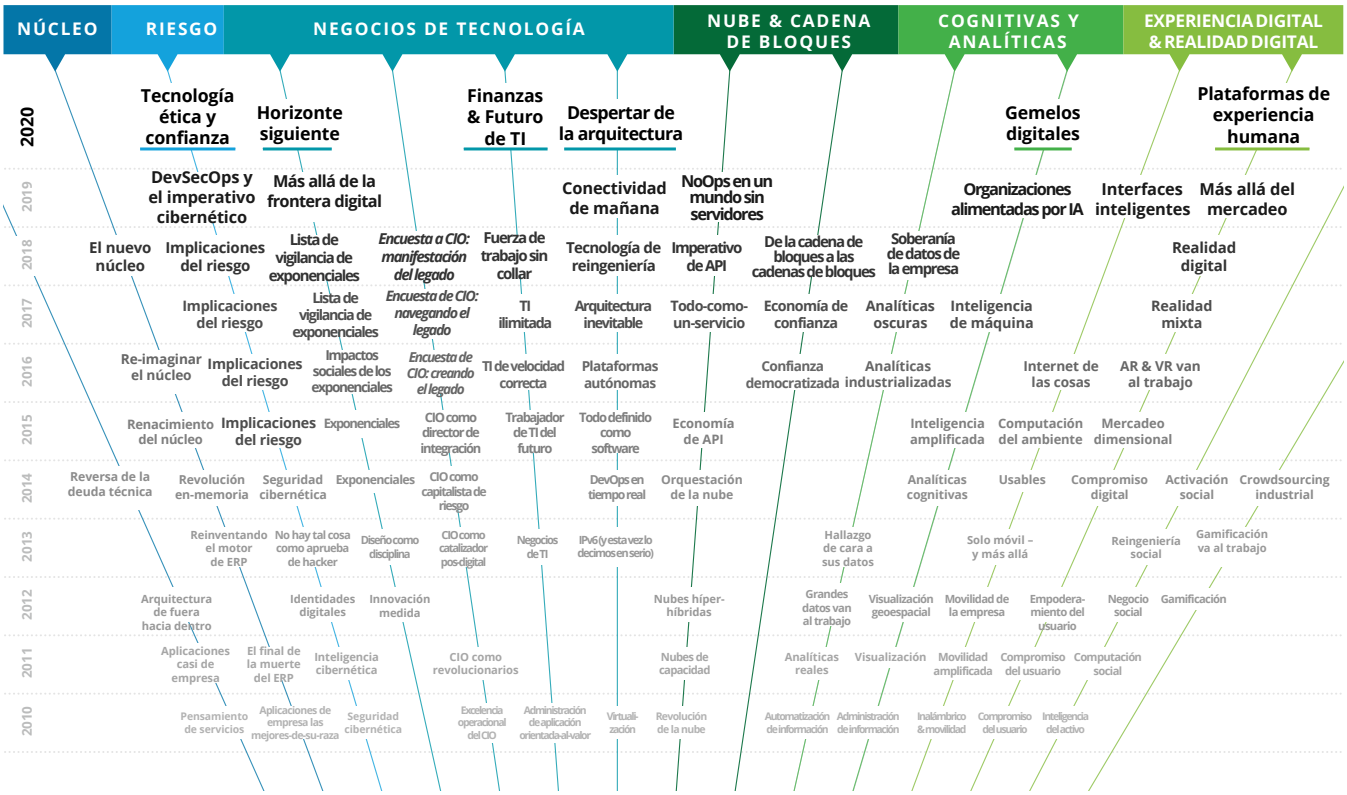
Deloitte.
Insights

Tendencias de tecnología 2020

Tendencias de las tendencias: Once años de investigación



Introducción

EN EL AÑO 2020, la siguiente etapa de la evolución digital nos recibe con la promesa de interfaces emocionalmente inteligentes y capacidades cognitivas híper-intuitivas que transformarán los negocios de maneras impredecibles. Pero como nos preparamos para la próxima década de cambio disruptivo, sería sabio recordar un punto importante acerca de las innovaciones de vanguardia de ayer: los arquitectos de los años 1980 diseñaron sistemas de mainframe que continúan operando y generando valor de negocios hoy. Claro, están pasados de moda según los estándares de hoy, pero ¿cómo muchos de nosotros construiremos sistemas que operen por décadas? ¿Y cómo es eso para un legado?

Hacer arquitectura para longevidad y adaptabilidad requiere un entendimiento profundo tanto de las realidades de hoy como de las posibilidades del mañana. Requiere una apreciación de la tecnología y de las fuerzas del mercado que orientan el cambio. Y finalmente, requiere un compromiso de largo plazo para con el progreso centrado e incremental.

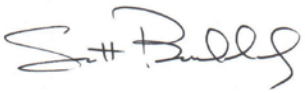
Con este telón de fondo, presentamos *Tech Trends 2020* [Tendencias de tecnología 2020], el 11º. Examen anual que Deloitte realiza de las tendencias emergentes de tecnología que afectarán su organización en los próximos 18-24 meses. Varias de las tendencias de este año son respuesta a persistentes desafíos de TI. Otras representan dimensiones específicas-de-tecnología de grandes oportunidades para la empresa. Todas están preparadas para orientar cambio importante.

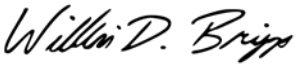
Nosotros comenzamos *Tech Trends 2020* [Tendencias de tecnología 2020] con una actualización oportuna de las nueve fuerzas macro de la tecnología que examinamos en el reporte del año anterior. Esas fuerzas – experiencia digital, analíticas, nube, modernización del núcleo, riesgo, el negocio de la tecnología, realidad digital, cognitiva, y cadena de bloques – forman el fundamento de la tecnología a partir del cual las organizaciones construirán el futuro. La actualización de este año da una mirada fresca a la adopción que la empresa ha hecho de esas macro fuerzas y cómo ellas están dando forma a las tendencias que nosotros predecimos generarán disrupción de los negocios en los próximos 18 a 24 meses. También miramos tres tecnologías que probablemente se convertirán en macro fuerzas por su propio derecho: experiencia del ambiente, inteligencia exponencial, y cuántico.

En capítulos subsiguientes, discutimos tendencias que, si bien están fundamentadas en realidades de hoy, informarán la manera como trabajaremos mañana. Nuestro capítulo sobre tecnología ética y confianza da una mirada profunda a cómo cada aspecto de una organización que recibe disrupción por la tecnología se convierte en una oportunidad para perder – o ganar – la confianza de clientes, empleados, y *stakeholders*. Seguimos con una discusión de las plataformas de experiencia humana que permitirán que los sistemas del mañana entiendan el contexto y sientan emoción humana para responder apropiadamente. Organizaciones pioneras ya están explorando maneras mediante las cuales esas plataformas pueden satisfacer la necesidad muy humana de conexión.

Las tendencias evolucionan de maneras inesperadas. Y a menudo, las oportunidades más interesantes ocurren en los lugares donde se intersectan. Varias de las tendencias de este año representan combinaciones fascinantes de macro fuerzas y otros avances tecnológicos. Por ejemplo, los gemelos digitales representan la culminación de núcleos modernizados, modelos cognitivos avanzados, sensores incrustados, y más – una receta que es en sí misma una tendencia, incluso cuando se basan en tecnologías individuales que evolucionan.

Nosotros esperamos que *Tech Trends 2020* [Tendencias de tecnología 2020] ofrezca las perspectivas y la inspiración que usted necesitará para el viaje digital que está por delante. El camino desde las realidades de hoy hacia las posibilidades del mañana será largo y estará lleno de sorpresas, así que sueña en grande y arquitecte de acuerdo con ello.





Scott Buchholz
Emerging Technology research director
and Government & Public Services
chief technology officer
Deloitte Consulting LLP
sbuchholz@deloitte.com

Bill Briggs
Global chief technology officer
Deloitte Consulting LLP
wbriggs@deloitte.com
Twitter: @wdbthree

RESUMEN DE LA TENDENCIA

En un tiempo de constante disrupción tecnológica, ganar confianza es un desafío – y una oportunidad – de 360 grados.

DEFINICIÓN

e-thi-kal / tecnology

El conjunto general de valores que dirige el enfoque de la organización para su uso de tecnologías en su conjunto y las maneras como son desplegadas para orientar el negocio.

POR LOS NÚMEROS

de quienes respondieron en un estudio de Deloitte, provenientes de compañías de alto crecimiento, está altamente preocupado acerca de las ramificaciones éticas de las tecnologías, comparado con solo el 27% de las compañías de bajo crecimiento.†

RUPTURA DE LA TENDENCIA

†Timothy Murphy et al., *Ethical technology use in the Fourth Industrial Revolution*, Deloitte Insights, July 15, 2019.

