

REQUERIMIENTOS LEGALES PARA LA IMPLEMENTACIÓN DE HERRAMIENTAS IA EN EL TRATAMIENTO DE DATOS

Lima, 23 de septiembre de 2026

INTELIGENCIA ARTIFICIAL v. DATOS PERSONALES

LLONA & BUSTAMANTE

ABOGADOS

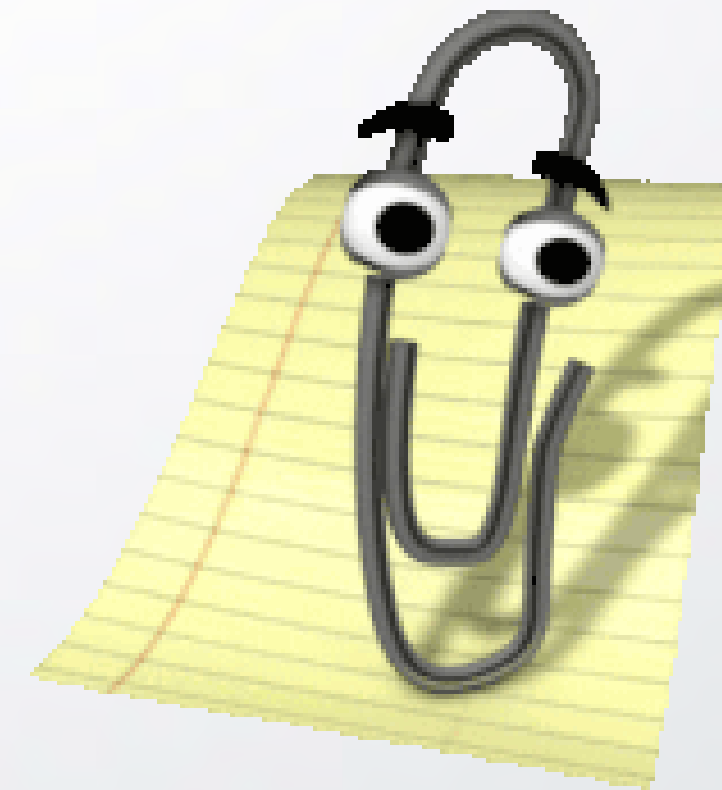


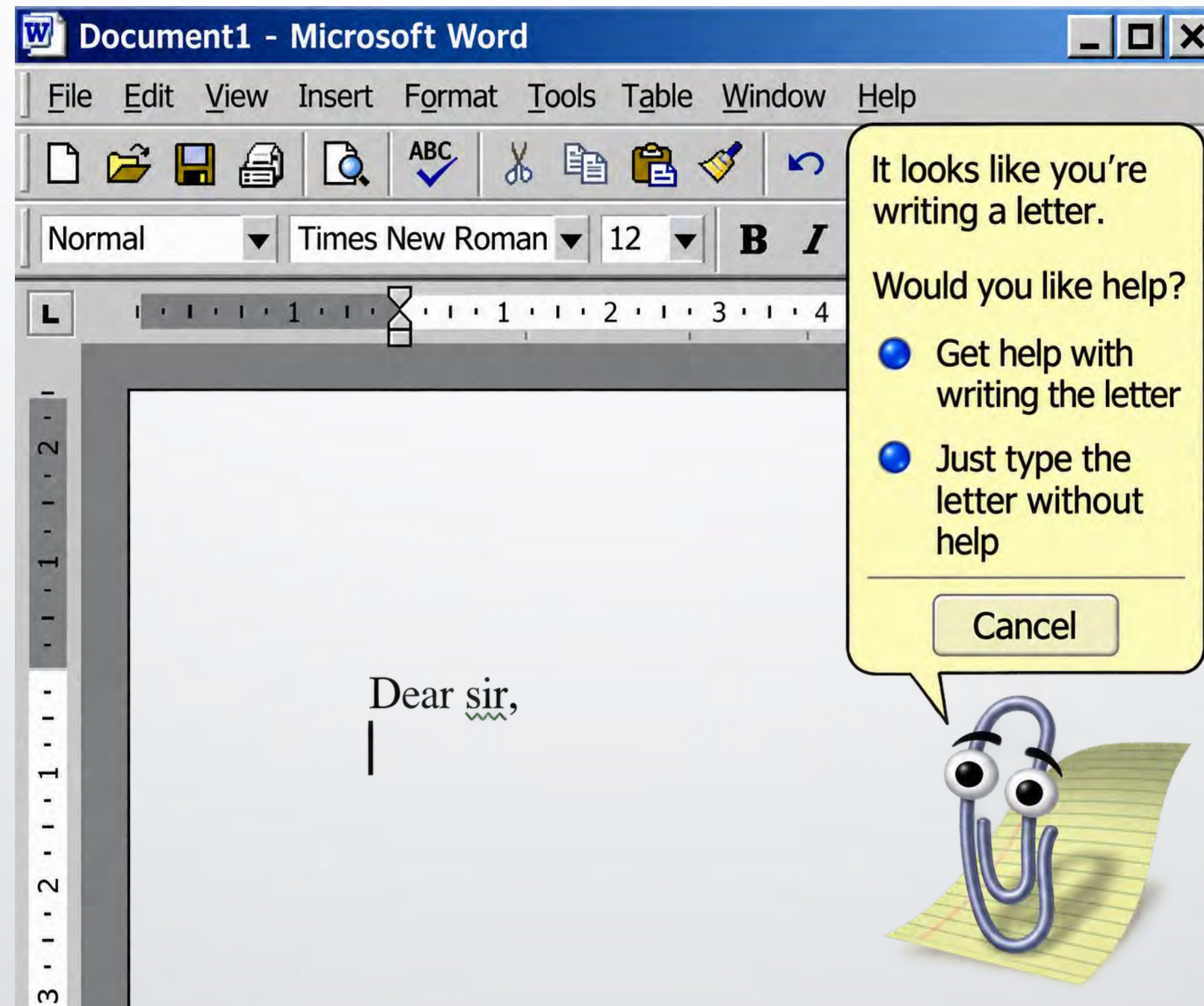
- **Principios de la Protección de Datos Personales aplicables a la IA:**
 - Legalidad: prohíbe la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos.
 - Consentimiento: libre, previo, informado, expreso e inequívoco del titular.
 - Transparencia: conocimiento de las condiciones del tratamiento en el entorno IA.
 - Responsabilidad proactiva (Gobernanza): principios, normas, reglas, procedimientos de toma de decisión y programas que determinan la evolución y el uso de internet.



