CONTROLALTSUP
TECNOLOGÍA Y SERVICIOS

GARANTE PRIVACY
PROTECCIÓN DE DATOS
Y RESPONSABILIDAD ACTIVA

SERVICIOS DE CONSULTORÍA SOBRE SISTEMAS DE GESTIÓN DE LA INTELIGENCIA ARTIFICIAL.

ISO/IEC 42001 Tecnología de la información. Inteligencia artificial. Sistema de gestión.
ISO/IEC 38507:2022. Tecnología de la información. Gobernanza de TI. Implicaciones de gobernanza en el uso de inteligencia artificial por las organizaciones.
ISO/IEC 23894:2024. Tecnología de la información. Inteligencia artificial. Guía sobre gestión de riesgos (ISO/IEC 23894:2023).

91 109 05 11
info@controlaltsup.com
C/ Puerto de la Cruz Verde, 26. 28045 - Madrid

El Servicio de CONTROLALTSUP sobre Inteligencia Artificial.

El Servicio de CONTROLALTSUP tiene como propósito la ayuda externa a la organización para la adecuación a las nuevas normas que la Organización Internacional de Normalización (ISO) ha publicado en diciembre de 2023 denominada **ISO/IEC 42001:2023. Tecnología de la información. Inteligencia artificial. Sistema de gestión. (SGIA),** la cual está diseñada para ayudar a las organizaciones a actuar con responsabilidad en su uso y roles con los sistemas de IA, y otras afines.

ISO/IEC 42001:2023, pertenece a una familia de estándares ISO que se ocupan de la IA, tales como la **ISO/IEC 38507:2022. Tecnología de la información. Gobernanza de TI. Implicaciones de gobernanza del uso de inteligencia artificial por parte de las organizaciones**, que aborda las implicaciones de gobernanza del uso de la IA y la **ISO/IEC 23894:2024. Tecnología de la información. Inteligencia artificial. Guía sobre gestión de riesgos (ISO/IEC 23894:2023),** publicada en febrero de 2024 que aborda la gestión de riesgos de la IA.

Asimismo, el Servicio de CONTROLALTSUP establece para el Cliente los aspectos técnicos, tales como los Controles (Anexo A) e Implementación (Anexo B), que, siendo opcionales para el cumplimiento, se debe justificar si no se implementa un control, en términos de objetivos, controles para lograr un objetivo y aspectos prácticos para la implementación.

¿Cuál es la utilidad de los sistemas de gestión?

Las normas sobre sistemas de gestión configuran un tipo de estándar que puede ayudar a las organizaciones a implementar un sistema integrado para abordar cuestiones como el apoyo a la alta dirección, la capacitación a las personas de la organización, los procesos de la gobernanza y la gestión de los riesgos.

Al igual que con otros estándares de sistemas de gestión, el SGIA se desarrolla en relación con una gestión de procesos en forma de círculo virtuoso para el establecimiento, implementación, mantenimiento y mejora continua de la IA.

Las normas sobre los sistemas de gestión están desarrolladas de forma deliberadamente general a base de cláusulas que hay que cumplir, para ser utilizados como esquema de certificación en organizaciones de cualquier tamaño involucradas en el desarrollo, suministro o uso de productos o servicios en relación con la calidad, el medio ambiente, la seguridad de la información o la seguridad y salud laboral, entre otros enfoques.

Son aplicables a todas las industrias y para todos los sectores, siendo relevante para el sector público, así como para empresas u organizaciones sin ánimo de lucro.

En esencia, las normas sobre los sistemas de gestión ayudan a las organizaciones a:

- Mejorar su desempeño especificando pasos repetibles que puedan implementar para lograr sus metas y objetivos; y a
- Crear una cultura en la organización que reflexivamente se involucre en un ciclo continuo de autoevaluación, corrección y mejora de operaciones y procesos a través de una mayor conciencia de los empleados y de las partes interesadas, así como también, mediante el liderazgo y compromiso de la dirección.

Ejemplos de estándares de sistemas de gestión conocidos son ISO 9001 para la calidad e ISO 27001 para la seguridad de la información.

La ISO/IEC 42001:2023 es la primera norma de sistema de gestión de IA del mundo y proporciona una guía valiosa para este campo de tecnología que cambia rápidamente. El SGIA surge para ser un esquema de referencia del sistema de gestión sobre el desarrollo y uso responsable de la IA, comparable con la ISO 9001 de la calidad e ISO 27001 de la seguridad de la información.

