AteneA
Centro de Pensamiento de Auditoría

VI Encuentro Latinoamericano de Auditoría

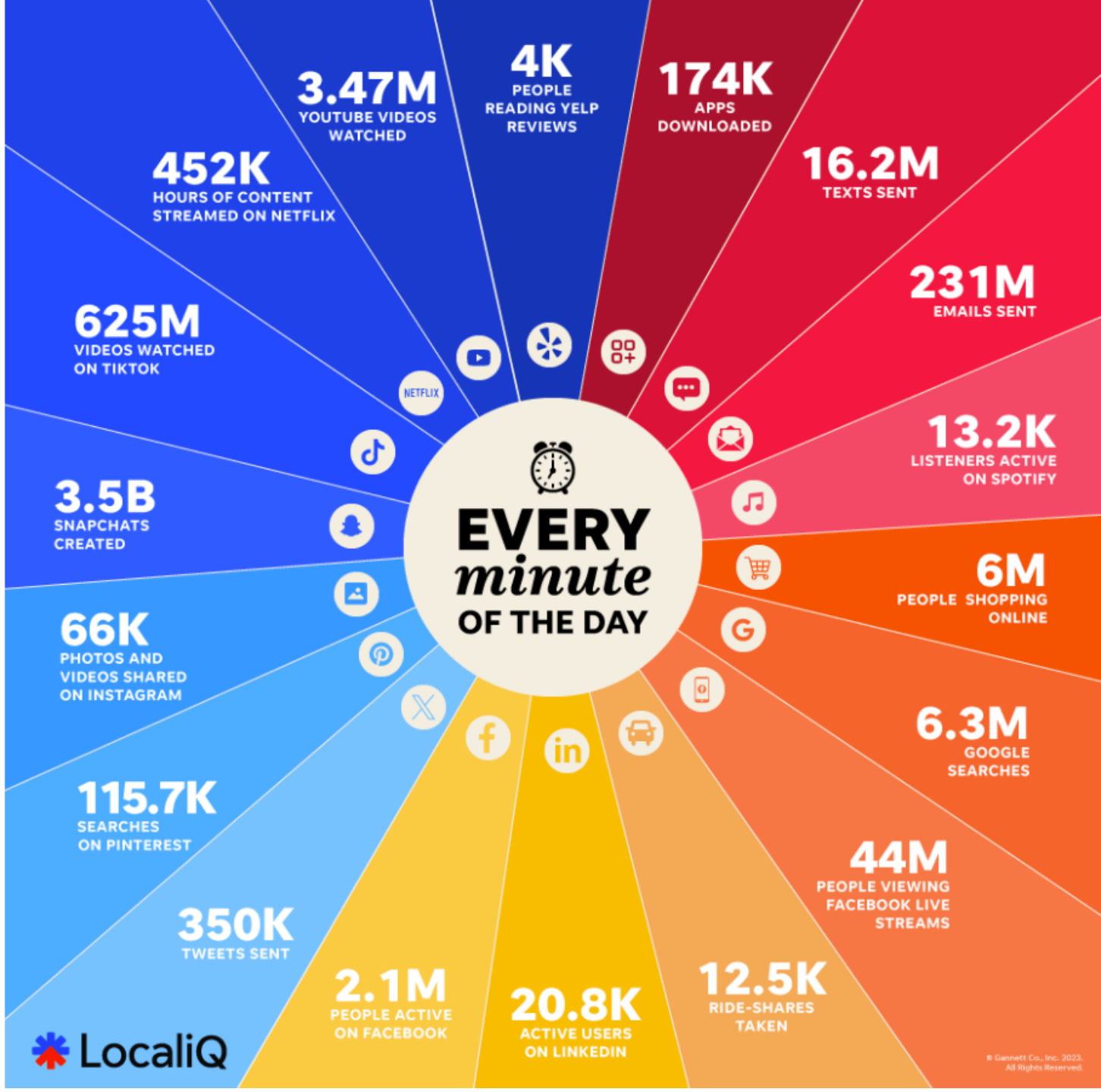
Conocimiento y aplicación en la era digital

Innovación desde los ojos de un *hacker*

Jaime Rios, socio líder BDO Digital LATAM

¿Un minuto de silencio?

¿Y los ciberataques?



https://localiq.com/blog/what-happens-in-an-internet-minute/

Panorama general de riesgos – Cyber + AI

FIGURE C **Global risks ranked by severity over the short and long term**

"Please estimate the likely impact (severity) of the following risks over a 2-year and 10-year period."

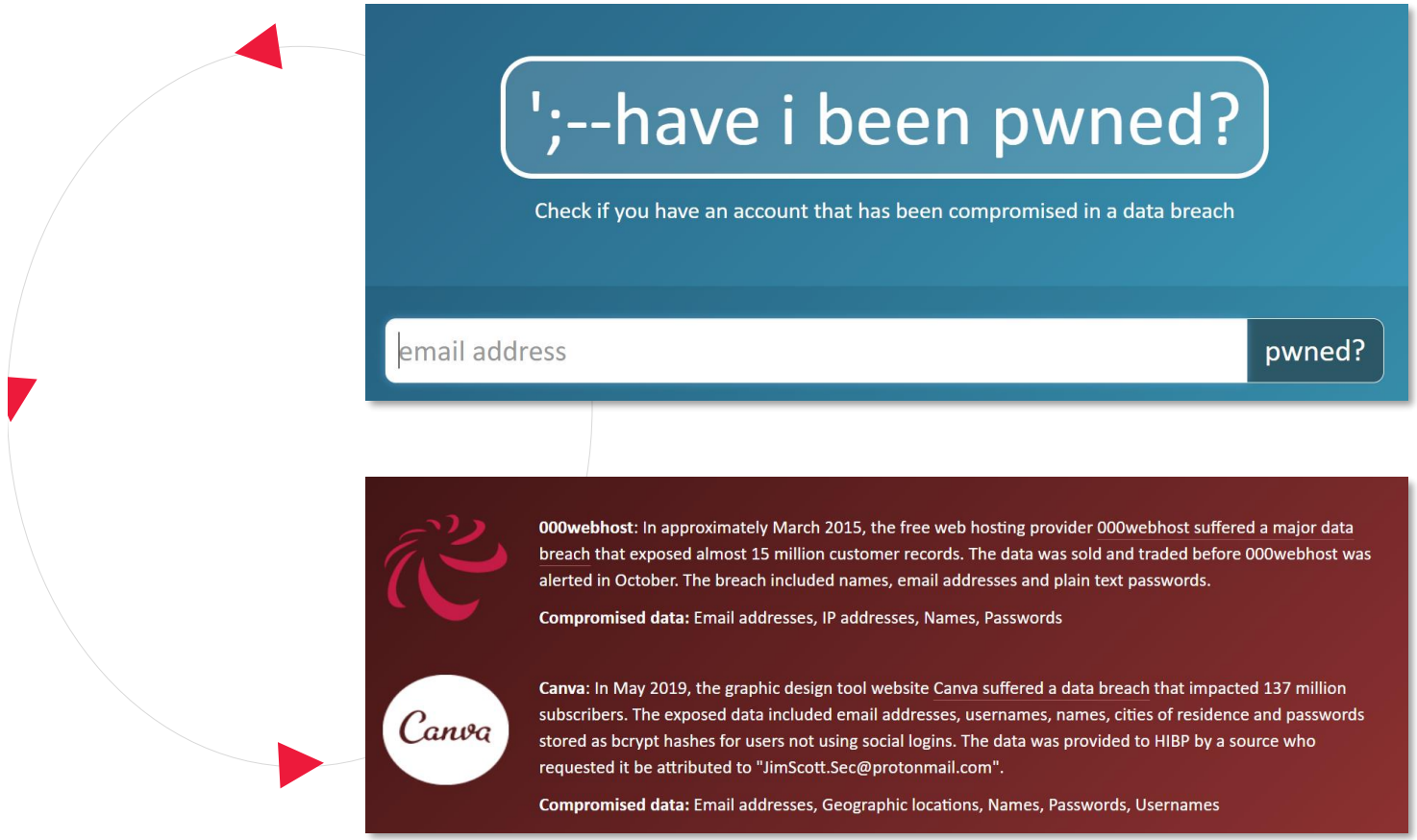
Source
World Economic Forum Global Risks Perception Survey 2023-2024.

- Las industrias más afectadas por ataques cibernéticos: manufactura, salud, sector financiero y educación
- El *phishing* fue identificado como el vector primario de infección en el 41% de los casos de incidentes de ciberseguridad.
- Los blancos más comunes desde la tecnología son:
  - Servicios y productos Cloud
  - APIs
  - Sitios web
  - Aplicaciones móviles

Se espera que el costo de los ciberataques se acerque a los $9.5 trillones. El ransomware seguirá siendo el tipo de ciberataque más frecuente en el 2024, y se espera que incremente, llegando a representar más del 72% de los ataques cibernéticos que representó en el 2023.

© BDO

¿Será posible que mis datos se hayan filtrado?



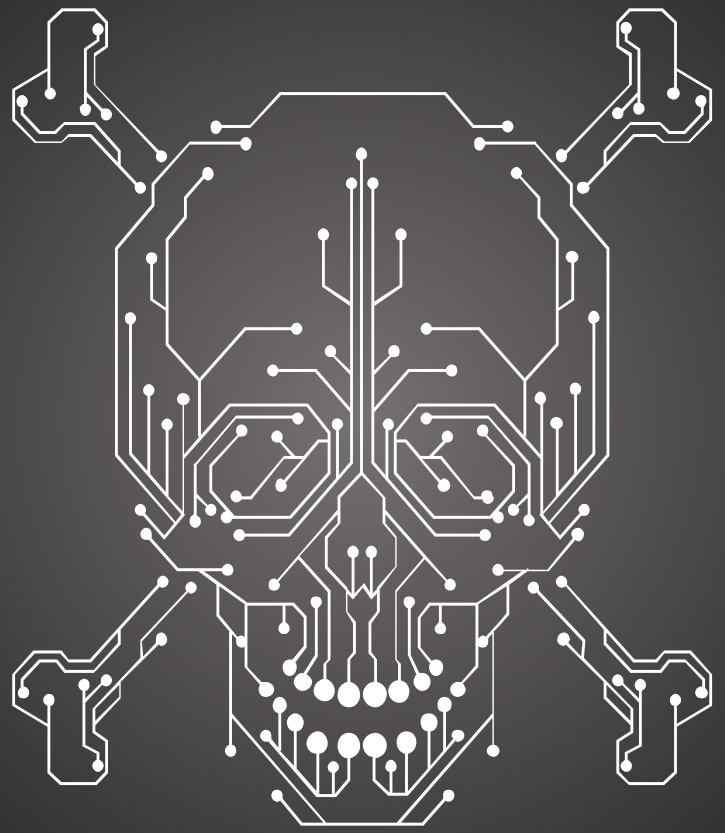
Información Interna

© BDO

EL DESAFÍO: Innovación + Cyber

Innovación

Es la **introducción** de un ***nuevo o mejorado*** producto, proceso o servicio que difiere significativamente de los productos o procesos previos de la Unidad



Ciberseguridad

¿Qué es hacking?

El acto de resolver problemas complejos por vías poco ortodoxas, descubriendo enfoques no convencionales que generan nuevos conocimientos

ALICE

EDAD: 29

OCUPACIÓN: *Hacker*

EDUCACIÓN: Sin definir

¿CÓMO ME DEFINO?

Soy una persona con una curiosidad insaciable, con voluntad de experimentar con enfoques poco convencionales para superar retos, el deseo de renunciar al pensamiento tradicional en favor de nuevas posibilidades.

MINDSET

- *Toda barrera puede ser sobrepasada*
- *Brújulas en lugar de mapas*
- *Nada es estático*
- *Curiosidad & Experimentación incrementada*
- *Formación evolutiva*

Información Interna

Toda barrera puede ser sobrepasada

- $7.5M
- Año 2013
- Al menos 40 millones de números de tarjetas de crédito fueron robados y la información personal de cerca de 110 millones de personas

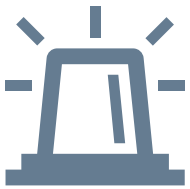
El primer enfoque adoptado para cualquier problema inicia con la identificación de la barrera que será infiltrada

En el ataque los hackers lograron establecer su blanco, sobrepasaron los obstáculos y generaron diferentes enfoques creativos para identificar vulnerabilidades y las explotaron.

Información Interna

Cyber: errores comunes

Cuando se presentan filtraciones de datos



Notificaciones tardías

A mayor tiempo en comunicar a clientes, mayor la probabilidad de que los criminales utilicen sus datos comprometidos.

Servicio al cliente

Ausencia de foco en cliente, alineado con la severidad de la filtración.

Transparencia

Evadir la verdad y no suministrar información precisa sobre el incidente.

Responsabilidad

Una filtración de datos masiva no es un problema tecnológico. Es una situación de carácter organizacional y responsabilidad de la alta dirección.

