



XXIII Congreso Latinoamericano
de Auditoría Interna y Evaluación de Riesgos
Santa Cruz, Bolivia

CLAIN 2019
MAYO
16 Y 17



ASOBAN
ASOCIACIÓN DE BANCOS PRIVADOS DE BOLIVIA



FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

"El enfoque de la auditoría interna ante la revolución digital y las innovaciones disruptivas"

AUDITORIA EN TIEMPOS DIGITALES

Implicaciones de ciber riesgo

Agenda

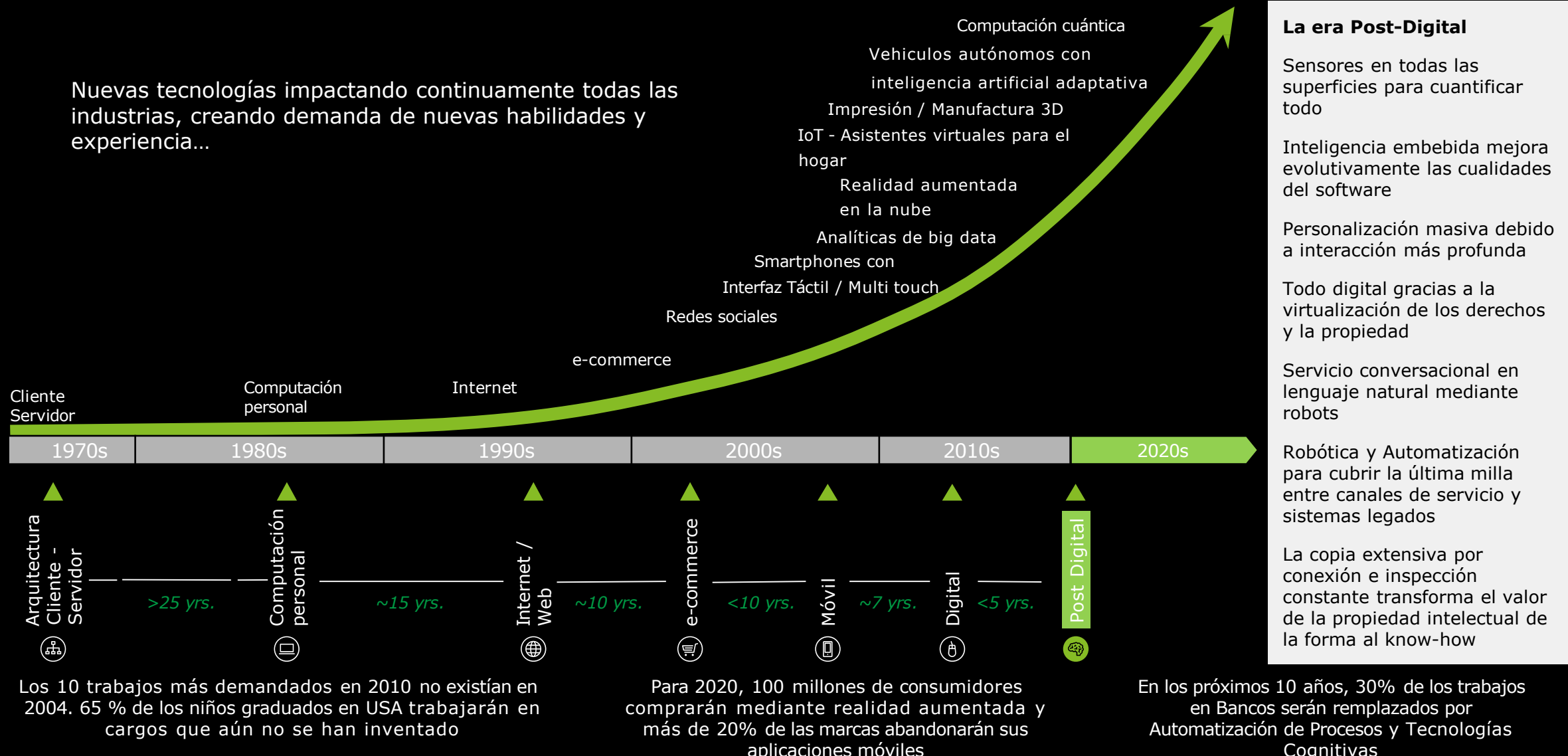
- Tendencias tecnológicas
- Efecto en la auditoría interna

Tendencias tecnológicas

Las fuerzas macro de la tecnología en acción y las tendencias tecnológicas para los negocios

Tendencias tecnológicas

Nuevas tecnologías impactando continuamente todas las industrias, creando demanda de nuevas habilidades y experiencia...



Los 10 trabajos más demandados en 2010 no existían en 2004. 65 % de los niños graduados en USA trabajarán en cargos que aún no se han inventado

Para 2020, 100 millones de consumidores comprarán mediante realidad aumentada y más de 20% de las marcas abandonarán sus aplicaciones móviles

En los próximos 10 años, 30% de los trabajos en Bancos serán remplazados por Automatización de Procesos y Tecnologías Cognitivas

Tendencias tecnológicas



- Centrado en el cliente:**
Pasarse de un enfoque de producto a una verdadera orientación al cliente
- FinTech y big techs:**
Aceptar el ecosistema cambiante
- Recalibración regulatoria:**
Modernizar el cumplimiento normativo.
- Gestión tecnológica:**
Lograr un equilibrio entre la tecnología interna para la diferenciación y la tercerización para la eficiencia.
- Mitigación del riesgo cibernético:**
Considerar la ciberseguridad en cada paso del proceso de transformación
- Reimaginando la fuerza laboral:**
Repensar el talento futuro en línea con la creciente automatización y diversidad

