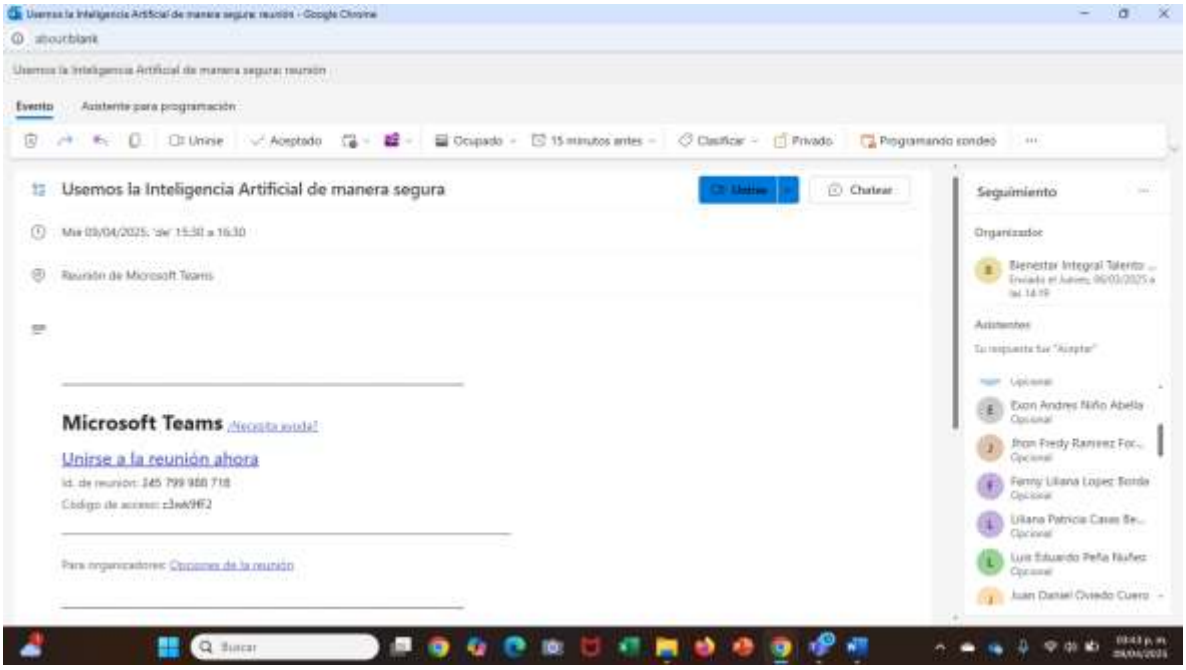
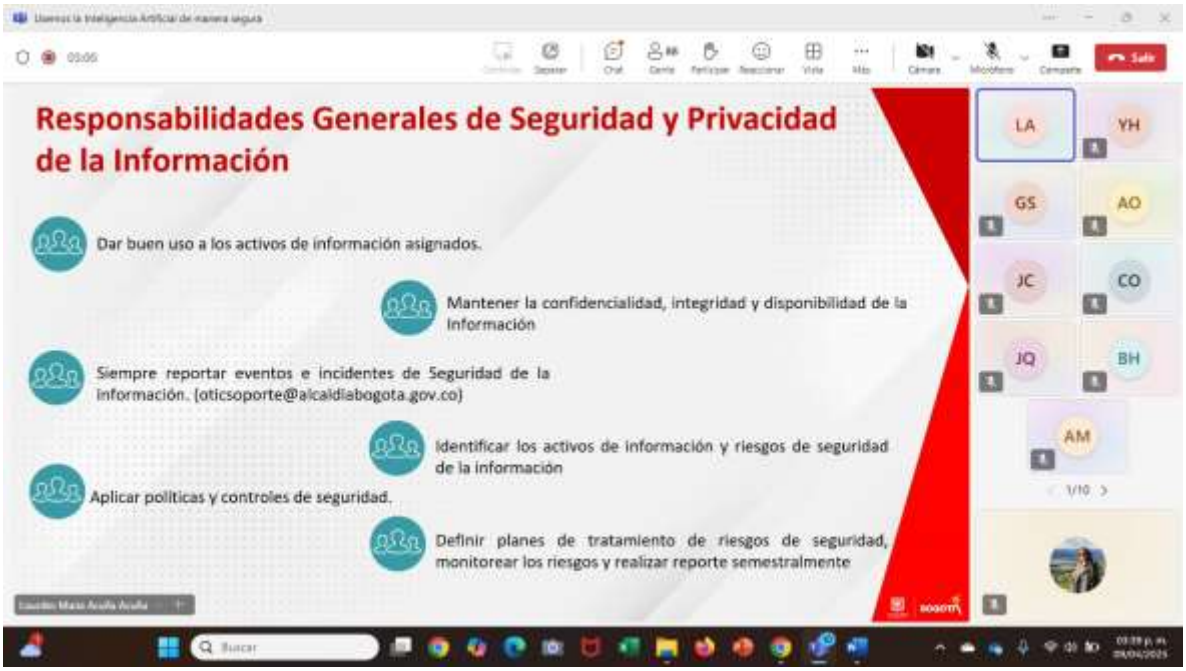
CAPACITACIÓN “USEMOS LA INTELIGENCIA ARTIFICIAL DE MANERA SEGURA”
09 de abril de 2025