Tecnología ética y confianza

Aplicación de los valores de su compañía a la tecnología, las personas, y los procesos

UN ESTRIBILLO FRECUENTE en los reportes *Tech Trends*, de Deloitte, es que cada compañía es ahora una compañía de tecnología. Con el advenimiento de la tecnología digital, los negocios les han estado pidiendo a los clientes confiar en ellas de nuevas y más profundas maneras, desde pedir información personal para hacerle seguimiento en línea del comportamiento hasta migas de pan digitales. Al mismo tiempo, los titulares regularmente muestran crónicas de problemas basados-en-tecnología tales como violaciones de seguridad, vigilancia inapropiada o ilegal, mal uso de datos personales, distribución de información engañosa, sesgo algorítmico, y carencia de transparencia. La desconfianza que esos incidentes alimentan en los *stakeholders* – sean clientes, empleados, socios, inversionistas, o reguladores – puede dañar de manera importante la reputación de la organización.[1] Además, la confianza del consumidor en las empresas comerciales está declinando, los ciudadanos se están volviendo cautelosos con las instituciones públicos, y los trabajadores les están pidiendo a los empleadores que de manera explícita establezcan los valores centrales.[2]

En lo que reconocemos como una tendencia emergente, algunas compañías están enfocando la confianza no como un problema de cumplimiento o de relaciones públicas, sino como una meta crítica-del-negocio a ser alcanzada – una que pueda diferenciarles en un mercado crecientemente complejo y saturado. Tal y como se discute en el reporte 2020 Global Marketing Trends, de Deloitte, la confianza en la marca es para los negocios más importante que nunca antes – y lo abarca todo. Clientes, reguladores, y los medios de comunicación esperan que las marcas sean abiertas, honestas, y consistentes a través de todos los aspectos de sus negocios, desde productos y promociones hasta cultura de la fuerza de trabajo y relaciones del socio.[3]

Cada aspecto de la compañía que es disruptido por la tecnología representa una oportunidad para ganar o perder confianza con clientes, empleados, socios, inversionistas, y/o reguladores. Los líderes que a través de sus organizaciones incrustan los valores organizacionales y los principios de la tecnología ética están demostrando un compromiso con “hacerlo bien” que pueda

construir un fundamento de confianza de largo plazo con los *stakeholders*. Con esta luz, la confianza se convierte en un emprendimiento de 360 grados para ayudar a asegurar que la tecnología, los procesos, y las personas de la organización están trabajando en concierto para mantener ese fundamento.

Tal y como el adagio nos lo recuerda, la confianza es difícil de ganar y fácil de perder.

El terreno de la tecnología ética

El término tecnología ética se refiere a un conjunto general de valores que no está limitado a o centrado en una sola tecnología, abordando en lugar de ello el enfoque de la organización para con su uso de las tecnologías en su conjunto y las maneras como son desplegadas para orientar las estrategias y las operaciones del negocio.[4] Las compañías deben considerar proactivamente evaluar cómo pueden usar la tecnología de maneras que estén alineadas con su propósito fundamental y con sus valores centrales.

Las políticas de la tecnología ética no reemplazan el cumplimiento general o la ética de negocios, pero todas deben estar conectadas de alguna manera. Así como su enfoque para la seguridad cibernética no toma el lugar de las políticas de privacidad más generales de su compañía, su enfoque de tecnología ética debe complementar su enfoque general para la ética y servir como su extensión lógica en el ámbito digital. Algunas compañías están expandiendo la misión de la ética, aprendizaje, e inclusión para incluir la tecnología ética, al tiempo que mantienen programas separado de ética de la tecnología. Hacerlo ayuda a mantener la ética de la tecnología en lo alto de la mente a través de la organización y fomenta que los ejecutivos consideren la distinción entre los problemas éticos relacionados-con-la-tecnología y las preocupaciones más amplias de la ética corporativa y profesional.

El quinto estudio anual de negocios digitales realizado por *MIT Sloan Management Review* y Deloitte encontró que solo el 35 por ciento de quienes respondieron consideran que los líderes de su organización dedican suficiente tiempo pensando acerca de y comunicando el impacto de las iniciativas digitales en la sociedad. Si bien quienes respondieron provenientes de compañías digitalmente maduras son los que más probablemente dicen que sus líderes están haciendo suficiente, incluso entonces, el porcentaje apenas llega a una mayoría del 57 por ciento.[5]

Esos hallazgos sugieren que las organizaciones todavía tienen espacio importante para dar un paso adelante. Las compañías que desarrollen una mentalidad de tecnología ética – demostrando un compromiso para con la toma de decisiones ética y promoviendo una cultura que la apoye – tienen la oportunidad para ganar la confianza de sus *stakeholders*.

En búsqueda de la confianza

En la era digital, la confianza es un problema lleno de tensión, con una miríada de amenazas existenciales para la empresa. Y si bien las tecnologías disruptivas a menudo son vistas como vehículo para el crecimiento exponencial, la tecnología sola no puede construir confianza de largo plazo. Por esta razón, las organizaciones líderes están tomando un enfoque de 360 grados para mantener el nivel alto de confianza que sus *stakeholders* esperan.

EN LA TECNOLOGÍA CONFIAMOS

nteligencia artificial (IA), aprendizaje de máquina, realidad digital, y otras tecnologías emergentes se están integrando en nuestras vidas más rápida y profundamente que nunca antes. ¿Cómo pueden los negocios crear confianza con las tecnologías que sus clientes, socios, y empleados están usando?

- **Codifique los valores de su compañía.** Con la tecnología engranada en el negocio y el aprendizaje de máquina orientando decisiones y acciones de negocio, los valores de la organización deben ser codificados y medidos dentro sus soluciones de tecnología. Los sistemas digitales pueden ser diseñados para reducir el sesgo y permitir que las organizaciones operen en línea con sus principios.[6] Por ejemplo, el gobierno de una ciudad trabajó con institutos de política para desarrollar un conjunto de herramientas

algorítmicas que tienen la intención de identificar maneras para minimizar el daño no-intencional para sus miembros mediante limitar sesgos en el sistema de justicia criminal y otras instituciones.

Las salvaguardas pueden promover el bienestar del *stakeholder* mediante ayudar a prevenir que los usuarios se comprometan con la tecnología de maneras no-saludables o irresponsables. Los ejemplos incluyen una compañía que impone límites de tiempo y gastos en los juegos que forman hábito, un agregador de contenido que promueve que los usuarios sean escépticos acerca de la veracidad de la información proveniente de crowsourcing, y proveedores de computación en la nube que automáticamente emiten alertas antes que los clientes superen el presupuesto.

Las tecnologías de IA explicables pueden aclarar cómo se toman decisiones orientadas-por-IA. Por ejemplo, para mejorar la confianza en diagnósticos médicos apoyados-en-IA, las compañías de atención en salud están desarrollando soluciones que asignan a cada diagnóstico un puntaje de confianza que explica la probabilidad y la contribución de los síntomas de cada paciente (signos vitales, señales provenientes de reportes médicos, rasgos del estilo de vida, etc.) a ese diagnóstico. Los profesionales médicos pueden ver por qué la conclusión obtenida y hacer una diferente si se requiere.[7]

- **Construir un fundamento sólido de datos.** Sin metódica y consistentemente hacer seguimiento a los datos que usted tiene, dónde se encuentran, y quién puede tener acceso a ellos, usted no puede crear un entorno de confianza. Un fundamento sólido de datos unifica a los *stakeholders* alrededor de una sola visión de *accountability* de los datos y apoya la administración efectiva de los datos.[8] Los líderes deben darles a los *stakeholders* algún control sobre cómo sus datos serán usados y borrar los datos a la demanda, a menos que sea necesario mantenerlos para propósitos legales o regulatorios.

- **Fortalezca su defensa.** La 2019 Future of Cyber Survey,[9] de Deloitte, revela que los ejecutivos crecientemente están dedicando cantidades importantes de tiempo centrándose en los problemas cibernéticos, y con razón. Las defensas cibernéticas representan su compromiso para proteger a sus clientes, empleados, y socios de negocio de quienes no comparten sus valores – o los suyos. La estrategia del riesgo cibernético debe ser construida y administrada desde el principio, incrustada en la mentalidad, la estrategia, y las políticas del negocio, no solo dentro de TI. Los líderes del negocio pueden colaborar con TI para crear una estrategia comprensiva del riesgo cibernético – que comprenda seguridad, privacidad, integridad, y confidencialidad – para ayudar a construir la confianza del *stakeholder* y orientar la ventaja competitiva. Esto requiere considerar la tolerancia que frente al riesgo tiene la organización, identificar las brechas más vulnerables, así como también los datos y sistemas más valiosos, y luego idear planes para mitigación y recuperación.

QUÉ HAY EN UN PROCESO

El fundamento fuerte para la tecnología ética y la confianza estará enmarcado por los principios de los líderes de la organización y realizado en los procesos de negocio.

- **Respete la privacidad del stakeholder.** Uno de los efectos más generalizados de la disrupción de la tecnología ha sido acelerar el recaudo, análisis y difusión de la información. No hace tanto tiempo, los detalles transaccionales de nuestras vidas eran mantenidos en archivadores físicos, retirados y referenciados para necesidades específicas. Hoy, los sistemas rutinariamente recaudan esos detalles y los combinan con nuestras historias de compra, publicaciones en medios de comunicación social, búsquedas en línea, e incluso la ruta por la cual conducimos cada día de trabajo.[10] Si los consumidores tienen razón para considerar que sus datos están siendo usados de manera que ellos no aprueban, las reacciones pueden incluir llamados a boicots, consultas públicas, e incluso sanciones severas según regulaciones estrictas, tal como la General Data Protection Regulation, de la Unión Europea, y la Consumer Privacy Act, de California. Las compañías deben crear políticas de privacidad de los datos que construyan, más que erosionen, la confianza del público. Un natural primer paso puede ser asegurar que el uso de los datos esté alineado con la misión de

la compañía.[11] Por ejemplo, JD Wetherspoon, una compañía de pub que sirve al Reino Unido e Irlanda, recientemente eliminó más de 656,000 direcciones de correos electrónicos de clientes, dado que percibió a los correos electrónicos como un enfoque intrusivo para la interacción del cliente, que proporciona poco valor.[12] Este caso resalta la importancia de no solo alinear el recaudo y el uso de los datos con los valores de la compañía sino, por extensión, respaldar la relación de confianza de la compañía con el cliente.

