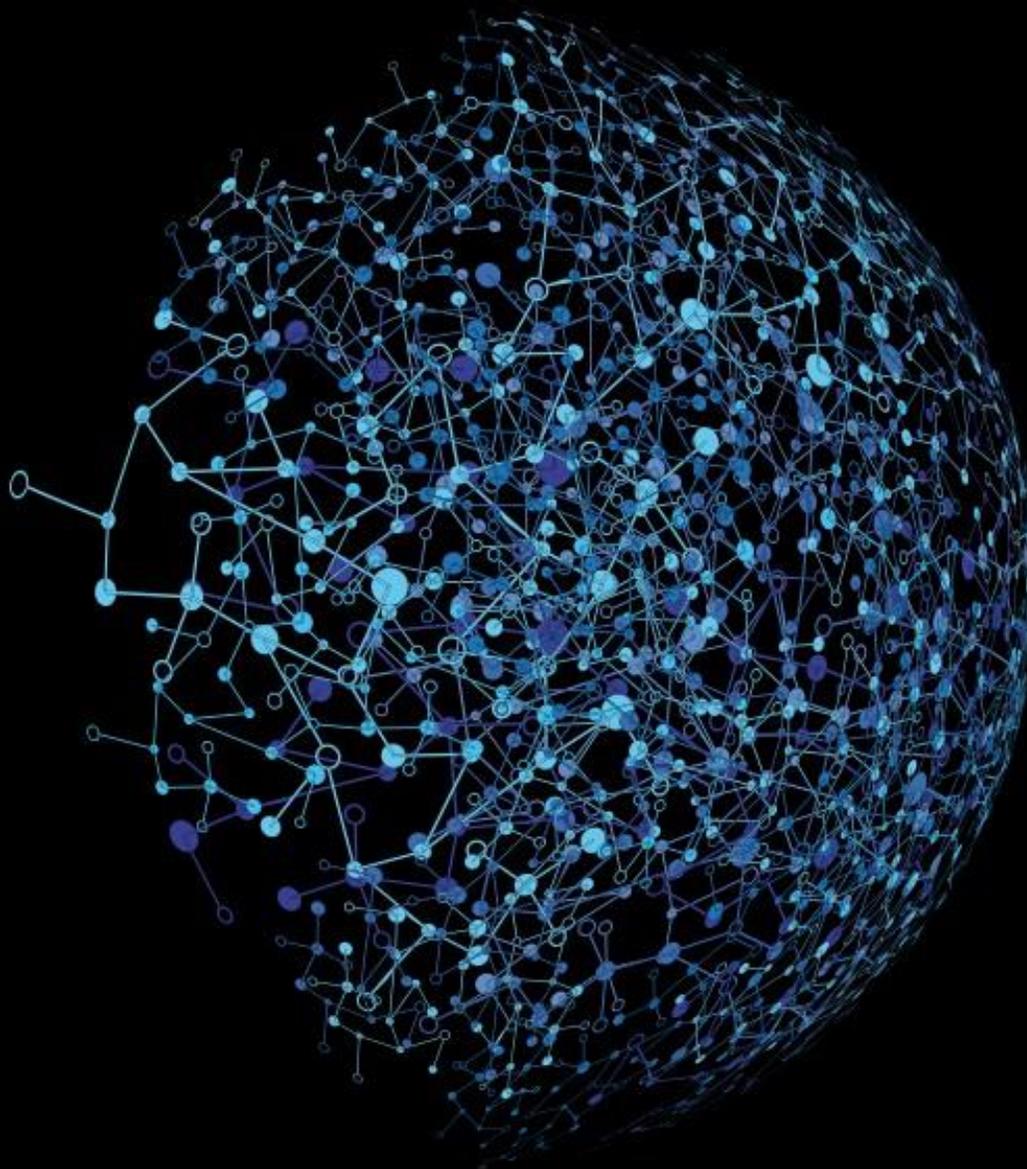


Deloitte.