1. TIPOS DE INTELIGENCIA ARTIFICIAL

- Analiza datos pasados para anticipar eventos futuros.
- Se usa desde los 80.





INTELIGENCIA ARTIFICIAL PREDICTIVA

LLONA & BUSTAMANTE

ABOGADOS



INTELIGENCIA ARTIFICIAL PREDICTIVA

LLONA & BUSTAMANTE

ABOGADOS





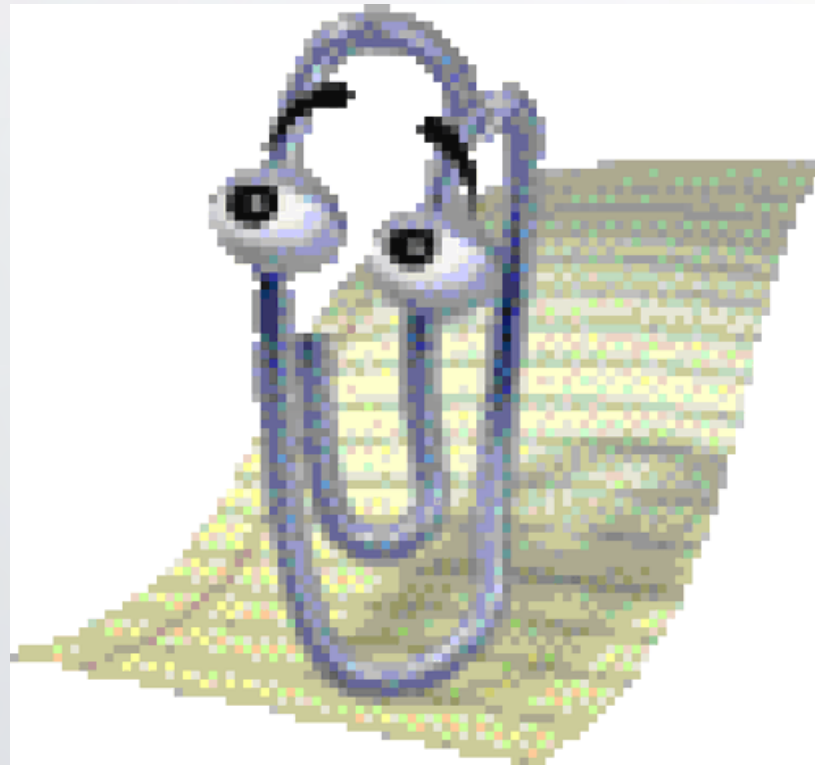
- Crea contenido nuevo, no necesariamente original, como texto, imágenes, audio o códigos.
- Necesita instrucciones de un usuario y patrones aprendidos en su entrenamiento.