- **Sea transparente.** Las compañías pueden construir confianza con los *stakeholders* mediante proactiva y transparentemente demostrar buen comportamiento. "La transparencia se vuelve vital e importante," dice el director ejecutivo de AI Global Ashley Casovan.[13] "Sea o no que las personas estén interesadas en ver los recursos y datos detrás de ello realmente no importa. Simplemente conocer que las compañías tienen políticas transparentes proporciona más confianza de que están haciendo las cosas correctas." La transparencia se extiende más allá de políticas que explican el recaudo de datos y las prácticas de uso. Por ejemplo, más que disfrazarlos como humanos, los agentes inteligentes o chatbots deben identificarse a sí mismos como tales. Las compañías deben revelar el uso de sistemas automatizados de decisión que afectan a los clientes[14] y deben mantenerse centradas en el cliente cuando ocurran problemas, proporcionando tanto calidad como calidad en la respuesta. Las consecuencias de incidentes negativos no tienen que incluir pérdida del cliente o titulares que dañen la reputación.[15]

- **Respete las diferentes normas culturales.** Cuando el enfoque general de la organización para construir confianza está informado por intereses, experiencias, y estándares profesionales, así como también por las normas sociales y el control del gobierno. Puede ser desafiante servir al mercado global en el cual las expectativas sobre la vigilancia del gobierno o la cooperación para hacer forzoso el cumplimiento de la ley varían ampliamente. Por ejemplo, lo que se espera de la vigilancia en algunos países puede ser visto como indignante en otros lugares; la cooperación con el hacer forzoso el cumplimiento de la ley es rutina en muchos países, pero quizás imprudente en lugares con corrupción rampante o carencia de protección para los derechos políticos o religiosos. Algunos países tienen regulaciones muy específicas alrededor de obtener consentimiento explícito del cliente para el uso de datos; otras municipalidades están aprobando legislación, tal como prohibir la tecnología de reconocimiento facial, que pueda entrar en conflicto con otras reglamentaciones. El gobierno efectivo de las tecnologías emergentes requiere que todos los *stakeholders* relevantes – industria, consumidores, negocios, gobierno, academia, y sociedad – trabajen juntos. Los negocios pueden jugar un rol clave en ayudar a los gobiernos cuando desarrollen leyes y estándares que incrementen la confiabilidad de las tecnologías emergentes - el discurso franco, sincero, acerca de las nuevas tecnologías, por ejemplo, podría llevar a nuevas reglas y orientación relacionadas con materias de privacidad, transparencia, inclusión, accesibilidad, desigualdad, y más.[17]

EMPODERE LAS PERSONAS

Dado que la tecnología presumiblemente es usada por la mayoría de, si no por todos, los individuos dentro de una organización, la tecnología ética y la confianza es un tema que toca a todos.

- **Despliegue el poder de todo.** Las compañías pueden gastar tiempo y dinero creando algo que excluye a un grupo de clientes o presta un servicio con efectos colaterales indeseables. Quizás aún peor, pueden construir soluciones que menoscaben la confianza del cliente. A menudo, los dilemas del diseño comienzan con un grupo homogéneo de personas que diseñan productos, procesos, o servicios sin pensar cómo otros grupos de personas pueden ser afectados. Las compañías líderes están cambiando esta dinámica mediante crear equipos y roles que reflejen su base diversa de clientes y ofrezcan múltiples puntos de vista diferentes provenientes de industrias, antecedentes económicos, experiencias educativas, géneros, y antecedentes étnicos.[18] Una encuesta que Harvard realizó en el año 2013 reveló que las organizaciones con equipos de liderazgo que tienen una combinación de al menos tres rasgos inherentes (con los cuales han nacido) y tres adquiridos (los que usted gana mediante la experiencia) de diversidad, innovan y superan a

las otras; esas organizaciones son 45 por ciento más probable que reporten crecimiento en la participación en el mercado y 70 por ciento más probable que reporten la captura de nuevo mercado.[19]

- **Enséñeles a pescar.** Entrenar a los tecnólogos para que reconozcan sus propios sesgos, y para que eliminen el sesgo en los productos que crean es un paso importante hacia la creación de una cultura que enfatice la confianza. Pero es solo un paso. Construir confianza de cómo la tecnología afecta la confianza del *stakeholder* en quienes no están directamente involucrados o son responsables por la tecnología y la creación de las estructuras asociadas de toma de decisiones son pasos adicionales que las organizaciones deben considerar. Esto es especialmente importante en organizaciones que no son nativas digitales, donde los efectos en cascada del uso diario de la tecnología pueden ser menos obvios para líderes y equipos. Las compañías deben considerar qué recursos se pueden necesitar para ayudar a que sus empleados reconozcan dilemas éticos, evalúen alternativas y tomen (y prueben) decisiones de la tecnología ética.[20]

- **Dé a los empleados una razón para confiar.** Mucha de la ansiedad sobre IA y otras tecnologías avanzadas surge del miedo al desplazamiento de la mano de obra. Desde una perspectiva ética, esto presenta a los líderes de negocio un desafío: balancear los mejores intereses del negocio, los empleados, y la comunidad y sociedad más amplias. Es una tarea que se hace más compleja por el hecho de que los sistemas de tecnología avanzada no son auto-suficientes. Si bien la IA puede reemplazar algunos trabajos, por ejemplo, crea otros que a menudo requiere habilidades y entrenamiento especializados.[21] Las compañías pueden construir confianza con los empleados mediante asesorarles en cómo la tecnología puede afectar sus trabajos en el futuro. Esto podría incluir re-entrenar los trabajadores cuyos roles puedan evolucionar y quienes probablemente trabajarán con sistemas automatizados.[22]

360 grados de oportunidad

Las compañías que no consideran que la tecnología sea su negocio central pueden asumir que esas consideraciones son ampliamente irrelevantes. En verdad, no importa la industria o geografía, la mayoría de las organizaciones crecientemente se están basando en tecnologías avanzadas, digitales y físicas, para llevar a cabo sus operaciones del día-a-día.

Si bien hay mucho énfasis en los desafíos que las tecnologías disruptivas ofrecen y las amenazas existenciales para la reputación de la organización cuando la tecnología no es manejada correctamente – sea mediante abuso de autoridad o crimen – esas mismas tecnologías disruptivas pueden ser usadas para incrementar la transparencia, fortalecer la seguridad, aumentar la privacidad de los datos, y en últimas reforzar la posición de una organización de confianza.

Por ejemplo, las organizaciones pueden pivotear algoritmos de personalización para proporcionar recomendaciones relevantes basadas en circunstancia – por ejemplo, ofrecer un paraguas en un día de lluvia, más que un paraguas después que alguien compre un impermeable. Mediante centrarse en relevancia más que en personalización, las recomendaciones de IA es probable que parezcan más útiles que invasivas.[23]

Deloitte surveys have found a positive correlation between organizations that strongly consider the ethics of Industry 4.0 technologies and company growth rates. For instance, in organizations that are witnessing low growth (up to 5 percent), only 27 percent of the respondents indicated that they are strongly considering the ethical ramifications of these technologies. By contrast, 55 percent of the respondents from companies growing at a rate of 10 percent or more are highly concerned about ethical considerations.[24]

Después de todo, la búsqueda de confianza no es solo un desafío de 360 grados. También es una oportunidad de 360 grados.

LECCIONES DE LAS LÍNEAS DEL FRENTE

Un fundamento saludable para la confianza

LAS DISRUPCIONES EN la industria de atención en salud – que incluyen nuevos modelos de entrega de atención, demanda del consumidor por experiencias digitales, declinación de los reembolsos, y crecimiento de las presiones regulatorias – están llevando a que muchas organizaciones de atención en salud usen tecnología para mejorar eficiencia, reducir costos, y mejorar la atención al paciente. Y podrían tener un beneficio inadvertido: la tecnología podría ayudar a que los sistemas de atención en salud construyan confianza con pacientes y proveedores.

Providence St. Joseph Health (PSJH) está aprovechando la tecnología para adherirla a su misión de mejorar la salud de poblaciones no-privilegiadas y no-atendidas, dice B.J. Moore, CIO de PSJH.[25] La tecnología está ayudando al sistema de salud católico sin ánimo de lucro a simplificar experiencias complejas para mejorar las atenciones entre cuidador y paciente, mejorar el entorno de operación y los procesos de negocio, e innovar con nube, analíticas de datos, IA, y otras tecnologías para ayudar a mejorar la atención al paciente.