COVID-19

Personas, tecnología y el camino
hacia la resiliencia organizacional

Contenido

Introducción	1
Respuesta inmediata: Plan, Personas y Consideraciones para los líderes de tecnología	3
Plan: Desarrollo de una estrategia de respuesta	4
Personas: Garantizar la salud, bienestar y productividad	6
Prácticas: Preservar la continuidad del negocio	8
El impacto a largo plazo: Convertirse en un líder resiliente mientras se reinventa el futuro del trabajo	10

El 11 de marzo de 2020, la Organización Mundial de la Salud (OMS) declaró oficialmente el COVID-19 como una pandemia. A medida que el mundo sigue lidiando con la incertidumbre en torno a la propagación del COVID-19 y su creciente impacto en los mercados, las cadenas de suministro y otros pilares de la economía mundial, es importante recordar que este evento es ante todo acerca de las personas, sus familias, su bienestar, y las organizaciones e instituciones de las que dependen y confían en tiempos de necesidad. Desde hospitales hasta bancos, tiendas y transporte, es fundamental que estas organizaciones y empresas sean fuertes y resilientes para que puedan servir a las personas que dependen de ellas para proveer productos, servicios y sustento. Sin embargo, según una encuesta reciente de Forrester, sólo el 43% de los encuestados cree que su organización tiene un plan para hacer frente a una crisis como la pandemia COVID-19¹

Desde que el nuevo coronavirus fue identificado en China a finales de diciembre de 2019, cientos de miles de personas en más de 100 países y regiones han contraído el virus COVID-19, en algunos casos con víctimas mortales². Con un porcentaje cada vez mayor de casos positivos ahora fuera de China continental, así como la propagación sin precedentes del virus en Italia, la propagación del COVID-19 a otras regiones del mundo representa una grave amenaza para la economía mundial. Ya vemos que está interrumpiendo las cadenas de suministro, la operación de negocios y mercados. Es posible que el impacto total del virus en las organizaciones no sea realmente conocido durante meses. Sin embargo, a medida que las ramificaciones del COVID-19 se extienden a través de la economía mundial y el sector financiero, una cosa es cierta: la tecnología está entre las armas más poderosas en las organizaciones para responder con eficacia y decisión a este desafío.

¹<https://go.forrester.com/blogs/fewer-than-half-have-pandemic-plan/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6> <https://gisanddata.maps.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6>

²<https://gisanddata.maps.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6>

Al igual que otros ejecutivos, los líderes de tecnología tienen la responsabilidad de liderar durante esta crisis. Pero más allá de eso, también tienen una responsabilidad crítica para apoyar a toda la empresa, particularmente a medida que los negocios dependen cada vez más de la tecnología. Más allá de asegurarse de que los sistemas centrales estén operativos a lo largo de esta crisis, los líderes de tecnología también deben buscar y apoyar las áreas del negocio que es probable que se vean afectadas, como la cadena de suministro y los recursos humanos. Por ejemplo, es probable que las cadenas de suministro se golpeen duramente, y estos líderes puedan ser capaces de apoyarlos a través de la automatización operativa y la analítica. Con recursos humanos puede haber oportunidades de apoyar a las personas de la organización proporcionando las herramientas y canales de comunicación confiables que necesitan para trabajar en forma remota.

Los líderes de tecnología tienen la oportunidad y la obligación de ayudar a guiar a sus organizaciones a través de esta crisis con su conocimiento y el poder de la tecnología, y deben priorizar sus esfuerzos. La resiliencia de la organización depende de la tecnología y los sistemas de información, por esto los líderes de tecnología deben asumir el papel de un líder de crisis. Es importante recordar que crisis como esta se han presentado en el pasado y lo harán de nuevo en el futuro. Como tal, hay una necesidad de estar preparados, racionales e incluso altruistas a la respuesta. Si hay disrupción, también habrá recuperación, por lo que la forma en que los líderes de tecnología actúan en un momento de crisis también puede dar una visión de cuál será el impacto a largo plazo.

Respuesta inmediata: Plan, Personas y Consideraciones para los líderes de tecnología

Para responder al desafío inmediato que se avecina, los líderes de tecnología deben diseñar sus estrategias y ejecutarlas en tres dimensiones principales: planes, personas y prácticas. Cada uno de estas dimensiones son esenciales para ofrecer una respuesta reflexiva, mantener a las personas seguras y productivas, y crear una organización resiliente.



Plan: Desarrollo de una estrategia de respuesta

Los líderes de tecnología en las organizaciones a menudo son llevados a responder rápidamente a los desafíos tácticos, operativos y logísticos en crisis, como la pandemia COVID-19. Aunque es posible que las organizaciones de TI deban responder rápidamente a problemas, como la mejora de las capacidades de trabajo remoto y la protección de activos críticos, es esencial que establezcan la estrategia y los planes organizacionales para garantizar la resiliencia de la organización. Este enfoque temprano en la planeación puede en última instancia, ayudar a tomar acciones rápidas y eficazmente.

