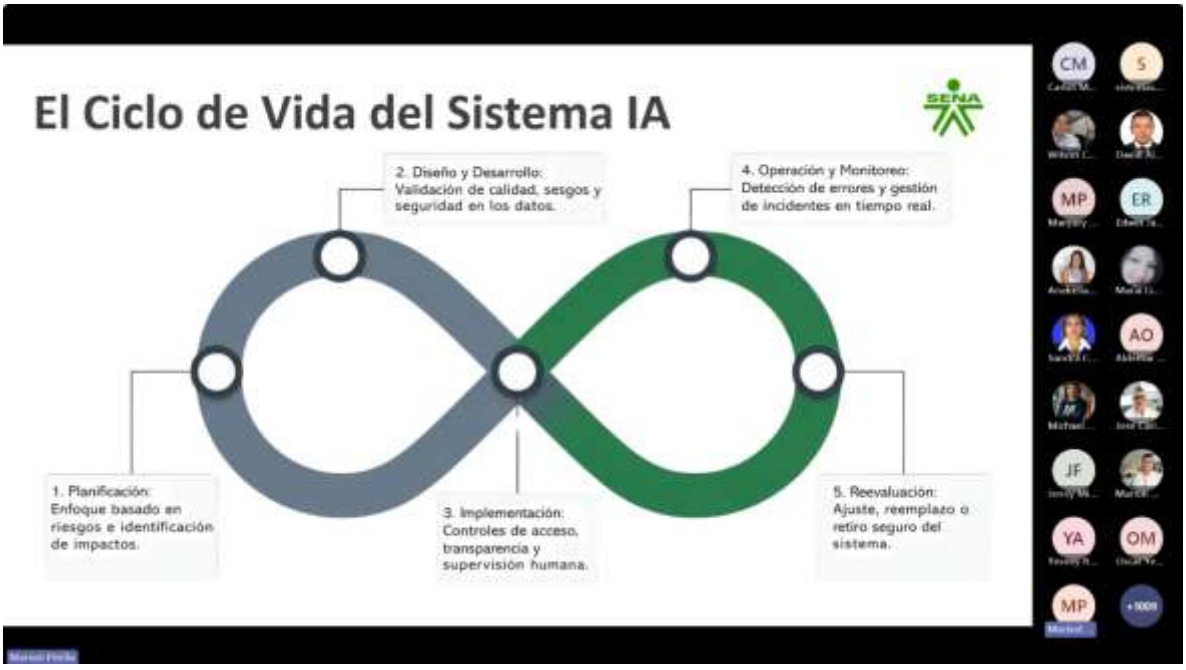
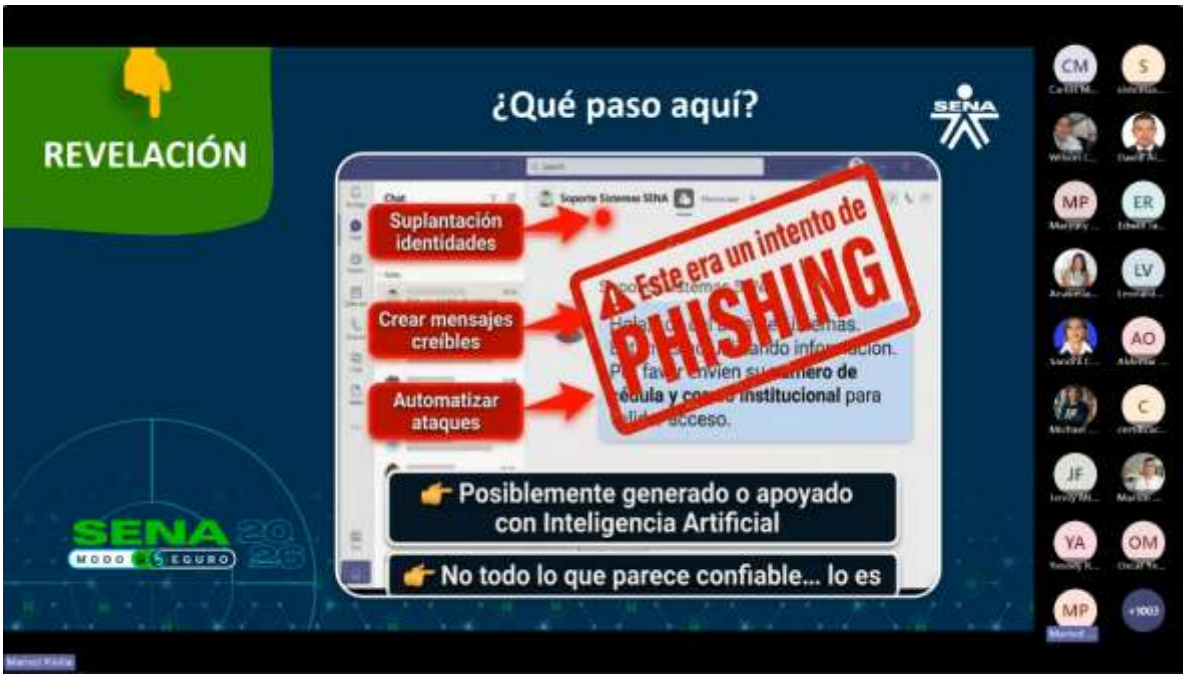