El SGIA es un estándar auditable y certificable. Las auditorías son una parte vital del enfoque del sistema de gestión, ya que permiten a una organización verificar en qué medida sus logros cumplen con sus objetivos y muestran conformidad con el estándar.

Aborda los desafíos únicos que plantea la IA, tales como por ejemplo las consideraciones éticas, la transparencia y el aprendizaje continuo.

Para las organizaciones, establece una forma estructurada de gestionar los riesgos y las oportunidades asociados con la IA, equilibrando la innovación con la gobernanza.

¿Por qué se necesita un SGIA?

La ISO/IEC 42001:2023 señala que un SGIA es aplicable a cualquier organización, independientemente de su tamaño, tipo y naturaleza, que proporcione o utilice productos o servicios que utilicen sistemas de IA.

El uso de sistemas de IA comprende su desarrollo, utilización, verificación o suministro de productos o servicios que utilicen IA. Proporcionar sistemas de IA implica consideraciones que van más allá de las de otros sistemas, tales como el de la calidad o ambiental, seguridad de la información, etc. El SGIA se centra en:

- Sistemas de IA que tienen el potencial de cambiar su comportamiento mediante el uso, lo que presenta un desafío para garantizar el seguimiento continuo y el cumplimiento de las reglas y/o prácticas aceptadas;
- Sistemas de IA involucrados en la toma automática de decisiones (posiblemente de forma no explicable o transparente), que requieren una gestión específica más allá de la de un sistema tradicional; y
- La sustitución de la interacción humana por el aprendizaje automático, el conocimiento y el análisis de datos, lo que aumenta las oportunidades para aplicar sistemas de IA y al mismo tiempo cambia la forma en que esos sistemas se justifican, desarrollan o implementan.

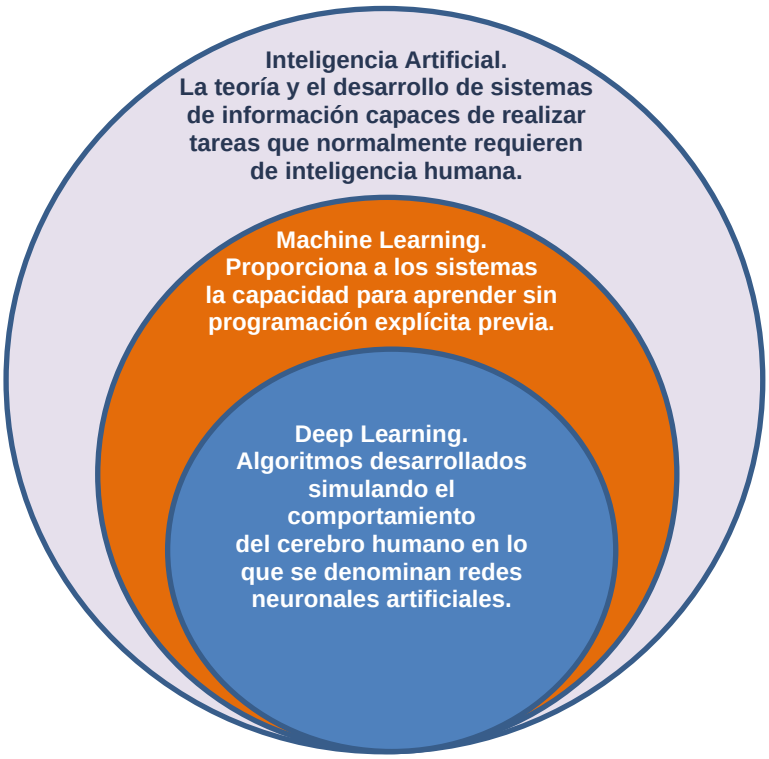
La IA es un amplio campo de estudio que engloba diversas técnicas y tecnologías. Desde los primeros días de la informática hasta la actualidad, la IA ha pasado de ser un concepto teórico a una herramienta práctica que tiene aplicaciones en innumerables dominios, incluida la ciberseguridad.

En el contexto de ciberseguridad, por ejemplo, la IA actúa como un multiplicador de fuerzas, ofreciendo capacidades avanzadas que van más allá de lo que es posible con métodos tradicionales.