1. **Revise los planes de continuidad del negocio (BC)/recuperación ante desastres (DR)**
Los planes de BC ayudan a garantizar que las personas y los lugares son seguros y operativos, mientras que los planes DR se centran en los datos y las aplicaciones. Evaluar los riesgos y su impacto potencial, desarrollar estrategias de recuperación y tener procedimientos de escalamiento claros son parte de un plan de BC. Planes DR, por otro lado se enfocan en cómo hacer que el entorno tecnológico retorne a la normalidad. Ambos planes requieren pruebas periódicas y actualizaciones continuas para garantizar que sean eficaces y utilizables cuando se ejecuten.
2. **Establezca una oficina de gestión de crisis.** Esto debe ser una estructura permanente y virtual que se activa para eventos como la pandemia COVID-19 y otros incidentes. Disponer de una oficina de gestión de crisis puede ayudar a garantizar que haya pruebas iterativas de los planes de continuidad y recuperación, en vez de hacer ejercicios de actualización una vez cada década. Esta oficina de gestión de crisis es a menudo parte de un equipo inter-disciplinario, el papel de la organización de TI no es sólo riesgos de TI, sino también apoyar a las otras funciones en su respuesta.
3. **Desarrollar un plan de comunicaciones.** El líder de TI debe ser capaz de comunicarse rápidamente y de manera eficiente (buenas y malas noticias) y asumir que los trabajadores pueden no tener sus computadoras portátiles/canales de comunicación de oficina disponibles. Sea inclusivo en sus planes de comunicaciones para incluir infraestructura tecnológica, software y proveedores de servicios, así como proveedores y socios de ecosistemas más amplios. Además, asegúrese de que haya canales de comunicación establecidos con clientes, socios comerciales, su gente, reguladores y otras partes interesadas.

4. **Realice la planeación de escenarios para comprender las necesidades tecnológicas.**
Piense con anticipación en cómo una situación podría presentarse y analice múltiples escenarios posibles. Podría incluir interrupciones masivas en la fuerza de trabajo, cadenas de suministro globales o demanda de bienes y servicios. Algunos de estos escenarios pueden simular varios plazos en la respuesta: estar preparados para una propagación rápida que requiere una acción inmediata frente a una propagación gradual que requiere un enfoque global a largo plazo. Considere la posibilidad de ejecutar pruebas de esfuerzo empresariales para diferentes escenarios epidémicos, que podría incluir un resultado leve y contenido, una epidemia mundial más amplia, o incluso una pandemia, como es el caso de COVID-19.
5. **Definir el papel y las expectativas del liderazgo en la planificación y las comunicaciones.**
Su equipo espera información y soporte precisos y autorizados. También necesita transparencia: tratar de ocultar el riesgo puede potencialmente crear más riesgo. Los actores más importantes en su plan de comunicaciones son sus líderes, así que proporcione una guía clara para ellos y establezca expectativas para ellos. Asegúrese de que estén equipados, preparados y que tengan conversaciones con su gente, socios y demás partes interesadas.
6. **Planifique la vuelta a la recuperación.** Los líderes también deben considerar de antemano cómo reiniciar la interrupción de la operación del negocio, a pesar de que las medidas de prevención y control de la pandemia todavía se están promulgando. Tenga en cuenta que las cuarentenas y las restricciones de viaje, que varían según geografía, podrían hacer que el retorno a la capacidad completa sea un proceso más largo y más complicado de lo que se encontraría en un cierre planeado. Por ejemplo, reiniciar las operaciones puede requerir diferentes niveles de personal, capacidad o turnos de producción, lo que a su vez podría traducirse en flexibilidad, escalabilidad o necesidades de seguridad para la tecnología.
7. **Conozca su organización, roles y prioridades** Prepare planes de sucesión temporal para ejecutivos clave y roles críticos en el negocio. Ya que el COVID-19 se ha extendido a nivel mundial, existe un mayor riesgo de que las personas clave no estén disponibles temporalmente debido a la cuarentena o enfermedad. En caso de enfermedad, la organización de TI debe asegurar que las decisiones se puedan seguir tomando rápidamente y con confianza ante la crisis, y que las operaciones de TI se mantengan. Además, ciertas funciones críticas como la nómina y la gestión de pedidos deben ser priorizadas, no sólo garantizar que los sistemas que los apoyan sigan haciéndolo, sino también asegurarse de que el personal podrá acceder a ellos. Debe haber planes de contingencia para estas operaciones.



Personas: Garantizar la salud, bienestar, y productividad

Garantizar la salud y la seguridad de la gente es la máxima prioridad.

Las organizaciones deben educar a su personal, así como a sus proveedores clave sobre los síntomas del nuevo coronavirus, COVID-19, así como formas de prevenir el contagio. Demostrar su voluntad de escuchar para asegurarse de que los equipos se sientan seguros al hablar sobre dudas que tengan en la realización de su trabajo que ponga en riesgo su salud, o la de los demás.