Manual de Políticas y control
rivacidad
de la información y políticas
Esperando en la sala de espera
Denegar
Admitir
01
Identificación
02
Definició n
03
Revisión
04
Validación
05
Verificación
06
Finalización
Política general, políticas de apoyo o secundarias
controles establecidos
De lo implementado
Ajustes a controles en general
Proceso de mejora continua
En Daruma: https://sistemadegestion.alcaldiabogota.gov.co/app.php/staff/document/viewPublic?index=136
LA
YH
GS
AO
JC
CO
JQ
BH
AM

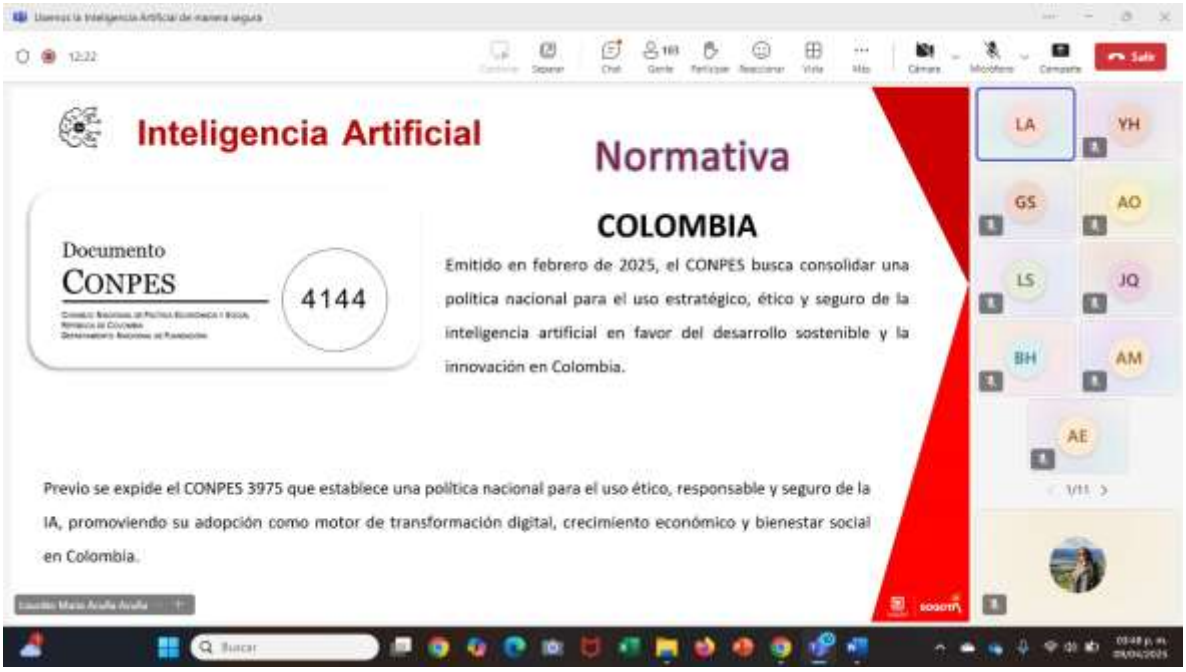

Responsabilidades Generales de Seguridad y Privacidad de la Información
Dar buen uso a los activos de información asignados.
Mantener la confidencialidad, integridad y disponibilidad de la Información
Siempre reportar eventos e incidentes de Seguridad de la Información. (oticsoporte@alcaldiabogota.gov.co)
Identificar los activos de información y riesgos de seguridad de la información
Aplicar políticas y controles de seguridad.
Definir planes de tratamiento de riesgos de seguridad, monitorear los riesgos y realizar reporte semestralmente
LA
YH
GS
AO
JC
CO
JQ
BH
AM