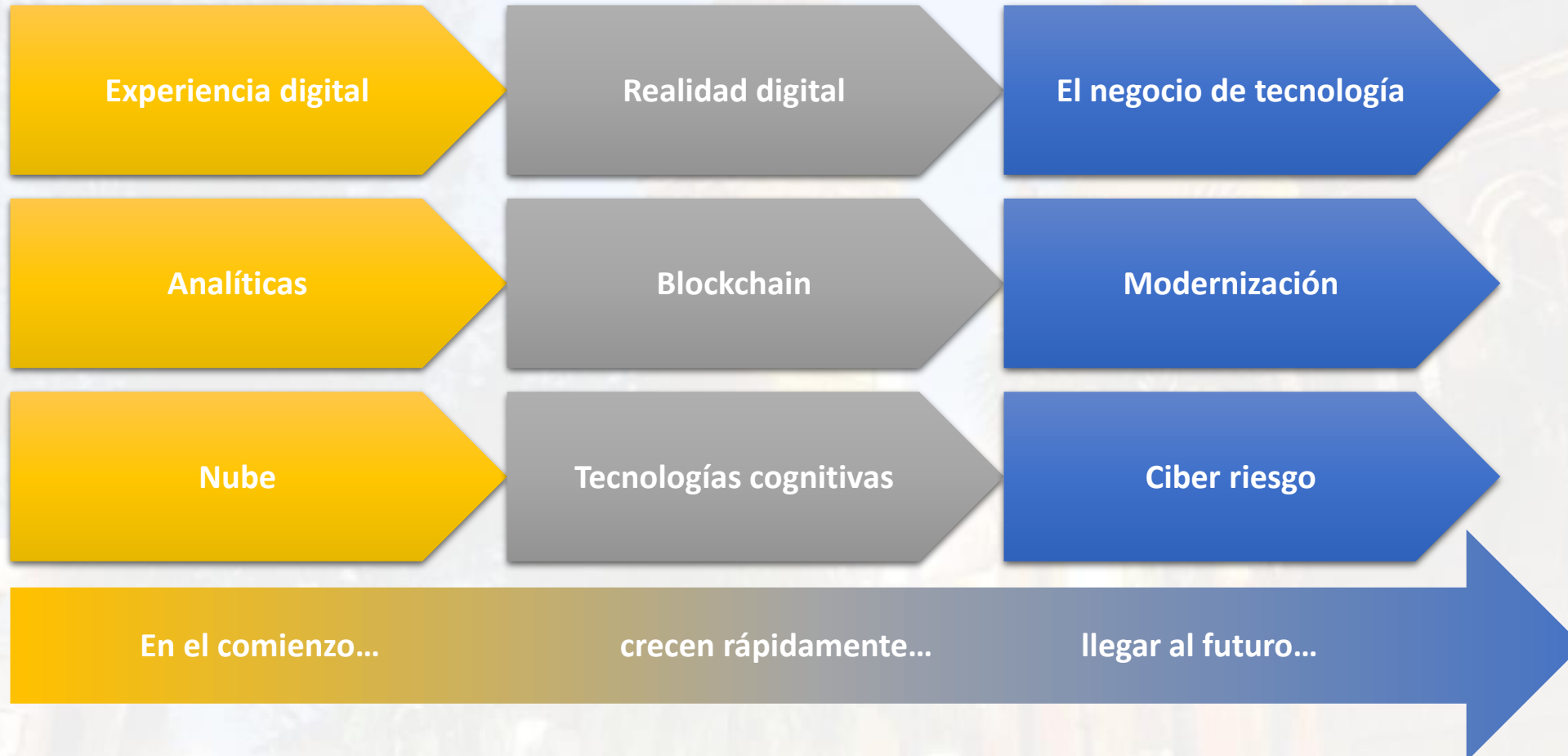
Tendencias tecnológicas

- Las fuerzas macro de la tecnología en acción
- Las tendencias tecnológicas para los negocios
- Organizaciones alimentadas por la inteligencia artificial
- Sin operaciones en un mundo sin servidores
- Conectividad del mañana
- Interfaces inteligentes
- Más allá del Mercadeo: La experiencia reimaginada
- Tendencia de ciber riesgo: DevSecOps



Las fuerzas macro de la tecnología en acción

Pasado, presente y futuro de las tendencias tecnológicas



Las fuerzas macro de la tecnología en acción

Pasado, presente y futuro de las tendencias tecnológicas

Experiencia digital

Hace 10 años eran tendencias y era previsible su potencial disruptivo, hoy día son base fundamental de las iniciativas de negocio de cualquier organización.

Su potencial total aún es desconocido, pero muchas organizaciones ya avanzan en su aplicación.

Analíticas

Sin embargo, a veces son iniciativas aisladas que compiten por los mismos recursos. Su mayor potencial hoy día se alcanza con iniciativas que integren a estas 3 macro fuerzas en el logro de objetivos estratégicos.

Nube

En el comienzo...

crecen rápidamente...

llegar al futuro...

Las fuerzas macro de la tecnología en acción

Pasado, presente y futuro de las tendencias tecnológicas

3 nuevas tendencias que van creciendo en importancia.

- Realidad virtual, realidad aumentada, cambiando la forma de interacción de los humanos con su entorno.
- Blockchain, de la criptomoneda a proveedor de confianza en procesos y ecosistemas.

Realidad digital

Blockchain

Tecnologías cognitivas

- Tecnologías cognitivas: redes neuronales, inteligencia artificial, machine learning, automatización robótica de procesos, procesamiento de lenguaje natural. De aplicación en silos, a ser un habilitador de la estrategia organizacional.

En el comienzo...

crecen rápidamente...

llegar al futuro...

Las fuerzas macro de la tecnología en acción

Pasado, presente y futuro de las tendencias tecnológicas

3 macro fuerzas en formación son esenciales en la búsqueda de la transformación digital:

- Reingeniería de la función de tecnología para entregar ágilmente la promesa de valor de tecnologías emergentes y existentes, generando alto impacto en las organizaciones. IT debe generar disrupción a sí misma.
- Modernizar los sistemas misionales del negocio.
- Elevar la ciber seguridad y su amplio cubrimiento en términos de riesgo, pasando de ser una función de cumplimiento a una función embebida en la estrategia de la organización.

El negocio de tecnología

Modernización

Ciber riesgo

En el comienzo...

crecen rápidamente...