En el proceso, PSJH está construyendo confianza. Por ejemplo, la organización está colaborando con socios de tecnología para estandarizar las plataformas en la nube y las herramientas de productividad y colaboración a través de sus 51 hospitales y 1,085 clínicas, un movimiento que mejorará el compromiso del proveedor y del paciente y permitirá la toma de decisiones clínica y operacional orientada-por-datos. También tiene la intención de desarrollar el primer sistema integrado de reclamos proveedor-pagador empoderado-por-cadena-de-bloques. Tales avances tecnológicos pueden incrementar la confianza – pero el despliegue descuidado y la negligencia pueden rápidamente erosionarlos. Tasta es la razón por la cual Moore se ha duplicado en establecer y mantener un sólido fundamento tecnológico para la innovación y, por extensión, la confianza. “La tecnología es muy prometedora para ayudar pacientes a escala,” dice. “Pero también tiene el potencial para causar daño a escala.”

Por ejemplo, analíticas de datos, IA, y aprendizaje de máquina pueden ayudar a que investigadores y clínicos predigan riesgo crónico de enfermedad y organicen temprano intervenciones, monitoreen síntomas del paciente y reciban alertas si se necesitan intervenciones, estimen más exactamente los costos del paciente, reduzcan atención innecesaria, y asignen personal y recursos más eficientemente. Cuando los pacientes entienden esos beneficios, generalmente están dispuestos a compartir su información personal y de salud con los prestadores de salud. Pero su confianza podría disminuir – o desvanecerse - si protocolos débiles de seguridad o gobierno resultaran en una violación de datos o en uso no-autorizado de información privada sobre la salud. Esto podría causar que los pacientes oculten información a los profesionales de atención, pierdan confianza en los diagnósticos, o ignoren recomendaciones de tratamiento.

Los avances tecnológicos pueden incrementar la confianza – pero el despliegue descuidado y la negligencia pueden rápidamente erosionarlos.

Una serie de regulaciones de la industria ayuda a asegurar la privacidad y la seguridad del paciente, y PSJH tiene otro mecanismo efectivo de gobierno y vigilancia: un concilio de patrocinadores, compuesto por clérigos y personal laico, que tiene la *accountability* moral por las acciones de PSJH en el servicio de su misión. Los patrocinadores ayudan a desarrollar guías que aseguran la adherencia a la misión y los valores y asesoran al liderazgo ejecutivo

de la organización y a la junta de fideicomisarios sobre materias relacionadas con tecnología, tales como el uso ético de datos y el impacto de la tecnología en empleados y cuidadores.

"Nosotros trabajamos continuamente para elevar la conciencia del rol que la tecnología tiene en el mejoramiento de la salud," dice More. "Educar y comunicar con pacientes, profesionales de atención en salud, cuerpos regulatorios, y otros *stakeholders* clave puede ayudar a prevenir las potenciales barreras a la rápida experimentación e innovación y nos permite a nosotros – y a nuestros pacientes – a experimentar plenamente los beneficios de la tecnología."

Hacer lo que es correcto: el enfoque estratégico de CIBC para construir confianza y compromiso

CIBC ESTÁ USANDO tecnología para entender y anticipar las necesidades individuales del cliente con la meta de entregar experiencias altamente personalizadas – una iniciativa que ellos denominan Clientnomics™. Terry Hickey,[26] director jefe de analíticas de CIBC, reconoció que algoritmos basados-en-IA podrían entregar las perspectivas del cliente que se requieren para orientar Clientnomics, pero para que sean exitosos, los líderes necesitan entender y compartir con los empleados cómo la IA complementará y apoyará el trabajo que están haciendo, versus reemplazar sus trabajos. Los bancos también necesitan mantener la confianza de los clientes mediante proteger sus datos y gobernar su uso.

A principios de 2019, líderes de los equipos de analíticas, riesgo, y estrategia corporativa del banco colaboraron para desarrollar una estrategia de IA para toda la organización, con el compromiso del comité ejecutivo senior de CIBC y la aprobación de la junta de directores. En el corazón de la estrategia están principios guías que abordan preguntas tales como: *¿Cuándo usaremos la tecnología? ¿Cuándo no la usaremos? ¿Cómo nos aseguramos de que tenemos permiso de nuestros clientes?*

Para reforzar la confianza del empleado, el plan estratégico estableció que el propósito primario de IA sería aumentar las capacidades de los empleados para lograr las metas de la compañía. Los líderes acordaron centrarse en financiar casos de uso de IA que apoyen a los empleados en sus roles y mejoren prácticas que actualmente no estén siendo optimizadas.

Con la estrategia en funcionamiento, el siguiente paso fue construir un proceso de gobierno de IA que asegure que los nuevos proyectos de tecnología cumplen con la estrategia y con los principios guía. Cuando se propone un proyecto nuevo, los stakeholders responden una serie de preguntas que les ayudan a planear y documentar lo que quieren lograr. Esas preguntas cubren un rango amplio de consideraciones éticas, incluyendo metas del proyecto, posibles sesgos inherentes, y permisos del cliente. Los documentos aprobados del proyecto son almacenados en una biblioteca centralizada que reguladores, auditores internos, y otros revisores pueden referenciar para explicar el proceso de pensamiento que está detrás del algoritmo o modelo.

El CIBC también ha desarrollado técnicas analíticas avanzadas para ayudar a gobernar su uso de los datos – por ejemplo, codificando datos del cliente de una manera que no pueda ser objeto de ingeniería reversa a fin de identificar un individuo. El equipo de analíticas también ideó una manera para asignar un puntaje de veracidad de los datos – basado en calidad e integridad de los datos, posible sesgo, ambigüedad, oportunidad, y relevancia – para cada pieza de información que podría ser usada por un algoritmo. Los modelos algorítmicos son diseñados para reconocer y tratar apropiadamente la veracidad de los datos, apoyar interacciones más confiables, dignas de confianza, y comprometedores.

A medida que el equipo de analíticas lanza Clientnomics, los miembros están centrados en desarrollar experiencias personalizadas del cliente apoyadas-por-IA, más que proyectos de tecnología de gran escala. Hasta aquí, han acumulado 147 casos de uso, completando 40 en el primer año.

Por ejemplo, cuando un cliente llama al centro de contacto del CIBC, un modelo predictivo dinámicamente configura el menú interactivo de respuesta de voz, haciéndolo con base en las transacciones recientes del cliente y ofrece la información más relevante en lo alto del menú. El banco intenta cimentar las relaciones del cliente con el tiempo mediante un esfuerzo continuo de interacciones personalizadas.

"En mi rol anterior", dice Hickey, "dediqué una cantidad de tiempo con organizaciones de todo el mundo. Todos hablaban acerca de los beneficios y el potencial futuro de la IA, y algunos completaron pruebas-de-concepto, pero pocos pudieron implementarlos, especialmente en banca y finanzas. Mediante proactivamente abordar cómo usará – y cómo no usará – la tecnología, el CIBC ha acogido los beneficios positivos que puede entregar para empleados y clientes. Todo esto en menos de un año."

Confianza codificada en el DNA de Abbott

EN LA INDUSTRIA de atención en salud, la confianza es un orientador primario del comportamiento del paciente: las organizaciones de confianza tienen una ventaja para influir en los comportamientos que pueden crear resultados de salud más positivos. Para Abbott, una compañía global de atención en salud de 130 años, la confianza está en lo alto de la mente cuando evoluciona y amplía su portafolio de productos de diagnóstico, dispositivos médicos, nutricionales, y medicina genérica de marca, dice la CMO Melissa Brotz.[27]

Con productos orientados-por-tecnología tales como sistemas de monitoreo de glucosa basados-en-sensores, y monitores cardíacos insertables conectados al teléfono inteligente, y desfibriladores y marcapasos de implante conectados a la nube, Abbot asume un enfoque multifacético para la confianza, añade el CIO Mark Murphy.[28] A través de la empresa y sus tecnologías conectadas, esto incluye políticas comprensivas de protección de datos, programas de entrenamiento del empleado, y un ecosistema externo de socios basados-en-confianza, y otros componentes.

Por ejemplo, Abbot está explorando múltiples oportunidades facilitadas-por-datos para mejorar la atención en salud, tales como soluciones de aprendizaje de máquina que combinan datos de desempeño proveniente de las plataformas de diagnóstico de la compañía con datos globales clínicos y demográficos del paciente para ayudar a los proveedores de atención en salud a diagnosticar ataques al corazón.[29] Para salvaguardar los datos y la privacidad del paciente – una faceta central de la confianza – Abbott ha promulgado para toda la empresa una serie de políticas, procedimientos, y programas anuales de entrenamiento y certificación del empleado relacionados con manejo y protección de datos y cumplimiento con mandatos regulatorios nacionales y globales. Los líderes también han hecho inversiones importantes en capacidades de seguridad cibernética y controles inmersos en los diseños del producto, lo cual es crecientemente crítico para una compañía tal como Abbott, con productos y servicios que están fuertemente conectados e integrados – a menudo con otros productos, sistemas, y aplicaciones.