1. **Hacer cumplir las medidas cautelares y revisar las políticas de licencias por enfermedad.** Primero, eduque a sus trabajadores en los protocolos de detección, contención y contaminación y políticas flexibles de licencia por enfermedad. Si bien los síntomas pueden no ser en última instancia COVID-19 (es decir, resfriado común o gripe), las empresas deben exagerar por precaución en este momento. Pérdida de productividad por la ausencia de varias personas debido a licencias por enfermedad puede ser significativamente menos costoso que cerrar un sitio de oficina, un centro de datos o un centro de servicio debido al personal enfermo. Sin mencionar que antes de que un sitio pudiera ser reabierto, tendría que ser desinfectado.
2. **Revisar/modificar las políticas para el trabajo remoto, incluidas las directrices sobre viajes.** Se sabe que los viajes se han relacionado con varios casos de transmisión de COVID-19. Muchas empresas ya han implementado políticas para restringir los viajes que no son esenciales para proteger a su personal. Siempre que sea posible, deben considerarse los mecanismos de trabajo remotos y flexibles. El desarrollo de directrices apropiadas para los viajes y el trabajo a distancia es esencial para los equipos de proyectos y profesionales de TI orientados al cliente.
3. **Plan para el ausentismo.** El ausentismo aumentará a medida que se refuerzan los protocolos de chequeo, las personas que tienen síntomas están en cuarentena o las que han estado expuestas se han auto-aislado en casa. Las políticas locales de contención también pueden contribuir al ausentismo, escasez, e interrupciones. Tenga en cuenta que los principales proveedores y socios de tecnología, también podrían tener tasas de ausentismo que pueden afectar sus operaciones. Esto puede variar desde cuarentena para aquellos que pueden haber estado expuestos a COVID-19 pero que aún no están mostrando síntomas, a las restricciones de viajes, a los cierres de escuelas que afectarán a los padres de familias jóvenes que no tienen opciones de cuidado alternativo.



4. **Garantice la disponibilidad de recursos críticos a través de la sucesión y la fuerza laboral contingente.** Prepare planes de sucesión para puestos clave en su organización. Como el COVID-19 se ha extendido a más de 100 países (y en aumento), existe un riesgo cada vez mayor de que las personas clave no estén disponibles temporalmente debido a cuarentena o enfermedad. En casos de enfermedad, tendrá que tener listas alternativas claras para seguir con el liderazgo y otras funciones críticas. Debe haber planes a corto y largo plazo para operar la empresa durante al menos los próximos seis meses. Esto incluye la planeación de escenarios, identificación de los responsables en la toma de decisiones, y las rutas de escalamiento para decisiones urgentes.
5. **Establecer canales de comunicación alternos.** Los canales de comunicación regulares pueden no estar disponibles (por ejemplo, debido a una interrupción del centro de datos) o accesibles (por ejemplo, acceso a la tecnología para trabajar). Investigue maneras de llegar a su gente, contratistas, clientes y socios a través de canales alternativos, herramientas y aplicaciones en línea. Además, explore proveedores de comunicación basados en la nube para reducir la dependencia del centro de datos y servidores de correo electrónico de su organización. En algunas partes del mundo, la conectividad a internet y el ancho de banda debe tenerse en cuenta en la estrategia general de comunicación.
6. **Comunicar políticas, expectativas y procedimientos de manera clara (y repetidamente).** El primer paso es revisar y ajustar políticas como licencias, viajes, reuniones y redes sociales. Solamente hacer referencia o adjuntar políticas actualizadas no ayudará. Definir claramente las circunstancias, escenarios y términos tales como viajes esenciales/no esenciales y reforzarlos en comunicaciones posteriores es esencial. Algunas personas sienten que la sobre comunicación podría ser perjudicial para la moral, pero en caso de crisis, la sobre comunicación es mejor que comunicación medida, lo que puede conducir al miedo y a la incertidumbre.



Prácticas: Preservar la continuidad del negocio

Después de desarrollar una estrategia reflexiva y garantizar la salud y el bienestar de su personal, los líderes tienen la obligación de preservar la continuidad de la operación del negocio. Estas son algunas consideraciones para que los líderes establezcan las mejores prácticas.