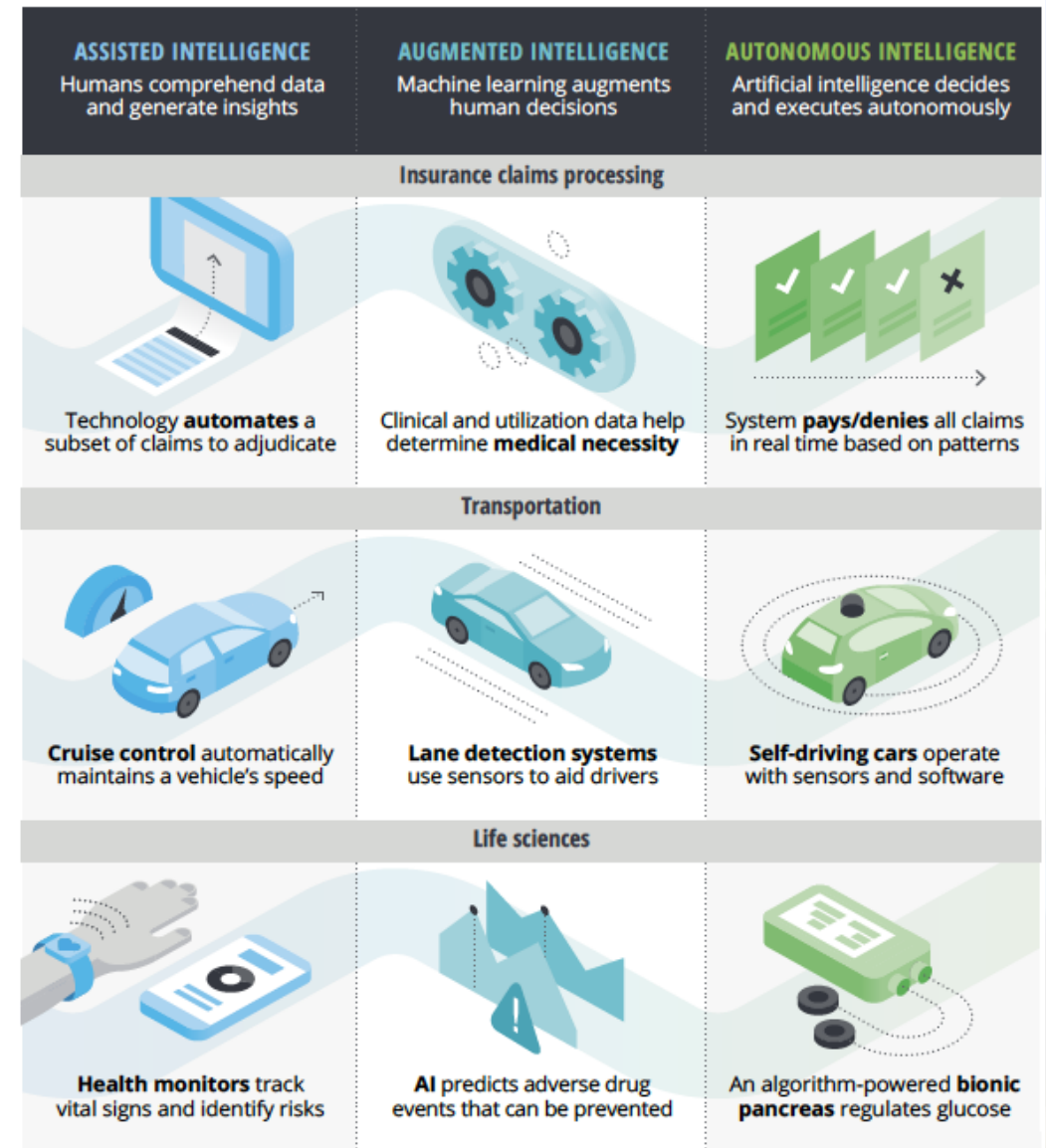
llegar al futuro...

Las tendencias tecnológicas para los negocios

Organizaciones alimentadas por la inteligencia artificial

- **Inteligencia Asistida:** bots, analíticas y ciencia de datos para tomar decisiones de negocio dirigidas por datos.
- **Inteligencia Aumentada:** aprendizaje de máquina como una hiper capa que integre a las soluciones analíticas existentes para aumentar las capacidades analíticas de los humanos.
- **Inteligencia Autónoma:** procesos digitalizados y automatizados al punto que los bots, máquinas y sistemas pueden actuar directamente a partir de la inteligencia que ellos mismos generan.

Bringing the evolution of artificial intelligence to life



Source: Thomas H. Davenport, *The AI Advantage*. Deloitte analysis.

Las tendencias tecnológicas para los negocios

Organizaciones alimentadas por la inteligencia artificial

- Las empresas líderes ya trabajan en inteligencia artificial para generación de ingresos, más que para reducción de costos.
- Iniciativas:
 - Mejor cumplimiento regulatorio
 - Personalización en masa de productos y servicios
 - Activos de TI que actúen sobre ellos mismos a partir de la inteligencia que generan

39%

de quienes respondieron la segunda encuesta anual de Deloitte State of AI identificó los “problemas de datos” entre los primeros tres mayores desafíos que enfrentan con las iniciativas de IA.

- **Implicaciones de ciber riesgo**
 - Atacantes ganando acceso o exfiltrando información mediante el uso de inteligencia artificial
 - Automatización para detectar y luchar frente a ciber amenazas
 - Aprendizaje de máquinas para anticiparse a amenazas emergentes.
 - Inteligencia artificial vs inteligencia artificial
 - Primero, un adecuado modelo de gobierno, roles y responsabilidades frente a la IA

Las tendencias tecnológicas para los negocios

Sin operaciones en un mundo sin servidores

La computación sin servidores es un término paraguas para un espectro de opciones basadas-en-la-nube disponibles para las organizaciones que deseen salir del negocio de la administración de servidores.

