE**
**Gianluca D'Antonio, miembro independiente**

**VICEPRESIDENTE**
**Carlos Alberto Saiz, Ecix Group**

**TESORERO**
**Roberto Baratta, Abanca**

**VICESECRETARIO**
**Francisco Lázaro, RENFE**

**SECRETARIO DEL CONSEJO ASESOR**
**Juan Miguel Velasco**

**VOCALES**
**Agustín Muñoz, Accenture**
**Gonzalo Asensio, Bankinter**
**Virginia Rodríguez, CaixaBank**
**Rafael Hernández, CEPSA**
**Fanny Pérez, Codere**
**Rubén Frieiro Barros, Deloitte**
**Ricardo Sanz, Evolutio**
**Edwin Blom, FCC**
**Francisco Navarro, Grupo Cajamar**
**Luis Buezo, Hewlett Packard Enterprise**
**Jesús Mérida, Iberia**
**Susana del Pozo, IBM**
**Marcos Gómez, INCIBE**
**David Barroso, miembro independiente**
**Guillermo Llorente, miembro independiente**
**Jesús Sánchez, Naturgy**
**José Ramón Monleón, Orange**
**Javier Urtiaga, PwC**
**Javier García Quintela, REPSOL**
**Pablo Echevarría, S21sec**
**Iván Sánchez, Sanitas**
**Elena García, Indra**
**Miguel Ángel Pérez, Telefónica**
**Toni García, miembro independiente**
**Jesús García del Valle, Santander**






# CONTENIDOS

ISMS FORUM MA







# GAZINE

# CARTA DEL PRESIDENTE

# ISMS Forum Impulsa la Gobernanza de la Inteligencia Artificial en el Sector de la Ciberseguridad

*Gianluca D'Antonio, Presidente, ISMS Forum*

Cuando hablamos de Inteligencia Artificial nos imaginamos un mundo de posibilidades y aplicaciones que potenciarán nuestras capacidades hasta niveles inimaginables hace solo unos años.

La inteligencia artificial generativa se ha convertido en el nuevo paradigma de la innovación hasta el punto que algunos ya la consideran una Transformación Digital 2.0.

Para el ISMS Forum, como Asociación española dedicada a la seguridad de la información y la ciberseguridad, sin embargo la IA supone quizá el mayor reto y a la misma vez el aliciente para seguir impulsando una mirada critica hacia la gestión de los riesgos tecnológicos.

Es en este contexto que ISMS Forum ha creado un grupo de trabajo sobre AI con el propósito de ayudar las organizaciones y profesionales en la Gobernanza, Seguridad y Cumplimiento de este nuevo paradigma tecnológico.

El GIA (así es como se denomina este grupo de trabajo) ha identificado diferentes líneas de acción que servirán para ofrecer un soporte y líneas guías en aspectos de la IA tan significativos como la elaboración de modelos de referencia para cláusulas contractuales con terceros, controles de seguridad para servicios o proyectos que empleen esta tecnología y seguridad ante Deepfakes para citar solo algunas.

El 21 de marzo la Asociación celebrará el primer congreso dedicado al análisis de los riesgos relacionados con la IA.

Invitamos todos los asociados a participar y sumarse a esta nueva iniciativa.

# ACTUALIDAD ISMS

# ISMS Forum presenta GIA: el nuevo grupo de trabajo dedicado a la Inteligencia Artificial

*Redacción ISMS Forum*

> Grupo de Inteligencia Artificial (GIA), así se llama la nueva iniciativa transversal a todas las áreas de ISMS Forum, que impulsa el aprendizaje y mejora en el desarrollo de la Inteligencia Artificial.

El Grupo de Inteligencia Artificial (GIA) se establece como un equipo multidisciplinario con la misión de:

- Generar y difundir conocimiento en temas de seguridad, gobernanza y cumplimiento, orientado tanto a sus miembros como a la sociedad en general.
- Consolidarse como un actor relevante e influyente en dichos ámbitos frente a terceros.
- Facilitar una participación dinámica de los asociados y otros stakeholders clave para lograr los objetivos mencionados anteriormente.

Dada la omnipresencia de la Inteligencia Artificial en todas las áreas de trabajo de la asociación, el grupo de IA se concibe como una iniciativa transversal que contribuye de manera integral a cada una de ellas.

En esta nueva área, a través de sus grupos de trabajo y foros anuales, se busca fomentar el intercambio de conocimientos, informes y estudios que impulsen actividades relacionadas con la materia.

Hasta la fecha el grupo de trabajo ha presentado los siguientes trabajos:


El Modelo de Gobierno de la IA describe los principios para una apropiada gobernanza en el desarrollo y uso de sistemas de IA, para así incrementar la seguridad y la confianza en dichas tecnologías.

En la guía Ética y compliance en el uso de la IA se analizarán los elementos que la UE ha considerado más relevantes para abordar los riesgos generados por los usos específicos de la IA. Aunque se considera que la mayoría de los sistemas de IA no generan riesgos para los ciudadanos, ciertos sistemas de IA sí pueden dar lugar a riesgos o consecuencias negativas para personas concretas o la sociedad en su conjunto.



A lo largo de las páginas de la Introducción a la IA para profesioanles de Seguridad de la Información de 2023 se tratan diversos conceptos y aspectos relacionados con la Inteligencia Artificial (IA en adelante), por eso se ha ido buscando una definición de IA que entender qué es.

La Guía sobre Inteligencia Artificial y Ciberseguridad detalla los riesgos asociados con el uso de la IA, destacando incidentes mediáticos relevantes. Ofrece frameworks y guías para mitigar los riesgos de seguridad en la IA, así como mecanismos de auditoría. Además, aborda la gestión de proyectos con IA, diferenciando entre el uso de servicios externos y el desarrollo de sistemas propios. También examina el uso malicioso de la IA para ataques y proporciona recomendaciones para prevenir su abuso. Por último, reflexiona sobre los posibles fallos en la implementación de sistemas de IA.