Además, asegurar la confianza del paciente es una responsabilidad que recae en los 103,000 empleados de Abbott, desde la junta de directores y el liderazgo de la sala directiva hasta investigadores, diseñadores de producto, e ingenieros. El liderazgo de la compañía, por ejemplo, está involucrado en grupos de vigilancia y sub-comités de la junta para la seguridad de datos y productos, al tiempo que los empleados participan en rigurosos programas de educación sobre las implicaciones de privacidad de datos, seguridad, y transparencia. "Abbott está centrada a ayudar a las personas a vivir mejor, con vidas más saludables," observa Murphy. "A menudo, la tecnología es el facilitador que nos ayuda a hacer eso, pero ello siempre comienza con el paciente. Nosotros sabemos que cuando construimos tecnología, lo estamos haciendo a nombre de la

persona que la lleva, accede a ella, o vive con ella al interior de su cuerpo. Y ello significa que tenemos que protegerla – segura y responsablemente."

Abbott también se basa en un fuerte ecosistema externo para mantener la confianza del paciente. Terceros independientes y grupos de investigación prueban los productos y servicios de Abbott y valoran sus vulnerabilidades sobre una base continua. Por ejemplo, la compañía hace parte de la iniciativa #WeHeartHackers, una colaboración entre comunidades de dispositivos médicos e investigación de seguridad que busca mejorar la seguridad de los dispositivos médicos. En un evento reciente, Abbott trabajó en equipo con investigadores universitarios para construir un simulacro de hospital de inmersión que permitió que los investigadores practicaran técnicas de defensa de seguridad cibernética.[30]

Redondeando el ecosistema de confianza de Abbott están los mismos pacientes y proveedores de atención. Para aprender qué significan conceptos tales como confianza, seguridad, y privacidad, para los diferentes usuarios de sus productos y servicios, la compañía regularmente tiene grupos focales con ellos y produce material educativo para elevar la conciencia sobre esos problemas.

En últimas, dice Brotz, las tecnologías facilitadas-por-datos que ayudan a que las personas vivan mejores vidas son una extensión de los productos y

"Nosotros sabemos que cuando construimos tecnología, lo estamos haciendo a nombre de la persona que la lleva, accede a ella, o vive con ella al interior de su cuerpo. Y ello significa que tenemos que protegerla – segura y responsablemente."

servicios que salvan vidas en que los pacientes y sus proveedores de atención han confiado durante 130 años. "Los pacientes colocan en nosotros los niveles más altos de confianza, y nosotros tomamos ello muy en serio," dice ella. "Hace parte de nuestro DNA. Nuestra mayor responsabilidad es mantenerlos a ellos y a sus datos seguros y protegidos."

Reconstruyendo la seguridad desde cero para mantener la confianza del cliente

DADO QUE EL enfoque de la compañía para con la tecnología afecta directamente la confianza del *stakeholder* en su marca, los negocios que estén aprovechando tecnologías avanzadas pueden beneficiarse de considerar el impacto de las tecnologías en los socios del ecosistema, empleados, clientes, y otros *stakeholders* clave. Los controles y prácticas de seguridad son elementos fundamentales para construir y mantener la confianza del *stakeholder*. Reconociendo el impacto que las violaciones de seguridad tienen en la confianza del cliente, Google fue más allá de las apuestas esperadas en la mesa, haciéndolo mediante rediseñar su modelo de seguridad para proteger los sistemas y datos de la empresa.

Hace una década, en la medida en que Google movió hacia la nube aplicaciones y recursos internos, su perímetro de seguridad fue expandiéndose y cambiando constantemente, complicando la defensa del perímetro de su red. Al mismo tiempo, las compañías estuvieron viendo ataques más sofisticados por parte de hackers patrocinados por estados-nación, probando los límites del modelo de seguridad basado-en-el-perímetro. Por consiguiente, Google decidió revisar por completo su enfoque de seguridad e implementó un nuevo modelo de seguridad que dio vuelta al estándar de seguridad existente, dice Sampath Srinivas, director de administración de producto de Google para seguridad de la información.[31]

Los expertos en seguridad de Google ya no podrían asumir que bloquear la red proporcionaría la seguridad requerida para mantener la integridad del sistema y la confianza del cliente. Buscan reinventar la estructura de seguridad existente en la compañía, dado que el modelo tradicional de castillo-y-foso – basado en un perímetro seguro de red don acceso del empleado basado-en-VPN – ya no era adecuado. La meta: asegurar que los empleados podrían usar cualquier corporación corporativa desde cualquier localización en cualquier dispositivo tan fácilmente como si estuvieran usando Gmail y tan seguros como si estuvieran en una oficina de Google.

Google acogió el concepto de confianza cero, un modelo innovador de seguridad que elimina la confianza basada-en-la-red, dice Srinivas, en lugar de aplicar controles de acceso a las aplicaciones con base en la identidad del usuario y el estado de sus dispositivos, independiente de su localización de la red.

La estrategia de seguridad de confianza cero, de Google, trata cada solicitud individual de la red como si proviniera de internet. Aplica políticas de acceso conscientes-del-contexto a indicios tales como identidad del usuario, atributos del dispositivo, información de la sesión, dirección IP, y contexto de la solicitud misma de acceso, recaudados en tiempo real por un servicio de inventario de dispositivos. Un servidor proxy reverso distribuido protege al servidor objetivo, y encripta el tráfico para proteger los datos en transmisión, y actúa como un motor de reglas sofisticadas que determina derechos de acceso con base en el contexto del usuario y del dispositivo, de manera que está completamente parcheado. Cada solicitud de acceso está sujeta a autenticación, autorización, y encriptado. Para proteger contra suplantación de identidad, la compañía – trabajando con las organizaciones de estándares de la FIDO Alliance – desarrolló y desplegó una nueva forma de autenticación criptográfica de hardware de dos factores denominada Security Keys.[32]

Hoy, el flujo de trabajo de seguridad centrada-en-usuario-y-dispositivo, de Google, permite a los usuarios autorizados trabajar de manera segura desde una red no confiable sin el uso de VPN. El usuario experimenta las aplicaciones internas como si estuvieran directamente en internet. Empleados, contratistas, y otros usuarios pueden tener una experiencia sin problemas de acceso de usuario desde cualquier localización mediante simplemente teclear una dirección de la red – un proceso que dramáticamente reduce la carga de soporte. “Para entregar nuestra meta de mantener la privacidad y la confianza del cliente, tuvimos que mirar más allá de soluciones del status quo, innovar, y asumir riesgos,” dice Sirivans. “Cuando rompimos con la tradición y cambiamos la manera como pensamos acerca de nuestra infraestructura de seguridad, nos permitió desarrollar una manera más efectiva para proteger datos y sistemas.”

MI PARTE

CUANDO HABLO con líderes en el mundo corporativo, ellos a menudo piden consejo sobre cómo construir una marca en la cual clientes y empleados confíen. Cuando hablamos, encuentro que algunos no han pensado de manera cuidadosa acerca de qué entienden por "confianza." Algunos la definen subjetivamente, como un cálido sentimiento difuso. En el otro extremo del espectro, otros asumen que, si un cliente está dispuesto a usar un servicio o producto, esa sola acción implica confianza. Yo considero que ninguna de esas definiciones es completa o exacta.end

DAVID DANKS, PH.D.
PROFESSOR OF PHILOSOPHY AND PSYCHOLOGY, CARNEGIE MELLON UNIVERSITY

Para mí, confianza es la disposición a hacerse usted mismo vulnerable porque usted espera que el sistema más amplio actúe de maneras que apoyen sus valores e intereses. Ello no significa que usted espera que la compañía nunca cometerá un error o experimentará un resultado no deseado. En lugar de ello, lo que es importante es que, si algo va mal, usted confía que la compañía se encargará de ello.

Esta definición aplica incluso si un producto de la compañía no es 100 por ciento confiable. Por ejemplo, es más probable que yo compre en una compañía en la cual confío, aún si su producto ocasionalmente no es confiable, dado que confío en que, si algo está mal, la compañía tendrá cuidado de mí y de mis intereses. Es menos probable que yo compre en una compañía que ofrece un producto altamente confiable si estoy preocupado de que lo inesperado ocurrirá, que tendré que manejar las consecuencias por mí mismo.

Entonces, ¿cómo deben los líderes corporativos enfocar la confianza? El primer paso es pensar a través de los valores relevantes y los intereses tanto de la compañía como de sus *stakeholders.* ¿Cuáles son las cosas que importan para clientes, usuarios, empleados, y accionistas? Esta pregunta respalda la discusión acerca de cómo el producto o servicio podría avanzar, proteger, o deteriorar esos grupos del *stakeholder*.

El segundo paso está relacionado con el diseño. ¿Cómo puede la organización diseñar un producto o servicio que respalde o endose esos valores relevantes? Aquí es donde la ética entra. Desde mi perspectiva, la ética es acerca de hacer dos preguntas: ¿Qué valores debemos tener? Entonces, dados esos valores, ¿qué hará que avancemos hacia ellos? Por supuesto, algunos valores están en conflicto, lo cual empuja a las organizaciones a que piensen acerca del problema de manera diferente. ¿Nosotros podemos diseñar el producto de tal manera que no tengamos que escoger? El enfoque de diseño puede generar productos innovadores y de confianza.

Es imposible evitar totalmente consecuencias inesperadas, pero los líderes que reúnen equipos multidisciplinarios de producto pueden mejorar las cosas a su favor. Un equipo conformado por personas provenientes de una variedad de antecedentes y culturas – que se sienten libres de compartir libremente sus experiencias y opiniones – a menudo puede descubrir soluciones creativas de diseño o potenciales problemas de diseño. Pero cuando el conflicto entre valores es inevitable, los líderes tienen que hacer escogencias inteligentes, auto-conscientes, deliberadas. El líder debe decidir qué es lo más importante para la compañía – y poseerlo.