INTELIGENCIA ARTIFICIAL GENERATIVA

LLONA & BUSTAMANTE

ABOGADOS





- Actúa, razona y toma decisiones de manera autónoma para cumplir un objetivo específico
- Mínima supervisión humana.

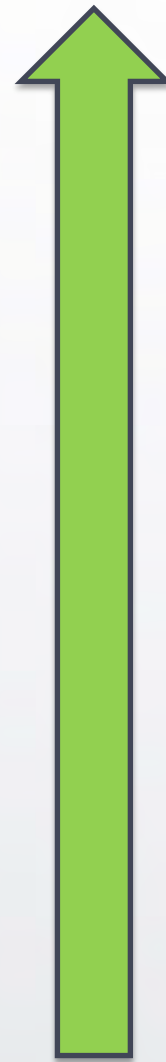
INTELIGENCIA ARTIFICIAL AGENTICA

LLONA & BUSTAMANTE

ABOGADOS



- **PREDICTIVA**
- **GENERATIVA**
- **AGENTICA**



CONTROL



RIESGO



Para visualizar el video, haz clic en el siguiente enlace: <https://sl1nk.com/o8do860>



Para visualizar el video, haz clic en el siguiente enlace: <https://sl1nk.com/6om6s5c>

- Estándares de seguridad basados en riesgos para el uso y desarrollo de la inteligencia artificial.
- Privacidad: la inteligencia artificial no debe transgredir la privacidad de las personas, debe actuar de manera segura para lograr un impacto positivo y de bienestar en los ciudadanos.

- Seguridad y fiabilidad: Los sistemas basados en IA deben ser fiables y seguros durante todo su desarrollo, implementación y uso.
- Supervisión Humana: asegurar que los sistemas basados en IA sean éticas, justas y respetuosas de los derechos fundamentales. La intervención humana es necesaria para corregir, modificar o detener el funcionamiento de estos sistemas, con el fin de prevenir abusos, fortalecer la transparencia y rendición de cuentas.

- **“Explicabilidad”**
 - Sencillez.
 - Ética.
- El encargado del tratamiento debe saber explicar cómo se han procesado los datos.
- El titular del dato debe poder entender el algoritmo y los riesgos de la herramienta.
- Constituye un techo v legalidad

Reglamento de la Unión Europea sobre Inteligencia Artificial (UE) 2024/1689

LLONA & BUSTAMANTE

ABOGADOS

- **Objetivos:**

- Promover la adopción de una inteligencia artificial centrada en el ser humano y fiable
- Requerimientos especiales para sistemas de Inteligencia Artificial de alto riesgo
- Prohibir ciertas prácticas de Inteligencia Artificial
- Reglas transparentes de ciertos sistemas de Inteligencia Artificial
- Reglas para el monitoreo, seguimiento, gobierno y ejecución de sistemas de Inteligencia Artificial
- Medidas para incentivar la innovación de todo tipo de empresas y emprendimientos.

- **Uso de sistemas de IA de alto riesgo:**
 - Para gestión de activos críticos para servicios esenciales (energía, telecomunicaciones, salud, transporte, agua y banca).
 - Procesos en el sector educativo.
 - Procesos de selección, evaluación, contratación y cese en el ámbito laboral.
 - Procesos para temas sociales.
 - Procesos financieros y crediticios.
 - Procesos de salud y bienestar de las personas.
 - Procesos relacionados a la libertad y dignidad de las personas.