1. **Racionalice Proyectos de tecnología y portfolios.** Con recursos limitados a su disposición, se debe ser muy claro sobre las prioridades durante una crisis. Las organizaciones de TI a menudo tienen cientos de proyectos andando en un momento dado, además de las operaciones normales del negocio. Tener una visión clara de la priorización y la planificación para detener o continuar proyectos en varios escenarios es importante. Además, dadas las limitaciones de recursos que las organizaciones pueden experimentar durante este tiempo, es posible que se necesite considerar desviar personas y recursos técnicos para mantener las operaciones críticas. Además, una crisis puede llevar a la necesidad de apoyar nuevos proyectos o acelerar proyectos que son importantes para el negocio con el fin de gestionar el riesgo y / o prepararse para el reinicio. Es fundamental para los líderes transmitir las prioridades a sus trabajadores, ayudarles a gestionar la demanda frente a la oferta para del trabajo tecnológico, y tomar decisiones sobre lo que se puede aplazar o se debe priorizar. En el caso del COVID-19 o cualquier otra amenaza para la salud, capacite a los equipos para que sean creativos en la forma como cubren el trabajo no esencial de manera que minimicen el riesgo o la exposición innecesarios.
2. **Equipe su conectividad, seguridad e infraestructura para nuevos patrones de tráfico y uso.** Como se prepara para un mayor trabajo remoto, asegurar que la organización tiene la capacidad tecnológica para apoyar ese trabajo: demandas de ancho de banda, infraestructura VPN, DevOps y autenticación y mecanismos de control de acceso, así como herramientas de seguridad deben ser capaces de soportar las demandas del tráfico pico. También se debe considerar proporcionar VPN/acceso remoto a contratistas y terceros que apoyan servicios críticos y comprar licencias adicionales para herramientas de colaboración como Zoom, Skype, Slack, etc. El repentino aumento de la actividad en línea puede tener grandes implicaciones en el sistema, estabilidad de la red y la seguridad de los datos, especialmente en partes del mundo donde las telecomunicaciones e infraestructura de sistemas no está tan bien desarrollada. Orientar a las personas para que preserven la capacidad del ancho de banda disponible y los recursos, también puede reducir el estrés en los sistemas. Por ejemplo, el uso de Zoom o Skype para 1:1 o reuniones de grupos pequeños, utilizar teléfonos celulares para liberar ancho de banda para reuniones más grandes, o evitar enviar archivos masivos en favor del uso de herramientas como SharePoint y Teams podría ayudar.
3. **Esté preparado para las interrupciones en su negocio y ecosistema tecnológico.** No olvide que su fuerza de trabajo abarca algo más que sus empleados. Es importante considerar el gran contingente de mano de obra de contratistas, subcontratistas y proveedores de servicios. Identifique a todos los proveedores, socios y proveedores de tecnología críticos y asegúrese de que son capaces de soportar los picos y ajustes de demanda. Determine el impacto si dejan de estar disponibles o tienen restricciones de capacidad. Pregunte por sus planes de recuperación de desastres, pandemia y planes de continuidad del negocio para obtener la garantía de su resiliencia.
4. **Prepárese para la operación sin el centro de datos.** Con el cambio a la nube, muchas organizaciones ya están en camino de garantizar que un evento importante en sus centros de datos no interrumpa sus operaciones de negocio críticas. Planificar la contingencia de un cierre del centro de datos, incluso si la infraestructura física está disponible, la posibilidad de no tener a las personas para operar el centro de datos es real. Hacer un balance de las operaciones críticas y evaluar la vulnerabilidad de infraestructura a las restricciones en el hardware físico u otros recursos. Asegúrese de que haya algún tipo de plan de contingencia para mitigar este riesgo.
5. **Comprender e incorporar los requisitos de seguridad, cumplimiento y privacidad en sus planes.** Durante una crisis, es fácil eliminar temporalmente los controles de seguridad o privacidad. Sin embargo, si los riesgos y sus tácticas de mitigación no se han considerado de antemano, puede conducir a vulnerabilidades de seguridad, privacidad o cumplimiento. No tener una VPN mientras se conecta de forma remota, o no tener una autenticación o control de acceso adecuado para aplicaciones críticas, o no encriptación, podría dar lugar a violaciones de seguridad, violaciones de cumplimiento y pérdida de propiedad.
6. **Determine los servicios empresariales críticos y ajuste los acuerdos de nivel de servicio (SLA).** La función tecnológica proporciona muchos servicios críticos al personal, clientes y socios. Cada una de estas partes interesadas tiene expectativas sobre la disponibilidad y los tiempos de respuesta para estos servicios. Priorizar los servicios y garantizar que los SLA se ajusten y son debidamente comunicados en consecuencia reducirá la confusión y el caos.
7. **Asegúrese de que los procedimientos de priorización del servicio de soporte y los planes de contingencia estén en su lugar.** El servicio de soporte es una función crítica que puede permitir a la organización orquestar la agilidad, agudeza y capacidad de respuesta a una crisis como la pandemia COVID-19. El servicio de soporte debe estar preparado para manejar el aumento del volumen de casos, tener una clara priorización y un proceso de escalamiento y enrutamiento. Tener automatización como chatbots y enrutamiento optimizado de las solicitudes y el establecimiento de un centro de mando para los trabajadores remotos puede mejorar la eficacia de la respuesta. Muchas organizaciones pueden aprovechar la ubicación geográfica de su equipo de soporte técnico mediante el desarrollo de una estrategia global para apoyar las áreas afectadas. Por ejemplo, a medida que China vuelve a estar en línea, tener un servicio de asistencia allí podría apoyar otras áreas, como Europa, donde la amenaza del virus puede ser más grave en un momento diferente. Al mismo tiempo, considerar las opciones en las que la funcionalidad del servicio de soporte pues ser proporcionado por personas que trabajan de forma remota.
8. **Esté preparado para las restricciones de flujo de efectivo, pero también esté listo para luchar por inversiones.** Una de las principales implicaciones de la propagación de COVID-19 son las restricciones de flujo de caja en las empresas. El turismo, la hospitalidad, el entretenimiento y el transporte aéreo han sido especialmente afectados a corto plazo. Sin embargo, incluso las empresas que parecen estar en forma financiera pueden no ser inmunes, dependiendo de cómo progresa la situación. La reacción más común es poner en espera todos los proyectos no esenciales, llevando a costos adicionales más adelante. Tener un plan proactivo y preciso para la priorización y el ahorro de costos permitirá restricción de costos más inteligentes. Sin embargo, la organización de TI también debe ser capaz de defender las inversiones en capacidades críticas como herramientas de colaboración, seguridad para apoyar las respuestas a riesgos como el COVID-19, y que pueden no haber recibido financiación o priorización adecuadas en el pasado.