Información Interna

Pablos Holman

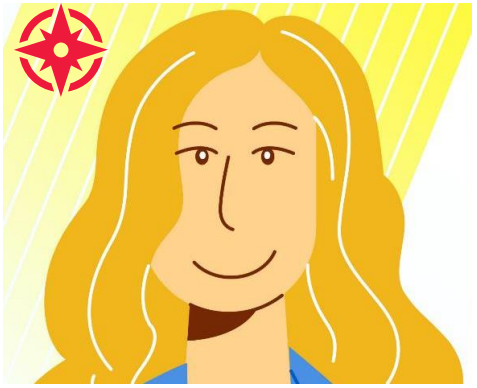
Pasión por los retos

Las reglas existen para romperse

Siempre hay una forma

¿Hacking para reducir la malaria?

Información Interna



Atributos de Alice

Valentía & Coraje

Espiritu de aventura

Pasión por el proceso tanto como el resultado

Brújula en lugar de mapas

Información Interna

Cyber

RED TEAM

- Offensive Security
- Ethical Hacking
- Exploiting Vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning

© BDO

Innovación

"Plans are nothing, planning is everything"

Eisenhower

© BDO

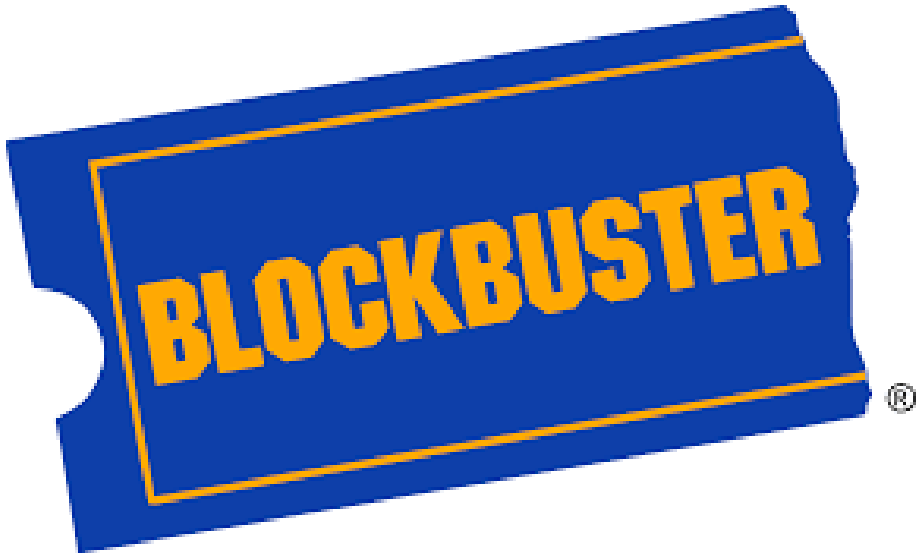
Nada es estático

El conocimiento y su aplicación nunca debe ser estacionario

Adaptación

Mejora continua

Innovación



NETFLIX

Nada es estático

Cyber: constante evolución

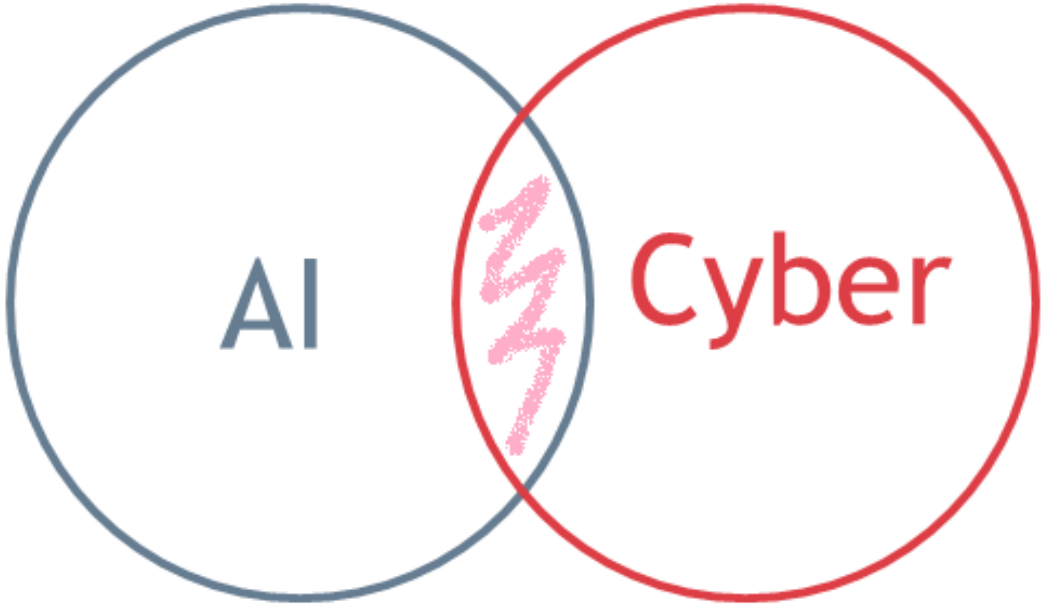
Cumplimiento

Riesgo

Transformación

Incertidumbre

Nada es estático



AI, lo que nos puede hacer

- *Phishing*
- *Malware*
- Desinformación

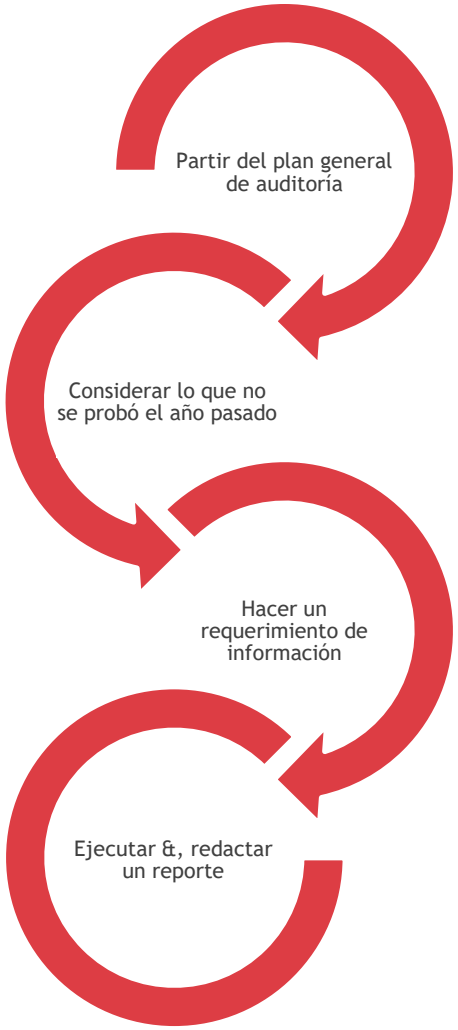
AI, lo que puede hacer por nosotros

- Análisis
- Automatización
- Interacción

Nada es estático

Curiosidad & experimentación incrementada

Caso de estudio: una auditoria de TIC



Traditionalist
Top-down
Monolithic
Few giant bets
Protect old ideas
Static
Rules-centric
Slow, clunky
Lethargic
Resource-heavy
Avoid risk

#1 Toda barrera puede ser sobrepasada: *"Haremos algo diferente y único para generar valor con esta auditoría"*

#2 Brújula en lugar de mapas: "¿Es el foco adecuado? ¿Qué quieren mis usuarios?"

#3 Nada es estático: "Vamos a aprender tanto como sea posible para identificar y aplicar diferentes enfoques"

「I f*cked up」

#4 Experimentación incrementada *"¿Cómo puedo probar muchas variables antes de una solución definitiva?"*

#4 Experimentación incrementada *"¿Cómo puedo probar muchas variables antes de una solución definitiva?"*

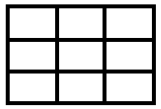
Hacker Approach
Bottom-up
Democratic
Many small experiments
Create new ideas
Constantly changing
Idea-centric
Fast, agile
Burning urgency
Scrappy
Embrace risk

Información Interna

Formación evolutiva & mérito es la única credencial válida

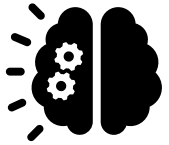
“Alfabetización de Datos”

Interpretar, crear y comunicar datos de manera efectiva.



Habilidades básicas de SQL

Visualización de Datos



Pensamiento analítico

Prompt Engineering

© BDO

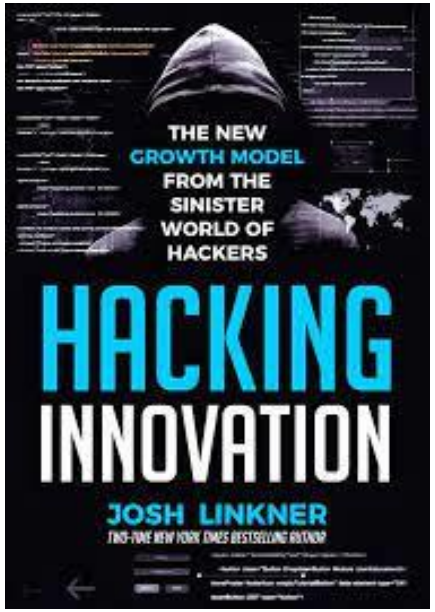
Mensajes clave

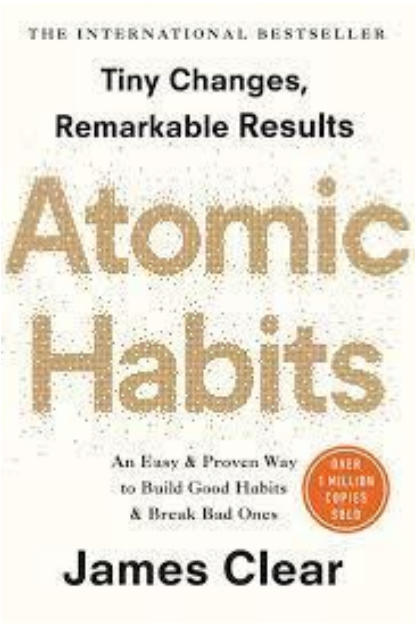
- *El hombre naturalmente puede resolver problemas, por tanto todos podemos ser hackers*
- *El proceso es tan importante como el resultado*
- *Los hackers pueden afectar redes, equipos de cómputo, también ideas, productos y procesos que no tienen que ver con tecnología*

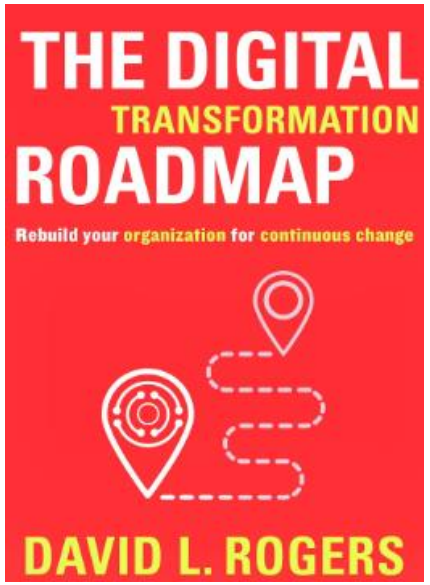
El poder de la tecnología e innovación reside en las manos de quien las adopta

© BDO

Mis recomendados







Jaime Rios – Advisory Partner, BDO en Colombia

Para más información

Carrera 16 # 97 – 46 pisp 8 , Bogotá D.C. Colombia
T (57 – 1) 6230199
comercial@bdo.com.co
www.bdo.com.co

BDO Colombia S.A.S., una sociedad por acciones simplificada colombiana, es miembro de BDO International Limited, una compañía limitada por garantía del Reino Unido, y forma parte de la red internacional BDO de empresas independientes asociadas.
BDO es el nombre comercial de la red BDO y de cada una de las empresas asociadas de BDO.
Copyright © Enero 2022. BDO en Colombia. Todos los derechos reservados. Publicado en Colombia.

Innovación desde los ojos de un hacker

AteneA
Centro de Pensamiento de Auditorio

Registro de asistencia y evaluación de conferencias

AteneA
Centro de Pensamiento de Auditoría

VI Encuentro Latinoamericano de Auditoría

Conocimiento y aplicación en la era digital

Deloitte.

Ética en ambientes de IA

Octubre 2024

Agenda

© 2024 Deloitte & Touche S.A.S., Deloitte Asesores y Consultores S.A.S., D Contadores S.A.S., Deloitte S.A.S. y D Profesionales S.A.S., según el servicio que presta cada una.

IA generativa

Las organizaciones pueden utilizar GenAI para obtener valor en seis categorías clave

Reducción de costos

Reducir los costos, principalmente, a través de la automatización de las funciones de trabajo.

Operaciones del centro de llamadas
(Intersectorial)

Eficiencia del proceso

Crear eficiencias en los procesos mediante la automatización de tareas estándar y la reducción de las intervenciones manuales.