Ley de transparencia y Acceso a la información pública
01
INFORMACIÓN PÚBLICA RESERVADA
Art. 19
Ley 1712 de 2014
Objeto: regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.
INFORMACIÓN PÚBLICA CLASIFICADA
Art. 18
02
03
INFORMACION PÚBLICA
01 INFORMACIÓN PÚBLICA RESERVADA
Art. 19
En esta categoría se encuentra aquella información que esté en poder o custodia de la entidad y a la cual debe restringirse su acceso por parte de la ciudadanía para evitar daños a intereses públicos.
02 INFORMACIÓN PÚBLICA CLASIFICADA
Art. 18
Esta información es propia de la entidad o de terceros y puede ser utilizada por los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por personal no autorizado o por terceros sin autorización del propietario del activo.
03 INFORMACIÓN PÚBLICA
Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
LA
YH
GS
AO
LS
JQ
BH
AM
AE

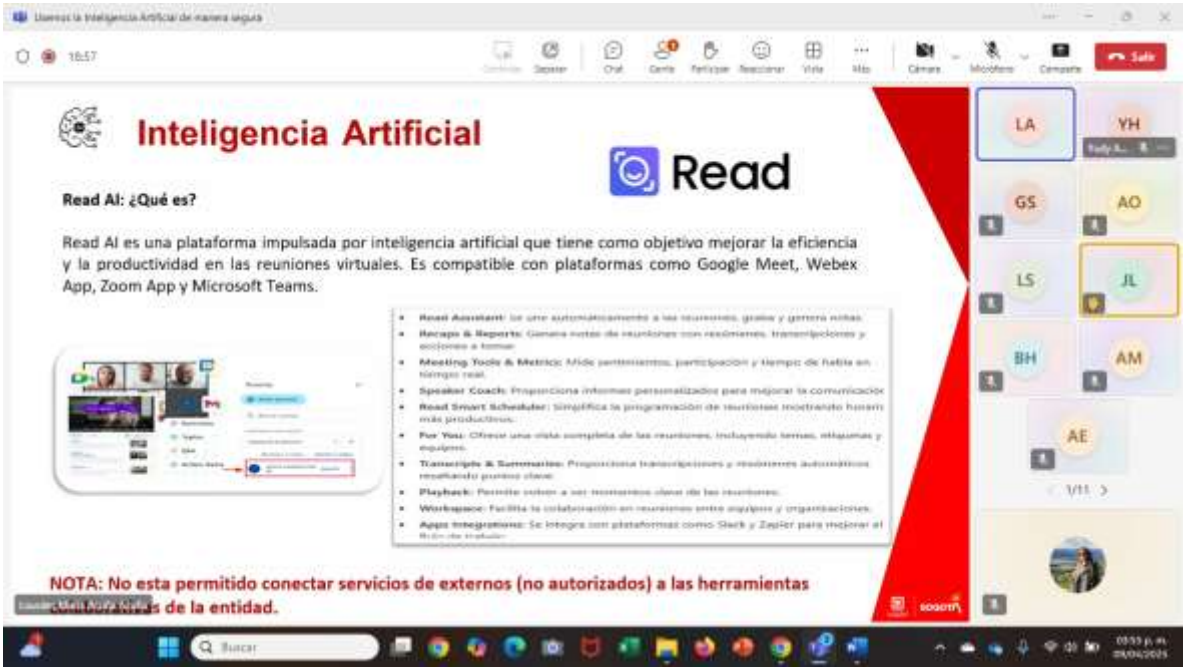

Inteligencia Artificial
Que abordaremos?
1
2
3
4
5
6
Qué es y Beneficios
Normativa
Herramientas
Mal Uso y Riesgos asociados
Caso Phising
Responsabilidades
LA
YH
GS
AO
LS
JQ
BH
AM
AE

