

● ● ● CONGRESO · INTELIGENCIA ARTIFICIAL · 2026

Congreso AI LATAM

El encuentro de la comunidad de Inteligencia Artificial de
Latinoamérica.



30 de Julio 2026



San Fabián · Chile



ialatam.com



IA LATAM · Comunidad

Congreso AI LATAM



● ● ● CHARLA MAGISTRAL · TRACK DE IA

La Inteligencia Artificial como aliada de la ciberseguridad: protegiendo el mundo digital presente y futuro

● **Yasmin Suarez** · Ingeniería Informática · Orientación en Ciberseguridad e IA – Colombia

 SOBRE EL PONENTE

Quién te acompaña hoy



Foto del ponente

Yasmin Rocio Suarez Ruiz

Ingeniera Informática · Universidad Santo Tomás · Colombia

Ingeniera Informática con enfoque en ciberseguridad, Ethical Hacking, inteligencia artificial, auditoría ISO 27001 y protección de datos personales, identidad y privacidad. Me encuentro en constante aprendizaje de tecnologías emergentes y buenas prácticas de seguridad de la información. Participo en este Congreso de IA con el propósito de fortalecer mis conocimientos, intercambiar experiencias con la comunidad y contribuir al desarrollo responsable e innovador de la inteligencia artificial..

- Participa en proyectos de Inteligencia Artificial y Ciberseguridad (Fundadora de CiberAngels)
- Líder de comunidad y divulgación regional (conscientization y prevención)
- Ponente en eventos de tecnología de LATAM (Evil Sec Comunidad y otras)



 AGENDA

Lo que veremos hoy

1

Introducción y contexto

¿Qué es nuestra vida digital? ¿Por qué debemos protegerla?

2

Desafío principal - El panorama actual de las amenazas

¿Qué está pasando? ¿Por qué aumentan los ataques?
Limitaciones del análisis humano.

3

Riesgos del mal uso de la IA y desafíos de la Ciberseguridad

Aprendizajes

4

La Inteligencia Artificial como aliada de la ciberseguridad

Ahora... ¿Cómo lo resolvemos?

5

Hoja de Ruta- Futuro y oportunidades

Qué viene a continuación

6

Conclusiones y preguntas

Cierre y conversación



01



SECCIÓN

Introducción y contexto

¿Qué es nuestra vida digital?

¿Por qué debemos protegerla?

Nuestra vida digital es todo aquello que hacemos, compartimos y almacenamos a través de Internet. Incluye nuestros correos electrónicos, redes sociales, fotografías, cuentas bancarias, compras en línea, documentos, conversaciones e incluso la información de nuestros dispositivos. En pocas palabras, es la extensión de nuestra vida real y cotidiana en el mundo digital.





CIBERSEGURIDAD E INTELIGENCIA ARTIFICIAL

La unión que construye un futuro más seguro

¿QUÉ ES LA CIBERSEGURIDAD?

La ciberseguridad es el conjunto de tecnologías, procesos y prácticas diseñadas para proteger sistemas, redes, dispositivos y datos de ataques, accesos no autorizados, daños o interrupciones.



PROTEGE



DETECTA



RESPONDE



RECUPERA

**DOS FUERZAS
PODEROSAS,
UN MISMO
PROPÓSITO**

Su objetivo es garantizar la **confidencialidad, integridad y disponibilidad** de la información.

¿QUÉ ES LA INTELIGENCIA ARTIFICIAL?

La inteligencia artificial es la capacidad de las máquinas para aprender de los datos, reconocer patrones, tomar decisiones y realizar tareas que normalmente requieren inteligencia humana.



APRENDE



ANALIZA



DECIDE



AUTOMATIZA

Su objetivo es crear **sistemas inteligentes** que puedan resolver problemas y mejorar continuamente.

¿POR QUÉ SU UNIÓN ES LA MEJOR ALIANZA?

La combinación de ciberseguridad e inteligencia artificial crea un entorno más resiliente, predictivo y autónomo.



DETECCIÓN AVANZADA DE AMENAZAS

La IA analiza millones de eventos en tiempo real para identificar comportamientos anómalos y amenazas que los humanos podrían pasar por alto.



RESPUESTA AUTOMÁTICA E INTELIGENTE

Permite actuar en segundos ante incidentes, contener ataques y reducir el impacto.



PREDICCIÓN Y PREVENCIÓN

Anticipa ataques antes de que ocurran, fortaleciendo la postura de seguridad de forma proactiva.



MENORES RIESGOS, MAYOR PROTECCIÓN

Reduce vulnerabilidades, errores humanos y brechas de seguridad.



EFICIENCIA Y OPTIMIZACIÓN

Automatiza tareas repetitivas, optimiza recursos y potencia el trabajo de los equipos de seguridad.



INNOVACIÓN CONTINUA

La IA aprende y evoluciona constantemente, adaptándose a nuevas amenazas y desafíos.

BENEFICIOS DE ESTA UNIÓN



Organizaciones más seguras y resilientes



Protección de datos y confianza digital



Continuidad del negocio y reducción de costos



Cumplimiento normativo y reputación fortalecida



Innovación con responsabilidad

**JUNTOS, CONSTRUIMOS
UN FUTURO DIGITAL
MÁS SEGURO
PARA TODOS.**



** La tecnología cambia el mundo. Pero cuando la usamos para **protegerlo**, creamos un **futuro mejor**.



Congreso AI LATAM

LA TRIADA DE LA SEGURIDAD DE LA INFORMACIÓN

Un modelo fundamental para proteger lo que más valor tiene:
tus datos, tu reputación y la continuidad de tu organización.



La **Triada** de la Seguridad de la Información es el modelo base que guía todas las estrategias de ciberseguridad y gobernanza.
Sin uno de estos pilares, la seguridad simplemente no existe.



08



CONFIDENCIALIDAD

Asegura que la información solo sea accesible para quienes están autorizados.

¿QUÉ PROTEGE?

Evita que la información sea revelada o interceptada por personas, sistemas o procesos no autorizados.

EJEMPLOS:

- Datos personales de clientes
- Información financiera
- Propiedad intelectual
- Estrategias y planes de negocio



CONTROLES CLAVE

- Cifrado de datos
- Control de accesos
- Autenticación multifactor (MFA)
- Políticas de clasificación de información
- Concienciación del personal



DISPONIBILIDAD

Asegura que la información y los sistemas estén disponibles cuando se necesitan.

¿QUÉ PROTEGE?

Garantiza el acceso oportuno y confiable a la información y a los servicios, evitando interrupciones que afecten la operación del negocio.

EJEMPLOS:

- Sistemas de ventas y atención
- Plataformas web y aplicaciones
- Correo electrónico corporativo
- Servicios en la nube



INTEGRIDAD

Asegura que la información sea precisa, completa y esté protegida contra modificaciones no autorizadas.

¿QUÉ PROTEGE?

Garantiza que los datos no sean alterados, ya sea de forma accidental o maliciosa, durante su almacenamiento, transmisión o procesamiento.

EJEMPLOS:

- Registros contables
- Datos en bases de datos
- Transacciones financieras
- Configuraciones de sistemas



¿QUÉ SUCEDE SI FALLA UNO DE LOS PILARES?



Sin Confidencialidad:
La información puede caer en manos equivocadas y generar daños irreparables.



Sin Integridad:
La información puede ser alterada, generando decisiones incorrectas y pérdidas.



Sin Disponibilidad:
Los sistemas y datos no estarán accesibles cuando se necesitan, afectando la operación y la confianza.



CONTROLES CLAVE

- Redundancia de sistemas
- Planes de continuidad del negocio
- Copias de seguridad y recuperación
- Monitoreo y alta disponibilidad
- Protección contra desastres (DRP)

BUENAS PRÁCTICAS PARA FORTALECER LA TRIADA



Capacita a tu equipo en ciberseguridad.



Aplica el principio de mínimo privilegio.



Monitorea y audita constantemente.



Realiza copias de seguridad periódicas.



Mantén políticas y procedimientos actualizados.



Prueba tus planes de respuesta a incidentes.

“

La Triada **CIA** no es solo un concepto, es la base sobre la que se construye toda la **ciberseguridad** moderna.

”



Congreso AI LATAM

02

SECCIÓN

Desafío principal - El panorama actual de las amenazas

¿Qué está pasando? ¿Por qué aumentan los ataques? Limitaciones del análisis humano.

Hoy prácticamente todo está conectado a Internet: nuestros teléfonos, computadores, cuentas bancarias, hospitales, empresas e incluso dispositivos inteligentes en nuestros hogares. Esta transformación nos facilita la vida, pero también crea más oportunidades para que los ciberdelincuentes intenten acceder a nuestra información..

EL PANORAMA ACTUAL DE LAS AMENAZAS CIBERNÉTICAS

LAS AMENAZAS EVOLUCIONAN. NUESTRA PROTECCIÓN TAMBIÉN DEBE HACERLO.