- **Serverless:** capacidad de procesamiento y almacenamiento en la nube.
- **NoOps:** las operaciones tradicionales de tecnología se automatizan al máximo
- No hay costos por tiempo ocioso
- Escalabilidad infinita y alta disponibilidad
- **Retos:**
 - Monitoreo y depuración
 - Dependencia del proveedor
 - Migración

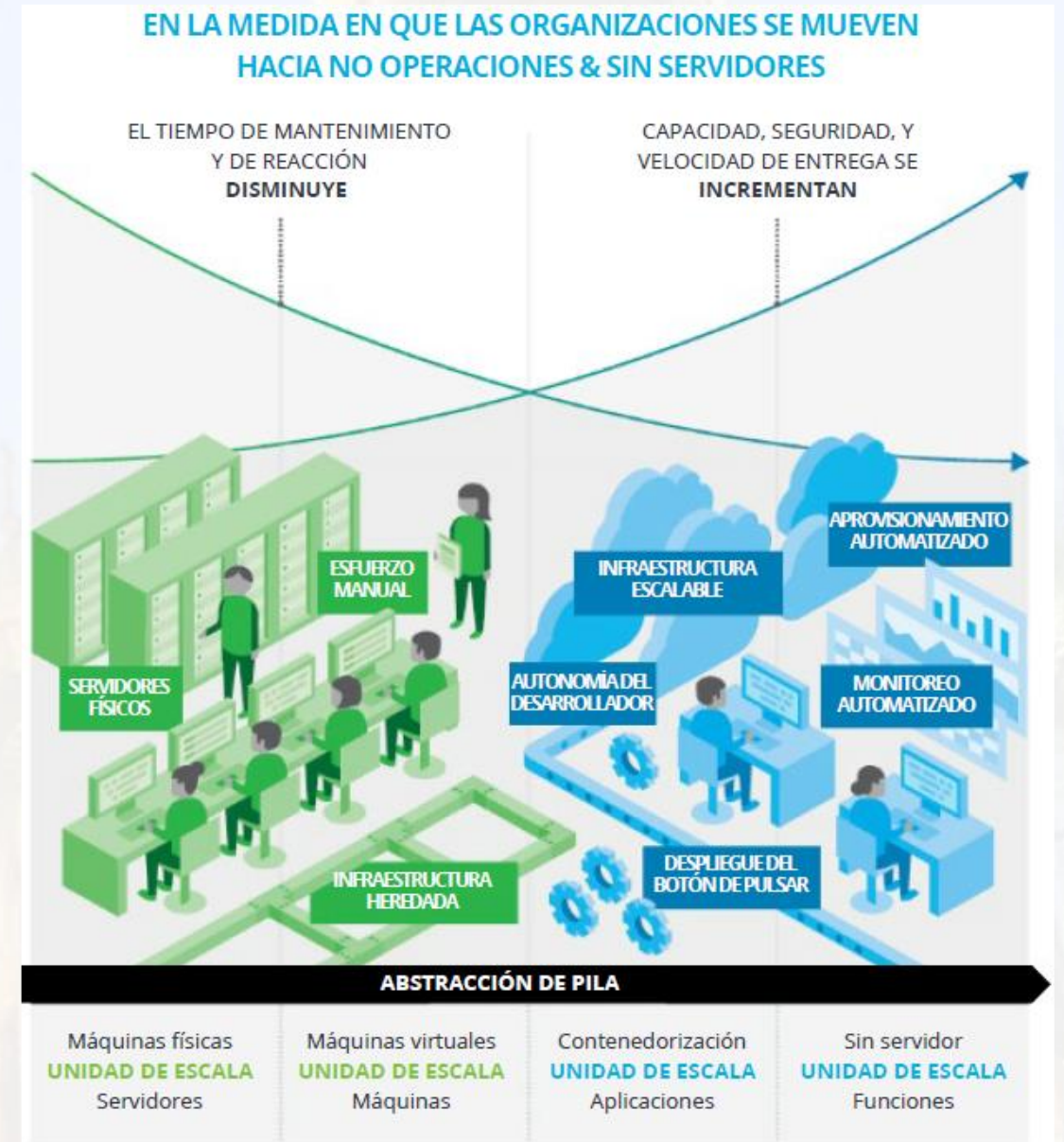
69%
de quienes respondieron la 2018 global CIO survey, de Deloitte, identificó “automatización y transformación de procesos” como el principal centro de atención de sus agendas digitales.

Las tendencias tecnológicas para los negocios

Sin operaciones en un mundo sin servidores

- **Implicaciones de ciber riesgo**
- Oportunidad para incorporar la seguridad en el código, reducir dependencia tradicional de medidas externas.
- Identifique vulnerabilidades de su red e infraestructura, lo que es vulnerable hoy lo será en la nube.
- Proveedores ofrecen servicios de seguridad, el caso de negocio sigue siendo válido si contrata esos servicios?

En un mundo sin servidores, la administración del riesgo cibernético requiere diarias revisiones, retoques y afinaciones, pero la automatización NoOps puede hacerlo más fácil.



Las tendencias tecnológicas para los negocios

Conectividad del mañana

- **5G:** despliegue público y privado.
- **Satélites estacionarios de órbita baja:** SpaceX, OneWeb y otros.
- **Redes definidas por software SDN:** todo el tráfico se maneja y dirige desde appliances. Se ha expandido desde data center a redes WAN.
- **Virtualización del trabajo de redes NFV:** software virtualizado realiza enrutamiento, firewalling, cifrado, tal como lo hacen los dispositivos físicos.

51

operators will have launched 5G services in at least part of their territory by the end of 2020, according to predictions by Deloitte Global.