El uso de los sistemas de IA, los diversos riesgos y obligaciones de cumplimiento de esta normativa han de gestionarse de manera adecuada, de manera que, como parte del sistema interno de Gobierno y el Compliance y la implantación de la estrategia corporativa y valores éticos de las organizaciones, resultará necesaria la elaboración de una política de uso de soluciones de IA que establezca claramente los principios, criterios y normas que deben regir el comportamiento de todos los empleados con relación al uso de esta tecnología. En la guía Polítia de Inteligencia Artificial se mostrarán los aspectos principales que deberán tenerse en consideración en el desarrollo de una política de este tipo y un detalle de los principales epígrafes a contemplar en la misma.

# ISMS inaugura el Capítulo Regional de Andalucía e inicia su andadura internacional poniendo en marcha los capítulos de Portugal y México

*Redacción ISMS Forum*

**En 2019, ISMS Forum decide abrir sus fronteras y crecer nacionalmente, apostando por la creación de capítulos regionales en territorio español para llevar los objetivos de la Asociación de forma más específica a zonas que tienen sus propias particularidades y problemáticas en materia de ciberseguridad y protección de datos. Hoy, ISMS Forum sigue expandiéndose nacionalmente intentando atender al interés de aquellas empresas y profesionales no ubicados en Madrid que encuentran la necesidad de mantener una actividad mayor fuera de la capital española.**

> Llegó el momento de constituir el Capítulo Regional de Andalucía y dar el paso para acercar la Asociación también fuera del país con los nuevos Capítulos internacionales: ISMS Portugal e ISMS México.

## ISMS FORUM ANDALUCIA

ISMS Forum inaugura el Capítulo Regional de Andalucía en el Centro de Ciberseguridad de Andalucía, ubicado en la ciudad de Málaga, consolidándose como actor central en la región. Este surge con el propósito de fomentar la colaboración entre los sectores público y privado en un entorno donde el cumplimiento regulatorio en ciberseguridad y privacidad presenta desafíos.

Las actividades planificadas se llevarán a cabo a nivel regional, abarcando a profesionales y entidades de las diversas provincias de Andalucía. Juan García, coordinador de ISMS Andalucía, destaca: **"El capítulo andaluz nace con el objetivo de promover la seguridad de la información y la protección de datos a nivel regional. La elección de Málaga como sede nos permite estar más cerca de la próspera comunidad de profesionales y entidades del sector que eligen la ciudad debido a la presencia significativa de empresas tecnológicas y de ciberseguridad".**

## ISMS FORUM MEXICO

Este nuevo capítulo internacional llevará a cabo eventos, nuevas guías y grupos de trabajo con el propósito de capitalizar y adaptar las mejores prácticas creadas en España, elevar los estándares de ciberseguridad a nivel nacional, establecer una amplia red de contactos para fortalecer la ciberseguridad en los sectores público y privado, y apoyar el intercambio de información más allá de las fronteras para una gestión efectiva de amenazas. Este capítulo jugará un papel fundamental en la promoción, fortalecimiento y representación de la ciberseguridad en México, con la colaboración de España.

Fanny Pérez, coordinadora de ISMS Forum México, afirma: **"La decisión de comenzar en México se debe a la relevancia que el país tiene en el ámbito de la ciberseguridad en Latinoamérica, además de la presencia de muchas empresas asociadas a ISMS Forum en este territorio".**

## ISMS FORUM PORTUGAL

En Portugal, ISMS Forum inaugura un nuevo capítulo internacional con sede en Lisboa. ISMS Forum Portugal nace con el objetivo de desarrollar mejores prácticas tecnológicas en el contexto portugués. La colaboración entre España y Portugal permitirá a ISMS Forum expandir sus conocimientos mediante la celebración de eventos, el desarrollo de nuevos grupos de trabajo y la elaboración de documentos que mejoren las prácticas en ciberseguridad y protección de datos en Portugal, así como promover una cultura de Seguridad de la Información a nivel internacional.

# CAFÉ CON EXPERTOS

# Desvelando el Futuro de la Ciberseguridad: Entrevista Exclusiva con Expertos de ISMS Forum sobre las Guías para la Era de la Inteligencia Artificial

*Redacción ISMS Forum*

**En una conversación esclarecedora con Ángel Pérez, CISO de Autopistas, y Francisco Lázaro, CISO y DPO de Renfe y miembro de la Junta Directiva de ISMS Forum, nos revelan el profundo compromiso del Grupo de Inteligencia Artificial (GIA) con el avance y la comprensión de la Inteligencia Artificial (IA) en el ámbito de la seguridad de la información. En particular, se destacan las recientes guías publicadas por este grupo, abordando aspectos cruciales como el uso ético, la implementación efectiva y el gobierno de la IA en las organizaciones.**

**Estas guías, presentadas en la última jornada internacional de ISMS Forum, no solo proporcionan orientación práctica, sino que también reflejan el compromiso de la comunidad de seguridad de la información con la adaptación y la evolución en un panorama tecnológico en constante cambio. La iniciativa surge en respuesta a la creciente importancia y presencia de la IA en diversas esferas de la sociedad y las organizaciones, reconociendo la necesidad de proporcionar recursos actualizados y relevantes para los profesionales en un campo tan dinámico como la IA. Con un enfoque en la concienciación, la educación y la adaptación continua, estas guías representan un valioso recurso para las empresas en su viaje hacia la comprensión y la integración efectiva de la IA en sus prácticas de seguridad de la información.**

Este grupo ya implementó unas guías sobre IA que se presentaron en la última jornada internacional de ISMS Forum recientemente, ¿qué utilidad van a tener para las empresas?