EL MUNDO ESTÁ CONECTADO. POR ESO, CADA AMENAZA EN CUALQUIER LUGAR ES UNA AMENAZA PARA TODOS.



AMENAZAS QUE LA INTELIGENCIA ARTIFICIAL PUEDE CREAR EN NUESTROS ESCENARIOS

LA IA PUEDE SER UNA GRAN ALIADA, PERO TAMBIÉN UN ARMA EN MANOS INCORRECTAS.

PERSONAS



SUPLANTACIÓN DE IDENTIDAD

La IA puede crear perfiles falsos muy realistas para engañar, extorsionar y cometer fraudes.



PHISHING AVANZADO

Correos, mensajes y audios falsos generados por IA que imitan a familiares, bancos o empresas.



DEEPFAKES Y MANIPULACIÓN

Videos y audios falsos que pueden dañar la reputación, generar chantajes o desinformar.



ROBO DE INFORMACIÓN PERSONAL

La IA automatiza la recolección de datos personales para venderlos o usarlos con fines maliciosos.



EXTORSIÓN Y SEXTORSIÓN

Uso de IA para amenazas personalizadas basadas en datos íntimos o sensibles.



RIESGO: PÉRDIDA ECONÓMICA, EMOCIONAL Y DAÑO A LA REPUTACIÓN PERSONAL.

COMUNIDADES



DESINFORMACIÓN MASIVA

La IA crea y difunde noticias falsas a gran escala para manipular opiniones y generar pánico.



POLARIZACIÓN Y MANIPULACIÓN SOCIAL

Algoritmos que analizan emociones y comportamientos para dividir comunidades y manipular decisiones.



VIGILANCIA MASIVA

La IA permite monitorear y predecir comportamientos, afectando la privacidad y las libertades.



ATAQUES A INFRAESTRUCTURAS CRÍTICAS

La IA puede ser usada para atacar servicios esenciales como agua, energía, transporte y salud.



AUTOMATIZACIÓN DE CIBERATAQUES

La IA permite lanzar ataques más rápidos, inteligentes y difíciles de detectar contra comunidades enteras.



RIESGO: PÉRDIDA DE CONFIANZA, DIVISIÓN SOCIAL, CAÍDA Y VULNERABILIDAD COLECTIVA.



UN PODER SIN ÉTICA PUEDE GENERAR DAÑO A GRAN ESCALA.

EMPRESAS



ATAQUES INTELIGENTES Y ADAPTATIVOS

La IA analiza defensas en tiempo real para encontrar vulnerabilidades y evolucionar los ataques.



FRAUDE FINANCIERO AUTOMATIZADO

La IA puede generar transacciones fraudulentas, suplantación de clientes y lavado de dinero.



ROBO DE PROPIEDAD INTELECTUAL

Extracción masiva de datos, modelos y códigos usando IA para acelerar el espionaje corporativo.



INGENIERÍA SOCIAL AVANZADA

La IA permite ataques personalizados a empleados para obtener acceso a información crítica.



SABOTAJE Y DISRUPCIÓN OPERATIVA

Ataques dirigidos a sistemas, cadenas de suministro y procesos para causar interrupciones y pérdidas millonarias.



RIESGO: PÉRDIDAS ECONÓMICAS, DAÑO REPUTACIONAL, INTERRUPTIÓN DEL NEGOCIO Y PÉRDIDA DE CLIENTES.

¿CÓMO PROTEGERNOS?



EDUCACIÓN DIGITAL
Aprender y compartir conocimiento sobre los riesgos de la IA.



PENSAMIENTO CRÍTICO
Verificar antes de creer, no compartir información sin confirmar.



PROTECCIÓN DE DATOS
Quitar nuestra información personal y configurar la privacidad.



USO ÉTICO DE LA IA
Promover el desarrollo y uso responsable de la inteligencia artificial.



COLABORACIÓN
Trabajar juntos: personas, comunidades, empresas y gobiernos.



CULTURA DE CIBERSEGURIDAD
Hacer de la seguridad digital un hábito diario en todos los entornos.



LA TECNOLOGÍA ES NEUTRAL, PERO NUESTRAS DECISIONES CONSTRUYEN UN FUTURO MÁS SEGURO PARA TODOS.



Proyecto CiberAngels -Autoria



03

SECCIÓN

Riesgos del mal uso de la IA y desafíos de la Ciberseguridad

¿cómo podemos utilizarla de manera ética, segura y responsable?

la IA también presenta desafíos importantes. Su uso debe ir acompañado de principios éticos, protección de la privacidad y supervisión humana para garantizar decisiones responsables..

LIMITACIONES HUMANAS QUE NO PERMITEN DETECTAR Y MITIGAR AMENAZAS A TIEMPO



SOBRECARGA DE INFORMACIÓN

Miles de alertas diarias generan fatiga y hacen que lo importante pase desapercibido.

ALERTAS DIARIAS
12,398



FATIGA Y ERROR HUMANO

Largas jornadas y estrés provocan distracciones, errores y decisiones tardías.



VISIBILIDAD LIMITADA

Los humanos no pueden monitorear todos los eventos, sistemas y redes al mismo tiempo.



FALTA DE CONTEXTO EN TIEMPO REAL

Dificultad para correlacionar eventos dispersos y entender el panorama completo del ataque.



CONOCIMIENTO Y ACTUALIZACIÓN LIMITADOS

Las amenazas cambian más rápido de lo que podemos aprender y capacitarnos.



AUTOMATIZAR Y PRIORIZAR

La IA filtra, prioriza y enfoca lo importante.



VISIBILIDAD UNIFICADA

Monitoreo continuo de todos los eventos en tiempo real.



ANÁLISIS INTELIGENTE Y CONTEXTO

La IA correlaciona eventos y detecta patrones ocultos.



RESPUESTA INMEDIATA

La IA actúa en milisegundos, no en minutos.



EDUCACIÓN CONTINUA

Equipos capacitados y actualizados constantemente.



IA + HUMANO: MEJOR EN EQUIPO

La colaboración potencia nuestras fortalezas.

LAS AMENAZAS EVOLUCIONAN EN MILLISEGUNDOS. LOS HUMANOS NO.



+2,500

NUEVAS AMENAZAS POR MINUTO



197

MINUTOS
TIEMPO PROMEDIO DE DETECCIÓN HUMANA



CONSECUENCIAS DE LA DETECCIÓN TARDÍA



PÉRDIDAS ECONÓMICAS



DAÑO REPUTACIONAL



PÉRDIDA DE DATOS



INTERRUPCIÓN DEL NEGOCIO



PÉRDIDA DE CONFIANZA



SANCIÓNES LEGALES



DEPENDENCIA DE PROCESOS MANUALES

Tareas repetitivas y manuales retrasan la detección y respuesta efectiva.



SESGOS Y JUICIOS SUBJETIVOS

Las decisiones basadas en la experiencia personal pueden llevar a falsos positivos o falsos negativos.



RECURSOS HUMANOS LIMITADOS

No hay suficientes expertos para monitorear todo, 24/7, en todas las áreas.

EXPERTOS DISPONIBLES
3 / 50



DIFICULTAD PARA ADAPTARSE

Adaptarse a nuevas tácticas y técnicas de ataque requiere tiempo que los atacantes no dan.



NEW EXPLOIT



LA OTRA CARA DE LA IA
La misma tecnología que nos ayuda a avanzar, también puede ser utilizada por cibercriminales para engañar, manipular y robar información y dinero a personas y empresas.

RIESGOS Y DESAFÍOS PARA EL ROBO DE IDENTIDAD Y FRAUDES FINANCIEROS

PERSONAS Y EMPRESARIOS

¿POR QUÉ ES TAN PELIGROSO?

- Más automatización = más alcance
- Más realismo = más engaño
- Más datos = más personalización
- Menos barreras técnicas = más atacantes

PRINCIPALES RIESGOS Y DESAFÍOS

SUPLANTACIÓN DE IDENTIDAD AVANZADA


La IA permite crear perfiles falsos muy realistas con fotos, videos, voces o información personal robada para hacerse pasar por otras personas.

PHISHING INTELIGENTE Y PERSONALIZADO


Los ataques de phishing generados por IA son más creíbles, están personalizados y adaptados al comportamiento de cada víctima, aumentando la tasa de éxito.

DEEPFAKES Y AUDIOFRAUDES


Videos y audios falsos casi indetectables que imitan a familiares, ejecutivos o personas de confianza para solicitar dinero o información.

ROBO DE IDENTIDAD A ESCALA


La IA recopila y combina datos de múltiples fuentes para crear identidades sintéticas o donar identidades reales y abrir cuentas, solicitar créditos y más.

FRAUDES FINANCIEROS AUTOMATIZADOS


Bot con IA realiza transacciones fraudulentas, cruces de tarjetas, movimientos de dinero y lavado de activos de forma rápida y difícil de detectar.