Procesamiento de reclamos
(Seguro)

Crecimiento

Aumentar el crecimiento a través de recomendaciones de productos de banca minorista y *marketing* dirigido hiperpersonalizado.

Generación de contenido
(Marketing/Publicidad)

Acelerar la innovación (productos/servicios)

Aumentar el ritmo de desarrollo de nuevos productos o servicios y agilizar la comercialización.

Cajeros de la banca digital
(Banca minorista)

Nuevos descubrimientos y perspectivas

Revelar nuevas ideas, conocimientos, preguntas y, en general, dar rienda suelta a la creatividad.

IA contra el blanqueo de capitales
(Servicios Financieros)

Servicios a la ciudadanía

Aumentar la precisión de varios programas federales y locales, así como facilitar el acceso a las poblaciones en riesgo.

Educación financiera personalizada
(Gobierno)

© 2024 Deloitte & Touche S.A.S., Deloitte Asesores y Consultores S.A.S., D Contadores S.A.S., Deloitte S.A.S. y D Profesionales S.A.S., según el servicio que presta cada una.

Riesgos del uso de GenAI

Con los avances tecnológicos viene un conjunto emergente de riesgos

Riesgos emergentes de la IA generativa	
Ampliación de sesgos	Se relaciona con los modelos que propagan sesgos inherentes o históricos en los datos de entrenamiento subyacentes.
Uso seguro	Están asociados con cómo y dónde se utilizan los modelos de lenguaje grandes (LLM) .(Por ejemplo, el uso de LLM para generar acciones autónomas para la maquinaria en una fábrica).
Aplicaciones responsables	Está relacionado con los diversos casos de uso que probablemente se contemplarán (por ejemplo, el uso de LLM para aumentar las amenazas cibernéticas automatizadas).
Soberanía	Se refieren a la expectativa de que los modelos de IA entrenados en ciertos conjuntos de datos estén sujetos a regulaciones de soberanía/residencia y se requiere que se ejecuten solo en centros de datos en esa jurisdicción.
Falta de certificaciones	Se refiere a que los LLM se enfrenten a futuras regulaciones, ya que se utilizan cada vez más para obtener información o asesoramiento, y el riesgo de que las personas confíen en los resultados del modelo y busquen una solución legal cuando las cosas van mal.

Protecciones	
Entornos seguros	Utilizar LLM, previamente entrenados en entornos seguros (centro de datos o nube), para reducir la probabilidad de fugas de información de la empresa.
Uso restringido	Limitar el uso inicial de la IA generativa para aumentar la precisión de las inferencias, ampliar y escalar una vez que haya una creciente sensación de comodidad con los resultados.
Utilice los LLM previamente formados de manera segura	Implemente LLM, previamente entrenados y potencialmente aumentados, con conjuntos de datos empresariales en los procesos de trabajo centrales.
Auditoría	Trabajar con los datos de la empresa que se utilizan para aumentar los LLM previamente entrenados para tener un registro de auditoría del tipo de datos que se utilizaron.
Confiar pero verificar	Mantener al personal involucrado durante todo el proceso para ayudar a validar y verificar el resultado generado y para hablar sobre la precisión de la IA.
Gestión de aplicaciones	Formar equipos centrados en operar y gobernar las aplicaciones para evitar estar a la deriva a lo largo del tiempo y garantizar que los modelos subyacentes sigan siendo adecuados para su propósito.

Se prevé que muchos riesgos en torno al uso de GenAI en aplicaciones B2C se reduzcan en un entorno B2B más controlado que se centre en la automatización del flujo de trabajo, la automatización de tareas cognitivas y los LLM preentrenados aumentados con los datos patentados (no públicos) de una empresa.

© 2024 Deloitte & Touche S.A.S., Deloitte Asesores y Consultores S.A.S., D Contadores S.A.S., Deloitte S.A.S. y D Profesionales S.A.S., según el servicio que presta cada una.

A medida que los algoritmos y la IA se integran más en las empresas, aumenta la posibilidad de riesgos e incidentes relacionados con la IA

1. **Riesgo reputacional:** los algoritmos y la IA pueden plantear riesgos reputacionales si las partes interesadas perciben una falta de alineación con la ética o los valores de la organización. El riesgo surge si estos están diseñados para manipular de forma encubierta a los consumidores, los reguladores o los empleados.
2. **Riesgo financiero:** los algoritmos y la IA defectuosos, especialmente en la toma de decisiones financieras y estratégicas, pueden provocar una pérdida sustancial de ingresos y socavar la integridad de los informes financieros.
3. **Riesgo regulatorio:** los algoritmos y la IA que toman decisiones que violan la ley, eluden las reglas y regulaciones existentes o discriminan a ciertos grupos de personas pueden exponer a las organizaciones a acciones regulatorias y legales.
4. **Riesgo estratégico:** dado que los algoritmos y la IA se utilizan cada vez más como fuentes para la toma de decisiones estratégicas, los errores o vulnerabilidades en ellos pueden poner a una organización en desventaja competitiva.
5. **Riesgo operativo:** al utilizarse a menudo para automatizar áreas operativas, los errores pueden provocar importantes interrupciones operativas.

El impacto de los algoritmos no conformes

440 millones USD

Pérdidas en poco más de 30 minutos debido a un algoritmo defectuoso que provoca operaciones inexactas en una plataforma financiera estadounidense. Resultó en la quiebra de la empresa.

$389 millones

Multa del regulador por controles de privacidad ineficaces, prácticas de transparencia engañosas y configuraciones de privacidad injustas. Afectó a 1,4 millones de usuarios infantiles.

$1.3 mil millones

Multa del regulador por fallas algorítmicas en las transferencias de datos que violaron las regulaciones de privacidad. Impactó a 533 millones de usuarios.

$78.3 millones

Indemnización total a 555 personas condenadas falsamente por robo de contabilidad debido a un software informático defectuoso. Más de 4.000 personas afectadas, de las cuales 230 fueron encarceladas injustamente.

$1.2 mil millones

Acuerdo proporcionado a 394.000 víctimas de un algoritmo de promedio de ingresos defectuoso. La deuda de más de 1.100 millones de dólares fue notificada injustamente, lo que causó angustia financiera y mental.

$865 millones

Multa del regulador por incumplimiento de la recopilación y el procesamiento legal de datos personales. Resultado de 10.000 denuncias.

© 2024 Deloitte & Touche S.A.S., Deloitte Asesores y Consultores S.A.S., D Contadores S.A.S., Deloitte S.A.S. y D Profesionales S.A.S., según el servicio que presta cada una.

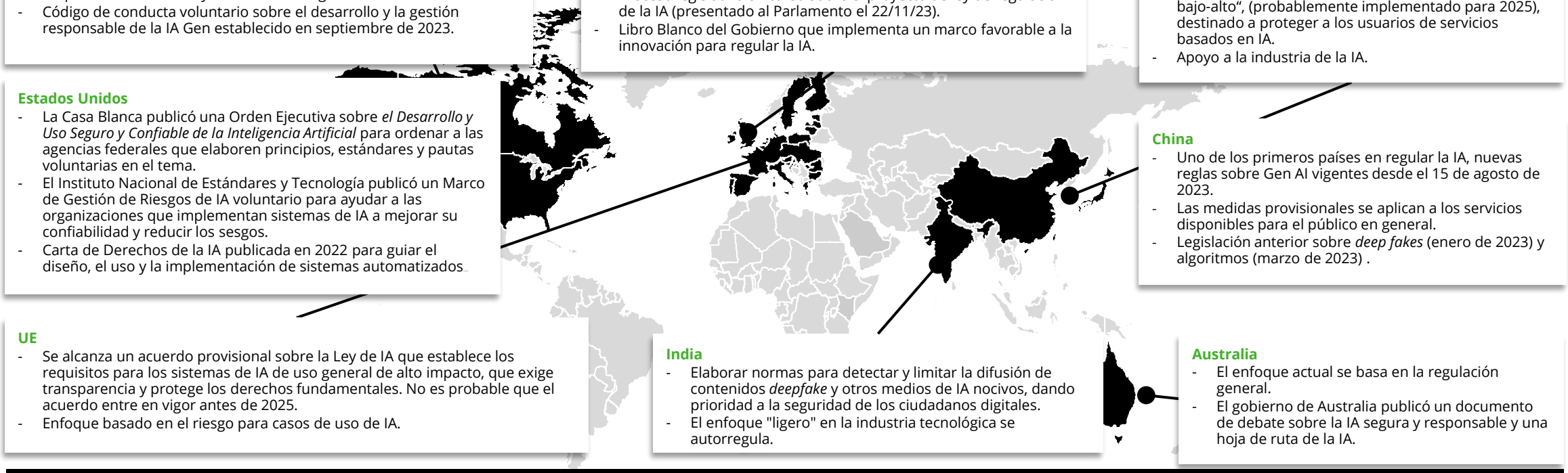
Países de todo el mundo están diseñando e implementando regulación sobre gobernanza de la IA para responder a la proliferación de tecnologías impulsadas por esta

Canadá
- Se redacta la Ley de IA y Datos (AIDA) para regular el desarrollo y el uso de los sistemas de IA que entraría en vigor en 2025.
- Requisito de identificar y abordar los riesgos de los sistemas de IA.
- Código de conducta voluntario sobre el desarrollo y la gestión responsable de la IA Gen establecido en septiembre de 2023.

Reino Unido
- AI Summit (1 y 2 de noviembre de 2023), compromiso para hacer del Reino Unido el 'hogar global' de la regulación de la IA.
- Proceso legislativo en curso sobre el proyecto de ley de regulación de la IA (presentado al Parlamento el 22/11/23).
- Libro Blanco del Gobierno que implementa un marco favorable a la innovación para regular la IA.

Corea del Sur
- Proyecto de ley de IA con evaluación marco de "riesgo bajo-alto“, (probablemente implementado para 2025), destinado a proteger a los usuarios de servicios basados en IA.
- Apoyo a la industria de la IA.

Estados Unidos
- La Casa Blanca publicó una Orden Ejecutiva sobre *el Desarrollo y Uso Seguro y Confiable de la Inteligencia Artificial* para ordenar a las agencias federales que elaboren principios, estándares y pautas voluntarias en el tema.
- El Instituto Nacional de Estándares y Tecnología publicó un Marco de Gestión de Riesgos de IA voluntario para ayudar a las organizaciones que implementan sistemas de IA a mejorar su confiabilidad y reducir los sesgos.
- Carta de Derechos de la IA publicada en 2022 para guiar el diseño, el uso y la implementación de sistemas automatizados.



China
- Uno de los primeros países en regular la IA, nuevas reglas sobre Gen AI vigentes desde el 15 de agosto de 2023.
- Las medidas provisionales se aplican a los servicios disponibles para el público en general.
- Legislación anterior sobre *deep fakes* (enero de 2023) y algoritmos (marzo de 2023) .

UE
- Se alcanza un acuerdo provisional sobre la Ley de IA que establece los requisitos para los sistemas de IA de uso general de alto impacto, que exige transparencia y protege los derechos fundamentales. No es probable que el acuerdo entre en vigor antes de 2025.
- Enfoque basado en el riesgo para casos de uso de IA.

India
- Elaborar normas para detectar y limitar la difusión de contenidos *deepfake* y otros medios de IA nocivos, dando prioridad a la seguridad de los ciudadanos digitales.
- El enfoque "ligero" en la industria tecnológica se autorregula.

Australia
- El enfoque actual se basa en la regulación general.
- El gobierno de Australia publicó un documento de debate sobre la IA segura y responsable y una hoja de ruta de la IA.

Siguen surgiendo regulaciones que exigen la gestión de riesgos

*Este mapa no representa hasta qué punto las jurisdicciones de todo el mundo son activas en la legislación sobre gobernanza de la IA o en las estrategias de IA.