La mayoría de líderes la conocen la acción correcta a tomar si la meta última es construir confianza. Pero algunos se preocupan más por la reducción de costos. O la eficiencia incrementada. O la velocidad al mercado. La lista continúa. Y eso está bien. Los líderes pueden escoger construir cosas que no incrementen la confianza del usuario, si entienden por qué están haciendo esa escogencia y están dispuestos a aceptar las consecuencias – esperadas o inesperadas. Ocurren problemas cuando los líderes hacen escogencias que dañan la confianza sin darse cuenta de lo que están haciendo.

Otra concepción equivocada que los líderes a menudo tienen es que ser ético está en conflicto con ser rentable. Esta es otra falsa dicotomía. Las compañías han probado que pueden elaborar productos confiables, poderosos, amigables para el usuario – y rentables. Y si bien los productos no se pueden desempeñar perfectamente en todo momento, las compañías de confianza tienen maneras para monitorear y detectar problemas, así como también métodos para abordar problemas rápida y efectivamente.

Mi sueño es que, en 20 años los líderes corporativos no necesitarán preguntarles a asesores en ética y otros asesores acerca de los impactos humanos o sociales que podrían resultar de sus decisiones de diseño de producto. Yo espero que las respuestas serán internalizadas en las culturas corporativas de manera que hacer preguntas tales como "¿Estamos seguros de que esta es una buena idea?" es solo parte de lo que las organizaciones consistentemente hacen.

PERSPECTIVAS DEL EJECUTIVO

ESTRATEGIA

La marca de la compañía es, por definición, un contrato de confianza. Pero en los negocios, la confianza en la marca se puede erosionar de la noche a la mañana. Los CEO y líderes de la sala ejecutiva a través de la organización pueden comunicar la importancia que la confianza tiene para la misión de su compañía y establecer barandillas éticas claras. Además, establecer políticas claras para el uso ético de la tecnología – un primer paso importante para ganar confianza – podría beneficiar su negocio. En últimas, los empleados individuales están actuando con base en su mejor entendimiento y conciencia de las políticas y valores de la organización. Ellos querrán tomar decisiones deliberadas acerca de la confianza que se manifestarán en la estrategia, el propósito y desempeño en el mercado de su compañía. Por otra parte. Si los líderes no se apropian de la agenda de la confianza y la ética, tomarán decisiones de una manera difusa. Los CEO tienen la oportunidad para proporcionar claridad, educación, y comunicación continua. Con toda la empresa alineada detrás de las guías de la sala ejecutiva sobre tecnología ética y confianza, los CIO pueden ayudar a asegurar que las estrategias de tecnología, los esfuerzos de desarrollo, y los enfoques cibernéticos respaldan esas guías.

FINANZAS

Una de las responsabilidades primarias de la función de finanzas es construir y mantener confianza entre clientes, socios de negocio, e inversionistas. Pero las crecientes expectativas de transparencia están haciendo más difícil que finanzas satisfaga esta responsabilidad. Considere este escenario: usando cámaras basadas-en-drones, los analistas identifican un problema potencial en las facilidades de fabricación o distribución de su compañía que su equipo de operaciones puede haber pasado por alta. Los analistas inesperadamente llevan el problema a un boletín sobre las ganancias. Los mercados ahora esperan que las compañías respondan a tales situaciones casi en tiempo real. La falla en hacerlo genera dudas, lo cual a su vez puede erosionar la confianza del mercado. Para satisfacer este desafío, las organizaciones de finanzas probablemente necesitarán recaudar más datos a través de la empresa y desplegar analíticas avanzadas que permitan presentar reportes en tiempo real. También pueden colaborar con pares para educar empleados sobre el valor que la ética y la confianza pueden crear. Finalmente, los CEO serán capaces de ayudar a que sus compañías entreguen el tipo de respuestas detalladas, exactas y oportunas que los mercados – y los analistas e inversionistas que los ven – demandan.

RIESGO

Los vectores de amenaza del riesgo cibernético han evolucionado rápidamente, y los ataques se han vuelto crecientemente sofisticados, deliberados, y de naturaleza implacable. El cincuenta y siete por ciento de las compañías que participaron 2019 Future of Cyber Survey, de Deloitte, experimentó sus más recientes incidentes cibernéticos en los últimos dos años. Y el riesgo no solo es que los incidentes cibernéticos destruirán confianza en el sentido clásico. El costo de oportunidad de que las vulnerabilidades cibernéticas puedan impedir que las organizaciones hagan puede ser aún mayor: el espectro del crimen cibernético y sus efectos adversos puede arrojar una sombra sobre los esfuerzos de la organización para hacer un mejor uso de la tecnología, estrangular la organización y ralentizando los esfuerzos de transformación digital. También puede afectar la línea de resultados, rápida y dramáticamente, una encuesta encontró que el 48 por ciento de quienes respondieron habían dejado de usar servicios en línea que reportaron violaciones de datos. Los problemas de tecnología ética y confianza constantemente capturarán la mentalidad del CXO. Los CIO tienen la responsabilidad de ayudar a que otros líderes de la empresa se vuelvan más expertos en tecnología y entiendan el impacto que sus estrategias digitales pueden tener en marca de confianza de la organización.

¿ESTÁ USTED PREPARADO?

1. ¿Cuál es su posición actual de confianza con sus empleados, clientes, socios, accionistas, y comunidad?

2. En una escala de "¿Qué es tecnología ética?" a "Entendemos las implicaciones éticas de nuestras iniciativas de tecnología" a "Tenemos en funcionamiento políticas de tecnología ética," ¿dónde se califica su equipo de liderazgo?

3. ¿Usted mide cada nueva iniciativa digital contra su alineación con los valores organizacionales y el impacto en la confianza del *stakeholder*?

LÍNEA DE RESULTADOS

Las compañías que todavía tienen que reconocer que la tecnología disruptiva puede mediblemente afectar – positiva o negativamente – cada faceta del riesgo de negocios, están siendo eclipsadas por los competidores que hacen de la confianza una misión crítica del negocio. Los líderes deben estar pensando acerca de las potenciales consecuencias de emplear tecnologías disrputivas a través de su organización. Para dominar la ecuación de la confianza, lo que se necesita es un esfuerzo cohesionado que comienza desde lo alto de la organización: alinear el uso de la tecnología con los valores organizacionales, articular claramente las políticas y quías que todos deben seguir, e incrustar esas políticas en el tejido de la organización.

APRENDA MÁS

ACCELERATING DIGITAL INNOVATION INSIDE AND OUT

Aprenda cómo las organizaciones maduras usan ecosistemas y equipos multifuncionales para innovar de maneras nuevas.

RESILIENT PODCAST SERIES

Escuche este postcast ganador de premios que destaca conversaciones con líderes que han hecho frente a riesgo, crisis, y disrupción.

ETHICAL TECHNOLOGY USE IN THE FOURTH INDUSTRIAL REVOLUTION

Explore estrategias de liderazgo para confrontar problemas éticos asociados con tecnologías de Industria 4.0

Autores

CATHERINE BANNISTER es director administrativo de Deloitte Services LP y lidera el desempeño y desarrollo de profesionales de Deloitte. También es el arquitecto del programa Tech Fluency, de Deloitte, que se originó en la práctica de Technology, de Deloitte Consulting LLP, para desarrollar y cultivar la profundidad y amplitud de las capacidades técnicas, así como también del programa Tech Savvy, de Deloitte, permitiendo que profesionales de Deloitte estén familiarizados con las tecnologías disruptivas.

DEBORAH GOLDEN es directivo de Deloitte & Touche LLP y líder de US Cyber Risk Services, de Deloitte. Tiene más de 25 años de experiencia en tecnología de la información en industrias que incluyen gobierno y servicios públicos [government and public services (GPS)], ciencias de la vida y atención en salud, y servicios financieros para el rol, y previamente sirvió como líder cibernético de GPS, de Deloitte, así como también líder de oferta de mercado de GPS Advisory. Golden también sirve en las juntas asesoras de Virginia Tech's Business Information Technology and Masters in Information Technology.