INGENIERÍA SOCIAL POTENCIADA


La IA analiza redes sociales, correos y hábitos para manipular emocionalmente a las víctimas y convencerlas de entregar datos o dinero.

ATAQUES A EMPRESAS Y CADENAS DE SUMINISTRO


Los atacantes usan IA para acceder a sistemas empresariales, robar datos críticos y comprometer proveedores para fraudes mayores.

IMPACTO EN PERSONAS

- Robo de identidad y suplantación
- Pérdida de dinero en cuentas, tarjetas o billeteras digitales
- Solicitudes de créditos o préstamos fraudulentos
- Daño reputacional y emocional
- Extorsión y amenazas con información personal
- Dificultad para recuperar el acceso a cuentas y servicios

EJEMPLOS REALES

- Llamadas falsas con voz clonada de un familiar pidiendo ayuda urgente.
- Deepfakes en video para engañar y pedir transferencias.
- Phishing que imita a tu banco con tu nombre y datos reales.
- Publicidad engañosa generada por IA para robar datos.

VÍCTIMAS MÁS FRECUENTES

- Adultos mayores
- Jóvenes en redes sociales
- Usuarios de banca digital

¿CÓMO LA IA HACE POSIBLES ESTOS ATAQUES?

- Recopila datos públicos y privados
- Analiza patrones y comportamiento
- Genera contenido realista y convincente
- Autoriza accesos y engaños
- Obtiene dinero, datos o acceso no autorizado

IMPACTO EN EMPRESAS

- Pérdidas financieras millonarias
- Robo de información confidencial
- Fraudes en pagos a proveedores y nóminas
- Interrupción de operaciones y servicios
- Daño a la reputación y pérdida de clientes
- Sanciones legales y regulatorias

EJEMPLOS REALES

- Fraude del CEO: IA imita la voz o el correo del directivo para ordenar transferencias.
- Facturas falsas generadas por IA que parecen legítimas.
- Clonación de sitios web y perfiles empresariales para robar credenciales.
- Infiltración en la cadena de suministro para comprometer a la empresa.

SECTORES EN RIESGO

- Financiero
- Salud
- Comercio
- Tecnología
- Gobierno

CÓMO PROTEGERTE

- Desconfía de mensajes, llamadas o correos inesperados.
- Verifica siempre la identidad por otro canal.
- No compartas información personal o financiera en línea.
- Activa la autenticación en dos pasos (2FA).
- Usa contraseñas fuertes y únicas.
- Mantente informado y capacitado.

RECUERDA

La IA no es buena ni mala, depende de cómo se usa.
La mejor defensa es la conciencia, la prevención y la educación digital.



RECOMENDACIONES PARA EMPRESAS

- Capacita a tu equipo en ciberseguridad y fraudes con IA.
- Implementa tecnologías de detección de fraudes con IA.
- Verifica siempre comprobantes de pagos y cuentas por cobrar.
- Segmenta accesos y protege la información crítica.
- Monitorea continuamente y responde rápidamente.
- Ten un plan de respuesta ante incidentes.

EL DESAFÍO ES DE TODOS

Personas, empresas y gobiernos debemos trabajar juntos para usar la IA de forma ética, segura y responsable.

¡PROTÉGETE, INFÓRMATE Y ACTÚA A TIEMPO!



LA TECNOLOGÍA EVOLUCIONA. LOS ATAQUES TAMBIÉN. TU PREVENCIÓN ES LA MEJOR DEFENSA.



¿QUÉ ES LA INGENIERÍA SOCIAL?

Es el arte de engañar a las personas para que revelen información, confidencial, entreguen accesos o realicen acciones que comprometan la seguridad propia, de su empresa o de su país.

INGENIERÍA SOCIAL

LA AMENAZA QUE NO USA CÓDIGO, USA PERSONAS

Manipulación psicológica para engañar, obtener información confidencial, acceder a sistemas o provocar acciones que ponen en riesgo la seguridad.

¿POR QUÉ FUNCIONA?



- Se basa en la confianza y las emociones humanas: curiosidad, miedo, urgencia, autoridad, amabilidad.
- Las personas somos el eslabón más vulnerable de la cadena de seguridad.
- No necesita romper sistemas, solo convencer personas.

TÉCNICAS MÁS COMUNES



PHISHING

Correos, mensajes o sitios falsos que parecen reales para robar credenciales o información.



VISHING

Llamadas telefónicas suplantando entidades para obtener datos sensibles o acciones.



SMISHING

Mensajes de texto o WhatsApp con enlaces maliciosos o engañosos.



PRETEXTING

El atacante inventa un pretexto o historia falsa para ganarse la confianza y obtener información.



BAITING

Se ofrece algo atractivo (ej. USB, regalos, descargas) para inducir a la víctima a interactuar.



TAILGATING / PIGGYBACKING

El atacante se hace pasar por alguien autorizado para entrar a áreas restringidas.



OSINT (INTELIGENCIA DE FUENTES ABIERTAS)

Recolección de información en redes sociales y sitios públicos para planear ataques más efectivos.

¿CÓMO FUNCIONA?



1. INVESTIGA

Recolecta información sobre la víctima o la organización.



2. CONECTA

Establece contacto generando confianza o interés.



3. ENGAÑA

Usa manipulación psicológica para obtener lo que quiere.



4. EXPLOTA

Obtiene acceso, datos o induce acciones que comprometen la seguridad.

¿A QUIÉN VA DIRIGIDA?



PERSONAS

- Empleados
- Usuarios comunes
- Directivos
- Familiares

Buscan obtener datos personales, accesos, dinero o generar daño emocional y reputacional.



EMPRESAS

- Colaboradores
- Proveedores
- Clientes
- Socios de negocio

Buscan robar información confidencial, acceder a sistemas, dinero, interrumpir operaciones o dañar la reputación.



GOBIERNO

- Funcionarios públicos
- Entidades estatales
- Infraestructuras críticas
- Ciudadanos

Buscan obtener información clasificada, acceder a sistemas, gubernamentales, desestabilizar servicios o influir en decisiones.

EJEMPLOS REALES



Un correo falso de la banca le pide a la víctima credenciales y se roba información.



Alguien llama telefónicamente y pide que se le envíe un documento a la computadora.



Se encuentran a un USB "perdido" y al tomarlo la víctima infecta su red local o empresa.



Un atacante llama a un empleado y se ofrece a ayudarle con un problema de seguridad.



Se informa de un correo sospechoso, el atacante solicita una combinación o número de seguridad.

SEÑALES DE ALERTA

- Solicitudes urgentes o fuera de lo común.
- Errores ortográficos o de formato.
- Remitentes o números desconocidos.
- Ofertas demasiado buenas para ser verdad.
- Presión para tomar decisiones rápidas.
- Solicitudes de información confidencial.
- Enlaces o archivos inesperados.

CÓMO PROTEGERTE (PERSONAS)

- ✓ Desconfía y verifica siempre la identidad del remitente.
- ✓ No compartas información personal o financiera.
- ✓ No hagas clic en enlaces sospechosos.
- ✓ Usa contraseñas fuertes y activa la autenticación en 2 pasos.
- ✓ Reporta cualquier incidente o intento de engaño.
- ✓ Infórmate y capacítate continuamente.



CÓMO PROTEGER TU EMPRESA



- Capacita a todos los colaboradores en seguridad y conciencia.
- Implementa políticas de seguridad claras.
- Verifica identidades antes de otorgar accesos o información.
- Usa autenticación multifactor y controles de acceso.
- Realiza simulaciones de phishing e ingeniería social.
- Fomenta una cultura de seguridad y concienciación.



CÓMO PROTEGER EL GOBIERNO

- Capacitación continua a funcionarios y contratistas.
- Verificación rigurosa de identidades y accesos.
- Protección de infraestructuras críticas.
- Monitoreo y respuesta ante incidentes.
- Cooperación internacional y con la ciudadanía.
- Estrategias de ciberseguridad y concienciación nacional.

RECUERDA



La mejor tecnología puede fallar, pero una mente informada y desconfiada marca la diferencia.



LA INGENIERÍA SOCIAL EXPLOTA LA CONFIANZA. TU CONCIENCIA Y PREVENCIÓN SON TU MEJOR DEFENSA.



¿QUÉ ES LA COMPUTACIÓN CUÁNTICA?



Una qbit y principios de la mecánica cuántica para procesar información a velocidades exponencialmente mayores que la computación clásica.

PRINCIPALES RIESGOS DE LA COMPUTACIÓN CUÁNTICA



ROMPE EL CIFRADO ACTUAL

Algoritmos cuánticos como Shor pueden romper criptografía asimétrica (RSA, ECC) que protege comunicaciones, datos y firmas digitales.



RIESGO PARA DATOS ALMACENADOS HOY

Datos cifrados que se capturan hoy pueden descifrarse en el futuro cuando existan computadores cuánticos potentes ("Harvest Now, Decrypt Later").