Ángel Pérez: Si bien creemos que son de gran utilidad, los ritmos de adopción de las tecnologías de inteligen-cia artificial son distintos en función del sector de actividad de cada organización, debido a ello entendemos que algunos documentos serán consultados en tiempo distinto por cada profesional de seguridad de la información en función de la necesidad que tengan.

Hasta el momento los trabajos publicados han sido: Disclaimer uso de IA en las organizaciones; Encuesta Adopción y Gobierno de la IA; Introducción a la IA para profesionales de Seguridad de la Información; Ética y Compliance en IA; Política de Uso de la IA; Modelo de Gobierno de la IA; IA y Ciberseguridad.

**ÁNGEL PÉREZ BEUMALA**

CISO, Autopistas.

Los dos primeros documentos creemos que son de interés general, el primero porque ofrece consejos prácticos para concienciar a los usuarios de las organizaciones frente al uso de estas herramientas públicas y gratuitas como ChatGPT o Google Gemini y los riesgos asociados, y el segundo trabajo porque ofrece una foto del estado de arte sobre la adopción y el gobierno de la IA en las organizaciones en que cada uno puede compararse.

El trabajo de "Introducción a la IA para profesionales de seguridad de la Información" supone un esfuerzo de los voluntarios que lo llevaron a término para explicar conceptos clave de estas tecnologías y que sirva para actualizar conocimientos.

Por su parte el documento "Ética y compliance en IA" es referente en el ámbito de gestión de riesgos regulatorios, se ha basado en gran parte en el borrador del Reglamento de Inteligencia Artificial de la UE, con lo que lo consideramos de lectura obligada para cualquier profesional que deba afrontar este reto.

Relacionado con el anterior y, por el singular interés que tienen, hemos publicado como entregables aparte los trabajos "Política de Uso de la IA", que ofrece una plantilla y reflexiones sobre cómo elaborar una política de estas características, y el trabajo "Modelo de Gobierno de la IA", dedicado a presentar buenas prácticas y recomendaciones en esta materia.

El último trabajo publicado "IA y Ciberseguridad" es el que debería haber sido el primero pero se retrasó por su complejidad, un documento extenso que ofrece diversas perspectivas desde el ámbito Ciber, siendo las más relevantes el planteamiento de uso de la IA a favor de ciber, como herramienta adversa y modelos de gestión de riesgos asociados.

**¿Qué motivó a ISMS Forum a publicar estas guías sobre inteligencia artificial?**

Ángel Pérez: Los expertos en IA nos avisan que esta tecnología ya es pervasiva, lleva décadas desplegándose en las organizaciones y la sociedad en general, algunas veces en aplicaciones tan supuestamente triviales como las redes sociales y otras en aplicaciones de propósito más serio como sistemas de detección de anomalías.

Francisco Lázaro: Noviembre de 2022 supuso un punto de inflexión provocado por la presentación de chatgpt, el primer modelo de IA Generativa abierto al público y de muy fácil acceso. Esta nueva rama de la IA ha provocado una disrupción en las estrategias de transformación digital de las organizaciones.

Siendo conscientes de que muchos profesionales de Seguridad de la Información tenemos lagu-nas de conocimiento frente esta nueva tecnología, decidimos impulsar un trabajo sobre IA y Ciberseguridad, posteriormente nos dimos cuenta de que el trabajo merecía ser más extenso y ello derivó en los 7 trabajos publicados hasta la fecha así como un grupo de trabajo permanente (el GIA) y nuevos proyectos para 2024 como es la primera edición del "IA & Cybersecurity Forum".

**¿Cómo se pueden mantener actualizadas estas guías en un campo tan dinámico como la Inteligencia Artificial?**

Francisco Lázaro: La actualización de estas guías es un reto similar al que tienen los otros trabajos que lleva ya tiempo publicando la asociación, muy probablemente algunos de los mismos algunos deberán tener nuevas revisiones próximamente y otros probablemente dejarán de tener sentido.

Lo bueno de las ediciones digitales es que permiten una más rápida actualización, las cuales pueden incluso no ser extensas pero sin embargo responder a una necesidad de actualizar, complementar o corregir, si esas nuevas contribuciones son relevantes para la nuestros asociados; como por ejemplo con la reciente aprobación del Reglamento de la UE sobre la IA.

Por seguir con ese ejemplo de necesidad de tener actualizada las guías, tendremos que entender, analizar y divulgar lo que la Ley

> Si bien creemos que son de gran utilidad, los ritmos de adopción de las tecnologías de inteligencia artificial son distintos en función del sector de actividad de cada organización, debido a ello entendemos que algunos documentos serán consultados en tiempo distinto por cada profesional de seguridad de la información en función de la necesidad que tengan.

establece y su repercusión en la sociedad y las Organizaciones. Así por ejemplo, conforme lo aprobado por el parlamento europeo, los sistemas de aprendizaje automático se dividirán en cuatro categorías principales en función del riesgo potencial que supongan para la sociedad. Los sistemas considerados de alto riesgo estarán sujetos a normas estrictas que se aplicarán antes de que entren en el mercado de la UE. Las normas generales sobre IA se aplicarán un año después de su entrada en vigor, en mayo de 2025, y las obligaciones para los sistemas de alto riesgo en tres años. Estarán bajo la supervisión de las autoridades nacionales. En este ejemplo, creo que vemos claro que hay etapas y que conformen se acerquen las mismas seguro que hay cuestiones relevantes sobre las que debatir e incorporar.