CONTRIBUYENTES SENIOR

Dan Frank
Principal
Deloitte & Touche LLP

Kirsty Hosea
Partner
Deloitte Touche Tohmatsu

Dalibor Petrovic
Partner
Deloitte LLP

Yang Chu
Senior manager
Deloitte & Touche LLP

Anand Ananthapadmanabhan
Manager
Deloitte & Touche LLP

Anu Widyalankara
Manager
Deloitte MCS Limited

Notas finales

1. Nancy Albinson, Sam Balaji, and Yang Chu, *Building digital trust: Technology can lead the way*, Deloitte Insights, September 23, 2019.
2. Edelman, "2019 Edelman Trust Barometer," January 20, 2019.
3. Diana O'Brien et al., *2020 Global Marketing Trends: Beyond technology to connection*, Deloitte Insights, October 15, 2019.
4. Catherine Bannister, Brenna Sniderman, and Natasha Buckley, "Ethical tech: Making ethics a priority in today's digital organization," *Deloitte Review*, January 27, 2020.
5. Gerald C. Kane et al., *Accelerating digital innovation inside and out*, Deloitte Insights, June 4, 2019.
6. Deloitte, *AI ethics: A new imperative for businesses, boards, and C-suites*, accessed August 30, 2019.
7. Albinson, Balaji, and Chu, *Building digital trust*.
8. Cynthia Dwork and Vitaly Feldman, "Privacy-preserving prediction," Conference on Learning Theory, 2018; David J. Wu, "Fully homomorphic encryption: Cryptography's holy grail," March 27, 2015.
9. Deloitte, *2019 future of cyber survey*, accessed December 24, 2019.
10. Tracy Kambies et al., *Dark analytics: Illuminating opportunities hidden within unstructured data*, Deloitte Insights, February 7, 2017; Tiffany Hsu, "They know what you watched last night," *New York Times*, October 25, 2019.
11. Diana O'Brien et al., *Are you a trust buster or builder?*, Deloitte Insights, October 15, 2019.
12. Rowland Manthorpe, "Wetherspoons just deleted its entire customer email database—on purpose," *Wired*, July 3, 2017.
13. Ashley Casovan (executive director, AI Global), phone interview with authors, October 4, 2019.
14. David Schatsky et al., *Can AI be ethical?*, Deloitte Insights, April 17, 2019.
15. Deloitte, *Taking a customer-centric approach to a data breach*, July 2018.
16. Microsoft, *The Future Computed: Arti icial Intelligence and Its Role in Society* (Microsoft, 2018), p. 64.
17. Deloitte, *Ethics in the age of technological disruption: A discussion paper for the 2018 True North Conference*, 2018.
18. Kavitha Prabhakar, Kristi Lamar, and Anjali Shaikh, *Innovating for all: How CIOs can leverage diverse teams to foster innovation and ethical tech*, Deloitte Insights, November 18, 2019.
19. Sylvia Ann Hewlett, Melinda Marshall, and Laura Sherbin, "How diversity can drive innovation," *Harvard Business Review*, December 2013.
20. Bannister, Sniderman, and Buckley, "Ethical tech."
21. Deloitte, *Ethics in the age of technological disruption*.
22. Mark MacCarthy, "Planning for artificial intelligence's transformation of 21st Century jobs," *CIO*, March 6, 2018; Rachel Louise Ensign, "Bank of America's workers prepare for the bots," *Wall Street Journal*, June 19, 2018; Genpact, "New ways of working with artificial intelligence," accessed March 27, 2019.
23. O'Brien et al., *Are you a trust buster or builder?*
24. Timothy Murphy et al., *Ethical technology use in the Fourth Industrial Revolution*, Deloitte Insights, July 15, 2019.
25. B.J. Moore (CIO, Providence St. Joseph Health), phone interview with authors, October 10, 2019.

26. Terry Hickey (chief analytics officer, CIBC), phone interview with authors, September 16, 2019.
27. Melissa Brotz (CMO, Abbott), phone interview with authors, November 8, 2019.
28. Mark Murphy (CIO, Abbott), phone interview with authors, November 8, 2019.
29. Nicholas Fearn, "Artificial intelligence can help doctors better detect heart attacks," *Forbes*, September 10, 2019.
30. Joseph Marks, "The cybersecurity 202: Hackers are going after medical devices—and manufacturers are helping them," *Washington Post*, August 8, 2019.
31. Sampath Srinivas (product management director for information security, Google), phone interviewed with authors, November 11, 2019.
32. Eran Feigenbaum, "The key for working smarter, faster and more securely," G Suite, April 2015.
33. Deloitte, *The future of cyber survey 2019*.
34. Jason Reed and Jarad Carleton, *The global state of online digital trust: A Frost & Sullivan white paper*, Frost & Sullivan, 2018.

Editores ejecutivos

Bill Briggs
Global chief technology officer
Deloitte Consulting LLP
wbriggs@deloitte.com

Los más de 20 años de Bill Briggs en Deloitte han sido dedicados a entregar programas complejos de transformación para clientes en una variedad de industrias, incluyendo servicios financieros, atención en salud, productos de consumo, telecomunicaciones, energía, y el sector público. Es un estratega con experiencia profunda de implementación, ayudando a clientes a anticipar el impacto que las tecnologías nuevas y emergentes pueden tener en sus negocios en el futuro – y conseguir ir hacia allá a partir de las realidades de hoy.

En su rol como CTO, Briggs es responsable por investigación, eminencia, e incubación de tecnologías emergentes que afectan los negocios de los clientes y darle forma al futuro de los servicios y ofertas relacionados-con-tecnología de Deloitte Consulting LLP. También sirve como patrocinador ejecutivo del CIO Program, de Deloitte, ofreciendo a CIO y otros ejecutivos de TI perspectivas y experiencias para navegar los desafíos complejos que enfrentan en negocios y tecnología.

Scott Buchholz
Emerging Technology research director and
Government & Public Services chief technology officer
Deloitte Consulting LLP
sbuchholz@deloitte.com

Con más de 25 años de experiencia en innovación e implementación de tecnología, Scott Buchhols se centra en ayudar a clientes a transformar la manera como entregan sus misiones y negocios a través de la tecnología. Apoya organizaciones a través de industrias mediante proporcionar asesoría y perspectivas sobre cómo evolucionar su tecnología y sus organizaciones para mejorar el desempeño, la efectividad, y la eficiencia.

En su rol como CTO de la práctica de Government and Public Services, de Deloitte Consulting LLP, Buchhols trabaja con clientes para implementar innovación a través de un conjunto diverso de áreas, incluyendo modernización del legado, soluciones de eGovernment y eCommerce, y arquitectura de solución.

Como director de investigación de tecnologías emergentes y patrocinador de Tech Trends, ayuda a identificar, investigar y ser campeón de las tendencias de tecnología que se espera tengan impacto importante en el mercado y en los negocios de los clientes en el futuro.

Autores de perspectivas del ejecutivo

ESTRATEGIA

Benjamin Finzi
US Chief Executive Program leader | Deloitte Consulting LLP

Benjamin Finzi es director administrativo de Deloitte Consulting LLP y co-lidera el Chief Executive Program, de Deloitte. Como fundador de la New York's Deloitte Greenhouse® Experience, ha diseñado y facilitado cientos de experiencias de "lab" de inmersión para CEO y sus equipos de liderazgo, combinando principios de estrategia de negocios con ciencia comportamental y pensamiento de diseño para abordar los desafíos de los clientes. Finzi ha estado centrado durante más de 20 años en investigar y entender cómo las compañías tienen éxito en mercados disruptivos.

FINANZAS

Ajit Kambil
CFO Program global research director | Deloitte LLP

Ajit Kambil es el director global de investigación del Chief Financial Officer Program, de Deloitte LLP. Vigila investigación en áreas tales como liderazgo, mercados de capital, y riesgo. Kambil creó CFO Insights, una publicación bisemanal que sirve a más de 38,000 suscriptores, y desarrolló el Executive Transition Lab, de Deloitte, que ayuda a que CXO hagan una transición eficiente y efectiva en su nuevo rol. Es ampliamente publicado en revistas de negocios y tecnología.

Moe Qualander
Principal | Deloitte & Touche LLP

Moe Qualander es directivo de la práctica de Risk & Financial Advisory, de Deloitte & Touche LLP. Tiene más de 20 años de experiencia, especializado en valorar controles internos en operaciones financieras de negocio y TI. Qualander lidera el Center of Excellence, del Chief Financial Officer Program, de Deloitte, centrándose en crear y mejorar relaciones con CFO de clientes. Como decano de la Next Generation CFO Academy, de Deloitte, ayuda a futuros ejecutivos de finanzas con mejorar sus habilidades de liderazgo, influencia, y competencia.

RIESGO

Deborah Golden
US Cyber Risk Services leader | Deloitte & Touche LLP

Deborah Golden es directivo de Deloitte & Touche LLP y lder del US Cyber Risk Services, de Deloitte. Tiene ms de 25 aos de experiencia en tecnologa de la informacin en industrias ue incluyen gobierno y servicios pblicos government and public services (GPS) , ciencias de la vida y atencin en salud, y servicios financieros para el rol, y previamente sirvi como lder ciberntico de GPS, de Deloitte, as como tambin como lder de ofertas de mercado de GPS Advisory. Golden tambin sirve en las juntas asesoras de Virginia Tech's Business Information Technology and Masters in Information Technology.