AMENAZA A INFRAESTRUCTURAS CRÍTICAS

Sectores como energía, finanzas, salud, transporte y defensa podrían verse gravemente afectados por la ruptura de sus sistemas criptográficos.



DESBALANCE GEOPOLÍTICO

Los países u organizaciones que lleguen primero a la supremacía cuántica tendrán ventajas estratégicas y de seguridad.



INCERTIDUMBRE Y FALTA DE ESTÁNDARES

Aún no existen estándares globales maduros para criptografía poscuántica (PQC) ni para el uso seguro de esta tecnología.

EJEMPLOS DE AMENAZAS CUÁNTICAS

- Descifrado de comunicaciones gubernamentales y militares.
- Robo de información financiera y de propiedad intelectual.
- Falsificación de firmas digitales y certificados.
- Compromiso de blockchain y criptomonedas.
- Acceso no autorizado a sistemas críticos y redes privadas.



RIESGOS Y DESAFÍOS

COMPUTACIÓN CUÁNTICA, IA Y CIBERSEGURIDAD

Tecnologías poderosas que transformarán el mundo, pero que también plantean nuevos riesgos que debemos entender y gestionar hoy.

LA CONVERGENCIA: CUÁNTICA + IA + CIBERSEGURIDAD



IMPACTOS POTENCIALES



DESAFÍOS AL COMBINAR COMPUTACIÓN CUÁNTICA, IA Y CIBERSEGURIDAD



ESTRATEGIAS PARA MITIGAR RIESGOS Y ENFRENTAR LOS DESAFÍOS



MENSAJE CLAVE

La computación cuántica y la IA ofrecen oportunidades sin precedentes, pero también riesgos que pueden transformar el panorama de la ciberseguridad.



EL FUTURO YA COMENZÓ

Prepararse hoy es la clave para proteger nuestro mundo digital mañana.



INNOVAR, PROTEGER, CONFIAR

La combinación correcta de tecnología, personas y procesos construye un futuro digital seguro y resiliente.



¿QUÉ ES LA IA?



Sistemas capaces de aprender, razonar y tomar decisiones. Potencian la detección de amenazas, pero también pueden ser usados con fines maliciosos.

PRINCIPALES RIESGOS DE LA INTELIGENCIA ARTIFICIAL



USO MALICIOSO DE LA IA

IA generativa para crear phishing, malware, deepfakes, desinformación y automatización de ataques.



FUGA Y EXPOSICIÓN DE DATOS

Entrenamiento de modelos con datos sensibles puede provocar filtraciones y pérdida de privacidad.



DECISIONES AUTOMÁTICAS RIESGOSAS

IA mal entrenada o manipulada puede tomar decisiones incorrectas que afecten la seguridad de sistemas críticos.



POCA TRANSPARENCIA Y EXPLICABILIDAD

Los modelos "caja negra" dificultan entender por qué toman decisiones, complicando la detección de abusos.



RIESGOS ÉTICOS Y LEGALES

Sesgos algorítmicos, discriminación, uso indebido de datos y responsabilidad legal aún no resuelta.

EJEMPLOS DE AMENAZAS CON IA

- Phishing y spear phishing automatizado y personalizado.
- Deepfakes para suplantación de identidad y fraude.
- Generación automática de malware y exploits.
- Bots inteligentes para ataques a gran escala.
- Manipulación de datos y desinformación masiva.



04



SECCIÓN

La Inteligencia Artificial como aliada de la ciberseguridad Ahora... ¿Cómo lo resolvemos?

La integración de la Inteligencia Artificial en la ciberseguridad permite analizar grandes volúmenes de datos, identificar comportamientos anómalos y responder de forma automatizada a las amenazas, fortaleciendo la capacidad de defensa frente a ataques cada vez más sofisticados..



¿QUÉ TIENE LA IA?

La IA combina tecnologías avanzadas para analizar grandes volúmenes de datos, encontrar patrones ocultos y actuar en milisegundos.



APRENDIZAJE AUTOMÁTICO (ML)

Aprende de los datos y mejora continuamente para detectar amenazas con mayor precisión.



ANÁLISIS DE PATRONES

Identifica comportamientos normales y anómalos en tiempo real.



PROCESAMIENTO DE LENGUAJE NATURAL (NLP)

Analiza texto, correos, chats, reportes y amenazas desde fuentes abiertas.



VISIÓN POR COMPUTADORA

Analiza elementos visuales, malware y comportamientos en interfaces.



AUTOMATIZACIÓN INTELIGENTE

Ejecuta acciones y respuestas automáticas para contener y mitigar amenazas.



RAZONAMIENTO Y TOMA DE DECISIONES

Evalúa riesgos, prioriza alertas y recomienda acciones basadas en contexto.

LA INTELIGENCIA ARTIFICIAL COMO ALIADA DE LA CIBERSEGURIDAD

Ahora... ¿Cómo lo resolvemos?

La IA nos da el poder de **PREVENIR, DETECTAR, RESPONDER** y **MITIGAR** amenazas digitales antes de que afecten a nuestros servicios, datos y procesos críticos.

¿CÓMO FUNCIONA LA IA EN CIBERSEGURIDAD?



APRENDE - SE ADAPTA - MEJORA CONTINUAMENTE

FUENTES DE DATOS

- Logs y eventos (SIEM)
- Tráfico de red (NDR)
- Endpoints y EDR
- Identidades (IAM)
- Vulnerabilidades
- Inteligencia de amenazas (TI)
- Fuentes abiertas (OSINT)
- Aplicaciones y nube

CAPACIDADES DE IA

- Machine Learning (Supervisado, No Supervisado, Refuerzo)
- Deep Learning
- Análisis de series temporales
- Clustering y clasificación
- Detección de anomalías
- Análisis de grafos
- NLP para análisis semántico

TECNOLOGÍAS Y HERRAMIENTAS

- Plataformas de ML (TensorFlow, PyTorch, Scikit-learn)
- SIEM con IA (Microsoft Sentinel, Splunk, IBM QRadar)
- SOAR con IA
- XDR/EDR con analítica avanzada
- UEBA (User & Entity Behavior Analytics)
- Threat Intelligence Platforms (TIP)
- Cloud AI Services (AWS, Azure, GCP)

ACCIÓN AUTOMÁTICA (SOAR)

- Aislamiento de host
- Bloqueo de IP/Dominios
- Revocación de accesos
- Cuarentena de archivos
- Actualización de reglas
- Notificaciones y tickets
- Ejecución de playbooks

INTEGRACIÓN

- Seguridad en la nube
- DevSecOps
- Zero Trust
- ITSM y Gestión de activos
- Compliance y auditoría
- Protección de datos
- Continuidad del negocio

IMPACTO PARA EL PROFESIONAL DE CIBERSEGURIDAD

- Más visibilidad y contexto para investigar con precisión.
- Menos tiempo en tareas manuales y más enfoque estratégico.
- Alertas inteligentes que priorizan lo crítico.
- Mayor efectividad en la protección de la organización.
- Apoio en decisiones basadas en datos y evidencia.
- Fortalece la resiliencia y la confianza digital.



EN RESUMEN: ASÍ RESOLVEMOS



¿EN QUÉ NOS BENEFICIA Y APOYA?



DETECCIÓN TEMPRANA Y PRECISA

Identifica amenazas conocidas, desconocidas y comportamientos sospechosos antes de que causen daño.



RESPUESTA MÁS RÁPIDA

Reduce el tiempo de detección y reacción de horas a segundos.



REDUCCIÓN DE FALSOS POSITIVOS

La IA prioriza lo que realmente importa, optimizando el trabajo del equipo.



ANÁLISIS CONTINUO 24/7

Monitorea sin descanso todos los sistemas, dispositivos, usuarios y redes.



MITIGACIÓN Y CONTENCIÓN AUTOMÁTICA

Aísla amenazas, bloquea ataques y limita su propagación al instante.



INTELIGENCIA DE AMENAZAS AVANZADA

Correlaciona datos internos y externos para anticipar ataques y vulnerabilidades.



MEJORES DECISIONES

Ofrece información clara y accionable para proteger servicios, procesos y personas.

EJEMPLOS DE LO QUE LA IA PUEDE DETECTAR

- Malware y ransomware nuevos (zero-day)
- Phishing avanzado y suplantación de identidad
- Movimientos laterales y escalamiento de privilegios
- Exfiltración de datos y fuga de información
- Comportamientos anómalos de usuarios y entidades
- Ataques a aplicaciones web y APIs
- Vulnerabilidades explotadas en tiempo real
- Amenazas internas y negligencias



LA IA NO REEMPLAZA AL PROFESIONAL. LO POTENCIA.

Juntos, humanos + IA, construimos un mundo digital más seguro, resiliente y confiable.