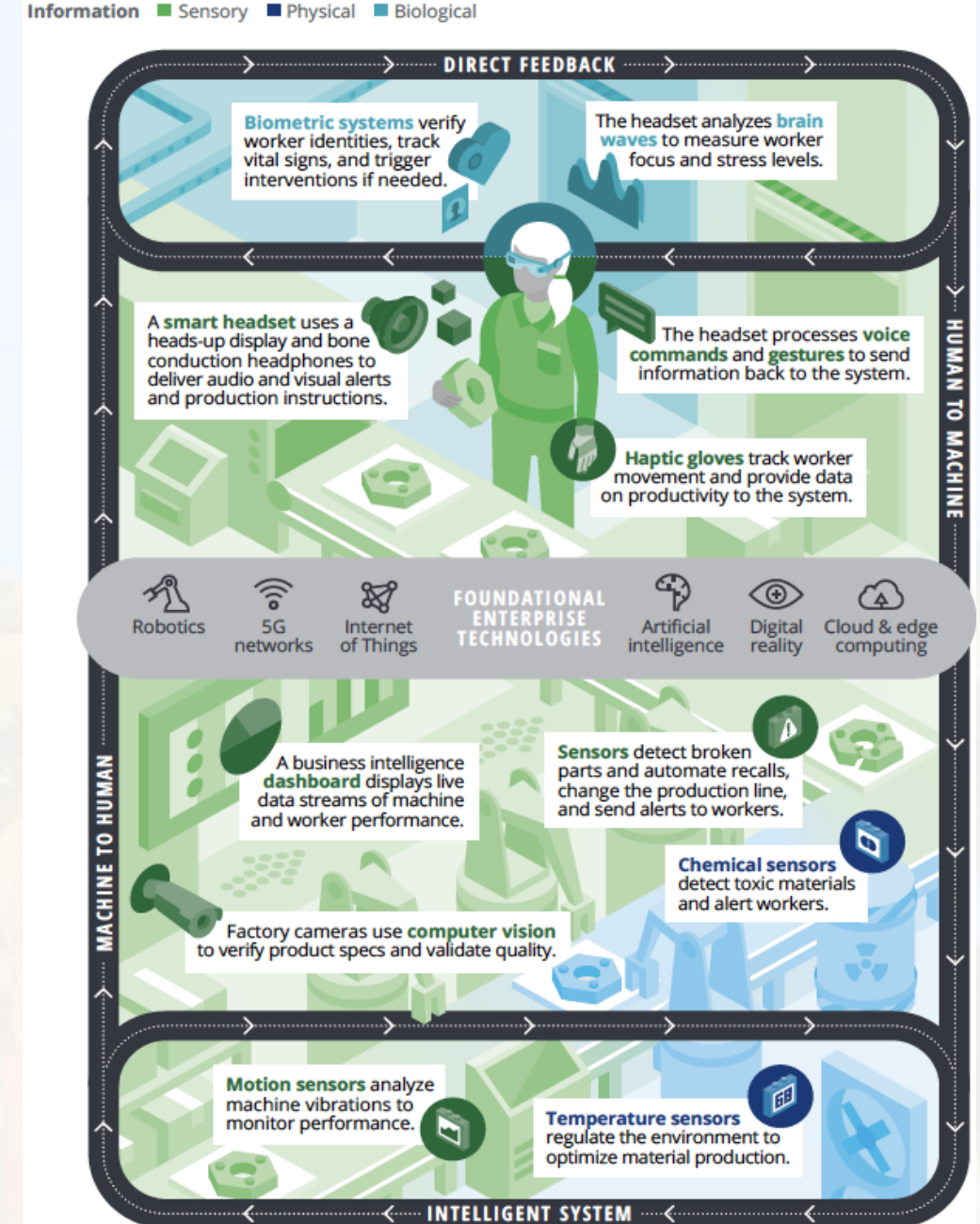
Implicaciones de ciber riesgo

- Las redes homogéneas protegidas por firewalls son una reliquia. La conectividad ya es y será un híbrido de redes Long Term evolution - LTE, 5G, SDN, NFV, WiFi, Satélite, entre otros. Los dispositivos proliferarán aún más (IoT). La seguridad debe atender este reto.
- Segmentación a nivel de red y microsegmentación a nivel de dispositivos.
- **Confianza cero:** cada actor y dispositivo debe ser identificado y autenticado individualmente
- Automatización de procesos de ciber seguridad, incorporando IA.

Las tendencias tecnológicas para los negocios

Interfaces inteligentes

- Tecnologías desplegadas para que el humano interactúe intuitivamente con la máquina, sensores, voz, tacto, datos de navegación de un móvil, etc.
- Mercado de computación afectiva (sensores de emoción) se estima en US\$ 41 billones en 2022.
- Interfaces de voz (Cortana, Siri, Google Assistant, Alexa). El siguiente hito es que sean capaces de mantener una conversación coherente y comprometida.
- Seguimiento al comportamiento offline de los clientes (hábitos y rutinas inferidas, por ejemplo, del GPS del móvil)
- Sensores de emoción para micropersonalizar productos y servicios (estrés, depresión, ira, tensión)
- Interfaces inteligentes para mejorar productividad (monitoreo de los empleados)



Las tendencias tecnológicas para los negocios

Interfaces inteligentes

Implicaciones para tecnología

- Mayor ancho de banda. 5G.
- Computación en el borde y en la nube. Muchas decisiones basadas en inteligencia artificial deben ser en tiempo real y no toleran la latencia de ir a “sistemas centrales”.
- Internet de las Cosas – IoT