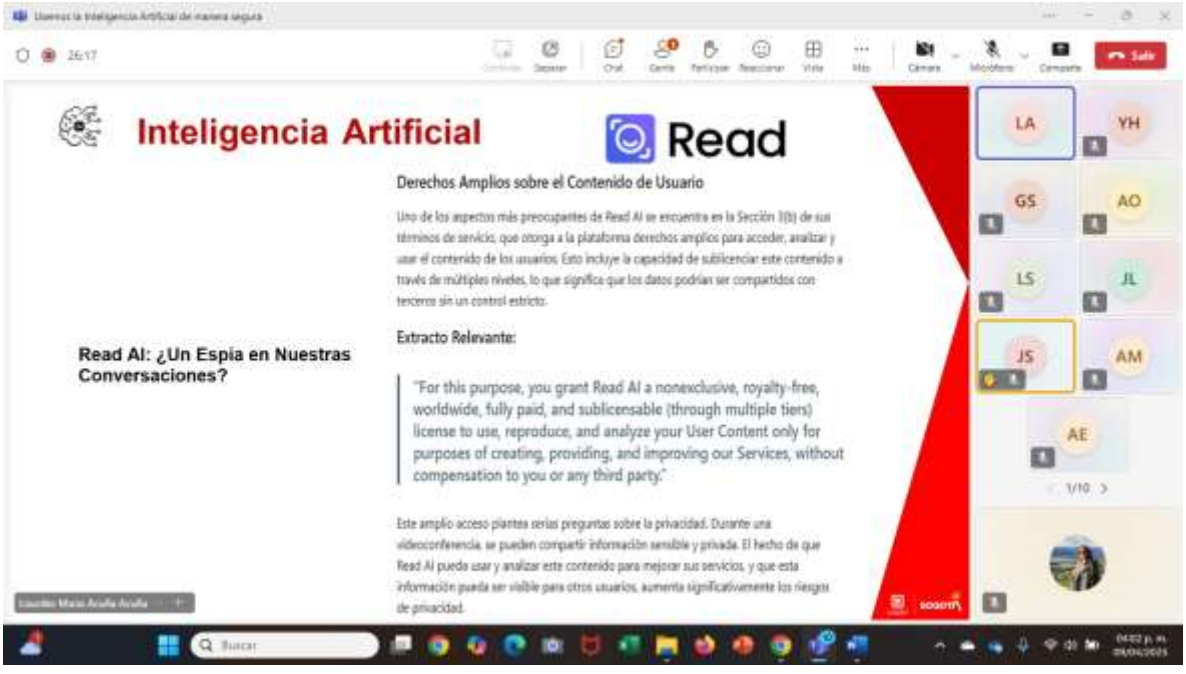

Inteligencia Artificial
Que es?
La inteligencia artificial (IA) es la capacidad que tienen algunas máquinas o sistemas para realizar tareas que normalmente requieren inteligencia humana. Estas tareas pueden incluir entender el lenguaje, reconocer imágenes, tomar decisiones o aprender de la experiencia.
Google Maps analiza el tráfico en tiempo real y te sugiere la ruta más rápida gracias a la IA.


Inteligencia Artificial
Beneficios
Ahorro de tiempo: Automatiza tareas repetitivas, lo que permite enfocarse en actividades más estratégicas.
Mejora la toma de decisiones: Analiza grandes cantidades de datos en segundos, entregando información útil para decidir mejor y más rápido.
Mayor precisión: Reduce errores humanos, especialmente en procesos rutinarios o técnicos.
Atención personalizada: Permite adaptar servicios y respuestas según las necesidades de cada usuario (como los asistentes virtuales).
Optimización de recursos: Ayuda a identificar ineficiencias y proponer soluciones automáticas.
Soporte 24/7: Algunos sistemas basados en IA (como los chatbots) están disponibles todo el tiempo para responder consultas o gestionar solicitudes.
Detección de amenazas de seguridad: Algunos sistemas de IA pueden identificar patrones anormales y alertar sobre posibles riesgos o ciberataques.


Usemos la Inteligencia Artificial de manera segura
12:22
Salir
Inteligencia Artificial
Normativa
COLOMBIA
Documento
CONPES
4144
Emitido en febrero de 2025, el CONPES busca consolidar una política nacional para el uso estratégico, ético y seguro de la inteligencia artificial en favor del desarrollo sostenible y la innovación en Colombia.
Previo se expide el CONPES 3975 que establece una política nacional para el uso ético, responsable y seguro de la IA, promoviendo su adopción como motor de transformación digital, crecimiento económico y bienestar social en Colombia.
LA
YH
GS
AO
LS
JQ
BH
AM
AE
1/11
Buscar


Usemos la Inteligencia Artificial de manera segura
14:51
Salir
Inteligencia Artificial
Herramientas
10 Generative AI Tools
ChatGPT: Modelo de lenguaje avanzado para generación de texto y asistencia conversacional.
Midjourney: Plataforma destacada en la creación de imágenes artísticas mediante IA
Gemini: Asistente de IA de Google que integra generación de contenido y acceso a diversas herramientas.
ElevenLabs: Reconocida por su capacidad para transformar texto en audio realista
SUNO: Herramienta especializada en la generación de música utilizando algoritmos de IA.
Runway: Herramienta versátil para la creación y edición de contenido visual y audiovisual.
LLaMA: Modelo de lenguaje de código abierto desarrollado por Meta, utilizado para diversas aplicaciones de generación de texto.
DeepSeek: Modelo de IA que ha ganado popularidad por su eficiencia y accesibilidad en la generación de contenido.
LA
YH
GS
AO
LS
JQ
BH
AM
AE
1/11
Buscar