**¿Cuáles consideran que son los aspectos más críticos que las organizaciones deben tener en cuenta al implementar soluciones de IA, y cómo abordan estas guías esos desafíos específicos?**

Francisco Lázaro: Probablemente como toda nueva tecnología y más cuando irrumpe con tanta fuerza como lo está haciendo la IA, exista dentro de las Organizaciones, múltiples impulsores que llevados por grandes expectativas de innovación, o por deseos de descubrir las capacidades potenciales o de liderar internamente el descubrimiento de esta nueva tecnología, desenfoquen la importancia de abordar estas nuevas capacidades con orden y criterio.

Por eso, es esencial elaborar una hoja de ruta estratégica, con foco en la entrega de valor

identificando los dominios y casos de uso , las fases graduales de adopción y crecimiento, donde se tomen las decisiones estratégicas e identificando elementos básicos tales como la definición de la visión y el valor en juego, la visión del estado futuro, así como la hoja de ruta que nos permita alcanzar las diferentes etapas, identificando los riesgos y controles de gestión de dicho riesgo. Como parte de esa ruta estratégica, no debemos olvidar la necesidad de identificar aquellas funciones y roles básicos que necesitaremos en esta etapa de estrategia.

En esta etapa, las Organizaciones que están iniciando el camino, lo hacen en la mayoría de los casos articulando la capa de Gobierno, mediante un comité de adopción de la IA, donde están presentes los perfiles/áreas que pueden ayudar a implementar con éxito (lo que incluye de forma segura y respetuosa con las leyes) la IA. El comité suele estar compuesto por profesionales de las áreas de legal, ciberseguridad, protección de datos, tecnología y Negocio. Reservando, habitualmente, el papel de liderazgo no a tecnología sino a Negocio.

En dicho comité se identifica y elabora la ruta estratégica, se definen funciones y competencias específicas de la IA (definiendo que funciones se desarrollarán internamente o incorporarán como internas, cuales se contratarán externamente a través de socios o vendedores). También el comité deberá diseñar un modelo operativo (modo de trabajo,

**FRANCISCO LÁZARO**

CISO y DPO, Renfe.

implicación y formación de usuarios, casos de uso o grado de centralización , entre otras cuestiones) y deberá identificar tanto un modelo de Tecnología (propia, comercial interna o dedicada o compartida), así como un modelo de gobierno / uso de Datos. Los proyectos concretos, se abordan en el comité o en mesas especificas para cada proyecto.

Para cada uno de los proyectos se deben identificar y gestionar los riesgos asociados a ese proyecto concreto (legales, privacidad, éticos, sesgo, ciber, etc..). Las Guías del grupo GIA, que ha citado Angel, analizan , reflexionan y divulgan estos riesgos.

A nuestro entender este tipo de comité no solo deben marcar la estrategia de adopción y posibilitarla sino que debe ser un comité de adopción y ampliación de la IA. Logrará adoptar y crecer, a través de la identificación y monitorización de los casos de uso, verificando que aporten los beneficios esperados, identificando e involucrando a las personas y departamentos clave para el cambio, con un alineamiento estratégico , donde finalmente la gestión de recursos técnicos y humanos sean claves para el éxito de esa adopción y ampliación del uso de la IA.

Las guías de una forma estructurada y didáctica nos aportan los conocimientos necesarios para entender y trabajar con la IA. Nos habla de sus conceptos básicos, de las amenazas y las oportunidades y nos da las claves tanto para

construir las capas de Gobierno, Operación y Recursos que nos permitan utilizar responsablemente y con éxito la IA, como para minimizar los diferentes riesgos que se identifican en estas (en las guías).

**La otra pata tecnológica es la ciberseguridad. ¿Qué riesgos y ayuda genera la IA?**

Francisco Lázaro: Si nos centramos en la práctica de la seguridad, las principales amenazas que nos pueden venir del uso de esta tecnología por parte de agentes maliciosos son:

- La automatización de ataques: La IA puede ser utilizada para automatizar ciber-ataques cibernéticos, tales como el phishing, haciendo que estos sean más eficientes y difíciles de detectar o para analizar grandes volúmenes de datos y personalizar los ataques a las vulnerabilidades específicas de un sistema, red o compañía.
- Evasión de la detección: Los sistemas de IA pueden ser entrenados para evadir las técnicas de detección tradicionales, haciendo que los ataques sean más difíciles de identificar y detener.
- Deepfakes y desinformación: puede ser utilizada para crear deepfakes mediante videos o audios falsos altamente realistas, los cuales pueden ser utilizados para propagar desinformación, manipular opiniones públicas o realizar estafas.

> Las guías de una forma estructurada y didáctica nos aportan los conocimientos necesarios para entender y trabajar con la IA. Nos habla de sus conceptos básicos, de las amenazas y las oportunidades y nos da las claves tanto para construir las capas de Gobierno, Operación y Recursos que nos permitan utilizar responsablemente y con éxito la IA.

- Ataques a la privacidad: La IA puede ser utilizada para analizar y extraer grandes volúmenes de datos personales, lo que representa un riesgo significativo para la privacidad de los individuos.

- Ataques a sistemas de IA: Los sistemas basados en IA también pueden ser vulnerables a ataques, como el envenenamiento de datos, donde se manipulan los datos de entrenamiento de un sistema de IA para que tome decisiones erróneas o malintencionadas o las propias del desarrollo y los algoritmos

- Riesgos asociados con la automatización por la IA: La dependencia de sistemas automatizados basados en IA puede llevar a una falta de supervisión humana, lo que podría resultar letal en la toma de decisiones erróneas en situaciones de ciberseguridad críticas.