NORMAS, MARCOS, ISOS Y LEYES QUE REGULAN LA IA

PROTECCIÓN DE EMPRESAS, DATOS PERSONALES Y CONTROLES DE SEGURIDAD (VIGENTES A 2026)

08



Protección de Empresas



Protección de Datos Personales



Controles de Seguridad y Gestión de Riesgos



LEYES Y REGULACIONES SOBRE IA



EU AI Act (Reglamento (UE) 2024/1689)
En vigor desde agosto 2024, aplicación completa en 2026/2027. Enfoque basado en riesgos.



Executive Order on Safe, Secure, and Trustworthy AI (EE. UU., 2023)
Directrices para el desarrollo y uso seguro de IA en organizaciones.



UK AI Regulation (2023-2026)
Marco pro-innovación centrado en seguridad, transparencia y rendición de cuentas.



Ley 2324 de 2023 (Colombia)
Regula el uso de IA, reconoce derechos de protección de datos y establece principios de transparencia y explicabilidad.



PL 2338/2023 (Brasil)
Proyecto de Ley de IA en discusión, basado en la gestión de riesgos y derechos fundamentales.



PROTECCIÓN DE DATOS PERSONALES



GDPR (Reglamento (UE) 2016/679)
Estándar global para protección de datos personales.



Ley 1581 de 2012 (Colombia)
Régimen general de protección de datos personales.



LGPD (Ley 13.709/2018 – Brasil)
Ley General de Protección de Datos.



CPRA (California Privacy Rights Act, 2020)
Derechos de privacidad y transparencia para residentes de California.



MARCO GLOBAL DE PRINCIPIOS

- Recomendación de la UNESCO sobre la Ética de la IA (2021)
- Principios de la OCDE sobre IA (2019)
- AI Risk Management Framework (NIST AI RMF 1.0, 2023)



NORMAS Y MARCOS DE GESTIÓN DE IA Y RIESGOS



ISO/IEC 42001:2023
Sistema de gestión para la IA.



ISO/IEC 23894:2023
Gestión de riesgos en IA.



ISO/IEC 22989:2022
Gobernanza de IA.



ISO/IEC 23053:2022
Marco de referencia para sistemas de IA.



NIST AI RMF 1.0 (2023)
Gestionar riesgos de IA: Gobernar, Mapear, Medir, Gestionar.



OECD AI Principles (2019)
Principios para IA confiable y centrada en las personas.



NORMAS Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN



ISO/IEC 27001:2022
Sistema de gestión de seguridad de la información.



ISO/IEC 27002:2022
Controles de seguridad de la información.



ISO/IEC 27701:2019
Gestión de privacidad (extensión de 27001).



ISO/IEC 27005:2022
Gestión de riesgos de seguridad de la información.



NIST Cybersecurity Framework 2.0 (2024)
Marco para gestionar y reducir riesgos de ciberseguridad.

ENFOQUE INTEGRAL PARA LAS EMPRESAS



Cumplimiento legal y regulatorio



Respeto y protección de los datos personales



Seguridad y resiliencia de la información



IA ética, transparente y explicable



Gestión de riesgos y resiliencia controlada



Gobernanza, políticas y cultura organizacional



Cumplir estas normas y marcos fortalece la confianza, reduce riesgos, protege a las personas y impulsa la innovación responsable en IA.



Congreso AI LATAM

Actualizado a mayo 2026

PROTÉGETE HOY, EVITA PROBLEMAS MAÑANA

CÓMO PERSONAS Y EMPRESAS PUEDEN PREVENIR FRAUDES, ESTAFAS, SUPLANTACIÓN, ROBO DE DATOS, FUGA DE INFORMACIÓN EMPRESARIAL Y HACKEOS

BUENAS PRÁCTICAS CLAVE PARA ESTAR SEGUROS EN 2026

PARA PERSONAS

- DESCONFÍA DE MENSAJES Y ENLACES SOSPECHOSOS**
No abras correos, SMS o mensajes de remitentes desconocidos. Verifica siempre la fuente antes de hacer clic.
- USA CONTRASEÑAS FUERTES Y ÚNICAS**
Crea contraseñas largas, combina mayúsculas, minúsculas, números y símbolos. Usa un gestor de contraseñas.
- ACTIVA LA AUTENTICACIÓN EN DOS PASOS (2FA)**
Añade una capa extra de seguridad en tus cuentas de correo, redes sociales, banca y servicios en línea.
- CUIDADO CON LLAMADAS Y MENSAJES URGENTES**
Los estafadores generan urgencia para que no pienses. Verifica por otro canal si es real (llama al número oficial).
- PROTEGE TU INFORMACIÓN PERSONAL**
No compartas datos sensibles (cédula, tarjetas, contraseñas, códigos) en redes sociales, formularios o con desconocidos.
- COMPRA SOLO EN SITIOS CONFIABLES**
Verifica que el sitio tenga "https://" y el candado de seguridad. Desconfía de ofertas demasiado buenas.
- EVITA REDES WI-FI PÚBLICAS PARA TRANSACCIONES**
No hagas compras ni accedas a banca en redes públicas. Usa datos móviles o una VPN confiable.
- MANTÉN TUS DISPOSITIVOS ACTUALIZADOS**
Instala las actualizaciones de sistema, navegador y aplicaciones para cerrar vulnerabilidades.
- HAZ COPIAS DE SEGURIDAD DE TU INFORMACIÓN**
Guarda copias de tus archivos importantes en la nube o en discos externos.
- INFÓRMATE Y PIENSA ANTES DE ACTUAR**
La educación es tu mejor defensa. Mantente informado sobre nuevas estafas y tácticas de fraude.

¡ALERTAS COMUNES! CONÓCELAS PARA EVITARLAS

- PHISHING**
Correos o sitios falsos que buscan robar tus datos o contraseñas.
- SUPLANTACIÓN DE IDENTIDAD**
Personas que se hacen pasar por alguien más para engañarte.
- VISHING Y SMISHING**
Llamadas o SMS falsos que buscan obtener información o dinero.
- DEEPPAKES Y CLONACIÓN DE VOZ**
Usan IA para hacerse pasar por familiares, jefes o amigos.
- ROBO DE DATOS**
Buscan obtener tu información personal o financiera.
- FUGA DE INFORMACIÓN**
Pérdida o exposición de información empresarial por descuido o ataques.
- HACKEOS**
Malware, ransomware, intrusiones y control de sistemas.

PARA EMPRESAS

- IMPLEMENTA UNA ESTRATEGIA DE CIBERSEGURIDAD**
Define políticas, responsables, procesos y controles de seguridad alineados con estándares ISO 27001, NIST, etc.
- CAPACITA A TU EQUIPO DE FORMA CONTINUA**
El 91% de los ataques comienzan con un error humano. Capacita en phishing, seguridad y manejo de información.
- CONTROLA EL ACCESO Y PRIVILEGIOS**
Aplica el principio de mínimos privilegios. Solo acceso a lo necesario, para lo necesario.
- USA AUTENTICACIÓN MULTIFACTOR EN TODOS LOS SISTEMAS**
Especialmente en correo, VPN, nube, ERP, CRM y sistemas críticos.
- PROTEGE EL CORREO ELECTRÓNICO Y NAVEGACIÓN**
Usa filtros antiphishing, antimalware y bloquea sitios maliciosos.
- CIFRA LA INFORMACIÓN SENSIBLE**
Tanto en tránsito como en reposo. Cifra bases de datos, documentos y copias de seguridad.
- HAZ COPIAS DE SEGURIDAD Y PRUEBAS DE RECUPERACIÓN**
Sigue la regla 3-2-1: 3 copias, en 2 medios diferentes, 1 fuera del sitio. Prueba la recuperación.
- MONITOREA Y DETECTA AMENAZAS**
Implementa monitoreo 24/7, EDR/XDR, SIEM y alertas tempranas.
- GESTIONA RIESGOS CON TUS PROVEEDORES**
Evalúa la seguridad de terceros que acceden a tu información o sistemas.
- TEN UN PLAN DE RESPUESTA A INCIDENTES**
Define cómo actuar ante un ataque: contener, erradicar, recuperar y comunicar.

SEÑALES DE QUE PUEDES ESTAR EN RIESGO



¿QUÉ HACER SI ERES VÍCTIMA?



LA CIBERSEGURIDAD ES RESPONSABILIDAD DE TODOS.
PREVENIR HOY, TE PROTEGE MAÑANA.



Personas
informadas



Empresas
seguras



Un mundo digital
más confiable.

RECURSOS ÚTILES

- Línea de atención de fraudes (Colombia): 01 8000 910 748
- Reporta incidentes: www.colcert.gov.co
- Policía Nacional - C4i Virtual: www.policia.gov.co



Congreso AI LATAM

05

SECCIÓN

Hoja de Ruta- Futuro y oportunidades

El futuro de la ciberseguridad no dependerá únicamente de tecnologías más avanzadas, sino de profesionales preparados para trabajar junto a ellas. La Inteligencia Artificial será una gran aliada, pero seguirá necesitando algo que ninguna máquina puede reemplazar: el criterio, la creatividad y la responsabilidad humana .