* NIST: Instituto Nacional de Estándares y Tecnología | **Fuentes:** Gartner |La geopolítica está dando forma a la IA generativa (y viceversa)

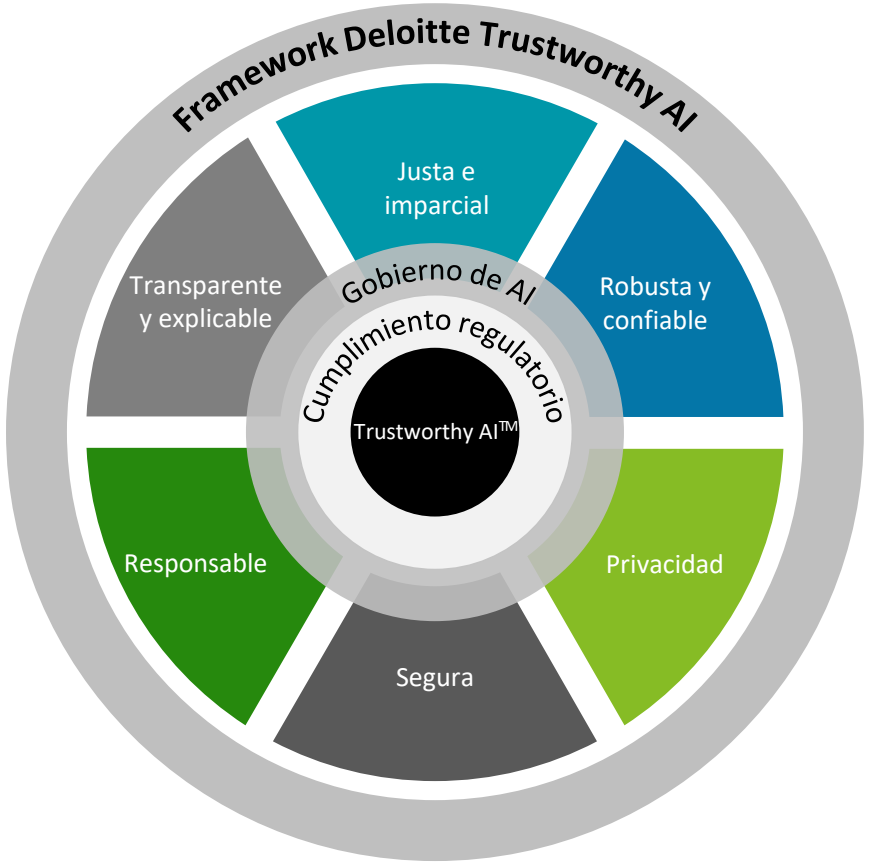
© 2024 Deloitte & Touche S.A.S., Deloitte Asesores y Consultores S.A.S., D Contadores S.A.S., Deloitte S.A.S. y D Profesionales S.A.S., según el servicio que presta cada una.

De todos modos, las organizaciones en el ámbito mundial están adoptando un enfoque de adopción de IA confiable

Transparente y explicable
Se entiende cómo la data se está utilizando por la IA y cómo la compañía está tomando las decisiones: algoritmos y variables están disponibles para su análisis.

Responsable
Se dispone de políticas para determinar quién es el responsable de una salida de un sistema que toma decisiones basadas en IA.

Segura
Se protege a los sistemas y datos de incidentes (incluyendo ciberseguridad) , lo que podría generar daño físico o digital.



Justa e imparcial
Se generan validaciones internas y externas para asegurar una aplicación justa e imparcial de la IA a todos los participantes.

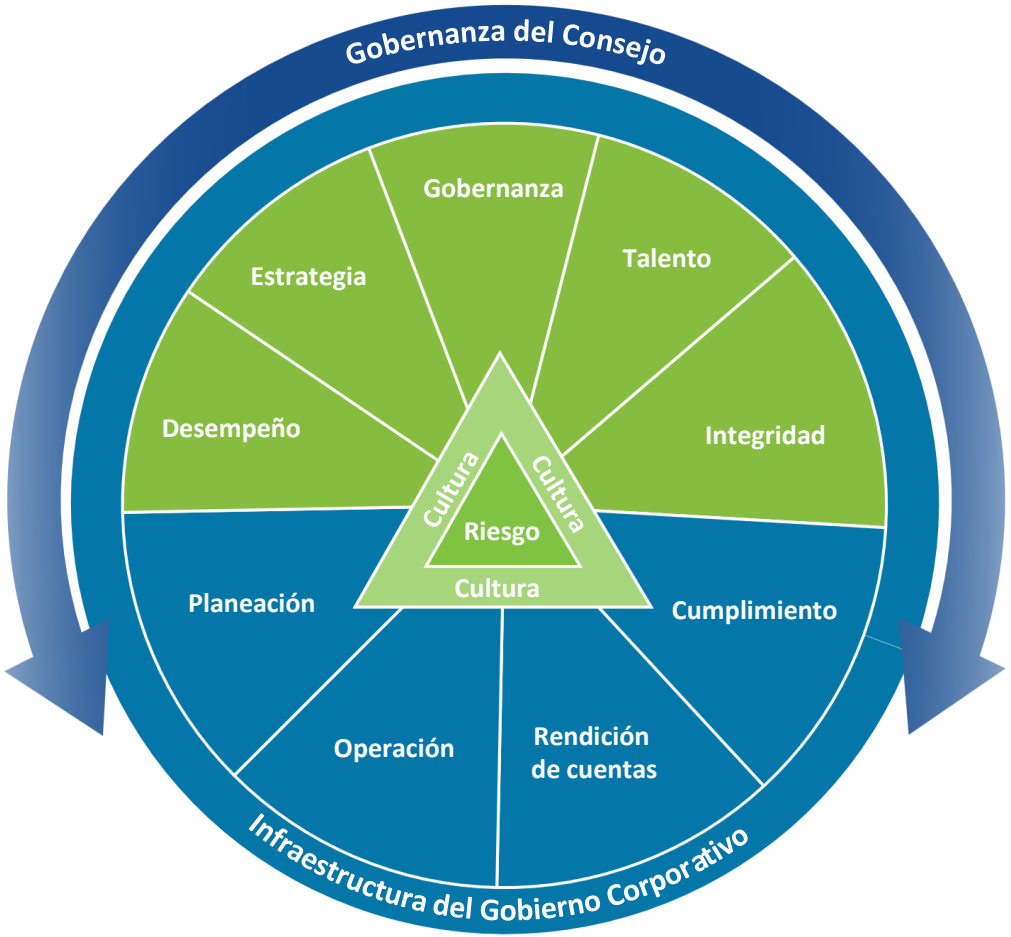
Robusta y confiable
Se tiene la capacidad de aprender de los humanos y otros sistemas para producir resultados consistentes y confiables.

Privacidad
Se respeta la privacidad del consumidor y su data no se usa más allá de su esperado y aprobado. Los consumidores pueden hacer *opt in / out* en cualquier momento al compartir la información.

© 2024 Deloitte & Touche S.A.S., Deloitte Asesores y Consultores S.A.S., D Contadores S.A.S., Deloitte S.A.S. y D Profesionales S.A.S., según el servicio que presta cada una.

Papel del Consejo de Administración

Los consejos de administración deben ser conscientes de cómo GenAI está afectando a su función y a su organización



El marco de gobernanza de Deloitte

Rendimiento	Estrategia	Gobernanza
Comprender dónde GenAI puede **generar valor** para la organización y asegurarse de que la administración adopte GenAI de **manera efectiva, eficiente** y **responsable.**	Identificar los **procesos de negocio principales** (por ejemplo, el ciclo de ingresos) que la organización espera que se vean más afectados por la GenAI.	Reconocer la GenIA como una nueva **categoría de riesgo** que puede requerir la supervisión del consejo y nuevos procedimientos de gobernanza que los que existen en la actualidad.

Talento	Integridad	Cultura	Riesgo
Reevaluar los roles, las habilidades y el desempeño de los ejecutivos, teniendo en cuenta la creciente necesidad de **alfabetización tecnológica.**	Establecer el **tono ético** de la empresa en lo que respecta a GenAI y promover el cumplimiento legal y normativo.	Garantizar la alineación entre el uso de la IA por parte de la organización**, sus valores fundamentales y los sistemas de** incentivos y recompensas.	Prepárese para **los nuevos riesgos** asociados con la ética, los sesgos, la transparencia de la toma de decisiones de la IA y la supervisión del consejo relacionada.

© 2024 Deloitte & Touche S.A.S., Deloitte Asesores y Consultores S.A.S., D Contadores S.A.S., Deloitte S.A.S. y D Profesionales S.A.S., según el servicio que presta cada una.

La gobernanza y la supervisión efectivas involucran muchos aspectos de una organización

Consejo de Administración

- Responsabilidad final de la supervisión del negocio y la estrategia.
- Se mantiene informado de los acontecimientos clave.

Consejo de Administración

- Tiene la responsabilidad última de supervisar el negocio y la estrategia de la empresa.
- Comprender las **implicaciones** de la IA generativa en el **modelo de negocio**.
- Garantizar que la **guía de uso de GenAI y los procedimientos de gobernanza** estén **integrados en las políticas existentes** de ERM, MRM e IA, incluidos los proveedores aprobados, los casos de uso aceptables, los casos de uso que pueden requerir la aprobación del Consejo, los datos o la información que pueden usarse como entradas, etc.

Comités del Consejo / Comité de Auditoría

- Comprender la estrategia de IA y el impacto relacionado con los informes financieros y el SCIIF.

Elementos de supervisión

- El Consejo de Administración debe asignar la **responsabilidad de supervisión de la GenAI** a los **Comités del Consejo**, en función de las áreas para las que se utilice la IA (por ejemplo, los temas relacionados con la remuneración y/o el talento pueden ser supervisados por el Comité de Compensación, mientras que el uso de la IA relacionado con la estrategia ESG puede ser controlado por el Comité de Nominaciones/Gobernanza). El Consejo debe trabajar con la administración para saber dónde se está utilizando la IA y dónde se supervisan dichos procesos.
- El **Comité de Auditoría** debe comprender **cómo se utiliza GenAI en la organización**, incluidas las operaciones comerciales y de *back-office*, así como el impacto en la información financiera y otras divulgaciones/medidas. Además, el Comité de Auditoría debe asegurarse de que los **riesgos asociados** con los procesos de **GenAI** se **identifiquen** e incluyan en la **matriz de riesgos** y el Comité de Auditoría debe trabajar con la administración para determinar dónde supervisa riesgos el consejo.

Administración

- Definición de la estrategia de IA generativa
- Funciones y responsabilidades
- Políticas y procedimientos
- Gestión de riesgos

Funciones y responsabilidades de la gerencia

Desarrollo, implementación y uso
(1ª línea de defensa)

- Proceso de diseño
- Evaluación de datos
- Pruebas de sistemas de IA
- Documentación
- Documentación del usuario
- Proceso de detección de errores
- Límites y umbrales de rendimiento
- Programación
- Interconexión
- Mandos

Validación del sistema de IA
(2ª línea de defensa)

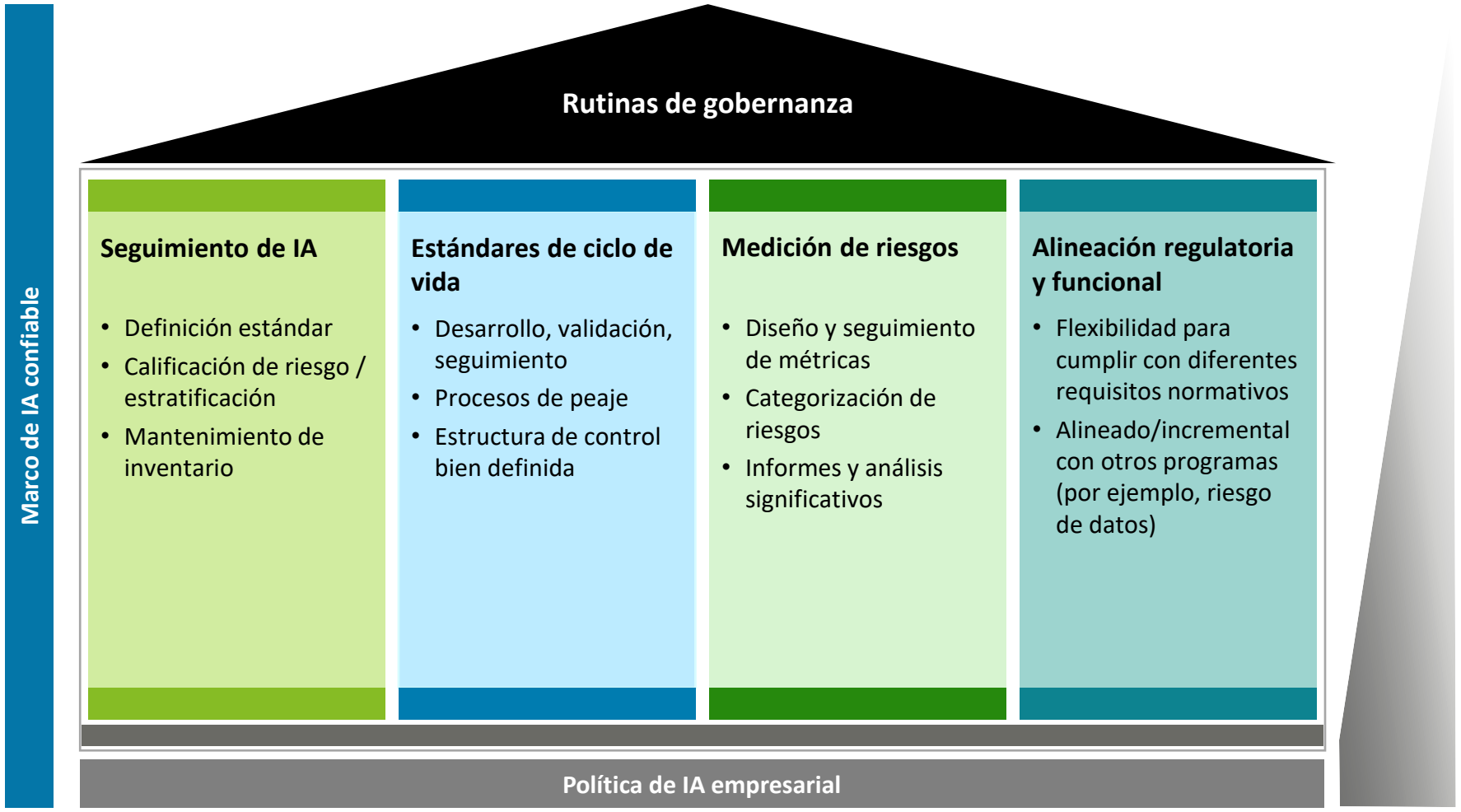
- Solidez conceptual
- Insumos y supuestos
- Implementación
- Análisis de resultados
- Entorno de control
- Interconexión
- Prueba de impugnación efectiva

Auditoría Interna/Cumplimiento
(3ª línea de defensa)

- Monitoreo continuo
- Confirmar que se siguen las políticas
- Confirmar pruebas
- Integridad del inventario de casos de uso de IA
- Desafío efectivo
- Revisión del cumplimiento general

© 2024 Deloitte & Touche S.A.S., Deloitte Asesores y Consultores S.A.S., D Contadores S.A.S., Deloitte S.A.S. y D Profesionales S.A.S., según el servicio que presta cada una.