- **Prácticas de IA prohibidas:**

- Influir de manera engañosa o manipulativa en la toma de decisiones de las personas
- Generar capacidad autónoma para afectar la vida y la integridad de las personas
- Analizar, clasificar o inferir datos sensibles sobre la base de sus datos biométricos
- Realizar identificación biométrica en tiempo real para la categorización de personas naturales en espacios públicos, o establecer perfiles criminales



2. REQUERIMIENTOS MINIMOS PARA EMPRESAS QUE IMPLEMENTEN HERRAMIENTAS IA

- **Respeto a la dignidad de las personas**

- Implementar medidas para prevenir, mitigar y corregir la generación, el reforzamiento o la perpetuación de resultados discriminatorios o sesgados
- Sistemas basados en IA se deben usar de manera segura, responsable, ética, justa, transparente, equitativa y respetuosa de los derechos humanos

- **Confianza digital**

- Medidas técnicas, organizativas y legales para preservar la seguridad de los datos personales, promover la transparencia de las condiciones del tratamiento de los datos personales y fortalecer la confianza digital
- Respeto del derecho de autor y derechos conexos
- Usar sistemas que respeten y cautelen los derechos de autor, tanto morales como patrimoniales.

- **Seguridad, proporcionalidad y fiabilidad**

- Usar sistemas fiables y seguros para que, en condiciones de uso, minimicen los riesgos del uso indebido u otras condiciones adversas vinculados a dichos sistemas, según su finalidad prevista.
- Salvaguardias y medidas de fiabilidad y seguridad debe ser proporcional al nivel de riesgo del sistema implementado.

- **Sensibilización y educación en IA**

- Charlas y capacitaciones sobre alfabetización digital y el desarrollo de habilidades relacionadas con la concienciación, comprensión y sensibilización sobre el uso y el impacto de los sistemas basados en IA.

- **Supervisión Humana**

- Usar sistemas que permitan una supervisión humana (freno de mano).
- + La intervención humana es necesaria para corregir, modificar o detener el funcionamiento de estos sistemas, para prevenir abusos, fortalecer la transparencia, rendición de cuentas y salvaguardar el bienestar colectivo.

- **Rendición de Cuentas**

- Los actores involucrados deben ser responsables de identificar, evaluar y responder por los impactos generados por la IA, ya sean positivos o negativos. Implementador debe facilitar mecanismos que permitan tales reportes.

- **Desarrollo ético para una IA responsable**

- Se promueve un enfoque ético para definir que en el desarrollo, implementación y uso de los sistemas basado en IA se garantice el respeto de los derechos de los titulares, conforme a los principios jurídicos, éticos y morales.

- **Estándares de seguridad basados en riesgos:**

- El uso de sistemas basados en IA, incluye una comprensión profunda de los riesgos específicos y sus implicancias en los datos de los titulares. Se identifican amenazas, vulnerabilidades y posibles consecuencias negativas, así como, la evaluación de la probabilidad de ocurrencia y el impacto asociado a cada riesgo.

- **Transparencia:**

- Sistemas basados en IA deben ser claros, explicables y accesibles, garantizando que los procesos, algoritmos y decisiones sean comprensibles para usuarios, implementadores, y autoridades.
- “Explicabilidad” sobre criterios de decisión y posibles sesgos, promoviendo la rendición de cuentas, la confianza pública y comprensión de resultados.

- **Transparencia Algorítmica:**

- Informar, de forma clara y sencilla, la finalidad o uso del sistema, sus funcionalidades principales y el tipo de decisiones que puede tomar, sobretodo resaltar limitaciones funcionales de la herramienta de IA.
- Cuando el sistema tome decisiones que impacten en derechos humanos, debe explicar sus resultados.

- Mantener un registro actualizado y accesible sobre funcionamiento del sistema, fuentes de datos utilizadas, lógica del algoritmo, impactos sociales y éticos esperados.
- Establecer políticas, protocolos y procedimientos claros, de seguridad privacidad, transparencia y “explicabilidad”.
- Fomentar la educación y concientización interna de sus colaboradores sobre los riesgos asociados con el uso de la IA.
- En salud, educación, justicia, finanzas y acceso a programas y servicios básicos, implementar mecanismos de supervisión humana en la toma de decisiones.
- Garantizar la responsabilidad y la rendición de cuentas. Evitar “sesgos” y “permisividad” de quienes utilicen herramientas IA.

- **Estándares técnicos internacionales y nacionales en:**
 - Seguridad de la información, ciberseguridad y protección de la privacidad (NTP-ISO/IEC 27002:2022)
 - Controles de seguridad de la información (ISO/IEC 38507: 2022)
 - Gobernanza en el uso de la IA por las organizaciones (NTP-ISO/IEC 42001:2025)
 - Sistemas de gestión (ISO/IEC 23053:2022)
 - Uso de sistemas de IA que utilizan aprendizaje automático (NTP-ISO/IEC 27005:2022).
- Procurar el uso de sistemas de software con estándares técnicos sobre gestión de seguridad de la información y las evaluaciones del uso.