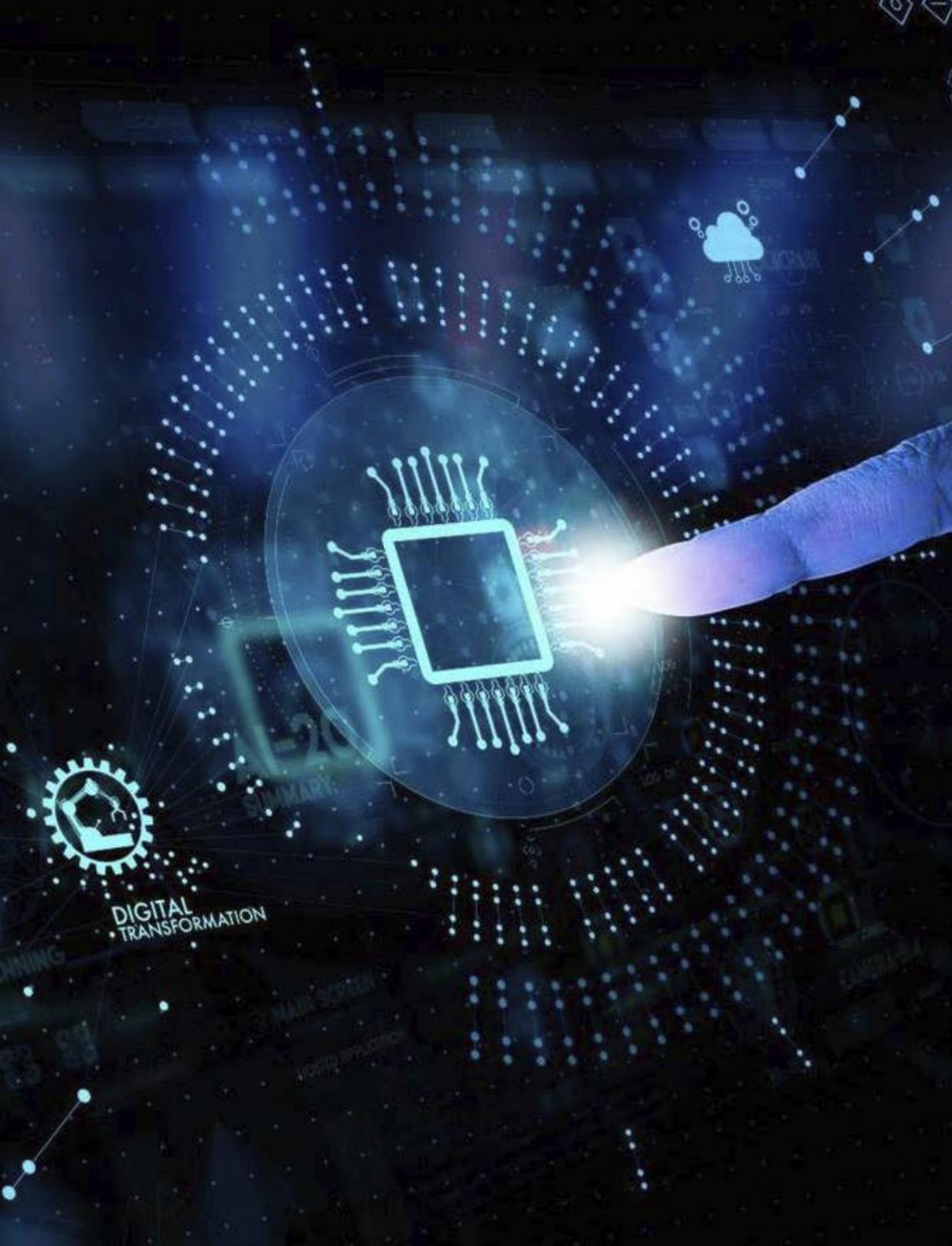
El impacto a largo plazo: Convertirse en un líder resiliente mientras se reiventa el futuro del trabajo