Implicaciones de ciber riesgo

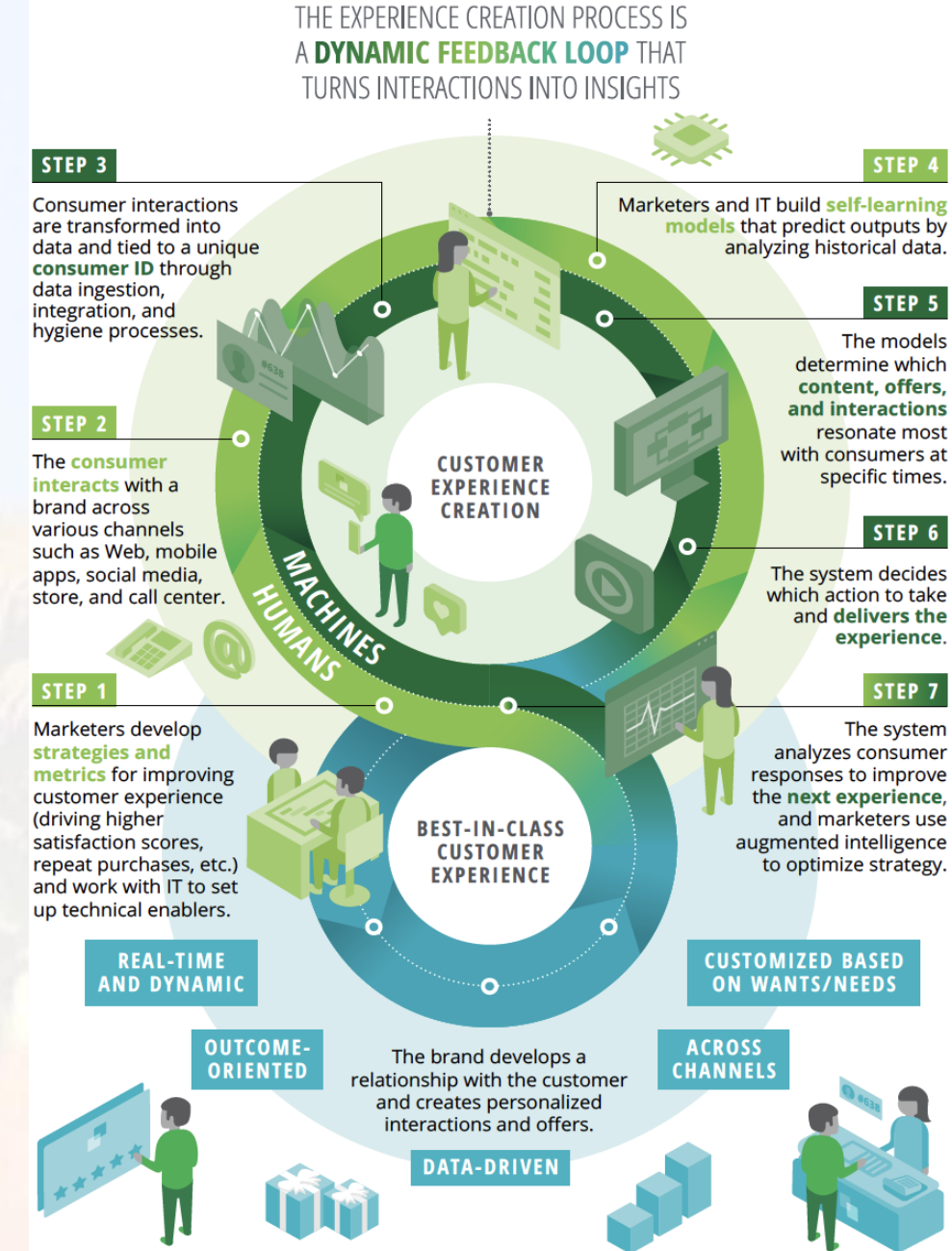
- Ciber seguridad para lo que hacen las interfaces y para la información que tratan.
- Interfaces inteligentes generan capacidades de ciber seguridad (identidad, autenticidad)
- El riesgo de que esta información biométrica sea comprometida sería devastador:
 - Riesgo ético por discriminación, segregación
 - Privacidad de estado de salud
 - Seguridad de los marcadores de identidad
 - Regulatorio: mirarlo como cumplimiento y no como un sistema de gestión que permita identificar y proteger adecuadamente los datos personales

Las tendencias tecnológicas para los negocios

Más allá del Mercadeo: La experiencia reimaginada

CIO y CMO trabajando juntos para reimaginar la experiencia humana

- Las personas están dispuestas a abandonar una marca que les de experiencias frustrantes, pobres e impersonales.
- Las expectativas de los clientes varían dramáticamente debido a su interacción continua con Internet.
- Reconectarse con las emociones es el imperativo.
- La tecnología (móviles, nube, IA, aprendizaje de máquinas) para optimizar la experiencia del consumidor.
- Las iniciativas de reimaginar la experiencia será parte de la agenda de cada vez más compañías en los próximos 2 años.



Las tendencias tecnológicas para los negocios

Más allá del Mercadeo: La experiencia reimaginada

Las 3 D requeridas en este camino más allá del mercadeo

- **Datos:** toda la información que tiene de sus clientes al interior de los sistemas está a su servicio. Y puede ser enriquecida con información externa, dentro de los estándares de protección de datos.
- **Decisión:** analíticas avanzadas y motores de decisión que hagan que los datos sean accionables con personalizaciones en tiempo real (mensajes, imágenes, precios, promociones), las cuales sean analizadas con aprendizaje de máquina para confirmar o descartar la decisión en interacciones futuras con el cliente.
- **Entrega:** orquestar las decisiones mediante las interacciones en los canales disponibles de manera consistente, de manera muy o totalmente automatizada.

Implicaciones de ciber riesgo

- Fraude y ciber crimen originado en el robo de credenciales de acceso, las cuales deben ser protegidas por ... humanos.
- Limitar la fricción mientras se aseguran los datos en múltiples puntos de contacto.
- La regulación es una fuerza más del mercado que debe considerarse, por la exigencia para crear estrategias integrales de protección de datos y seguridad.

La pila de tecnología requerida para comprometer y entregar experiencia del cliente de principio-a-fin puede ser increíblemente compleja y desafiante si no es desarrollada dentro de los parámetros de una estrategia digital.

Las tendencias tecnológicas para los negocios

Tendencia de ciber riesgo: DevSecOps

DevSecOps: Elevando, embebiendo y evolucionando la respuesta al riesgo

- Incorporar la seguridad, privacidad, políticas y controles en la cultura, procesos y herramientas DevOps.
- Automatizar modelos de amenazas, evaluación de riesgos y tareas de seguridad dentro de las iniciativas de desarrollo de productos.

DevSecOps fundamentalmente:

- Transforma ciber seguridad y gestión de riesgo, de una serie de actividades para cumplir y tardías dentro del ciclo de vida de desarrollo, en fundamentos esenciales que enmarcan el viaje del desarrollo de un producto.
- Codifica políticas y lineamientos dentro de las herramientas y plataformas DevOps, para que la ciber seguridad sea una responsabilidad compartida de toda la organización de TI.