- Antes de implementar sistemas IA de riesgo alto (generativas, agénticas), realizar un análisis de impacto para identificar y minimizar los riesgos potenciales.
- En caso se detecten riesgos que afecten los derechos de los titulares, o riesgo de decisiones automatizadas que generen pérdida de control, sesgos o resultados erróneos, se adoptarán medidas proactivas para mitigar los impactos y se realizarán ajustes en los modelos, mejora en la calidad de los datos y mecanismos de supervisión humana.
- Evaluar continuamente el impacto, mínimo cada 3 años, documentando los hallazgos y las medidas correctivas adoptadas, para facilitar la trazabilidad del sistema.

- **Recomendable:**
 - Oficial de inteligencia artificial o un cargo análogo.
 - Experiencia práctica y conocimientos en el uso de sistemas basados en IA.
- **La supervisión y el monitoreo incluye los siguientes principios:**
 - Comprometer a toda la institución y organización, incluyendo gerencias y directorio.
 - Entender las implicancias de riesgos cibernéticos.
 - Retroalimentar a la organización con experiencias de los colaboradores y alertas en el uso de sistemas basados en IA.
 - Gestionar el personal y el presupuesto necesario y óptimo para una gestión adecuada de los sistemas basados en IA, su monitoreo y supervisión.
 - Informar de manera constante sobre qué riesgos evitar, cuáles aceptar y cuáles mitigar, así como cubrir cualquier responsable con un seguro.

- Implementar canal electrónico de denuncias y ejercicio de derechos
- Dicho canal debería ser accesible a toda persona, sea trabajador, cliente o terceros, para alertar sobre el uso indebido de los sistemas basados en IA o el incumplimiento de las obligaciones
- Difundir canales de denuncias de la sede digital de la PCM de la Plataforma Digital Única del Estado Peruano para Orientación al Ciudadano (www.gob.pe/iaperu), el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), o la División de Investigación de Ciberdelincuencia de la Autoridad Nacional de Protección de Datos Personales (ANPDP) del Ministerio de Justicia y Derechos Humanos.

- **Reflexión 1:**

- La tecnología está avanzando de manera precipitada y atolondrada.
- Se sustenta en la prueba y error.
- Se sustenta en la buena fe, pero se usa más de mala fe.

- **Reflexión 2:**

- Uno no puede administrar lo que no puede controlar.
- Una vez que uno nutre a la IA de información, esta se independiza.
- Mecanismos de monitoreo constante de accesos y privilegios.
- Mecanismos de trazabilidad de ruta de datos.

- **Reflexión 3:**

- Cultura del exceso de cautela.
- Accesos internos a redes o aplicaciones de conversación.
- Medidas para evitar el uso indiscriminado de herramientas de IA para el tratamiento de datos.

- **Reflexión 4:**

- Monitoreo, seguimiento y alerta...
- Monitoreo, seguimiento y alerta...
- Monitoreo, seguimiento y alerta...

- **Reflexión 5:**

- Ciberseguridad
- La ciberseguridad comienza por cada uno
- Las generaciones actuales deben estructurar y aportar reglas, principios y límites en el uso de Inteligencia Artificial y la Ciberseguridad

- **Para el Estado:**

- Gobierno central, Poder Judicial, Congreso y órganos autónomos: 09/09/2026
- ESSALUD y empresas públicas: 09/09/2027
- Gobiernos locales: 09/09/2028

- **Para privados:**

- Sectores de salud, educación, justicia, seguridad, banca y seguros: 09/09/2026
- Sectores de transporte, comercio y trabajo: 09/09/2027
- Sectores de producción, agricultura, energía y minería: 09/09/2028
- Resto de empresas: 09/09/2029.

- **Para MYPES o emprendimientos:**

- Ventas entre 150 UIT y 1700 UIT: 09/09/2027
- Ventas menos de 150 UIT: 09/09/2028

LLONA & BUSTAMANTE

ABOGADOS

TU SOCIO ESTRATÉGICO

60
Años

Expositor:

Alfonso Fernández Maldonado
Socio y Jefe del área de Derecho
Administrativo

afernandezm@ellb.com.pe



www.ellb.com.pe

LLONA & BUSTAMANTE

ABOGADOS

T U S O C I O E S T R A T É G I C O

Gracias por su participación, los invitamos a
escanear el siguiente QR



¡Los esperamos en el próximo desayuno!