En las crisis, los líderes resilientes se definen primero por quiénes son, y luego por las acciones que toman. Con claridad y determinación, los más resistentes sabrán priorizar su misión. Estabilizarán la situación tomando medidas decisivas, priorizando la velocidad sobre la diplomacia. Sin embargo, al mismo tiempo, proporcionarán el tipo de liderazgo y visión que el momento les demanda, creando una narrativa de un camino claro hacia adelante sin perder la visión a largo plazo. Incluso en momentos de crisis, los líderes resilientes nunca pierden de vista las oportunidades que están en el mediano y largo plazo.

Muchos líderes de tecnología hoy en día están en una posición única para ayudar a sus organizaciones a re-imaginar el futuro del trabajo, de la fuerza laboral y del lugar de trabajo impulsados por la tecnología. Estamos en un punto de inflexión donde las capacidades tecnológicas están listas para transformar cada faceta del trabajo tal como lo conocemos. A través de la automatización, la robótica, la nube y computación cognitiva, el trabajo realizado por los seres humanos cambiará fundamentalmente. Al ofrecer virtualización y habilitación de la empresa extendida, la fuerza de trabajo se transformará. Permitiendo la colaboración, los servicios basados en la nube y el trabajo remoto, el sitio donde se trabaja se alterará para siempre. Esto requiere liderazgo y ejecución visionarios. Y hay una oportunidad de acelerar el futuro del trabajo debido a la crisis que plantea el COVID-19

La buena noticia es que muchos de los principales cambios tecnológicos propuestos están en marcha o deberían estar en marcha para muchas organizaciones. A medida que se desarrolla la crisis actual, hay una oportunidad de acelerar estos esfuerzos. La clave es iniciar ya la habilitación de las soluciones para dar forma a las futuras formas de trabajo, que son más eficientes, eficaces y colaborativas, más allá de los límites de la función de TI y de la empresa. Los líderes de tecnología tienen la oportunidad de mostrar liderazgo con visión y capacidad de ejecución en las siguientes dimensiones.