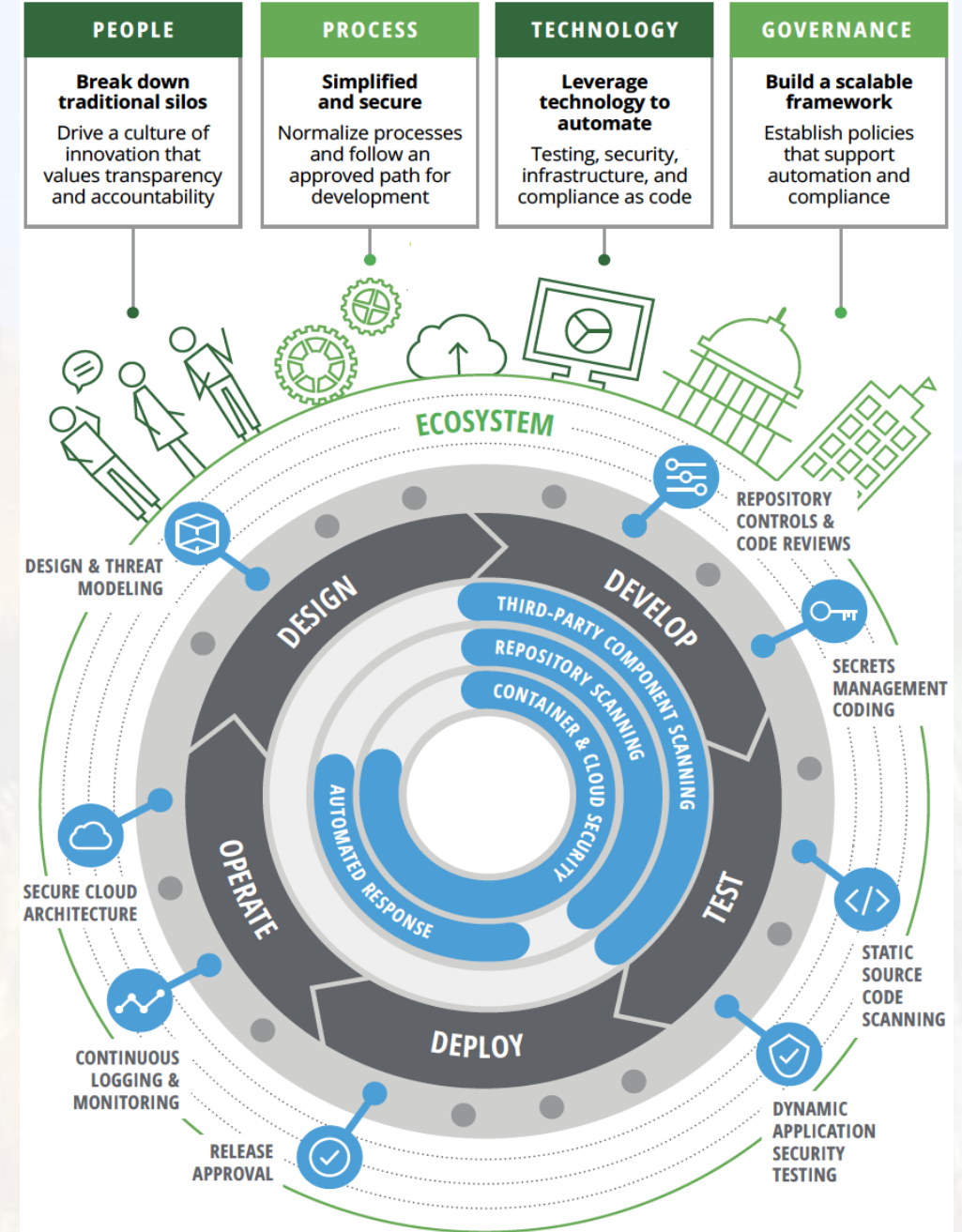
Porqué DevSecOps

- Seguridad del producto no va a la velocidad que el desarrollo del producto. La seguridad es vista por DevOps como impedimentos para la velocidad, agilidad, transparencia y efectividad.
- Embebiendo la cultura, prácticas y herramientas de seguridad en las fases de DevOps, es posible mejorar la madurez de la seguridad y cumplimiento de DevOps.
- Tradicionalmente la seguridad ha sido, y sigue siendo, vista como un adicional, no como una característica desde el diseño, enfoque incompatible con las metodologías ágiles, donde el producto es resultado de los requerimientos, no de accesorios superpuestos.
- DevSecOps no es una evolución de ciber seguridad, sino de DevOps, ofrece a las compañías practicar DevOps como una manera diferente de pensar en seguridad.

Las tendencias tecnológicas para los negocios

Tendencia de ciber riesgo: DevSecOps

A positive by-product of DevSecOps is that cybersecurity specialists often develop a greater understanding of development pressures and therefore drive more backend automation of security functions.



Efecto en la auditoría interna

“Utilizamos la negación como protección. Si no prestamos atención, podemos continuar nuestras vidas sin darnos cuenta de nada”

“Los supervivientes no tienen tiempo de preguntar, “¿por qué a mí?”. Para los supervivientes, la única pregunta relevante es “¿y ahora que?”

La bailarina de Auschwitz

Edith Eger

Fortalecer impacto e influencia de la auditoria interna

- 1 Desarrollar y lanzar una identidad de marca
- 2 Conectar actividades de asesoramiento con el aseguramiento
- 3 Proveer servicios de ciber aseguramiento
- 4 Auditar la función de riesgo “de principio a fin”
- 5 Validar los procesos de planeación estratégica
- 6 Adoptar analítica de datos
- 7 Sintetice y dinamice los reportes de Auditoria Interna
- 8 Mejorar las habilidades y capacidades de la Auditoría
- 9 Aumente su impacto personal

*Nine ways to strengthen Internal Audit´s impact and influence in the organization.
Deloitte. 2017.*