La política de IA empresarial debe servir de base para un marco de gestión de riesgos eficaz, responsable y ética



Política de IA empresarial

- Se alinea con un marco de gestión de riesgos más amplio e incorpora consideraciones específicas de GenAI (es decir, orientación de uso de código abierto, privacidad de datos, gestión de información errónea, gestión de atribuciones, pruebas de sesgo).
- Define **los roles, las responsabilidades** y los requisitos clave del ciclo de vida.
- **Impulsa la coherencia** en toda la empresa en las actividades de gestión de riesgos de IA.

© 2024 Deloitte & Touche S.A.S., Deloitte Asesores y Consultores S.A.S., D Contadores S.A.S., Deloitte S.A.S. y D Profesionales S.A.S., según el servicio que presta cada una.

Aumentar la preparación de los Consejos de Administración para abordar la IA generativa

Cinco acciones que los Consejos de Administración deben tener en cuenta para permitir su papel en la gobernanza de la IA generativa

01

Desarrollar la alfabetización en IA del Consejo

Ser un defensor del valor de la IA generativa y una guía para los riesgos relacionados exige una alfabetización profunda en IA debido a los nuevos riesgos.

Los miembros del Consejo pueden **mejorar sus conocimientos a través de métodos tradicionales** y experiencia práctica con herramientas de IA generativa.

02

Promover la fluidez de la IA en la alta dirección

A medida que crece la presencia de la IA generativa, los líderes necesitan conocimientos de tecnología para dar forma a los programas de manera responsable y tomar decisiones informadas sobre ética, seguridad y responsabilidad.

Como administradores de la empresa, los miembros del Consejo pueden **fomentar la fluidez de la IA generativa** en la alta dirección para abordar diversas oportunidades y riesgos.

03

Considere cómo llega la experiencia en IA al Consejo

Dado que la IA es un campo técnico y complejo que plantea su propia colección de obstáculos y riesgos, es posible que los Consejos de Administración deban considerar cómo mantenerse informados sobre las últimas tendencias.

Los Consejos de Administración pueden **mejorar y ampliar su experiencia en la materia** a través de la educación, los consejos, asesores o la contratación de profesionales con habilidades de IA y experiencia empresarial.

04

Preparar al Consejo para el futuro

Dado que las capacidades, las regulaciones y la trayectoria de la IA generativa están cambiando, es posible que los consejos deban garantizar un monitoreo continuo de los desarrollos relacionados.

Los Consejos de Administración pueden **establecer comités específicos para supervisar las actividades empresariales vitales (y los desarrollos del ecosistema)** o pueden ampliar los mandatos existentes para incluir componentes de IA generativa.

05

Gobernar la organización a medida que GenAI madura

A medida que la empresa explora cómo GenAI puede ser un potenciador de la productividad y un impulsor de la innovación, el Consejo desempeña un papel vital en la orientación de una implementación ética y confiable.

Los Consejos de Administración pueden **aprovechar los marcos para evaluar el riesgo y la confianza, prepararse para gobernar una fuerza de trabajo digital** y guiar a la organización hacia los usos más valiosos de GenAI

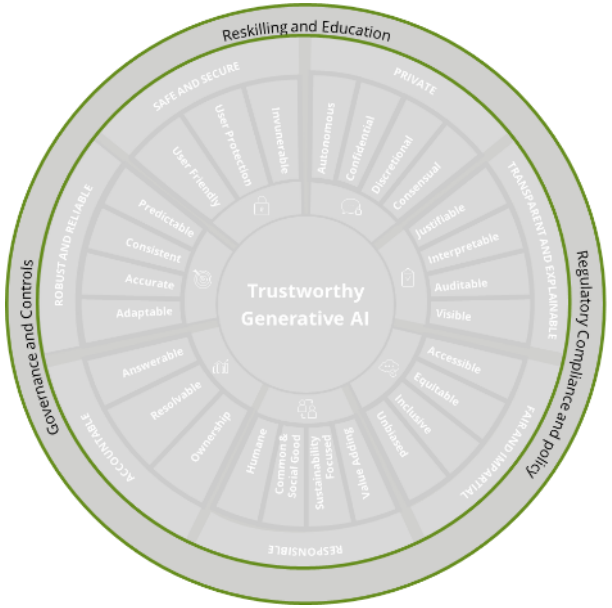
© 2024 Deloitte & Touche S.A.S., Deloitte Asesores y Consultores S.A.S., D Contadores S.A.S., Deloitte S.A.S. y D Profesionales S.A.S., según el servicio que presta cada una.

El marco de IA confiable de Deloitte

Visión general

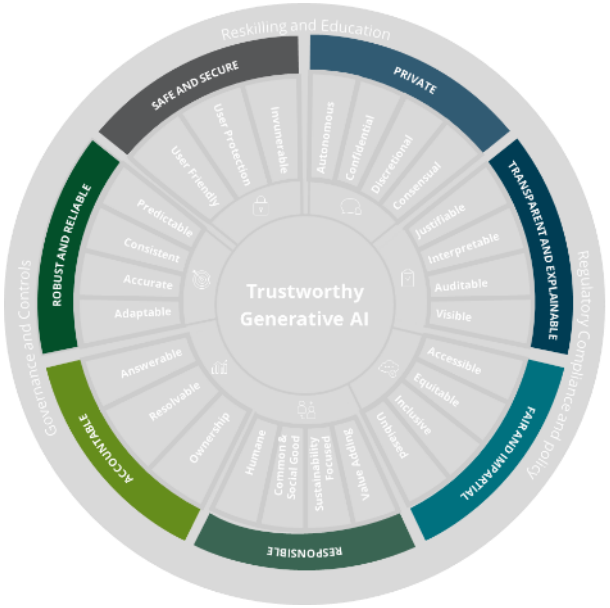
El marco de IA confiable de Deloitte está diseñado para ayudar a desarrollar salvaguardas éticas; hay tres capas en el marco de IA confiable

CAPA EXTERIOR



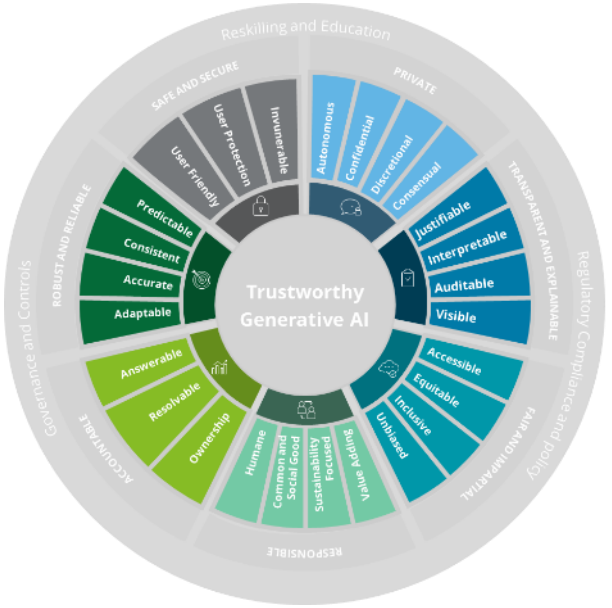
Nombra tres elementos fundamentales que deben estar presentes en una organización para preparar el escenario para TAI.

CAPA INTERMEDIA



Se compone de siete dimensiones.

CAPA MÁS INTERNA



Se compone de subdimensiones que encajan en una de las dimensiones centrales.

© 2024 Deloitte & Touche S.A.S., Deloitte Asesores y Consultores S.A.S., D Contadores S.A.S., Deloitte S.A.S. y D Profesionales S.A.S., según el servicio que presta cada una.

La capa intermedia del marco de IA confiable de Deloitte tiene siete dimensiones clave para construir una IA confiable y ética

Seguro y protegido

Los sistemas de IA pueden protegerse de riesgos (incluidos los cibernéticos) que pueden causar daños físicos y/o digitales.

Robusto / fiable

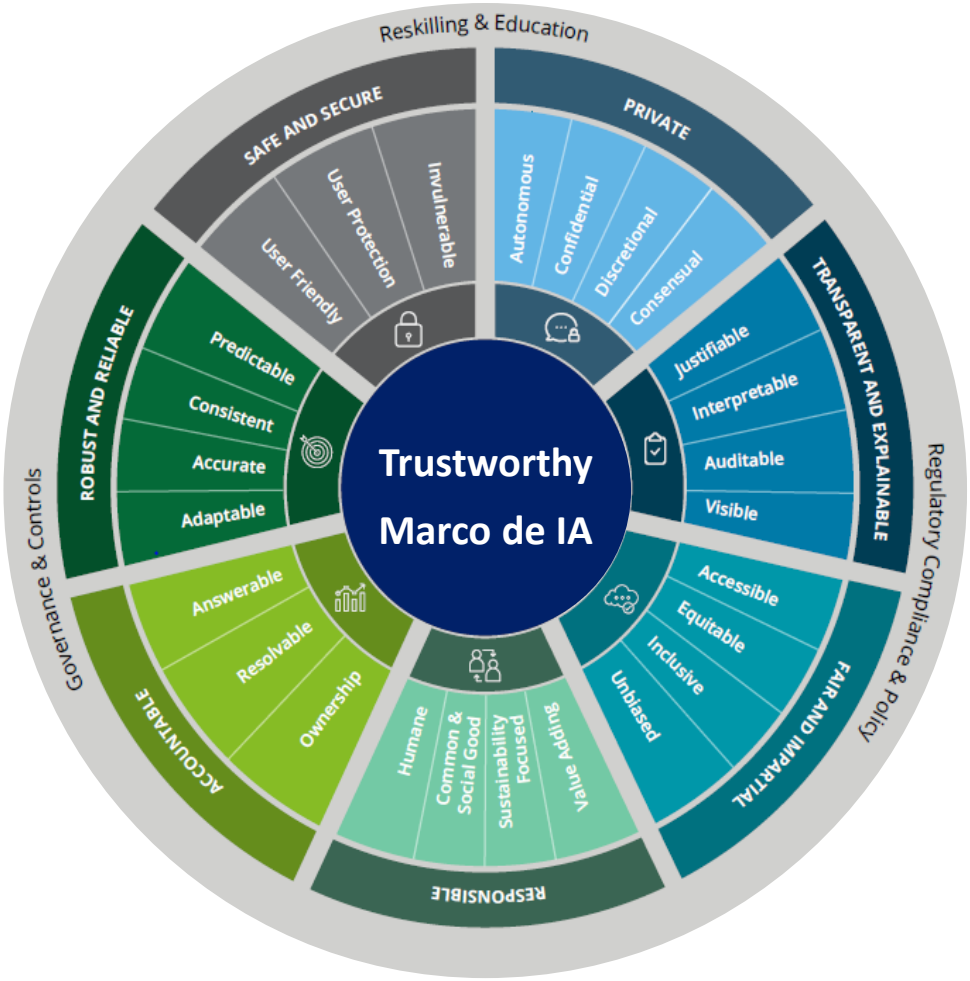
Pueden aprender de los humanos y de otros sistemas, cuando sea aceptable, y producir resultados coherentes y fiables.

Accountable

Existen políticas para determinar quién es responsable de las decisiones tomadas o derivadas con el uso de la tecnología.

Responsable

La tecnología se crea y opera de manera socialmente responsable.



Privado

La privacidad y la confidencialidad se respetan de acuerdo con las obligaciones contractuales y reglamentarias, y los datos no se utilizan más allá de su propósito previsto y declarado.