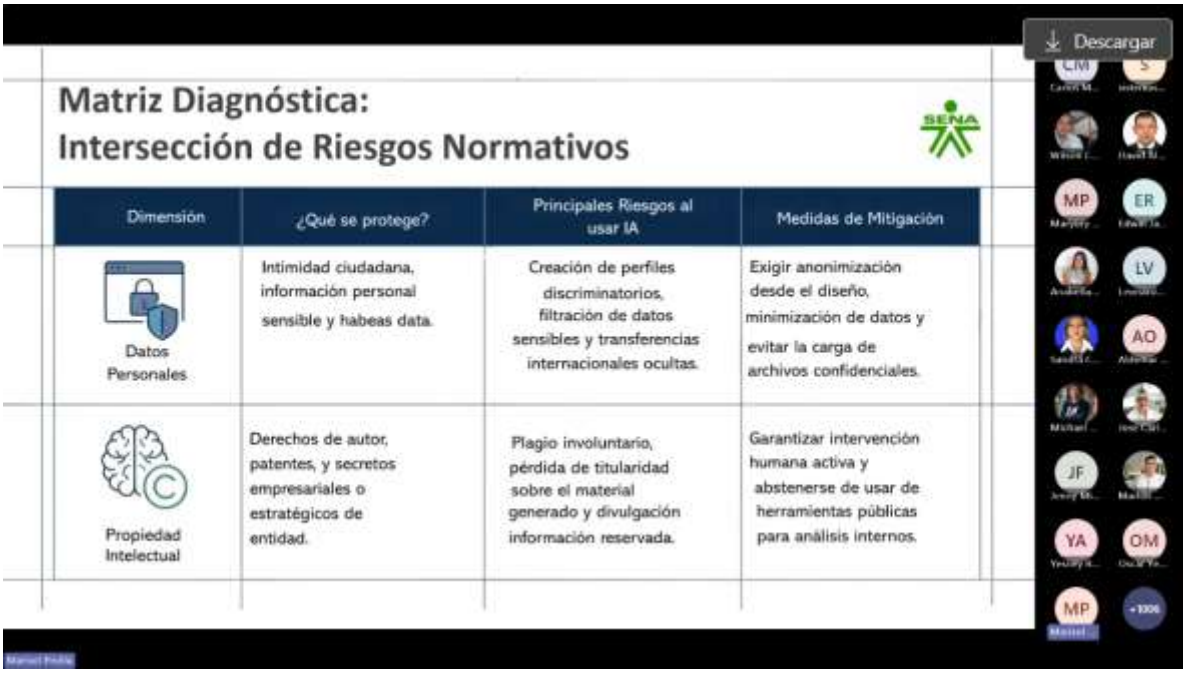
EVIDENCIAS CONFERENCIA INTELIGENCIA ARTIFICIAL