1. **Ser metódico y disciplinado en la automatización de procesos manuales.** Es claro que la automatización de los procesos clave reducirá la dependencia en seres humanos y mejorará procesos manuales propensos a errores. La oportunidad más obvia y más grande es para los CIO, que pueden identificar formas de automatizar los sistemas y procesos tecnológicos. Casi toda la operación tradicional de TI podría ser candidata para la computación autónoma, lo que realmente significa automatización al siguiente nivel mediante la arquitectura de entornos tecnológicos que se basan en activos virtualizados, contenedores y herramientas avanzadas de monitoreo, moviendo la carga de trabajo sin problemas de soluciones on-premises o plataformas de nube privada. La automatización también tiene el potencial de rediseñar los procesos del negocio para aumentar la eficiencia, la calidad, la velocidad y la dependencia en seres humanos. Muchos han predicho que éste sería el principio del fin para la fuerza de trabajo humana, de hecho, esta automatización da lugar a nuevas clases de empleos para los seres humanos, "super-empleos", que permitirán a las personas utilizar mejor sus fortalezas y crear un valor significativamente mayor para sus organizaciones.
2. **Abogar por un enfoque basado en la nube y migrar agresivamente a servicios en la nube**
Los servicios e infraestructura basados en la nube tienen ventajas obvias, y una pandemia como el COVID-19 lo hace aún más relevante. Proporcionan la comodidad de acceder a servicios desde cualquier lugar, en cualquier momento, desde prácticamente cualquier dispositivo. Se pueden insertar nuevos flujos de trabajo rápidamente para habilitar las capacidades de autoservicio y el proceso y configuración de cambios sobre la marcha. Los proveedores de servicios basados en la nube también tienen la elasticidad de dar soluciones con escalamiento, tales como ancho de banda, y capacidad de procesamiento, basados en las necesidades - una capacidad crítica, especialmente cuando se desconoce el alcance y la escala de la crisis. Adicionalmente en el largo plazo, las soluciones basadas en la nube son fundamentales para que las organizaciones logren un mejor time-to-market, apoyen soluciones de autoservicio para el negocio y proporcionen ambientes de tecnología para la experimentación y la innovación.
3. **Inserción de la colaboración virtual como valor predeterminado.** La última vez que las organizaciones invirtieron fuertemente en herramientas de colaboración fue hace aproximadamente una década en respuesta a la crisis creada por la pandemia de gripe H1N1. Hubo un enorme giro hacia el trabajo remoto. Desde entonces, las herramientas de colaboración han mejorado enormemente, y el ancho de banda y hardware son mucho más baratos y de mayor calidad para videoconferencias. Los dispositivos móviles son mucho más funcionales y las plataformas de colaboración son mucho más intuitivas. Investigar e invertir en estas herramientas no sólo será una buena mitigación de riesgos para la pandemia del COVID-19, sino que también podría permitir una colaboración más fácil, tiempos de respuesta más rápidos y ahorro de costos como resultado de menos viajes.
4. **Concebir nuevas oportunidades de negocio y modos de trabajo.** La pandemia del COVID-19 también puede ayudar a los líderes a repensar los paradigmas establecidos en torno a la presencia física. Industrias como los servicios profesionales y la educación pueden estar maduras para este cambio de mentalidad. La presencia física puede no ser un requisito para ofrecer servicios de consultoría o para tomar un curso en una universidad. Las empresas no solo deben invertir en capacidades de trabajo remoto, sino que también deben replantearse la creación de nuevos modelos de negocio utilizando la presencia virtual.



Como líderes de una función crítica dentro de la empresa, es responsabilidad del líder de TI estar preparado y vigilante. Más importante aún, es una oportunidad para que los líderes de TI lideren el camino y equipar a sus organizaciones para el futuro.

Autores del informe

Khalid Kark
Research Director, Deloitte CIO Program
kkark@deloitte.com

Anh Phillips
Research Lead, Deloitte CIO Program
anhphillips@deloitte.com

Mark Lillie
Partner, Deloitte Global Technology
Strategy & Transformation Leader
mlillie@deloitte.co.uk

Jim Kilpatrick
Partner, Deloitte Global Supply Chain
& Network Operations Leader
jimkilpatrick@deloitte.ca

John Ciaramella
Global Core Business Operations Leader
jciaramella@deloitte.com

Colaboradores

William Briggs
Partner, Deloitte,
Global Chief Technology Officer
wbriggs@deloitte.com

John Tweardy
Partner, Deloitte
US Tech Strategy & Business Transformation Leader
jtweardy@deloitte.com

Tim Paul Smith
Partner, Deloitte
US Tech Strategy & Business Transformation
timsmith6@deloitte.com

Kevin Russo
Partner, Deloitte
Australia Technology
Strategy & Transformation Leader
krusso@deloitte.com.au

Jagjeet Gill
Partner, Deloitte
US Tech Strategy & Business Transformation
jagjgill@deloitte.com

Jack Polson
Chief of Staff, Deloitte Global Technology
Strategy & Transformation
japolson@deloitte.co.uk

Doug McWhirter
Lead Writer, Deloitte CIO Program
dmcwhirter@deloitte.com



www.deloitte.ca

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

Deloitte provides audit and assurance, consulting, financial advisory, risk advisory, tax, and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and service to address clients' most complex business challenges. Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited. Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Our global Purpose is making an impact that matters. At Deloitte Canada, that translates into building a better future by accelerating and expanding access to knowledge. We believe we can achieve this Purpose by living our shared values to lead the way, serve with integrity, take care of each other, foster inclusion, and collaborate for measurable impact.

To learn more about how Deloitte's approximately 312,000 professionals, over 12,000 of whom are part of the Canadian firm, please connect with us on LinkedIn, Twitter, Instagram, or Facebook.

Copyright © 2020 Deloitte Development LLC. All rights reserved.
Designed and produced by the Deloitte Design Studio, Canada. 20-6545T