Autores de capítulo

FUERZAS DE LA MACRO TECNOLOGÍA

Bill Briggs
Global chief
technology officer
Deloitte Consulting LLP
wbriggs@deloitte.com

Scott Buchholz
Government & Public
Services chief technology officer
Deloitte Consulting LLP
sbuchholz@deloitte.com

Sandeep Sharma, PhD
Deputy chief
technology officer
Deloitte Consulting LLP
sandeepksharma@deloitte.com

TECNOLOGÍA ÉTICA Y CONFIANZA

Catherine Bannister
Technology Fluency and
Ethics global director
Deloitte Services LP
cbannister@deloitte.com

Deborah Golden
US Cyber Risk Services leader
Deloitte & Touche LLP
debgolden@deloitte.com

FINANZAS Y FUTURO DE TI

John Celi
Business Agility US leader
Deloitte Consulting LLP
jceli@deloitte.com

Ajit Kambil
CFO Program global
research director
Deloitte LLP
akambil@deloitte.com

Khalid Kark
US CIO Program
research leader
Deloitte Consulting LLP
kkark@deloitte.com

Jon Smart
Business Agility UK leader
Deloitte MCS Limited
jonsmart@deloitte.co.uk

Zsolt Berend
Business Agility senior manager
Deloitte MCS Limited
zsoltberend@deloitte.co.uk

GEMELOS DIGITALES: UNIENDO LO FÍSICO Y LO DIGITAL

Adam Mussomeli
Supply Chain & Network Operations leader
Deloitte Consulting LLP
amussomeli@deloitte.com

Aaron Parrott
Supply Chain & Network Operations managing director
Deloitte Consulting LLP
aparrott@deloitte.com

Brian Umbenhauer
Industrial Products and Construction leader
Deloitte Consulting LLP
bumbenhauer@deloitte.com

Lane Warshaw, PhD
Analytics & Cognitive managing director
Deloitte Consulting LLP
lwarshaw@deloitte.com

PLATAFORMAS DE EXPERIENCIA HUMANA

Tamara Cibenko
US Digital Experience lead
Deloitte Consulting LLP
tcibenko@deloitte.com

Amelia Dunlop
Deloitte Digital chief experience officer
Deloitte Consulting LLP
amdunlop@deloitte.com

Nelson Kunkel
Deloitte Digital chief design officer
Deloitte Consulting LLP
nkunkel@deloitte.com

DESPERTAR DE LA ARQUITECTURA

Saul Caganoff
Platform Engineering chief technology officer
Deloitte Consulting Pty Ltd
scaganoff@deloitte.com.au

Ken Corless
Cloud chief technology officer
Deloitte Consulting LLP
kcorless@deloitte.com

Stefan Kircher
Innovations & Platforms chief technology officer
Deloitte Consulting LLP
skircher@deloitte.com

HORIZONTE SIGUIENTE: UNA MIRADA FUTURA A LAS TENDENCIAS

Mike Bechtel
Managing director
Deloitte Consulting LLP
mibechtel@deloitte.com

Bill Briggs
Global chief technology officer
Deloitte Consulting LLP
wbriggs@deloitte.com

Scott Buchholz
Government & Public Services chief technology officer
Deloitte Consulting LLP
sbuchholz@deloitte.com

Contribuyentes

Mukul Ahuja, Zillah Austin, Randall Ball, Sonali Ballal, Tushar Barman, Neal Batra, Jonathan Bauer, Mike Brinker, Randy Bush, Rachel Charlton, Sandy Cockrell, Allan Cook, Megan Cormier, Amit Desai, Anant Dinamani, Sean Donnelly, Matt Dortch, Deborshi Dutt, Karen Edelman, Michael Fancher, Frank Farrall, Jourdan Fenster, Bryan Funkhouser, Andy Garber, Haritha Ghatam, Cedric Goddevrind, Jim Guszcza, Maleeha Hamidi, Steve Hardy, Blythe Hurley, Lisa Iliff, Siva Kantamneni, Mary-Kate Lamis, Blair Kin, Kathy Klock, Yadhu Krishnan, Michael Licata, Mark Lillie, Veronica Lim, Mark Lipton, Kathy Lu, Adel Mamhikoff, Sean McClowry, JB McGinnis, Meghan McNally, Kellie Nuttall, Melissa Oberholster, Arun Perinkolam, Ajit Prabhu, Aparna Prusty, Mohan Rao, Hannah Rapp, Scott Rosenberger, Mac Segura-Cook, Preeti Shivpuri, Lisa Smith, Gordon Smith, Tim Smith, David Solis, Alok Soni, Patrick Tabor, Sonya Vasilieff, Aman Vij, Jerry Wen, Mark White, Drew Wilkins, Abhilash Yarala, Andreas Zachariou, y Jim Zhu.

Equipo de investigación

LÍDERES

Cristin Doyle, Chris Hitchcock, Betsy Lukins, Dhruv Patel, Andrea Reiner, Y Katrina Rudisel.

MIEMBROS DEL EQUIPO

Stephen Berg, Erica Cappon, Enoch Chang, Tony Chen, Ankush Dongre, Ben Drescher, Ahmed Elkheshin, Harsha Emani, Jordan Fox, Riya Gandhi, Dave Geyer, Maddie Gleason, April Goya, Adhor Gupta, Alex Jaime Rodriguez, Morgan Jameson, Solomon Kassa, Pedro Khoury-Diaz, Emeric Kossou, Dhir Kothari, Shuchun Liu, James McGrath, Hannan Mohammad, Spandana Narasimha Reddy, Gabby Sanders, Joey Scammerhorn, Kaivalya Shah, Deana Strain, Samuel Tart, Elizabeth Thompson, Samantha Topper, Kiran Vasudevan, Greg Waldrip, y Katrina Zdanowicz.

Agradecimientos especiales

Mariahna Moore por lograr con gracia lo imposible año tras año, hacienda que parezca fácil, y asegurando que todos seguimos las reglas. Sus estándares de excelencia continúan ayudando a que *Tech Trends* esté a la altura de su potencial. Y su capacidad para mantenerse fresco, mantener una mano firme en la caña del timón, y siempre tener un plan para navegar los próximos desafíos es inigualable.

Doug McWhirter por consistentemente desarrollar una prosa hábil e incisiva a partir de copiosas corrientes de conciencia, innumerables entrevistas, montones de investigaciones, y estampidas de Pymes. Su ingenio, sabiduría y paciencia ayudan a que *Tech Trends 2020* sea el trabajo de investigación que es.

Dana Kublin por su talento por su talento para conjurar visuales perspicaces, infografías intuitivas y figuras fascinantes de la nada y descripciones poco claras. Su capacidad para sacarnos de nuestras ideas locas y luego mostrarnos una versión mejorada de lo que le contamos mejora todas las tendencias.

Stefanie Heng por su "suave persistencia en el manejo de las actividades del día a día, sin parar y siempre trayendo una sonrisa a todo lo que hace. Su gracia bajo presión y su compromiso inquebrantable para con el proyecto nos ha permitido "conseguir hacerlo."

Caroline Brown, **Tristen Click,** y **Linda Holland** por por su arte profundo, creatividad inspirada y paciencia inmensa. Ya sea que trate con infografías, capítulos o entrevistas, sus talentos colectivos, su atención al detalle y su disposición a hacer un esfuerzo adicional mejoraron *Tech Trends*.

Kaitlin Crenshaw, **Natalie Martella**, y **Camilo Schrader** por un fabuloso año fresco. Su apoyo como parte de la familia de *Tech Trends* ha sido invaluable dado que usted nos ha ayudado a mantenernos en el sendero para entrevistas preparatorias, investigación secundaria, revisiones de contenido, diseños, gráficas, y más.

Mitch Derman, **Tracey Parry**, y **Tiffany Stronsky** por continuar avanzando en nuestro juego de mercadeo, comunicaciones y relaciones públicas. Su disposición a cuestionar, impulsar y compartir sus ideas ha ayudado a llevar nuestro programa hasta el onceavo. Sus esfuerzos para obtener el zumbido correcto en los lugares correctos en los momentos correctos son sorprendentes.

Laura Elias, **Martina Jeune**, y **Faith Shea** por un impacto increíble en nuestro primer reporte de *Tech Trends*. Gtacias por traernos a la mesa nuevas ideas y por ayudarnos a empujar las fronteras de lo que podemos lograr.

Amy Bergstrom, Matthew Budman, **Sarah Jersild**, **Anoop K R**, **Emily Moreano**, **Joanie Pearson**, y todo el equipo de Deloitte Insights. Su increíble asociación con *Tech Trends* nos ayuda a alcanzar nuevos hitos cada año.

Deloitte.
Insights

Suscríbase para actualizaciones de Deloitte Insights en www.deloitte.com/insights.

Siga a @DeloitteInsight

www.deloitte.com/insights/tech-trends

Siga a @DeloitteOnTech

Colaboradores de Deloitte Insights
Editorial: Matthew Budman, Blythe Hurley, Abrar Khan, Rupesh Bhat, Anya George Tharakan, y Nairita Gangopadhyay
Creativo: Anoop K R and Emily Moreano
Promoción: Hannah Rapp
Artes: Vasava

Acerca de Deloitte Insights

Deloitte Insights publica artículos originales, reportes y publicaciones periódicas que proporcionan ideas para negocios, el sector público y ONG. Nuestra meta es aprovechar la investigación y experiencia de nuestra organización de servicios profesionales, y la de coautores en academia y negocios, para avanzar la conversación sobre un espectro amplio de temas de interés para ejecutivos y líderes del gobierno.
Deloitte Insights es una huella de Deloitte Development LLC.

Acerca de esta publicación

Acerca de Deloitte

Documento original:
Chapter: Ethical technology and trust – On: Tech Trends 2020 - Deloitte Insights, January 2020.
https://www2.deloitte.com/us/en/insights/focus/tech-trends/2020/ethical-technology-and-brand-trust.html
Traducción realizada por Samuel A. Mantilla, asesor de investigación contable de Deloitte &Touche Ltda., Colombia.