Inteligencia Artificial
Read
Read AI: ¿Qué es?
Read AI es una plataforma impulsada por inteligencia artificial que tiene como objetivo mejorar la eficiencia y la productividad en las reuniones virtuales. Es compatible con plataformas como Google Meet, Webex App, Zoom App y Microsoft Teams.
NOTA: No esta permitido conectar servicios de externos (no autorizados) a las herramientas
s de la entidad.


Inteligencia Artificial
Read
Derechos Amplios sobre el Contenido de Usuario
Uno de los aspectos más preocupantes de Read AI se encuentra en la Sección 3(b) de sus términos de servicio, que otorga a la plataforma derechos amplios para acceder, analizar y usar el contenido de los usuarios. Esto incluye la capacidad de sublicenciar este contenido a través de múltiples niveles, lo que significa que los datos podrían ser compartidos con terceros sin un control estricto.
Read AI: ¿Un Espia en Nuestras Conversaciones?
Extracto Relevante:
"For this purpose, you grant Read AI a nonexclusive, royalty-free, worldwide, fully paid, and sublicensable (through multiple tiers) license to use, reproduce, and analyze your User Content only for purposes of creating, providing, and improving our Services, without compensation to you or any third party."
Este amplio acceso plantea serias preguntas sobre la privacidad. Durante una videoconferencia, se pueden compartir información sensible y privada. El hecho de que Read AI pueda usar y analizar este contenido para mejorar sus servicios, y que esta información pueda ser visible para otros usuarios, aumenta significativamente los riesgos de privacidad.