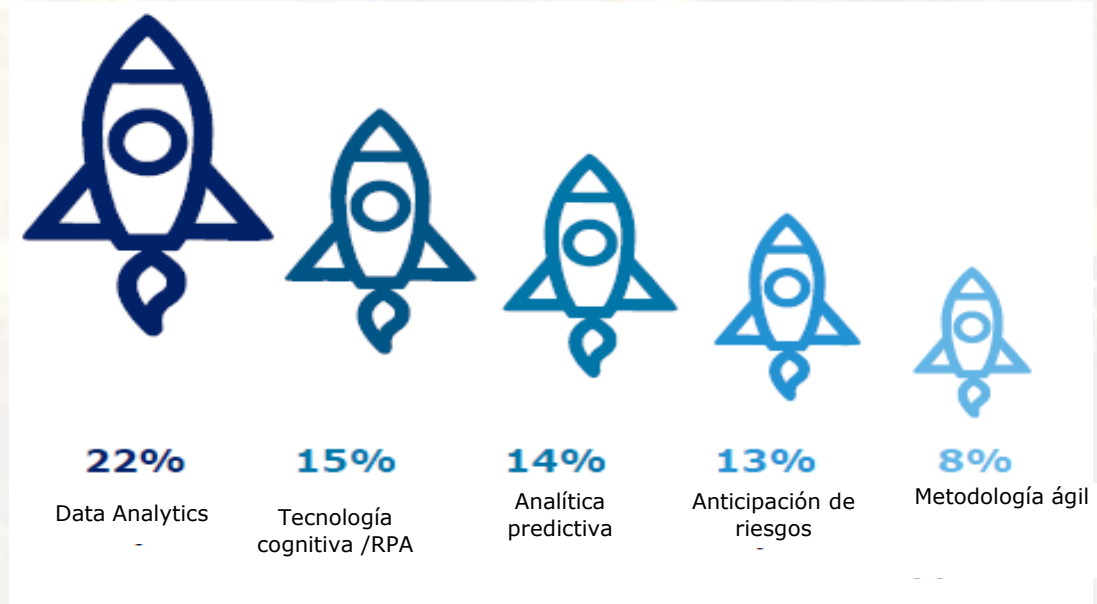
Preparación

Aquellas funciones de AI que han adoptado enfoques y métodos innovadores tienden a tener mayor impacto e influencia que aquellas que no.

71%

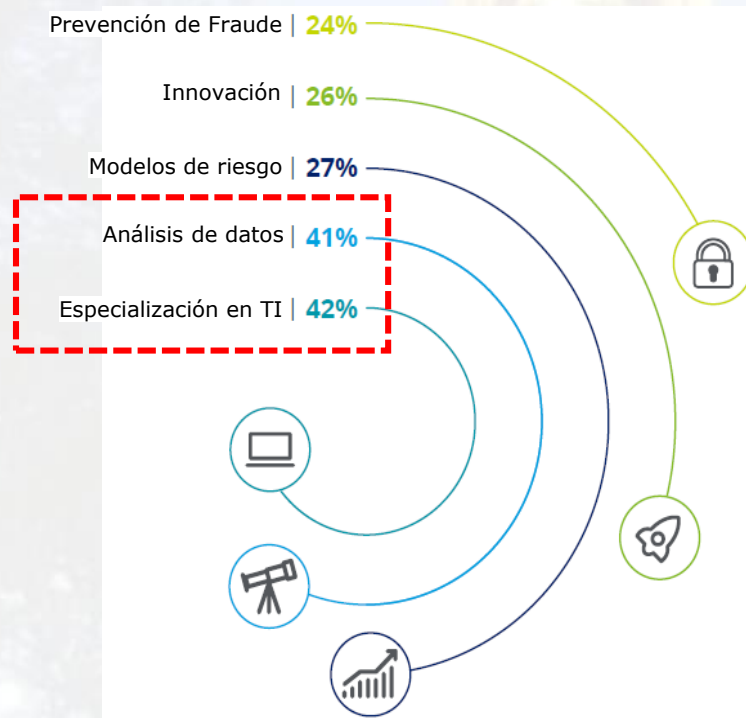
de los casos con **alto nivel de impacto e influencia**, planean incrementar su inversión en innovación en los próximos 3 a 5 años.

Iniciativas de innovación que tendrán mayor impacto en la función de AI en los próximos 3 a 5 años

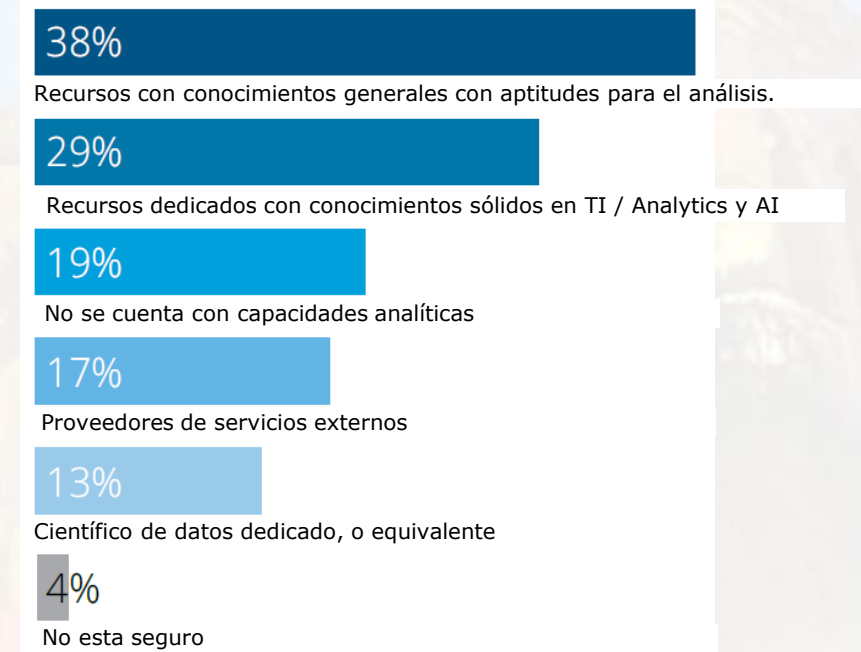


Preparación

Principales brechas en las habilidades De los Auditores Internos



Capacidad de la función de Auditoría Interna frente al análisis de datos.



Conclusión

“No podemos decidir tener una vida sin dolor. Pero podemos decidir ser libres, escapar del pasado, suceda lo que nos suceda, y adaptarnos a lo posible.”

**La bailarina de Auschwitz
Edith Eger**