MEJORANDO LAS FINANZAS

Transparencia, seguridad y eficiencia para un sistema financiero más justo e inclusivo.

1. EL ECOSISTEMA FINANCIERO DEL FUTURO

La integración de IA, Blockchain y Gobierno Descentralizado crea un nuevo modelo financiero más confiable, abierto y eficiente.



2. ¿CÓMO FUNCIONA?



3. BENEFICIOS CLAVE PARA LAS FINANZAS

- TRANSPARENCIA TOTAL:** Todas las transacciones son verificables y auditables por todos.
- REDUCCIÓN DE COSTOS:** Menos intermediarios = menores comisiones y procesos más ágiles.
- SEGURIDAD AVANZADA:** Criptografía + IA detectan fraudes y amenazas en tiempo real.
- INCLUSIÓN FINANCIERA:** Acceso global a servicios financieros sin barreras geográficas.
- GOBERNANZA PARTICIPATIVA:** Las comunidades deciden y gestionan los recursos de forma democrática.
- SOSTENIBILIDAD Y CONFIANZA:** Sistemas más éticos, responsables y alineados con el bien común.

4. CASOS DE USO EN FINANZAS



5. IA AL SERVICIO DE BLOCKCHAIN Y DAO



6. IMPACTO EN EL MUNDO REAL



7. EL FUTURO ES DESCENTRALIZADO E INTELIGENTE

La unión de IA, Blockchain y Gobierno Descentralizado está construyendo un nuevo paradigma financiero:



JUNTOS, CONSTRUIMOS FINANZAS MÁS INTELIGENTES, HUMANAS Y SOSTENIBLES.

La tecnología al servicio de las personas, no al revés.



1. EL ECOSISTEMA DE SALUD DEL FUTURO

La integración de IA, Blockchain y Gobierno Descentralizado crea un nuevo modelo de salud donde los datos son seguros, los procesos son transparentes y las decisiones son más justas y eficientes.



DATOS SEGUROS

Protección y privacidad garantizada



INTEROPERABILIDAD

Información compartida de forma estandarizada y segura



DECISIONES COLABORATIVAS

Comunidades y pacientes participan en la gestión de la salud

IA + BLOCKCHAIN + GOBIERNO DESCENTRALIZADO TRANSFORMANDO LA SALUD

Un ecosistema de salud más seguro, eficiente, transparente y centrado en las personas.

2. ¿CÓMO FUNCIONA?



3. BENEFICIOS CLAVE PARA LA SALUD



SEGURIDAD Y PRIVACIDAD TOTAL

Datos médicos inmutables, encriptados y bajo el control del paciente.



INTEROPERABILIDAD GLOBAL

Historia clínica compartida de forma segura entre instituciones y países.



INVESTIGACIÓN ACCELERADA

IA identifica patrones y acelera descubrimientos de tratamientos.



REDUCCIÓN DE COSTOS

Menos fracasos, procesos más eficientes y uso inteligente de recursos.



ATENCIÓN PERSONALIZADA

IA analiza el perfil único de cada paciente para tratamientos más efectivos.



GOBERNANZA ÉTICA Y PARTICIPATIVA

Las comunidades participan en las decisiones sobre políticas y uso de recursos en salud.



ACCESO EQUITATIVO Y GLOBAL

Servicios de salud más accesibles para todos, sin barreras geográficas.

4. CASOS DE USO EN SALUD



HISTORIA CLÍNICA DESCENTRALIZADA

El paciente controla y comparte su historia clínica de forma segura.



TRAZABILIDAD DE MEDICAMENTOS

Blockchain garantiza autenticidad y evita falsificaciones.



DIAGNÓSTICO INTELIGENTE

IA ayuda a detectar enfermedades de forma temprana y precisa.



GESTIÓN DE ENSAYOS CLÍNICOS

Transparencia total en datos, resultados y consentimiento.



TELEMEDICINA Y MONITOREO

Atención remota segura y monitoreo en tiempo real con IA.

5. IMPACTO EN EL MUNDO REAL



-30%
Reducción de costos administrativos



+40%
Eficiencia en procesos clínicos y operativos.



+50%
Acceso a servicios de salud.



Mejores resultados clínicos y calidad de vida.

6. UN FUTURO MÁS HUMANO, INTELIGENTE Y SOSTENIBLE

La tecnología al servicio de la vida. Un modelo de salud donde la confianza, la colaboración y la innovación mejoran la vida de millones de personas.



LA SALUD DEL FUTURO ES:



SEGURA

Protegida por Blockchain



INTELIGENTE

Potenciada por IA



DESCENTRALIZADA

Gestionada por comunidades



TRANSPARENTE

Auditable por todos



HUMANA

Centrada en las personas

Juntos construimos un ecosistema de salud más justo, eficiente y sostenible para todos.



1. EL ECOSISTEMA EDUCATIVO DEL FUTURO

La integración de IA, Blockchain y Gobierno Descentralizado crea un nuevo modelo educativo donde los datos son seguros, los logros son verificables y las decisiones se toman de forma participativa y transparente.



- DATOS SEGUROS Y PRIVADOS**
Los datos de estudiantes y docentes están protegidos y bajo su control.
- VERIFICACIÓN INMUTABLE**
Títulos, certificados y logros académicos verificables al instante.
- DECISIONES PARTICIPATIVAS**
Estudiantes, docentes y comunidades participan en las decisiones del sistema educativo.
- INCLUSIÓN Y EQUIDAD**
Más acceso, menos barreras, oportunidades para todos.

IA + BLOCKCHAIN + GOBIERNO DESCENTRALIZADO TRANSFORMANDO LA EDUCACIÓN

Educación más inclusiva, segura, transparente y personalizada para todos.

2. ¿CÓMO FUNCIONA?



3. BENEFICIOS CLAVE PARA LA EDUCACIÓN

- APRENDIZAJE PERSONALIZADO**
La IA adapta el contenido al estilo, ritmo e intereses de cada estudiante.
- CERTIFICACIÓN VERIFICABLE**
Títulos y credenciales inmutables, verificables por empleadores y universidades.
- TRANSPARENCIA TOTAL**
Todos los procesos y decisiones son visibles y auditables por la comunidad.
- REDUCCIÓN DE COSTOS**
Menos intermediarios, procesos más eficientes y accesibles.
- ACCESO GLOBAL E INCLUSIVO**
Educación sin fronteras, disponible para más personas en todo el mundo.
- MOTIVACIÓN Y PARTICIPACIÓN**
Estudiantes y docentes motivados al ser parte activa de las decisiones.
- INNOVACIÓN CONTINUA**
La IA analiza tendencias y resultados para innovar y mejorar constantemente.
- PROPIEDAD DE LOS DATOS**
Estudiantes y docentes son dueños de sus datos y deciden cómo usarlos.

4. CASOS DE USO EN EDUCACIÓN

- TÍTULOS Y CERTIFICADOS DIGITALES**
Verificación instantánea y sin fronteras.
- RUTAS DE APRENDIZAJE INTELIGENTES**
Personalizadas según el progreso y las habilidades.
- EVALUACIÓN AUTOMÁTICA INTELIGENTE**
Retroalimentación inmediata y justa.
- RECONOCIMIENTO DE LOGROS MICRO-CREDENCIALES**
Aprendizaje personalizado, verificable y acumulable.
- BECAS Y AYUDAS TRANSPARENTES**
Asignación justa y transparente para quienes más la necesitan.

5. IMPACTO EN EL MUNDO REAL

- +70%**
Mejora en la retención y éxito académico.
- 40%**
Reducción de costos operativos en instituciones.
- +60%**
Más acceso a educación de calidad en comunidades remotas.
- +50%**
Mayor participación de estudiantes y docentes en decisiones educativas.
- 100%**
Transparencia y verificabilidad de logros y certificaciones.

6. UN FUTURO MÁS HUMANO, INTELIGENTE Y COLABORATIVO

La tecnología nos empodera a las personas, las potencia. Juntos construimos una educación donde todos pueden aprender, enseñar y crecer sin límites, con confianza, justicia y propósito.



LA EDUCACIÓN DEL FUTURO ES:



SEGURA

Protegida por Blockchain



INTELIGENTE

Potenciada por IA



DESCENTRALIZADA

Gestionada por la comunidad



TRANSPARENTE

Auditable por todos



INCLUSIVA

Para todas las personas



JUNTOS CONSTRUIMOS UNA EDUCACIÓN

PARA EL PRESENTE Y EL FUTURO.



Congreso AI LATAM

1. EL ECOSISTEMA EMPRESARIAL DEL FUTURO

La integración de IA, Blockchain y Gobierno Descentralizado crea un nuevo modelo empresarial donde los datos, los procesos y las decisiones son más seguros, eficientes y colaborativos.