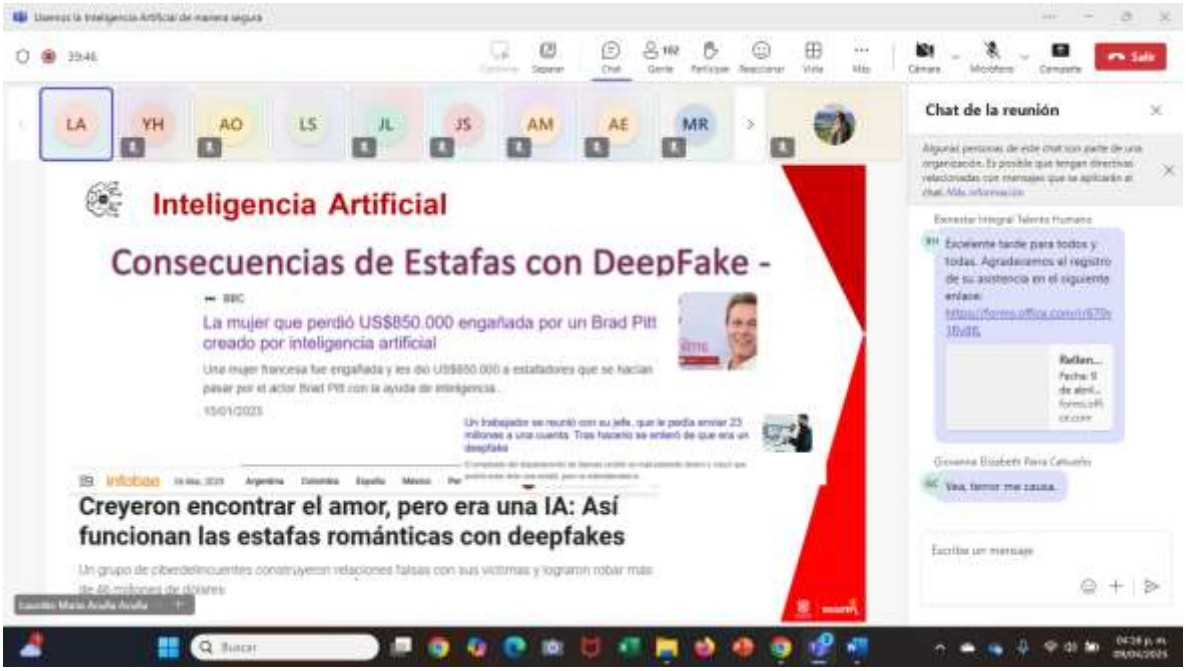

Inteligencia Artificial
Copilot es una herramienta de IA de Microsoft que funciona como asistente virtual en Word, Excel, PowerPoint y otras apps de Microsoft 365, ayudando a automatizar tareas, redactar textos y analizar datos de forma inteligente.
Copilot
Puedes abrir la ventana lateral de Copilot mientras estás en una reunión en Teams y hacer preguntas, redactar ideas o pedir resúmenes, pero no accede al contenido de la reunión directamente.
Uso de Copilot con una transcripción de reunión grabada
Si tienes una reunión virtual y la sesión fue grabada en Microsoft Teams. Como usuario autorizado puedes acceder a la transcripción y pasar este archivo a Copilot para generar un resumen general de la reunión.


Inteligencia Artificial
Copilot
Protección de Datos: Uso de cifrado tanto en tránsito como en reposo.
Privacidad y Seguridad: Las consultas y respuestas generadas por Copilot se manejan de manera que cumplan con las leyes y regulaciones de privacidad aplicables.
Cumplimiento Normativo: Cumple con los compromisos de privacidad, seguridad y cumplimiento establecidos en el Reglamento General de Protección de Datos (RGPD)
Uso de Datos: Accede al contenido y contexto a través de Microsoft Graph, utilizando datos de la organización como documentos, correos electrónicos, calendarios, chats, reuniones y contactos para generar respuestas. Sin embargo, estos datos no se utilizan para entrenar los modelos de lenguaje grandes (LLM) básico
Protección Contra Contenidos Dañinos: Incluye protecciones como el bloqueo de contenido dañino, la detección de material protegido y el bloqueo de ataques de inyección rápida.
Estas medidas aseguran que la información de la entidad esté protegida y no se comparta con terceros para sus propios fines.

G

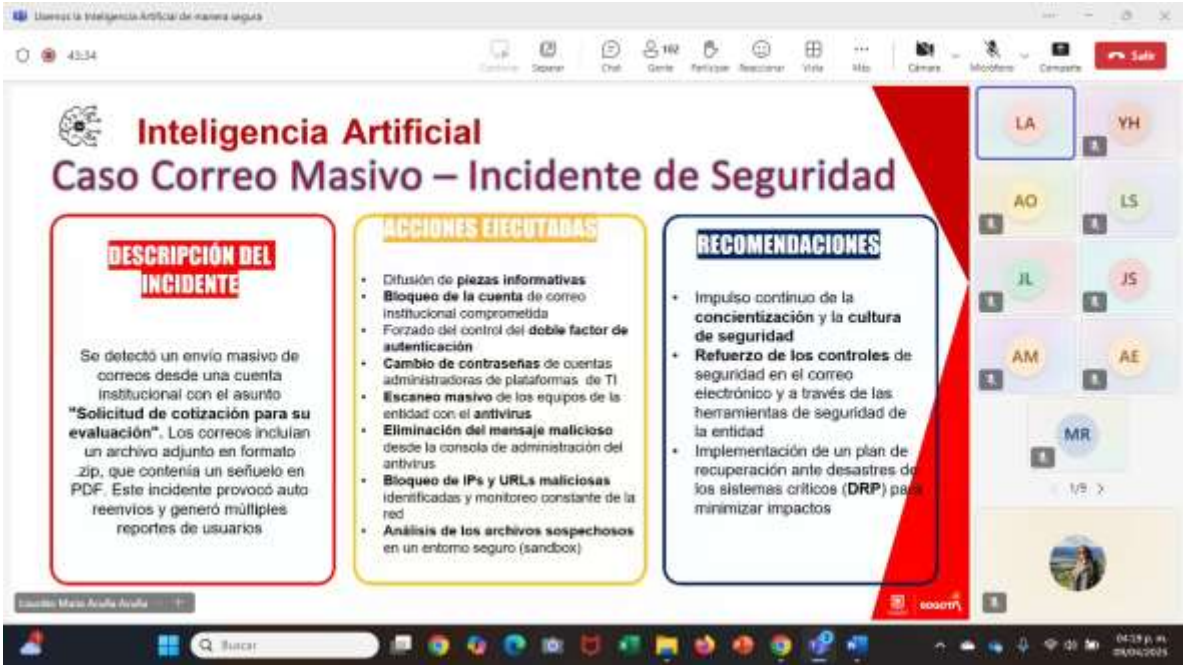

Usemos la Inteligencia Artificial de manera segura
Inteligencia Artificial
Mal Uso de la IA
La evolución del cibercrimen en la era de la inteligencia artificial
El cibercrimen avanza con la tecnología, volviéndose más frecuente, sofisticado y difícil de rastrear gracias al anonimato digital y el uso de herramientas automatizadas.
La extorsión digital, una amenaza en constante crecimiento que utiliza técnicas como el phishing, deepfakes, ransomware
La sextorsión para manipular, engañar o intimidar a las víctimas
NO solo afectan a individuos, sino también a organizaciones públicas y privadas, generando pérdidas económicas, daño reputacional y riesgos legales.
LA
YH
GS
AO
LS
JL
JS
AM
AE