Y estos usos por parte de delincuentes o de otros grupos maliciosos, no son teóricos, pues por ejemplo, recientemente Microsoft y OpenIA han publicado conjuntamente las investigaciones que les ha permitido desarticular los usos maliciosos de cinco grupos relevantes de actores maliciosos, que ponían en práctica los usos a los que nos acabamos de referir. Los grupos son dos de china (Charcoal Typhoon y , Salmon Typhoon ), uno de Irán (Crimson Sandstorm), otro de Corea del Norte (Emerald Sleet), así como Forest Blizzard de Rusia

En cuanto a la utilización de la IA como recurso del área de ciberseguridad, algunas de las principales utilidades las encontraríamos en:

- Detección de amenazas: y prevención de intrusiones La IA puede analizar grandes volúmenes de datos de tráfico de red en tiempo real para identificar patrones que coinciden con tácticas maliciosas o actividades sospechosas que podrían indicar una ciberamenaza, como malware, ransomware o intentos de intrusión, pudiendo detectar y bloquear ataques proactivamente antes de que causen daño, aprendiendo de los intentos de intrusión anteriores y adaptándose a nuevas tácticas utilizadas por los atacantes.

- Análisis de comportamiento: La IA puede monitorear el comportamiento de usuarios y dispositivos dentro de una red para detectar actividades anormales que podrían indicar una amenaza interna, como un empleado que accede a datos sensibles sin autorización.

- Gestión de vulnerabilidades: La IA puede ayudar a priorizar las vulnerabilidades de seguridad en función del riesgo que representan, considerando factores como la probabilidad de explotación y el impacto potencial, permitiendo a los equipos de seguridad enfocarse en las más críticas.

- Análisis forense y de causa raíz: Después de un incidente de seguridad, la IA puede

acelerar el análisis de cómo ocurrió el ataque, identificar la causa raíz y sugerir medidas para prevenir incidentes similares en el futuro.

- Mejora de la autenticación: pueden fortalecer los mecanismos de autenticación, haciéndolos más seguros y menos intrusivos para los usuarios.

- Respuesta automatizada: En caso de detección de una amenaza, sistemas automatizados basados en IA pueden tomar decisiones inmediatas para contenerla, como aislar un dispositivo infectado de la red, sin necesidad de intervención humana inmediata y por ejemplo, a través de SOAR, responder al ataque .

- Entrenamiento y concienciación: La IA también puede personalizar programas de entrenamiento en ciberseguridad para empleados, adaptándolos a sus conocimientos y áreas de mayor riesgo según su comportamiento y roles en la organización.

- Reporte : Esta tecnología, puede sintetizar, subrayar y hacer entendible tanto informes de incidentes , como información estrategica.

Si vamos a la guía de ENISA (European Cybersecurity Skills Framework Profiles) y cruzamos los doce roles de profesionales de ciberseguridad , con estos potenciales beneficios, vemos que la totalidad de roles pueden tener a la IA también como un potente recurso de ciberseguridad y dado que en muchas ocasiones tendemos , erróneamente, a hablar de la IA como si de una entidad humana se tratara, podríamos decir que contarán (contaremos) con una gran aliada.

**La entrevista con Ángel Pérez y Francisco Lázaro de ISMS Forum ofrece una visión esclarecedora sobre el papel crucial que desempeña la inteligencia artificial en la seguridad de la información. Las guías presentadas por el Grupo de Inteligencia Artificial (GIA) no solo proporcionan una orientación práctica y actualizada, sino que también reflejan el compromiso de la comunidad de seguridad de la información con la adaptación y evolución en un entorno tecnológico en constante cambio. Con un enfoque en la concienciación, la educación y la adaptación continua, estas guías representan un recurso invaluable para las organizaciones que buscan comprender y aprovechar de manera efectiva la IA en sus prácticas de seguridad. En definitiva, la colaboración y el enfoque proactivo son fundamentales para enfrentar los desafíos y aprovechar las oportunidades que la IA presenta en el panorama de la ciberseguridad.**

# FIRMA INVITADA

# La Inteligencia Artificial en la Administración de Justicia: Un Avance con Cautela y Garantías

**La Justicia es la primera de las funciones del Estado, pues antes que leyes los pueblos han necesitado iustitia. Y un poder judicial independiente es la garantía esencial del Estado democrático de Derecho: sólo a través de él se protegen los derechos de los ciudadanos, así como se ofrece seguridad jurídica y los mecanismos para una convivencia democrática. A pesar de ello, nuestra Administración de Justicia es uno de los servicios públicos peor valorados por los ciudadanos. Y eso es un signo de alarma. Ahora bien, para los profesionales que trabajamos con ella todos los días, hay extraordinarios jueces y magistrados, y las sentencias procuran hacerlas con calidad.**

Todo ello ha sido objeto de estudio y reflexión por parte de muchas instancias y organizaciones, y naturalmente su análisis desborda los límites de este artículo. Pero la inteligencia artificial sí puede ayudar a mejorar notablemente el funcionamiento de nuestros juzgados y tribunales, y además de forma practicable: automatizando algunos de los procedimientos más sencillos y que copan buena parte de su actividad. Se trataría, por ejemplo, de los procesos monitorios, las reclamaciones de consumo de baja cuantía o los litigios relativos a las cláusulas suelo, también conocidas como suelo hipotecario. A la vez, con esta decisión se reducirían las cargas de trabajo y los jueces podrían atender otros asuntos más intrincados.

**MOISÉS BARRIO ANDRÉS**

Letrado del Consejo de Estado.
Profesor de Derecho digital.
Abogado.