- DATOS CONFIABLES**
Información íntegra, inmutable y verificable.
- PROCESOS TRANSPARENTES**
Trazabilidad completa en toda la cadena de valor.
- DECISIONES INTELIGENTES**
IA analiza datos en tiempo real para mejorar la toma de decisiones.
- COLABORACIÓN SEGURA**
Contratos inteligentes y DAO alinean intereses y fomentan la confianza.
- INNOVACIÓN ACCELERADA**
Automatización, nuevos modelos de negocio y optimización continua.

4. CASOS DE USO EN EMPRESAS

- CONTRATOS INTELIGENTES**
Automatización de acuerdos y pagos en tiempo real.
- TRAZABILIDAD DE PRODUCTOS**
Seguimiento transparente de toda la cadena de valor.
- GESTIÓN DE PROVEEDORES**
Evaluación automática, contratos y pagos inteligentes.
- IDENTIDAD DIGITAL Y ACCESO**
Verificación segura de empleados, clientes y socios.
- TOKENIZACIÓN DE ACTIVOS**
Nuevas formas de financiamiento y liquidación.

LA EMPRESA DEL FUTURO ES:

- INTELIGENTE**
Usa IA para decidir mejor.
- SEGURA**
Protección por Blockchain.
- DESCENTRALIZADA**
Gestionada con confianza.
- TRANSPARENTE**
Auditable por todos.
- SOSTENIBLE**
Crea valor a largo plazo.

IA + BLOCKCHAIN + GOBIERNO DESCENTRALIZADO TRANSFORMANDO EL MUNDO EMPRESARIAL

Empresas más inteligentes, transparentes, seguras y competitivas en la economía digital.

2. ¿CÓMO FUNCIONA EN LA EMPRESA?



5. IMPACTO EN EL MUNDO REAL

- 30%**
Reducción de costos operativos.
- +45%**
Aumento de productividad.
- 60%**
Reducción de fraudes y errores.
- +35%**
Mejora en la toma de decisiones.
- +50%**
Mayor satisfacción de clientes.

EMPRESAS MÁS EFICIENTES, TRANSPARENTES Y RENTABLES
EN UN ENTORNO DIGITAL Y DESCENTRALIZADO.

3. BENEFICIOS CLAVE PARA LAS EMPRESAS

- TRANSPARENCIA TOTAL**
Todos los procesos y transacciones son visibles, verificables y auditables.
- REDUCCIÓN DE COSTOS**
Menos intermediarios, menos errores y procesos más eficientes.
- SEGURIDAD Y CONFIANZA**
Información inmutable, contratos inteligentes y menor riesgo de fraude.
- DECISIONES MÁS INTELIGENTES**
IA convierte datos en insights y recomendaciones para decisiones estratégicas.
- AGILIDAD Y COMPETITIVIDAD**
Automatización y optimización que permiten responder más rápido al mercado.
- INNOVACIÓN Y NUEVOS MODELOS**
Nuevas formas de crear, compartir y capturar valor en la economía digital.
- SOSTENIBILIDAD EMPRESARIAL**
Decisiones responsables, trazabilidad ESG y creación de valor a largo plazo.

6. UN FUTURO EMPRESARIAL MÁS HUMANO E INTELIGENTE

La tecnología potencia el talento humano. Juntos, construiremos empresas más éticas, colaborativas, resilientes y enfocadas en generar valor para las personas y la sociedad.

- ÉTICO
- TRANSPARENTE
- COLABORATIVO
- SOSTENIBLE
- INNOVADOR

TECNOLOGÍA + PERSONAS + EMPRESAS QUE
TRANSFORMAN EL PRESENTE Y CONSTRUYEN EL FUTURO.



1. EL ECOSISTEMA DE INFRAESTRUCTURAS CRÍTICAS

La integración de IA, Blockchain y Gobierno Descentralizado crea un nuevo modelo para proteger, monitorear y optimizar las infraestructuras que sostienen nuestra vida y la economía.



- SISTEMAS ESENCIALES PARA LA SOCIEDAD**
Afectan la seguridad, salud, economía y bienestar de millones.
- ALTO IMPACTO ANTE FALLAS O ATAQUES**
Un pequeño fallo puede generar graves consecuencias.
- OBJETIVO PRIORITARIO DE CIBERSEGURIDAD**
Su compromiso puede afectar servicios y vidas humanas.
- NECESITAN DISPONIBILIDAD, INTEGRIDAD Y RESILIENCIA**
Operación continua, segura y confiable.

4. CASOS DE USO

- DETECCIÓN DE INTRUSIONES EN REDES INDUSTRIALES (OT/I)**
La IA detecta comportamientos anómalos en SCADA, PLC y sensores.
- PREDICCIÓN DE FALLAS EN EQUIPOS CRÍTICOS**
Análisis de datos históricos y en tiempo real para anticipar fallos.
- GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD**
Flujos de trabajo automatizados y alertas en tiempo real.
- GESTIÓN DE ACCESOS Y PERMISOS**
Identidades descentralizadas y controles granulares inmutables.
- RAZABILIDAD DE EVENTOS Y ACCIONES**
Registro inmutable para auditorías y cumplimiento regulatorio.
- OPTIMIZACIÓN DE CONSUMO ENERGÉTICO Y RECURSOS**
IA aplicada en tiempo real para máxima eficiencia y sostenibilidad.

IA + BLOCKCHAIN + GOBIERNO DESCENTRALIZADO PROTEGIENDO Y OPTIMIZANDO INFRAESTRUCTURAS CRÍTICAS

Tecnología Inteligente y descentralizada para servicios esenciales más seguros, resilientes y eficientes.

2. ¿CÓMO FUNCIONA?



APLICADO A INFRAESTRUCTURAS CRÍTICAS



- MONITORIO 24/7**
Vigilancia constante en tiempo real.
- ALERTAS INTELIGENTES**
Solo lo importante, sin ruido.
- MANEJO DE PROBLEMAS**
Menos fallos, más vida útil de los activos.
- RESPUESTA AUTOMÁTICA**
Acciones inmediatas para reducir riesgos.
- MEJORA CONTINUA**
Aprendizaje constante para servir mejor.

5. IMPACTO EN EL MUNDO REAL

- 70%**
Menos incidentes de seguridad.
- 60%**
Tiempo de inactividad y recuperación más rápidos.
- 30%**
Reducción de costos operativos.
- +50%**
Resiliencia y continuidad del servicio.
- +40%**
Eficiencia energética y sostenibilidad.
- 100%**
Transparencia y trazabilidad de acciones y eventos.

3. BENEFICIOS CLAVE

- DETECCIÓN TEMPRANA DE AMENAZAS**
La IA identifica ataques y fallos antes de que se conviertan en incidentes críticos.
- RESILIENCIA Y CONTINUIDAD**
Menos interrupciones, recuperación más rápida y operación continua de servicios esenciales.
- TRANSPARENCIA Y CONFIANZA**
Blockchain garantiza trazabilidad y auditoría inmutable de eventos y decisiones.
- COORDINACIÓN DESCENTRALIZADA**
La DAO permite colaboración segura entre actores públicos y privados sin un único punto de falla.
- EFICIENCIA OPERATIVA**
Optimiza recursos, reduce costos y mejora el mantenimiento predictivo.
- CUMPLIMIENTO Y SEGURIDAD**
Automatiza cumplimiento normativo y mejora la gestión de riesgos y la ciberseguridad.
- SOSTENIBILIDAD**
Maximiza la eficiencia energética y promueve una operación más sostenible.

6. UN FUTURO MÁS SEGURO Y RESILIENTE

La combinación de IA, Blockchain y Gobierno Descentralizado fortalece la protección de nuestras infraestructuras críticas, garantiza servicios esenciales confiables y construye ciudades y sociedades más resilientes y sostenibles.



1. EL ECOSISTEMA AGROALIMENTARIO DEL FUTURO

La integración de IA, Blockchain y Gobierno Descentralizado crea un nuevo modelo agroalimentario más productivo, sostenible, seguro y resiliente.



Datos confiables - Trazabilidad total - Decisiones inteligentes
Comunidades empoderadas - Alimentos seguros

- ALIMENTOS MÁS SEGUROS Y NUTRITIVOS**
Trazabilidad completa desde el origen hasta el consumidor.
- PRODUCCIÓN MÁS EFICIENTE Y SOSTENIBLE**
IA optimiza recursos, reduce desperdicios y cuida el planeta.
- TRANSPARENCIA Y CONFIANZA**
Información verificable y accesible para todos los actores.
- INCLUSIÓN Y JUSTICIA**
DAO permite participación y decisiones más justas.
- RESILIENCIA ANTE RIESGOS**
Sistemas más preparados frente a crisis, plagas y crisis.