Usemos la Inteligencia Artificial de manera segura
Chat de la reunión
Inteligencia Artificial
DeepFake - Generación de Imágenes con IA
Los deepfakes usan IA para crear imágenes ultra realistas que pueden mostrar situaciones falsas, combinando o alterando rostros reales hasta hacer difícil distinguir lo falso de lo verdadero.
Excelente tarde para todos y todas. Agradecemos el registro de su asistencia en el siguiente enlace:
Vea, temor me causa.

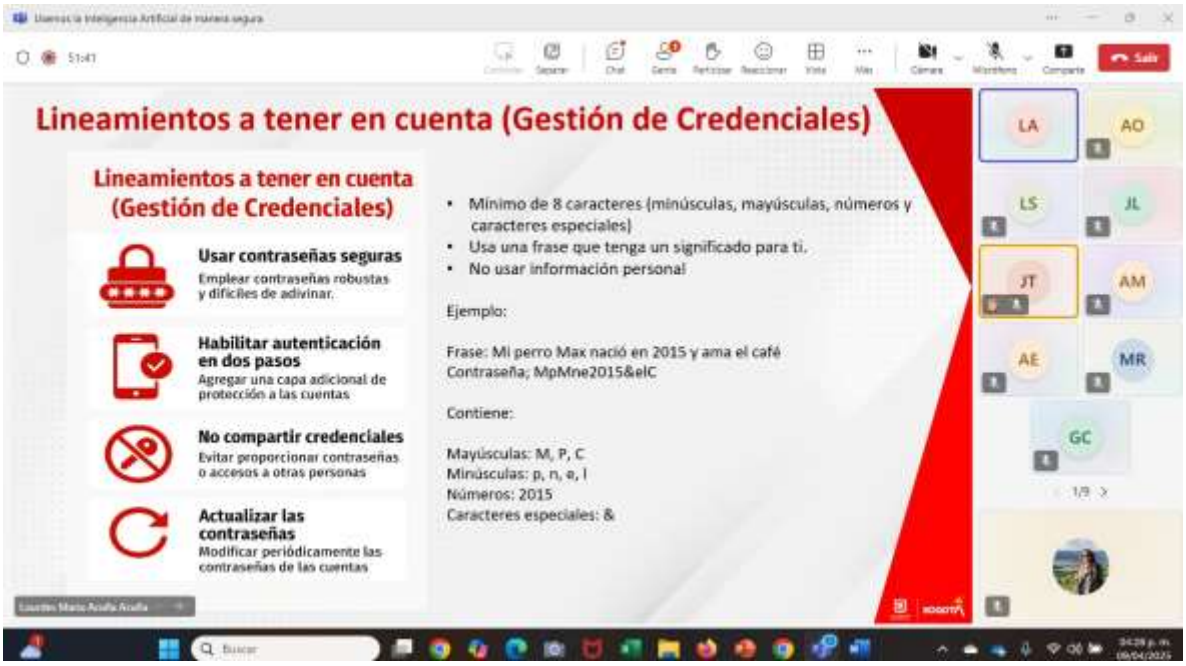

Usamos la Inteligencia Artificial de manera segura
39:46
Salir
LA
YH
AO
LS
JL
JS
AM
AE
MR
Chat de la reunión
Inteligencia Artificial
Consecuencias de Estafas con DeepFake -
BBC
La mujer que perdió US$850.000 engañada por un Brad Pitt creado por inteligencia artificial
Una mujer francesa fue engañada y les dio US$850.000 a estafadores que se hacían pasar por el actor Brad Pitt con la ayuda de inteligencia...
15/01/2025
Un trabajador se reunió con su jefa, que le pedía enviar 25 millones a una cuenta. Tras hacerlo se enteró de que era un deepfake
Infobae
Creyeron encontrar el amor, pero era una IA: Así funcionan las estafas románticas con deepfakes
Un grupo de ciberdelincuentes construyeron relaciones falsas con sus víctimas y lograron robar más de 46 millones de dólares
Escribe un mensaje
Buscar