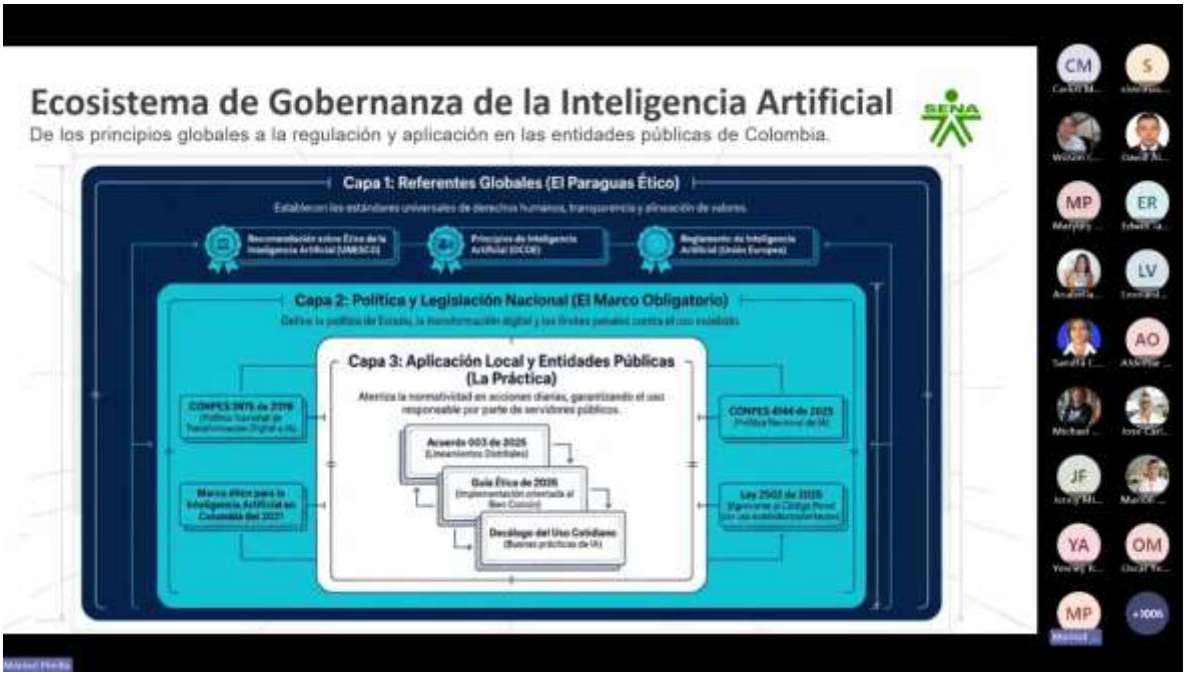






Matriz Diagnóstica: Intersección de Riesgos Normativos

Dimensión	¿Qué se protege?	Principales Riesgos al usar IA	Medidas de Mitigación
Datos Personales	Intimidad ciudadana, información personal sensible y habeas data.	Creación de perfiles discriminatorios, filtración de datos sensibles y transferencias internacionales ocultas.	Exigir anonimización desde el diseño, minimización de datos y evitar la carga de archivos confidenciales.
Propiedad Intelectual	Derechos de autor, patentes, y secretos empresariales o estratégicos de entidad.	Plagio involuntario, pérdida de titularidad sobre el material generado y divulgación información reservada.	Garantizar intervención humana activa y abstenerse de usar de herramientas públicas para análisis internos.


Ecosistema de Gobernanza de la Inteligencia Artificial
De los principios globales a la regulación y aplicación en las entidades públicas de Colombia.
SENA
Capa 1: Referentes Globales (El Paraguas Ético)
Establecen los estándares universales de derechos humanos, transparencia y alineación de valores.
Recomendación sobre Ética de la Inteligencia Artificial (UNESCO)
Principios de Inteligencia Artificial (OCDE)
Reglamento de Inteligencia Artificial (Unión Europea)
Capa 2: Política y Legislación Nacional (El Marco Obligatorio)
Define la política de Estado, la transformación digital y los límites penales contra el uso indebido.
Capa 3: Aplicación Local y Entidades Públicas (La Práctica)
Aterriza la normatividad en acciones diarias, garantizando el uso responsable por parte de servidores públicos.
CONPES 3975 de 2019
Marco ético para la Inteligencia Artificial en Colombia del 2021
Acuerdo 003 de 2025
Guía Ética de 2026
Decálogo del Uso Cotidiano
CONPES 4144 de 2025
Ley 2502 de 2026


RIESGOS DE LA INTELIGENCIA ARTIFICIAL
ALERTA
Riesgos Tradicionales
El uso de IA también implica riesgos:
Fuga de información
Uso indebido de datos personales
Sesgos en decisiones
Dependencia tecnológica
Prepárate.
En la siguiente pantalla verás un escenario real.
¿Sabrías cómo actuar?
La IA no elimina el riesgo... lo transforma


Gestión de Riesgos de Seguridad y Privacidad de la Información
El SGSPI incorpora la gestión de riesgos como un proceso clave para proteger la información y asegurar la continuidad de la operación, analizando amenazas, vulnerabilidades e impactos sobre los activos que soportan los procesos misionales. Esto permite priorizar riesgos, tomar decisiones informadas y fortalecer la protección de la información.
1 Identificamos
2 Analizamos
3 Evaluamos
4 Tratamos
5 Monitoreamos
Activos de Información con criticidad ALTA
Amenazas internas y externas
Vulnerabilidades
Impactos
SENA 2026


El Proceso de Defensa Activa
(Gestión de Riesgos SGSPI)
1. Identificamos
2. Analizamos
3. Evaluamos
4. Tratamos
5. Monitoreamos
Objetivos Prioritarios (Focus Data):
• Activos de criticidad ALTA
• Amenazas internas y externas
• Mitigar riesgos


GRACIAS
@SENAcomunica
www.sena.edu.co