Para comprender cómo la IA beneficia a la ciberseguridad, es esencial familiarizarse con las técnicas y tecnologías específicas que se están aplicando. Estas técnicas abarcan desde el aprendizaje automático y sus subdominios hasta la lógica difusa, pasando por redes neuronales o la más reciente IA generativa.

Cada una de estas técnicas posee sus propias características, ventajas, desafíos y aplicaciones dentro de la ciberseguridad, y, conjuntamente, componen un arsenal que las organizaciones pueden utilizar para defenderse contra las crecientes y cambiantes amenazas cibernéticas.

Desde el punto de vista descriptivo del SGIA, conviene situar los diferentes modelos de IA dentro de un contexto que permita una mejor comprensión de sus técnicas y características. La figura siguiente desarrolla esta idea.



Fuente: elaboración propia,
A partir de **CCN-CERT BP/30.**
Aproximación a la Inteligencia Artificial y la ciberseguridad.
https://www.ccn-cert.cni.es/es/

¿Cuál es la estructura de un SGIA?

El SGIA tiene 2 secciones clave:

- La parte de **Gestión** (cláusulas 5 a 10), que son requisitos sobre cómo gestionar un sistema de IA de forma responsable; y
- La parte de **Controles** (Anexo A) y la **Guía de Implementación** (Anexo B). Estas son las medidas técnicas y organizativas en apoyo de los requisitos de gestión.

Los requisitos sobre cómo **gestionar un sistema de IA de forma responsable**, son obligatorios para su cumplimiento e incluyen los siguientes elementos:

1. **Contexto:** las organizaciones deben comprender las cuestiones específicas relevantes para su propósito que se relacionan con el uso de sistemas de IA y el propósito detrás de su uso de la IA en general. Esto implica considerar las expectativas y necesidades de las partes relevantes (como cualquiera que use el sistema o se vea afectado por él), determinar el alcance del sistema y, más ampliamente, establecer un sistema de gestión de IA.

2. **Liderazgo**: las organizaciones deben garantizar que la dirección demuestre compromiso y liderazgo con los sistemas de IA, establezca una política de IA y delegue adecuadamente funciones, responsabilidades y su autoridad.

3. **Planificación:** como parte de su planificación para el sistema, las organizaciones deben asegurarse que tienen en cuenta el contexto de su uso del sistema (como se indica en 1 Contexto), por ejemplo, estableciendo y manteniendo criterios de riesgo de IA, planificando cómo abordar riesgos y oportunidades asociados con el sistema, creando una evaluación de riesgos de IA y, lo que es más importante, planificando cómo lograr los objetivos del sistema y gestionando cualquier cambio.

4. **Soporte:** las organizaciones deben garantizar que existan recursos, información, comunicaciones y concientización adecuados para el sistema en uso. Esto también podría implicar soporte para actualizar cualquier información de acuerdo con los cambios en el sistema.

5. **Operación**: estrechamente relacionado con la planificación, las organizaciones deben garantizar que los planes establecidos para el uso del sistema (teniendo en cuenta la evaluación de riesgos y cualquier otra documentación similar) se sigan y utilicen adecuadamente.

6. **Evaluación del desempeño**: las organizaciones deben garantizar que el uso de los sistemas de IA sea monitoreado, auditado y, en última instancia, revisado periódicamente por la gerencia para garantizar que se mantenga según lo planeado, que los procesos y planes sigan siendo relevantes y para garantizar que se cumplan los objetivos del sistema.

7. **Mejora continua**: las organizaciones deben garantizar que la eficacia, adecuación e idoneidad de los sistemas de IA mejoren continuamente. Cuando se produce alguna no conformidad, las organizaciones deben ser proactivas para corregir cualquier problema, comprender la causa raíz, implementar cualquier respuesta y realizar los cambios necesarios en el sistema. La información documentada deberá estar disponible como evidencia de (i) la naturaleza de las no conformidades y cualquier acción posterior tomada; y (ii) los resultados de cualquier acción correctiva.

Los Servicios sobre el **SGIA de CONTROLALTSUP** proporcionan una muy útil asistencia técnica para las organizaciones que implementan IA con el objeto de **ayudarlas a gestionar, controlar y documentar sistemáticamente su uso de la tecnología**. Además, por nuestra experiencia proporcionamos buenas prácticas a las organizaciones, para **ser más eficaces durante los procesos de auditoría interna y también de certificación** de su SGIA.

91 109 05 11
info@controlaltsup.com
C/ Puerto de la Cruz Verde, 26. 28045 - Madrid