Transparente / explicable

Los participantes pueden comprender cómo se utilizan sus datos y cómo los sistemas de IA toman decisiones. Los algoritmos, los atributos y las correlaciones están abiertos a la inspección.

Justo / imparcial

Las aplicaciones de IA incluyen controles internos y externos para ayudar a garantizar una aplicación equitativa entre los participantes.

© 2024 Deloitte & Touche S.A.S., Deloitte Asesores y Consultores S.A.S., D Contadores S.A.S., Deloitte S.A.S. y D Profesionales S.A.S., según el servicio que presta cada una.

La tercera y más interna capa del marco está compuesta por las subdimensiones que encajan en las siete dimensiones (1/2)

Privado	
Autónomo	La tecnología respeta y apoya la autonomía humana y la toma de decisiones y permite la elección, la libertad de control y/o influencia.
Confidencial	Se puede confiar a la tecnología la protección datos, personal, del cliente y otra información confidencial. El uso de los datos está alineado con las obligaciones contractuales y es coherente con el propósito original y los permisos de uso.
Discrecional	La tecnología utiliza y divulga los datos del usuario solo cuando es necesario y apropiado y los limpia de información identificable.
Consensual	La tecnología proporciona opciones de inclusión y exclusión voluntaria y cuenta con controles, por lo que no utiliza, comparte ni almacena información del usuario sin su consentimiento.

Justo e imparcial	
Accesible	La tecnología es adecuadamente compatible con la de asistencia, asequible y disponible de manera equitativa.
Equitativo	Los resultados y recomendaciones de la tecnología promueven la equidad entre todas las identidades sociales (por ejemplo, razas, géneros, etc.) y no tienen como objetivo imponer una carga desproporcionada o proporcionar más beneficios para un grupo que otro.
Inclusivo	La tecnología es integral y representativa de todas las identidades sociales, fomentando la prosperidad inclusiva.
Imparcial	La tecnología pretende eliminar y/o reducir los sesgos injustos teniendo en cuenta la igualdad social, la equidad matemática de los datos y el proceso de toma de decisiones como si las personas recibiera un trato justo.

Transparente y explicable	
Justificable	Los resultados y las decisiones tomadas con la tecnología son defendibles, y sus procesos y decisiones siguen un razonamiento lógico.
Interpretable	Los usuarios pueden entender fácilmente lo que está haciendo la tecnología y cómo funciona.
Auditables	Los resultados y las decisiones tomadas con la tecnología se pueden seguir hacia atrás hasta su origen o hacia adelante y registrarse/documentarse.
Visible	El propósito, los casos de uso, la lógica, los riesgos y los beneficios de la tecnología se comunican adecuadamente a los usuarios y son fácilmente accesibles para ellos. Somos transparentes con respecto a los datos utilizados por la tecnología y cómo se utilizan. Y, cuando sea relevante, que sea claro para los usuarios que están interactuando con la tecnología en lugar de con un ser humano.

Responsable	
Humano	La tecnología está arraigada en los estándares morales y éticos de la sociedad y en los **principios de ética**.
Bien común/social	Es socialmente responsable y minimiza el impacto dañino para las comunidades sociales más amplias en la mayor medida posible.
Centrados en la sostenibilidad	La tecnología apoya la sostenibilidad económica, ambiental y social a lo largo de todo su ciclo de vida.
Valor agregado	Se desarrolla teniendo en cuenta la creación de valor. Debido a los riesgos que genera la tecnología, es importante revisar los beneficios de la misma y su(s) caso(s) de uso para determinar si es apropiado implementarla.

© 2024 Deloitte & Touche S.A.S., Deloitte Asesores y Consultores S.A.S., D Contadores S.A.S., Deloitte S.A.S. y D Profesionales S.A.S., según el servicio que presta cada una.

La tercera y más interna capa del marco está compuesta por las subdimensiones que encajan en las siete dimensiones (2/2)

Accountable	
Responsable	La tecnología cuenta con un equipo de soporte dedicado que reaccionará a las preocupaciones planteadas por las partes interesadas, incluidos los usuarios.
Resoluble	Las preocupaciones imprevistas y los errores de la tecnología se pueden resolver de manera oportuna.
Propiedad	La responsabilidad entre desarrolladores, usuarios y otras partes interesadas se establece y se describe claramente para la tecnología y sus resultados/decisiones. Contamos con una estructura y políticas que ayudan a determinar claramente quién es responsable si algo sale mal, o si los resultados no se utilizan según lo previsto y entendemos los mecanismos de reparación.

Seguro y protegido	
Invulnerable	La tecnología cuenta con controles y equilibrios para reducir el riesgo y prevenir ataques internos/externos, conservando su seguridad, protección y funcionalidad. No puede ser reproducido ni sometido a ingeniería inversa. Valoramos la seguridad técnica y la resiliencia para reducir los daños físicos y digitales.
Protección del usuario	La tecnología y sus resultados no crean daños físicos, mentales, emocionales, ambientales y/o tecnológicos, individuales y/o colectivos, independientemente de la intención. Implementamos las medidas de seguridad pertinentes para regir el uso de una tecnología para proteger a las personas y a la sociedad.
Fácil de usar	Es intuitiva y no engaña a los usuarios.

Robusto y fiable	
Predecible	La tecnología, sus algoritmos y sus resultados son los esperados, basados en los patrones de los datos.
Consistente	Puede producir resultados consistentes si se vuelven a ejecutar en las mismas condiciones y con los mismos datos.
Preciso	Se puede confiar en que los resultados de la tecnología sean precisos y precisos.
Adaptable	La tecnología es lo suficientemente ágil y resistente como para adaptarse a las condiciones cambiantes.

© 2024 Deloitte & Touche S.A.S., Deloitte Asesores y Consultores S.A.S., D Contadores S.A.S., Deloitte S.A.S. y D Profesionales S.A.S., según el servicio que presta cada una.

¿Qué podemos hacer los AI?

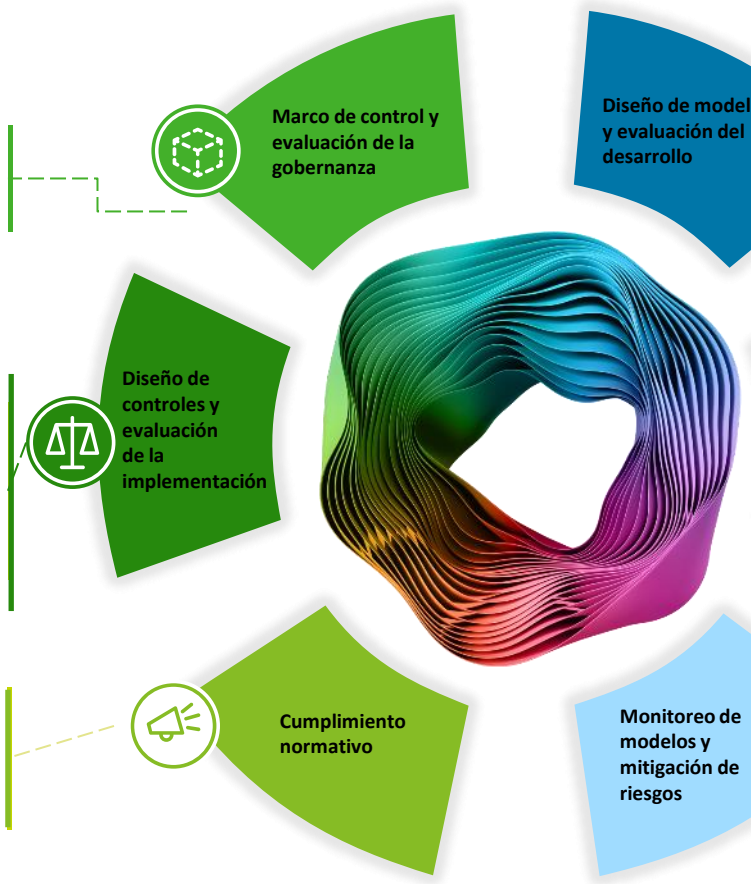
Una vista cercana para los auditores internos

Revisión del marco de control: componentes cualitativos de algoritmos e IA

Marco de control y evaluación de la gobernanza
Evaluación de las estructuras internas de gobernanza y control en torno a los riesgos de la IA.

Diseño de controles y evaluación de la implementación
Preparación para auditorías y evaluación sobre el diseño y la implementación de controles y gobernanza de algoritmos/sistemas de IA.

Cumplimiento normativo
Análisis de brechas de los requisitos de cumplimiento con respecto a las regulaciones más recientes/futuras.



Revisión de algoritmos e IA - Componentes cuantitativos de algoritmos e IA

Diseño de modelos y evaluación del desarrollo
Evaluación de la preparación de datos, diseño y desarrollo de modelos, pruebas y procedimientos de implementación.

Revisión operativa del modelo
Preparación para auditorías y revisión de algoritmos/sistemas y resultados de IA.

Monitoreo de modelos y mitigación de riesgos
Evaluación de barreras de seguridad y procesos de monitoreo para la detección oportuna de resultados no deseados o incorrectos.

© 2024 Deloitte & Touche S.A.S., Deloitte Asesores y Consultores S.A.S., D Contadores S.A.S., Deloitte S.A.S. y D Profesionales S.A.S., según el servicio que presta cada una.

Conectemos

Gustavo Mejía
Socio de Estrategia, Riesgos y Transacciones
Marketplace Región Andina
Deloitte Spanish Latin America
gmejia@deloitte.com

Descubra cómo podemos ayudarlo
www.deloitte.com/co

© 2024 Deloitte & Touche S.A.S., Deloitte Asesores y Consultores S.A.S., D Contadores S.A.S., Deloitte S.A.S. y D Profesionales S.A.S., según el servicio que presta cada una.

Deloitte.

Deloitte se refiere a una o más entidades de Deloitte Touche Tohmatsu Limited (“DTTL”), su red global de firmas miembro y sus sociedades afiliadas a una firma miembro (en adelante “Entidades Relacionadas”) (colectivamente, la “organización Deloitte”). DTTL (también denominada como “Deloitte Global”) así como cada una de sus firmas miembro y sus Entidades Relacionadas son entidades legalmente separadas e independientes, que no pueden obligarse ni vincularse entre sí con respecto a terceros. DTTL y cada firma miembro de DTTL y su Entidad Relacionada es responsable únicamente de sus propios actos y omisiones, y no de los de las demás. DTTL no provee servicios a clientes. Consulte www.deloitte.com/co/conozcanos para obtener más información.

Deloitte presta servicios profesionales líderes de auditoría y assurance, impuestos y servicios legales, consultoría, asesoría financiera y asesoría en riesgos, a casi el 90% de las empresas Fortune Global 500® y a miles de empresas privadas. Nuestros profesionales brindan resultados medibles y duraderos que ayudan a reforzar la confianza pública en los mercados de capital, permiten a los clientes transformarse y prosperar, y liderar el camino hacia una economía más fuerte, una sociedad más equitativa y un mundo sostenible. Sobre la base de su historia de más de 175 años, Deloitte abarca más de 150 países y territorios. Conozca cómo los aproximadamente 457,000 profesionales de Deloitte en todo el mundo crean un impacto significativo en www.deloitte.com.

Tal y como se usa en este documento, Deloitte & Touche S.A.S., Deloitte Asesores y Consultores S.A.S., D Contadores S.A.S., Deloitte S.A.S. y D Profesionales S.A.S., tiene el derecho legal exclusivo de involucrarse en, y limita sus negocios a, la prestación de servicios de auditoría, consultoría, consultoría fiscal, asesoría legal, en riesgos y financiera respectivamente y otros servicios profesionales bajo el nombre de “Deloitte”. Deloitte & Touche S.A.S., tiene el derecho legal exclusivo de involucrarse en, y limita sus negocios a, la prestación de servicios de auditoría y otros servicios profesionales bajo el nombre de “Deloitte”. Deloitte Asesores y Consultores S.A.S., tiene el derecho legal exclusivo de involucrarse en, y limita sus negocios a, la prestación de servicios de consultoría, asesoría en riesgos y financiera, legal y otros servicios profesionales bajo el nombre de “Deloitte”. D Contadores S.A.S., tiene el derecho legal exclusivo de involucrarse en, y limita sus negocios a, la prestación de servicios contables y otros servicios profesionales bajo el nombre de “Deloitte”. Deloitte S.A.S., tiene el derecho legal exclusivo de involucrarse en, y limita sus negocios a, la prestación de servicios de aseguramiento y otros servicios profesionales bajo el nombre de “Deloitte”. Y D Profesionales S.A.S., tiene el derecho legal exclusivo de involucrarse en, y limita sus negocios a, la prestación de servicios a las otras sociedades Deloitte en Colombia.