Para implementar esta novedad, sería suficiente con que las partes plantearan sus escritos a través de una aplicación, como ya sucede en la práctica con el sistema LexNET. Y como en estos casos la prueba es documental y los documentos presentan una tipología cerrada, la aplicación podría analizarlos y conseguir un tiempo de resolución incluso de días, el necesario para que el demandado pueda preparar su defensa. Tras ello el sistema podría elaborar una propuesta de sentencia que finalmente será aprobada por el juez. Este es, sin duda, el campo más sencillo por el que la inteligencia artificial debería aplicarse a nuestra Administración de Justicia. Así lo permiten aplicaciones como Modria®, utilizada por eBay o PayPal para la rápida resolución de reclamaciones y que comienza a introducirse en algunos Tribunales de los países más avanzados.

Ahora bien, la inteligencia artificial es una herramienta, sin duda muy relevante, y tiene un campo formidable para mejorar la justicia, pero no puede mitificarse ni devenir en el juez absoluto. El algoritmo desencadena un flujo incesante de datos, invenciones y disrupciones que no siempre se comprenden, estudian o controlan.

Más allá de los problemas de diseño incompleto, sesgo, parcialidad o discriminación de los algoritmos que han sido señalados por voces muy autorizadas, o de la necesidad impuesta por nuestra Constitución de que las decisiones judiciales sean motivadas (art. 120.3 CE) y de permitir ejercer con plenitud el derecho de defensa (art. 24.2 CE), lo cual no es posible con algoritmos cerrados y que no explican cómo han llegado a la decisión, me gustaría destacar aquí cómo la justicia no es un acto de predicción ni un modelo matemático que pueda encerrarse en fórmulas.

> La inteligencia artificial debe integrarse en la Administración de Justicia como un medio de ayuda para su agilización y gestión, pero de manera segura, responsable y transparente, previa evaluación de su impacto en los derechos fundamentales.

En efecto, no hay una metodología jurídica universal y existen diferentes teorías sobre el Derecho, sobre la argumentación o sobre la justicia que dificultan estandarizar y universalizar los razonamientos jurídicos. Todo ello sin olvidar el carácter nacional de muchas ramas jurídicas. O de que el juez no «predice» el derecho, dice el derecho, y ese derecho que el juez determina, si puede coincidir con lo que puede haber sido esperado, y es probablemente deseable que así sea, no es la realización de una predicción. La sentencia del juez es y debe ser la verdad judicial buscada y establecida por medio de un proceso judicial con todas las garantías y que es vinculante para las partes: la justicia en su esencia no puede ser reducida a una predicción matemática o científica.

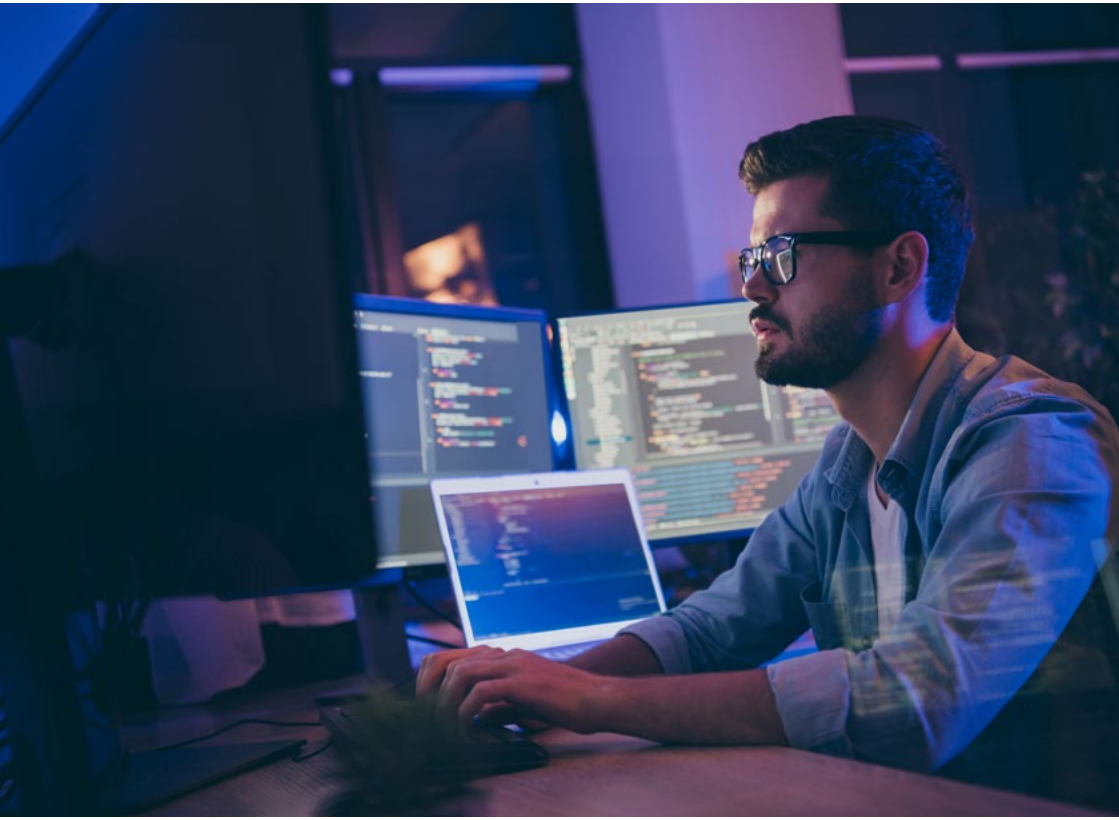
El Derecho no es un conjunto de proposiciones de sentido unívoco y de las que se extraigan respuestas únicas e intelectualmente indiscutibles a las cuestiones litigiosas que debe resolver. Posibilita, a través de un conjunto de leyes conocido, que las normas jurídicas y las decisiones judiciales sean responsablemente adoptadas, razonablemente justificadas y que puedan llegar a ser, tras los oportunos recursos, firmes e inatacables. Por el momento, es el mejor instrumento de certeza y de paz que los seres humanos hemos logrado ordenar hasta hoy. Es verdad que el Derecho es, en último término, una promesa de certeza. Pero la certeza definitiva sólo la puede dar la vida, como bien señaló Couture.