4. CASOS DE USO

- AGRICULTURA DE PRECISIÓN**
Siembra, riego y fertilización basados en datos reales.
- MONITORIO DE GANADO**
Bienestar animal, salud y productividad con IA e IoT.
- TRAZABILIDAD AGROALIMENTARIA**
Del campo a la mesa con Blockchain.
- GESTIÓN DE INVENTARIOS Y LOGÍSTICA**
Optimización de almacenamiento y transporte.
- SEGUROS PARAMÉTRICOS**
Pagos automáticos por eventos climáticos extremos.
- MERCADOS Y FINANCIAMIENTO DESCENTRALIZADO**
Acceso a crédito, inversión y pagos sin intermediarios.

IA + BLOCKCHAIN + GOBIERNO DESCENTRALIZADO TRANSFORMANDO LA AGRICULTURA Y LA SEGURIDAD ALIMENTARIA

Tecnología inteligente y descentralizada para un sistema alimentario más sostenible, transparente, eficiente y justo para todos.



APLICADO A LA AGRICULTURA Y SISTEMA ALIMENTARIO



TECNOLOGÍAS CLAVE EN ACCIÓN

- SENSORES IoT**
Monitoreo continuo de cultivos, suelo, agua y ambiente.
- VISIÓN POR COMPUTADORA**
Detección temprana de plagas y enfermedades.
- MACHINE LEARNING**
Predicción de cosechas, precios, demanda y riesgos.
- SMART CONTRACTS**
Automatización de pagos, seguros, certificaciones y acuerdos.
- TOKENS Y DAO**
Inversión, gobernanza participativa y fondos comunitarios.

5. IMPACTO EN EL MUNDO REAL

- 30%**
Reducción en uso de agua y fertilizantes.
- +25%**
Aumento promedio en productividad.
- 40%**
Menos pérdidas y desperdicio de alimentos.
- +20%**
Aumento en ingresos de productores.
- +50%**
Mayor seguridad alimentaria.
- 35%**
Reducción de huella ambiental.

3. BENEFICIOS CLAVE

- MAYOR PRODUCTIVIDAD**
IA optimiza cada etapa del cultivo y uso de recursos.
- ALIMENTOS MÁS SEGUROS**
Trazabilidad y control de calidad garantizados.
- REDUCCIÓN DE COSTOS**
Menos insumos, menos pérdidas y procesos más eficientes.
- SOSTENIBILIDAD AMBIENTAL**
Menor impacto ambiental, conservación de suelos, agua y biodiversidad.
- INCLUSIÓN DE PEQUEÑOS PRODUCTORES**
Acceso a tecnología, mercados y financiamiento en condiciones justas.
- CONFIANZA Y TRANSPARENCIA**
Información verificable para consumidores, empresas y gobiernos.
- RESILIENCIA ALIMENTARIA**
Sistemas más preparados ante crisis climáticas, sanitarias y económicas.

6. UN FUTURO SOSTENIBLE Y EQUITATIVO

La combinación de IA, Blockchain y Gobierno Descentralizado construye un sistema agroalimentario más inteligente, transparente y humano, que protege el planeta y garantiza alimento para todos, hoy y siempre.



EL FUTURO AGROALIMENTARIO ES:



INTELIGENTE
Decisiones basadas en datos y evidencia.



DESCENTRALIZADO
Poder y decisiones en la comunidad.



TRANSPARENTE
Información abierta y verificable.



SOSTENIBLE
En armonía con la naturaleza.



INCLUSIVO
Oportunidades para todos.



RESILIENTE
Preparados para cualquier desafío.

TECNOLOGÍA AL SERVICIO DE LA VIDA,
PARA UN SISTEMA ALIMENTARIO JUSTO,
SOSTENIBLE Y PARA TODOS.



1. EL ECOSISTEMA VERDE DEL FUTURO

La integración de IA, Blockchain y Gobierno Descentralizado crea un ecosistema ambiental más transparente, colaborativo y efectivo para proteger nuestro planeta y todas las formas de vida.



- DATOS CONFIABLES DEL PLANETA**
Monitoreo transparente y en tiempo real.
- DECISIONES COLABORATIVAS**
Comunidades y expertos actúan juntos por el bien común.
- RECURSOS PROTEGIDOS**
Uso responsable y eficiente para generaciones futuras.
- TRANSPARENCIA Y CONFIANZA**
Todos los acciones y resultados son verificables e inmutables.

4. CASOS DE USO

- MONITOREO DE DEFORESTACIÓN**
Detección temprana mediante IA y satélites.
- CONSERVACIÓN DE ESPECIES**
Seguimiento de animales y protección de hábitats críticos.
- CREDITOS DE CARBONO VERDES**
Transferibilidad en blockchain para proyectos verdes y mercados de carbono.
- GESTIÓN DE ÁREAS PROTEGIDAS**
Control de acceso, turismo sostenible y vigilancia comunitaria.
- AGRICULTURA REGENERATIVA**
Prácticas sostenibles que cuidan al suelo, el agua y la biodiversidad.

IA + BLOCKCHAIN + GOBIERNO DESCENTRALIZADO PROTEGIENDO NUESTRO PLANETA Y SU BIODIVERSIDAD

Tecnología inteligente y descentralizada para un futuro sostenible, saludable y en armonía con la naturaleza.

2. ¿CÓMO FUNCIONA?

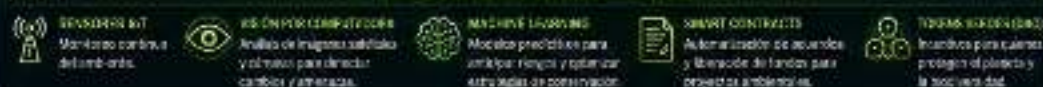


APLICADO AL MEDIO AMBIENTE Y LA NATURALEZA



CADA ACCIÓN CUENTA, CADA DATO IMPORTA,
CADA ESPECIE TIENE VALOR

TECNOLOGÍAS CLAVE EN ACCIÓN



5. IMPACTO EN EL PLANETA (Y EN NOSOTROS)



3. BENEFICIOS CLAVE

- PROTECCIÓN EFECTIVA**
Decisiones basadas en datos precisos y oportunos que generan mayor impacto positivo.
- TRANSPARENCIA TOTAL**
Información pública, verificable y auditable por todos.
- CONFIANZA Y PARTICIPACIÓN**
Las comunidades son protagonistas en la toma de decisiones ambientales.
- REDUCCIÓN DE COSTOS**
Procesos más eficientes, menor duplicación y uso óptimo de recursos.
- SOSTENIBILIDAD REAL**
Acciones medibles y responsables para un planeta saludable.
- JUSTICIA AMBIENTAL**
Acceso equitativo a información, beneficios y oportunidades verdes.
- RESILIENCIA PLANETARIA**
Ecosistemas más sanos y preparados ante el cambio climático y desastres.

6. UN FUTURO VERDE, SALUDABLE Y COMPARTIDO

La combinación de IA, Blockchain y Gobierno Descentralizado nos permite ser guardianes del planeta, proteger su biodiversidad y asegurar un futuro digno para todas las formas de vida.



EL FUTURO QUE ELEGIMOS:



INTELIGENTE
Decisiones basadas en datos y evidencia.



DESCENTRALIZADO
Poder y decisiones en la comunidad.



TRANSPARENTE
Información abierta y verificable.



SOSTENIBLE
En armonía con la naturaleza.



INCLUSIVO
Participación de todas las personas y comunidades.



RESILIENTE
Preparados para los retos del presente y el futuro.

**GUÍDEMOS HOY, PARA VIVIR MAÑANA.
UN PLANETA, UNA BIODIVERSIDAD,
UN FUTURO PARA TODOS.**



06

SECCIÓN

Conclusiones y Preguntas

Cierre y conversación

La **Inteligencia Artificial** y la **Ciberseguridad**

no solo protegen sistemas;
protegen **personas**, **empresas**,
comunidades y el futuro de
nuestra sociedad.



El futuro no depende
únicamente de la **tecnología**.

Depende de cómo
decidamos **utilizarla**.



ÉTICA

para tomar
decisiones correctas.



RESPONSABILIDAD

para generar
confianza.



COLABORACIÓN

para construir
juntos.



EMPATÍA

para poner a las
personas primero.



VISIÓN

para un futuro más
seguro y sostenible.



La tecnología es poderosa, pero nuestro propósito es lo que le da verdadero sentido.

PROTEJAMOS HOY, **CONSTRUYAMOS MAÑANA.**





¡Gracias!

Sigueme en mis redes
sociales

www.linkedin.com/in/s4kurak

<https://x.com/S4kurak>

***La Inteligencia Artificial no reemplaza el talento
Humano: lo amplifica y lo conecta.***



¡Gracias!

¿Conversamos? Espacio para preguntas.



Congreso AI LATAM

Comunidad de Inteligencia Artificial · Latinoamérica