Esta comunicación contiene solamente información general y ni Touche Tohmatsu Limited (“DTTL”), su red global de firmas miembro o sus Entidades Relacionadas (colectivamente, la “organización Deloitte”) está, por medio de esta comunicación, prestando asesoramiento profesional o servicio alguno. Antes de tomar cualquier decisión o tomar cualquier medida que pueda afectar sus finanzas o su negocio, debe consultar a un asesor profesional calificado.

No se proporciona ninguna representación, garantía o promesa (ni explícita ni implícita) sobre la veracidad ni la integridad de la información en esta comunicación, y ni DTTL, ni sus firmas miembro, Entidades Relacionadas, empleados o agentes será responsable de cualquier pérdida o daño alguno que surja directa o indirectamente en relación con cualquier persona que confíe en esta comunicación. DTTL y cada una de sus firmas miembro y sus Entidades Relacionadas, son entidades legalmente separadas e independientes.

© 2024 Deloitte & Touche S.A.S., Deloitte Asesores y Consultores S.A.S., D Contadores S.A.S., Deloitte S.A.S. y D Profesionales S.A.S., según el servicio que presta cada una.

Retos éticos de la IA generativa

AteneA
Centro de Pensamiento de Auditorio

Registro de asistencia y evaluación de conferencias

AteneA
Centro de Pensamiento de Auditoría

VI Encuentro Latinoamericano de Auditoría

Conocimiento y aplicación en la era digital

EXPERIENCIAS EN TRANSFORMACIÓN DIGITAL DE LA AUDITORÍA

NUESTRA ORGANIZACIÓN

10
países

80
compañías

30 mil
colaboradores

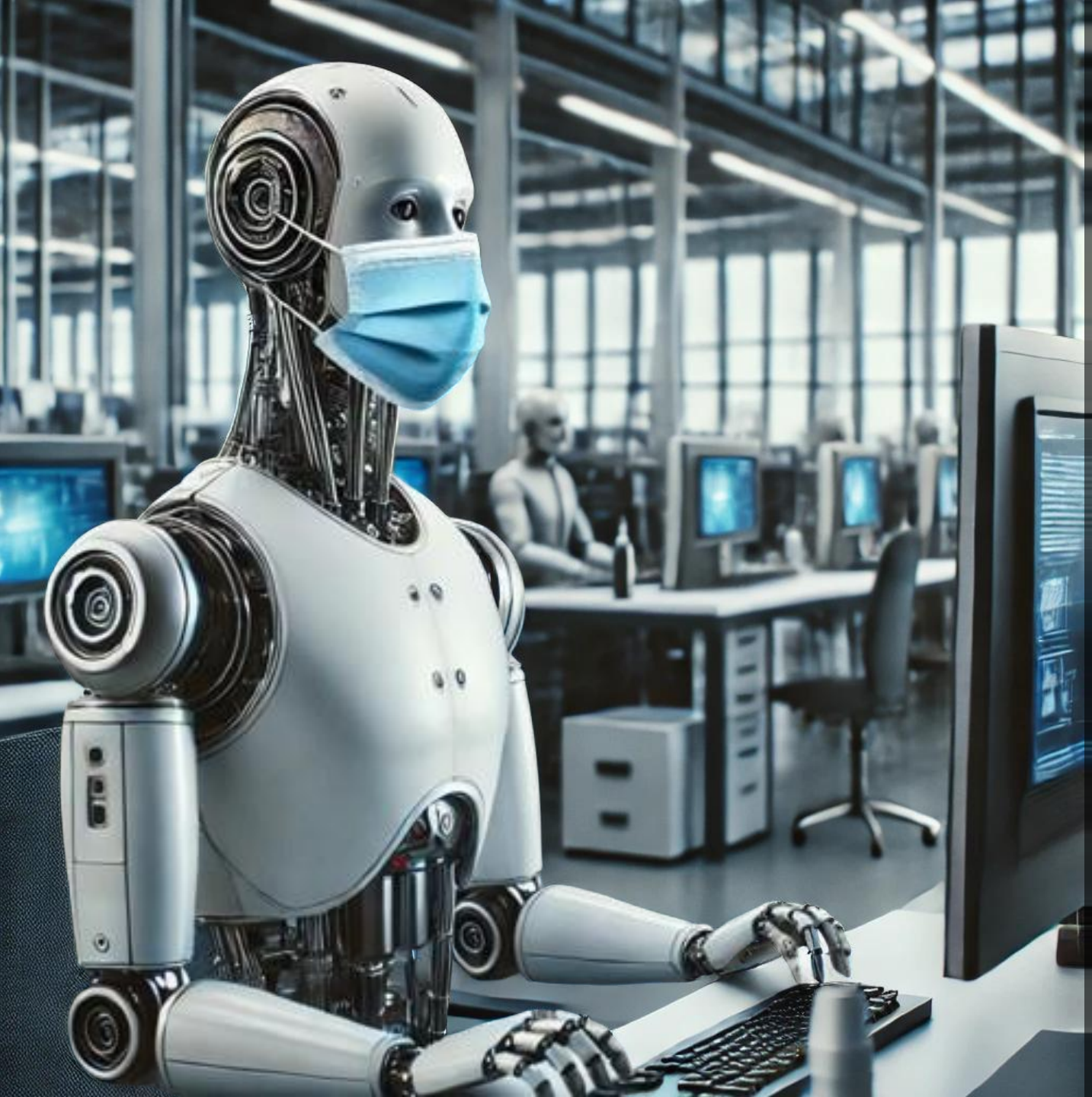
75 millones
de clientes

27 Comités de Auditoría
140 auditores internos
880 trabajos de auditoría anual

HOUSTON... TENEMOS UN PROBLEMA

AteneA
Centro de Pensamiento de Auditoría

HOUSTON... TENEMOS UNA OPORTUNIDAD



AteneA
Centro de Pensamiento de Auditoría

TRANSFORMACIÓN DIGITAL DE LOS NEGOCIOS

+

PANDEMIA COVID - 19

=

AteneA
Centro de Pensamiento de Auditoría

“ Sueña audazmente, ten el coraje para fracasar y actúa con urgencia. ”
Phil Knight – Fundador de Nike

ENFRENTANDO LOS PROBLEMAS

AteneA
Centro de Pensamiento de Auditoría

“ Sueña audazmente, ten el coraje para fracasar y actúa con urgencia. ”

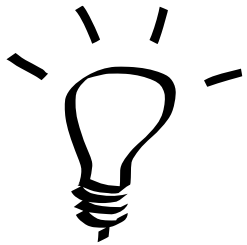
Phil Knight – Fundador de Nike

ENFRENTANDO LOS DESAFÍOS

DIVERSIDAD TI

AteneA
Centro de Pensamiento de Auditoría

MINDSET



RESTRICCIONES

ES CUESTIÓN...

Un entorno digital básico

Tableros BI conectividad

Pruebas auditoría continua

Implementación IA

2024

Automatización

+200

Nuevas tecnologías

2018

Nuevas tecnologías

Automatización

= 0

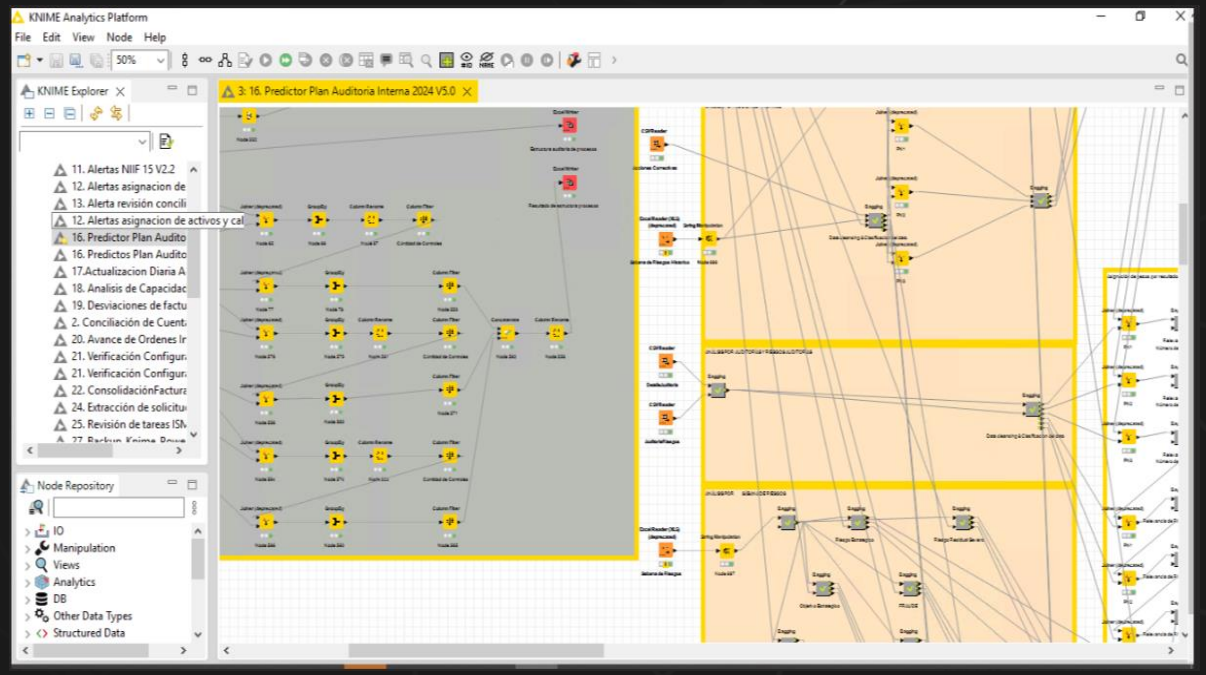
...DE EMPEZAR

Uso Interno


LIVE BEAUTIFUL

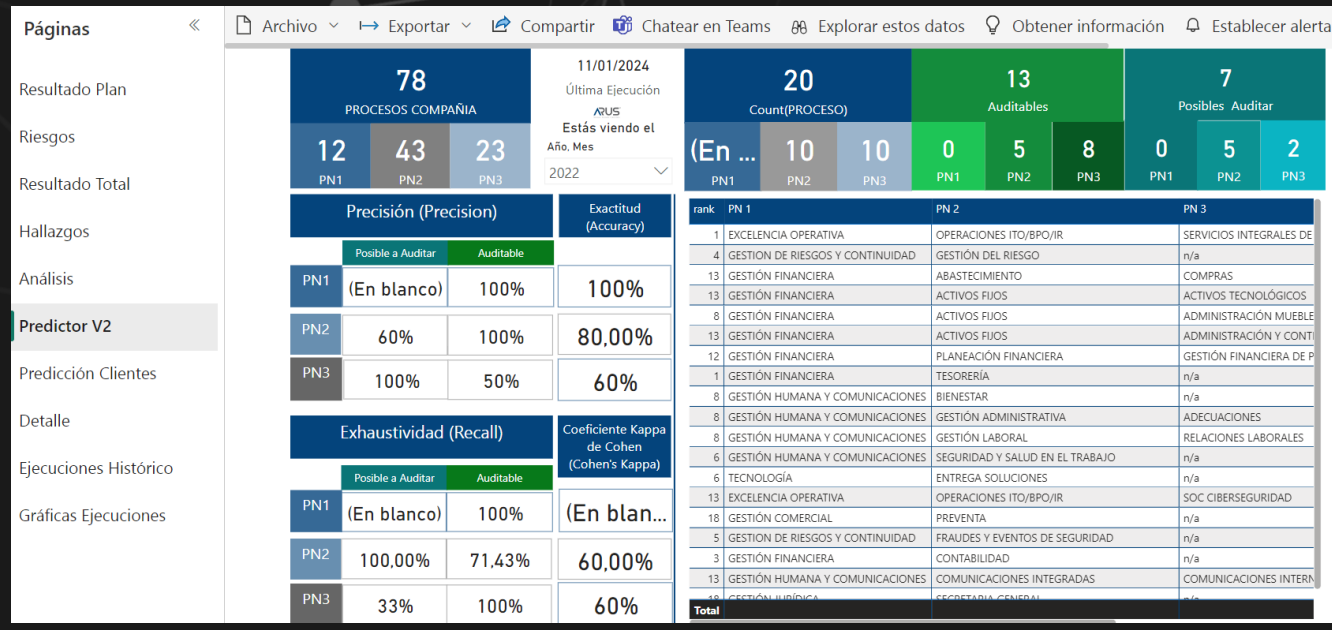
01. PREDICTOR PLAN DE AUDITORÍA

01. PREDICTOR PLAN DE AUDITORÍA



En un mundo donde el cambio es la constante, el Plan de Auditoría Interna debe **ser dinámico** y predecir con precisión las unidades auditables.

Nos estamos **anticipando** a la gestión de riesgos, alineados con los objetivos estratégicos de la Compañía y el entorno cambiante de los negocios.