> Y un poder judicial independiente es la garantía esencial del Estado democrático de Derecho: sólo a través de él se protegen los derechos de los ciudadanos, así como se ofrece seguridad jurídica y los mecanismos para una convivencia democrática.

Por eso, el artículo 57 del Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo condiciona las actuaciones judiciales asistidas por IA a ser un borrador, total o parcial, de documento complejo que puede constituir fundamento o apoyo de una resolución judicial.

El precepto establece también que dicho borrador documental sólo se generará a voluntad del usuario, "que podrá ser libre y enteramente modificado por éste", y que "en ningún caso el borrador documental constituirá la resolución judicial procesal sin la validación por parte de la autoridad competente", Juez o Magistrado, Fiscal o Letrado de la Administración de Justicia. Todo ello "en el ámbito de sus respectivas competencias y bajo su responsabilidad, así como [con] la identificación, autenticación o firma electrónica que en cada caso prevea la ley, además de los requisitos que las leyes procesales establezcan".

A mi juicio, el precepto es garantista al máximo con la función jurisdiccional. Estimo que la IA debe integrarse en la Administración de Justicia como un medio o instrumento de ayuda para su agilización y gestión, pero de forma segura, responsable y transparente, previa evaluación de su impacto, especialmente cuando atañe a los derechos fundamentales, y con articulación ex lege de mecanismos adecuados para su gobierno y control, de modo que sirva incluso como herramienta de apoyo para la toma de



decisiones por parte de quién debe ejercer la potestad jurisdiccional. Ahora bien, considero que el éxito del citado Real Decreto-ley 6/2023, de 19 de diciembre vendrá dado por la existencia de los suficientes medios, personales y materiales, para desarrollar y poner en marcha los sistemas previstos.

Por lo demás, estoy profundamente convencido que la seductora atracción por la Justicia digital no debe nunca hacernos olvidar que la función constitucional de los jueces no puede dejar jamás de ser una tarea genuinamente humana, ni apartarse de los principios constitucionales que legitiman la función jurisdiccional.

# EN CLAVE IA

# Europa aprueba el Reglamento de IA para proteger derechos fundamentales y minimizar riesgos

*Redacción ISMS Forum*

**La Agencia Española de Supervisión de Inteligencia Artificial (AESIA) representará a España ante el Comité Europeo de IA.**

> La nueva legislación, que se espera esté completamente en vigor para el primer trimestre de 2024, establece un enfoque integral para el uso de sistemas de IA en los Estados miembros de la UE, priorizando la seguridad, la transparencia y la responsabilidad.

La Unión Europea ha dado un paso trascendental en la regulación de la Inteligencia Artificial (IA) con la aprobación reciente de la Ley de Inteligencia Artificial (AI Act) en diciembre pasado. Este marco normativo, cuyo borrador inicial fue propuesto por la Comisión Europea en abril de 2021, está programado para entrar en vigor dos años después de su publicación en el Diario Oficial de la UE como un Reglamento, marcando un hito histórico en la regulación de esta tecnología a nivel mundial.

La nueva legislación, que se espera esté completamente en vigor para el primer trimestre de 2024, establece un enfoque integral para el uso de sistemas de IA en los Estados miembros de la UE, priorizando la seguridad, la transparencia y la responsabilidad. Se anticipa que este Reglamento tenga un impacto significativo no solo dentro de Europa, sino también como un modelo regulatorio global, promoviendo un desarrollo y uso seguro, ético y respetuoso con los derechos y libertades fundamentales.

La presidenta de la Comisión Europea, Ursula von der Leyen, enfatizó la importancia de la IA en la vida cotidiana y su potencial para

beneficiar la economía y la sociedad, reflejando los valores europeos y enfocándose en la regulación basada en riesgos identificables. Esta regulación promueve la «innovación responsable» y garantiza «la seguridad y los derechos fundamentales» tanto de individuos como de empresas, impulsando así la confianza en la IA dentro de la UE.

El Reglamento de IA adopta un enfoque basado en el riesgo, clasificando los sistemas de IA en diferentes niveles:

- **Mínimo riesgo:** La mayoría de los sistemas de IA, como los sistemas de recomendación o filtros de spam, están exentos de obligaciones, aunque las empresas pueden optar por comprometerse voluntariamente con códigos de conducta adicionales.

- **Alto riesgo:** Los sistemas de IA identificados como de alto riesgo deberán cumplir con requisitos estrictos, incluyendo sistemas de mitigación de riesgos, alta calidad de los conjuntos de datos, registro de actividades, documentación detallada, información clara para el usuario, supervisión humana y un alto nivel de solidez, precisión y ciberseguridad.

- **Riesgo inaceptable:** Se prohíben los sistemas de IA que representen una amenaza clara para los derechos fundamentales, incluyendo sistemas que manipulen el comportamiento humano, la puntuación social por parte de gobiernos o empresas, y ciertos usos de sistemas biométricos.

- **Riesgo específico de transparencia:** Los sistemas de IA, como los chatbots, deberán ser identificables por los usuarios, y se requerirá etiquetar los deep fakes y otro contenido generado por IA.

> La presidenta de la Comisión Europea, Ursula von der Leyen, enfatizó la importancia de la IA en la vida cotidiana y su potencial para beneficiar la economía y la sociedad, reflejando los valores europeos y enfocándose en la regulación basada en riesgos identificables.

El acuerdo para este Reglamento de IA ha sido histórico, como señala Carme Artigas, quien fue una figura clave en las negociaciones. «Se trata de un logro histórico y de un gran hito hacia el futuro», dijo la entonces Secretaria de Estado de Digitalización e Inteligencia Artificial de España.