Usamos la Inteligencia Artificial de manera segura
41:36
Salir
Cambiar la vista
Inteligencia Artificial
Creación de material sensible con deepfakes
Los ciberdelincuentes usan IA para crear imágenes o videos íntimos falsos y extorsionar a las víctimas, aunque esas situaciones nunca hayan ocurrido realmente.
LA
YH
AO
LS
JL
JS
AM
AE
MR
1/9
Buscar


Inteligencia Artificial
Phishing potenciado con Inteligencia Artificial
El phishing con IA crea mensajes falsos muy realistas y personalizados que imitan entidades confiables para engañar y robar información sensible.
Ejemplo:
Un funcionario recibe un correo que parece provenir de un usuario de su entidad, con su nombre y cargo e información muy convincente, solicitándole descargar un archivo adjunto.
Phishing potenciado con inteligencia artificial
Urgente:
Estimado usuario
Por favor actualice su información de acceso.
Haga clic aquí
AI


Inteligencia Artificial
Caso Correo Masivo – Incidente de Seguridad
DESCRIPCIÓN DEL INCIDENTE
Se detectó un envío masivo de correos desde una cuenta institucional con el asunto "Solicitud de cotización para su evaluación". Los correos incluían un archivo adjunto en formato .zip, que contenía un señuelo en PDF. Este incidente provocó auto reenvíos y generó múltiples reportes de usuarios
ACCIONES EJECUTADAS
Difusión de piezas informativas
Bloqueo de la cuenta de correo institucional comprometida
Forzado del control del doble factor de autenticación
Cambio de contraseñas de cuentas administradoras de plataformas de TI
Escaneo masivo de los equipos de la entidad con el antivirus
Eliminación del mensaje malicioso desde la consola de administración del antivirus
Bloqueo de IPs y URLs maliciosas identificadas y monitoreo constante de la red
Análisis de los archivos sospechosos en un entorno seguro (sandbox)
RECOMENDACIONES
Impulso continuo de la concientización y la cultura de seguridad
Refuerzo de los controles de seguridad en el correo electrónico y a través de las herramientas de seguridad de la entidad
Implementación de un plan de recuperación ante desastres de los sistemas críticos (DRP) para minimizar impactos


Lineamientos para evitar incidentes de seguridad de información en equipos de cómputo
Lineamientos para evitar incidentes de seguridad de la información en equipos de cómputo
1 Utiliza contraseñas robustas y seguras
2 Activa el doble factor de autenticación (2FA)
4 Bloquea tu equipo al ausentarte
5 No descargues archivos de fuentes desconocidas
6 Evita conectar dispositivos extraños o ajenos a tu equipo
7 Mantén tu sistema operativo y antivirus actualizados
8 No almacenes información sensible en el escritorio o en carpetas públicas
9 No reenvíes correos sospechosos, ni los respondas
10 Actúa con criterio y responsabilidad digital
10 Actúa con criterio y responsabilidad digital
LA
AO
LS
JL
JS
AM
AE
MR
GC
1/9


Lineamientos a tener en cuenta (Gestión de Credenciales)
Lineamientos a tener en cuenta (Gestión de Credenciales)
Usar contraseñas seguras
Emplear contraseñas robustas y difíciles de adivinar.
Habilitar autenticación en dos pasos
Agregar una capa adicional de protección a las cuentas
No compartir credenciales
Evitar proporcionar contraseñas o accesos a otras personas
Actualizar las contraseñas
Modificar periódicamente las contraseñas de las cuentas
• Mínimo de 8 caracteres (minúsculas, mayúsculas, números y caracteres especiales)
• Usa una frase que tenga un significado para ti.
• No usar información personal
Ejemplo:
Frase: Mi perro Max nació en 2015 y ama el café
Contraseña; MpMne2015&elC
Contiene:
Mayúsculas: M, P, C
Minúsculas: p, n, e, l
Números: 2015
Caracteres especiales: &
LA
AO
LS
JL
JT
AM
AE
MR
GC
1/9


Mecanismos de Doble Factor de Autenticación
Para Acceder A La Cuenta De Correo Institucional
Uso de la aplicación Microsoft Authenticator
Mediante correo electrónico alterno se puede recuperar contraseña del correo
Envió de mensaje de texto a celular
Llamada a celular o extensión telefónica
Mecanismos de Doble Factor de Autenticación
Para Acceder A La Cuenta De Correo Institucional
Sabias que....
Si una contraseña es robada o filtrada por una violación de datos, la doble autenticación es un control
LA
AO
LS
JL
JT
AM
AE
MR
GC