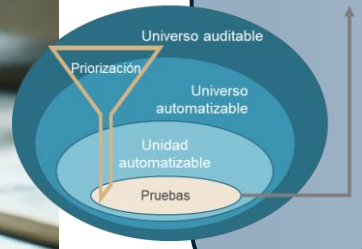
02. AUTOMATIZACION DE PRUEBAS - RPA

¿COMO LO HACEMOS?

Identificación
Evaluación del valor y factibilidad

Diseño
Caso de uso, scripts, atributos

Ejecución
Construcción propia, terceros, herramientas



MODELO DE PRIORIZACIÓN
INDICADORES DE MADUREZ
INDICADORES DE COBERTURA

Mantención
Proceso continuo de revisión

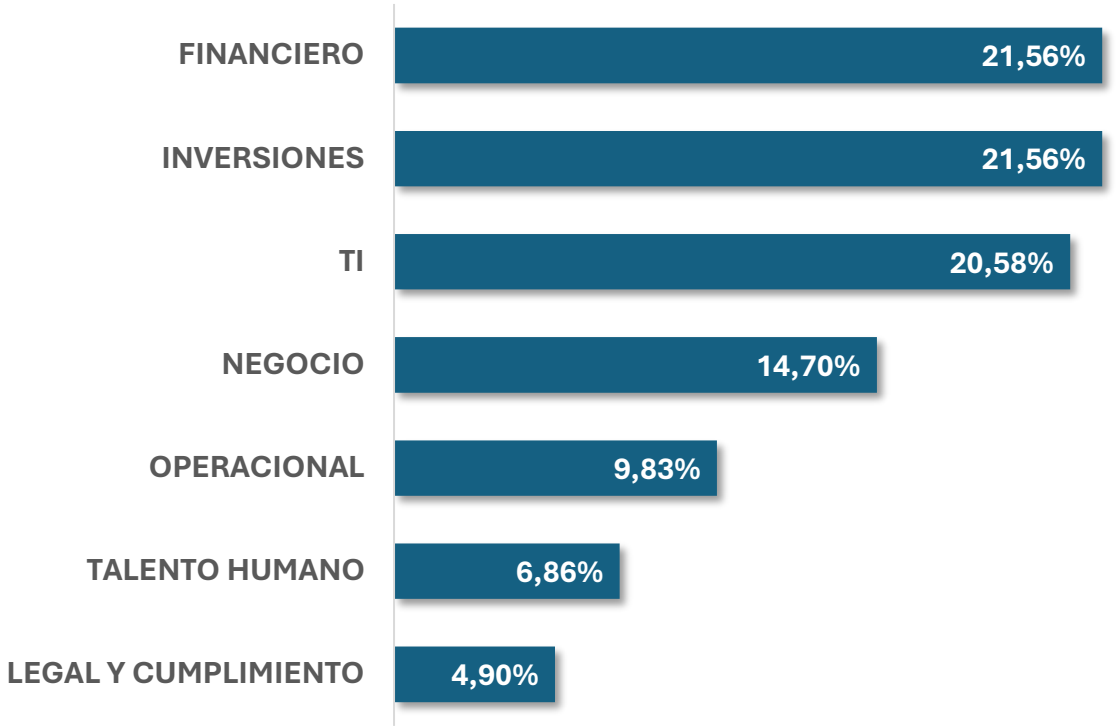
Comunicación
Tableros de control, instancias de gobierno

Validación
Monitoreo en línea, resultados/alertas

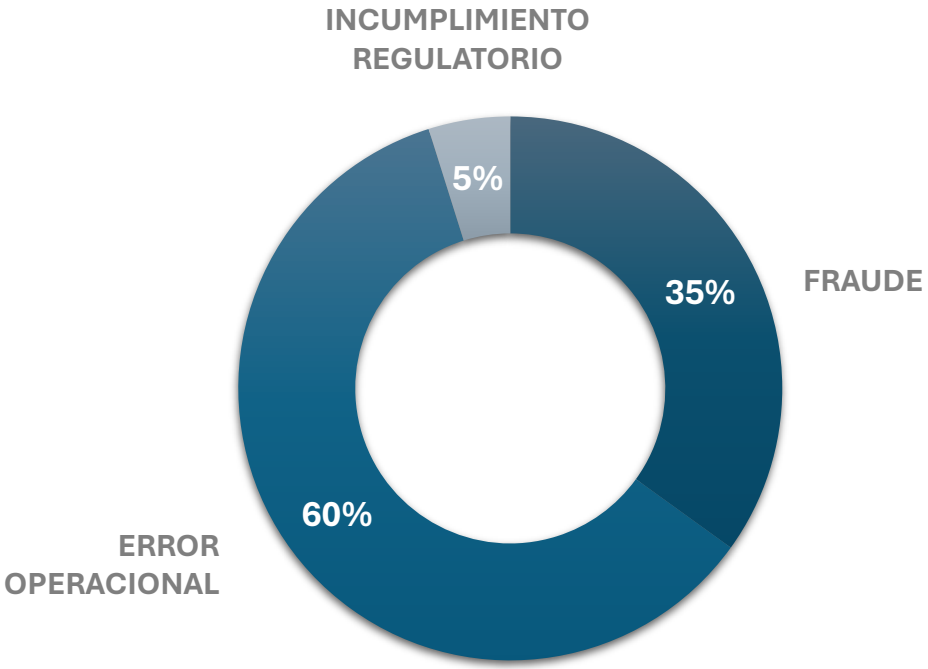
Uso Interno

02. AUTOMATIZACION DE PRUEBAS - RPA

ORIGEN



RIESGOS



Uso Interno

03. RADAR DEL SCI

Recolección de información de Opinión SCI de negocios y localidades

+800 procesos

+300 aud./año

10 países/negocs.

Análisis y consolidación de información para la Opinión SCI

Construcción y Presentación De Opinión SCI Regional
Macrotemas y
Focos de atención

Core Negocio
Operaciones | Comercial | inversiones

Tecnología
Resiliencia | Cyber & Seg.info. | Gob.TI

Habilitadores
Finanzas | TH | Riesgos | Gob.yCumpl.

- Adecuado
- Moderado +
- Moderado
- Moderado -
- Inadecuado

Uso Interno

03. RADAR DEL SCI

Capturador de datos de los negocios y localidades

+800 procesos

+300 aud./año

10 países/negocs.

Análisis y consolidación de información para la Opinión SCI

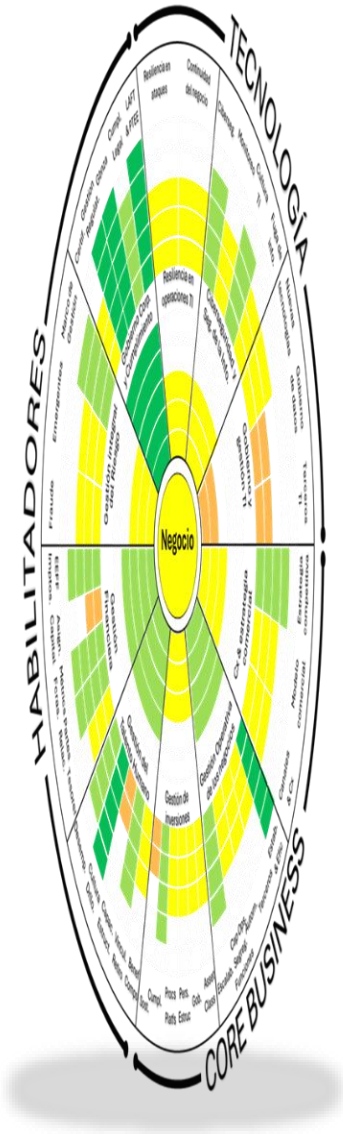
Visualizador Opinión SCI Regional
Macrotemas y Focos de atención

Core Negocio
Operaciones | Comercial | inversiones

Tecnología
Resiliencia | Cyber & Seg.info. | Gob.TI

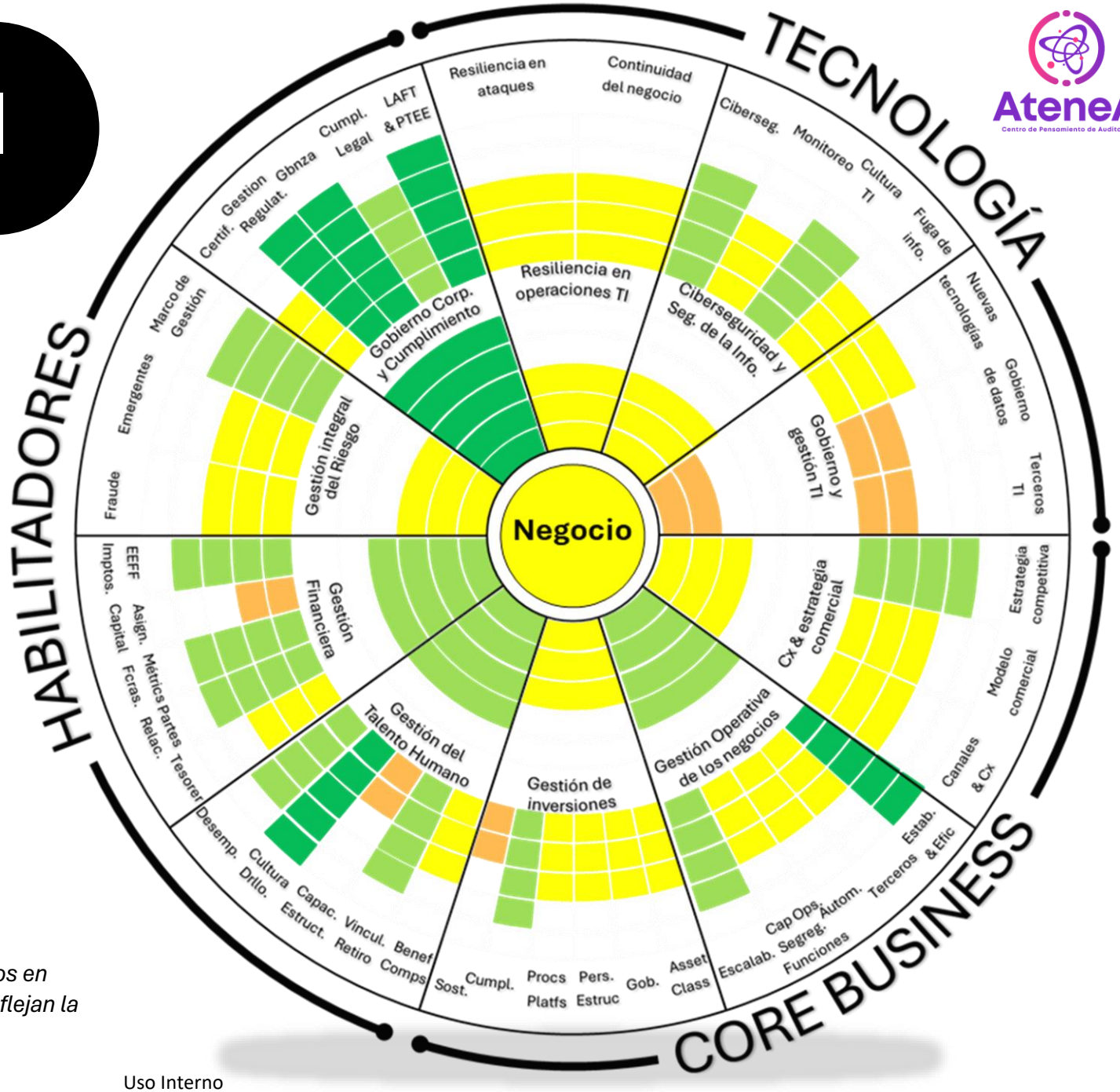
Habilitadores
Finanzas | TH | Riesgos | Gob.yCumpl.

- Adecuado
- Moderado +
- Moderado
- Moderado -
- Inadecuado



03. RADAR DEL SCI

Mayor foco en las conversaciones con los stakeholders



***Disclaimer**: Las calificaciones de opinión del SCI desplegados en este radar **fueron simuladas para esta presentación** y no reflejan la realidad de ninguna compañía.*

REFLEXIONES FINALES

¿Preguntas?

Ana Mora
Gerente de Auditoría
ARUS
Ana Maria Mora Vasquez
ana.mora@arus.com.co

Maurizio Olivares
VP de Auditoría
SURA Asset Management
maurizio.olivares@sura.cl

Experiencias en transformación digital de la auditoría casos de éxito de la aplicación de tecnologías emergentes en Grupo Empresarial SURA

AteneA
Centro de Pensamiento de Auditoria

Registro de asistencia y evaluación de conferencias

AteneA
Centro de Pensamiento de Auditoría

VI Encuentro Latinoamericano de Auditoría

Conocimiento y aplicación en la era digital

Explorando la Deep Web como aliado del aseguramiento

AteneA
Centro de Pensamiento de Auditoria

Registro de asistencia y evaluación de conferencias

La Auditoría Interna en transformación Visión 2035

AteneA
Centro de Pensamiento de Auditoria

Registro de asistencia y evaluación de conferencias