La creación de la AESIA (Agencia Española de Supervisión de Inteligencia Artificial) anticipándose a la entrada en vigor del Reglamento europeo de IA, establece a España como el primer país europeo en tener un órgano de supervisión de IA de esta índole, que representará al país ante el Comité Europeo de IA.

El Comité Europeo de Inteligencia Artificial será fundamental para una aplicación fluida y armonizada del nuevo Reglamento sobre IA. Emitirá recomendaciones y dictámenes a la Comisión en relación con los sistemas de IA de alto riesgo y otros aspectos pertinentes para la aplicación efectiva y uniforme de las nuevas normas.

Además, la Ley de IA permite la creación de entornos de pruebas regulatorias en el mundo real, lo que establece un entorno controlado para probar tecnologías innovadoras durante un período de tiempo limitado, fomentando así la innovación por parte de empresas, pymes y entidades emergentes en conformidad con la Ley.


EN CLAVE IA

# ISMS Forum lanza Forward Thinking como Observatorio para analizar el futuro de los CISOs

*Redacción ISMS Forum*

**El Grupo de Inteligencia Artificial (GIA) de ISMS Forum impulsará este evento, que tendrá una periodicidad semestral.**

> "Forward Thinking funciona como un entorno colaborativo donde los propios CISOs comparten sus experiencias previas en temas de IA y abordan las amenazas emergentes."

Mirar hacia el futuro es esencial en la profesión del CISO, quien garantiza la seguridad de la información en cualquier organización. En este contexto, ISMS Forum ha creado una iniciativa dirigida a estos profesionales, bajo el nombre de Forward Thinking, un Observatorio que tiene como objetivo analizar las cuestiones que enfrentarán en el futuro próximo.

Esta iniciativa surge del GIA, un grupo de expertos en IA recientemente establecido en ISMS Forum para abordar este tipo de desafíos. Según Ángel Pérez, CISO de Autopistas y director de este grupo de trabajo: «Desde Forward Thinking, buscamos realizar un análisis prospectivo de las tendencias emergentes que afectarán a los CISOs».

En el primer evento, que tuvo lugar recientemente en la capital de España, se abordó el tema de la Inteligencia Artificial y su impacto en los profesionales dedicados a la Seguridad de la Información, justo antes de su votación final en el Parlamento Europeo.

«Esta edición nos ha permitido presentar la iniciativa del GIA, cuya misión principal es generar y difundir conocimiento en seguridad, gobernanza y cumplimiento», comenta Pérez. «En la jornada se presentaron los trabajos

publicados por el GIA hasta la fecha, así como se anunciaron las próximas iniciativas y se validó el interés de la comunidad en ellas», añade Daniel García, socio gerente de ISMS Forum.

La idea principal es comprender e interpretar el futuro para anticiparse a las cuestiones que afectarán a los CISOs en su ámbito profesional, especialmente en relación con la implementación de la IA en las organizaciones. Además, varios participantes contribuyeron con su visión sobre tendencias asociadas al gobierno y la seguridad de la IA, enriqueciendo el debate y la generación de conocimiento compartido.

Ángel Pérez considera que era lógico abordar el fenómeno de la IA, dado que ya cuenta con un marco normativo establecido. En su opinión, la introducción de tecnologías de IA, combinada con el procesamiento de lenguaje natural, conducirá a un aumento en la toma automatizada de decisiones, lo que requerirá una supervisión cuidadosa por parte de los profesionales de seguridad de la información.

Daniel García destaca la importancia de que los profesionales de la seguridad de la información acompañen a sus organizaciones en esta reflexión estratégica. «Forward Thinking funciona como un entorno colaborativo donde los propios CISOs comparten sus experiencias previas en temas de IA y abordan las amenazas emergentes», comenta.

En cuanto al evento en sí, Pérez señala que se trabajó en dos aspectos clave: concienciar a la dirección sobre el significado y el gobierno de la IA, y abordar el desafío de seguridad que representan los deepfakes.

«La experiencia ha sido muy productiva, ya que hemos explorado posibles escenarios prácticos para el futuro de la IA», comenta

> La IA ha llegado para quedarse y transformará la seguridad y privacidad de los datos, por lo que es crucial que las organizaciones desarrollen estrategias para adaptarse a este nuevo entorno empresarial.

García. Durante el evento, los participantes elaboraron un documento y realizaron una encuesta cuyos resultados se presentarán en un evento específico sobre IA y ciberseguridad organizado por ISMS Forum.

En resumen, Forward Thinking tendrá dos ediciones al año, adaptándose a las temáticas relevantes del momento. La IA ha llegado para quedarse y transformará la seguridad y privacidad de los datos, por lo que es crucial que las organizaciones desarrollen estrategias para adaptarse a este nuevo entorno empresarial.

Es evidente que el papel del GIA de ISMS Forum ha sido fundamental para estructurar la sesión y generar contenido relevante. García concluye que Forward Thinking es una oportunidad para discutir y diseñar soluciones conjuntas ante los desafíos que plantea la IA en el futuro.


# GLOBAL SPONSORS

ISMS Forum - International Information Security Community, es una organización sin ánimo de lucro que promueve el desarrollo, conocimiento y cultura de la Seguridad de la Información en España. Creada con una vocación plural y abierta, se configura como un foro especializado de debate para empresas, organizaciones públicas y privadas, investigadores y profesionales donde colaborar, compartir experiencias y conocer los últimos avances y desarrollos en materia de Seguridad de la Información.


**+34 915 63 50 62**

**info@ismsforum.es**

**Calle Segre 29, 1B**
**28002, Madrid, Spain**

**@ISMSForum**

**ISMS Forum**