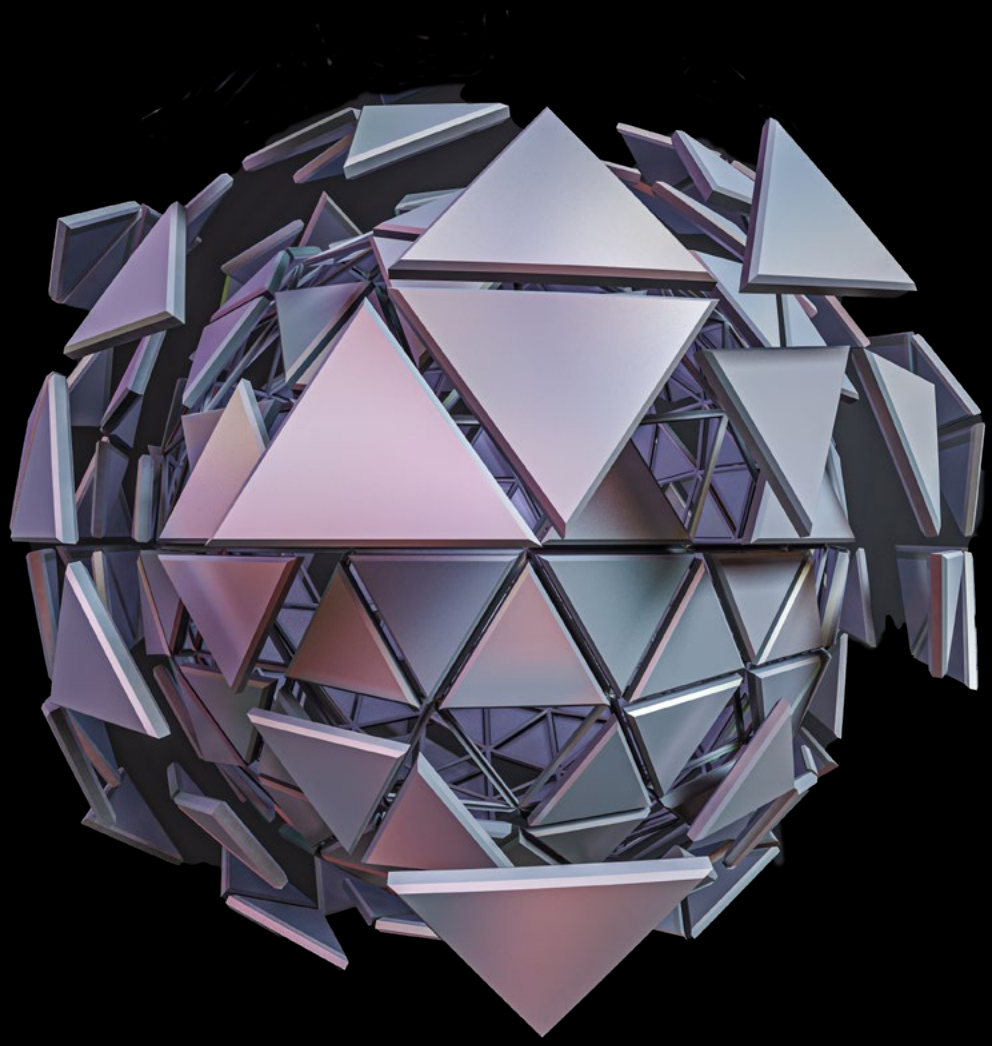
Deloitte.



Evolución de los riesgos y beneficios derivados de la transformación digital

Boletín de Gobierno Corporativo

La transformación digital ha emergido en el panorama empresarial como un fenómeno omnipresente que redefine la forma en que las empresas operan, interactúan con sus clientes y generan valor para mantenerse competitivas y no quedar fuera de mercado.

La adopción de tecnologías emergentes, como inteligencia artificial (IA), robots, automatización de procesos, internet de las cosas (IoT), ***blockchain***, entre otras, ha dado lugar a un cambio en la forma de operar, lo cual no solo implica la adopción de tecnologías avanzadas, sino que también plantea desafíos significativos en la gestión de riesgos, controles y procesos operativos. Estos riesgos y controles requieren comúnmente replantearse luego de un cambio tecnológico, sin embargo, durante los procesos de transformación es importante empezar a medir y mitigar algunos riesgos que surgen de dichos cambios.

A continuación, exploraremos los riesgos más relevantes que emergen de los procesos de transformación digital que las empresas deben observar y analizar, para adoptarlos o ajustarlos en los modelos de gestión de riesgos y en sus procesos de transformación.

01. Ciberseguridad: Uno de los aspectos más destacados de la transformación digital es el incremento en la complejidad y sofisticación de las amenazas cibernéticas y los ciberataques. A medida que las empresas adoptan nuevas tecnologías, la exposición a brechas de seguridad, robos de datos y ciberataques se incrementa. Los modelos de gestión de riesgos tradicionales, centrados en amenazas convencionales, están siendo superados rápidamente. Una respuesta correcta, ajustada a la nueva realidad, implica una reevaluación de los riesgos y la implementación de estrategias proactivas de ciberseguridad que se ajusten a la dinámica del mundo digital.

Por lo anterior, es importante que los equipos de ciberseguridad formen parte de la estrategia y procesos de transformación digital desde su definición, de manera que puedan adoptar tecnologías y mapear nuevamente los riesgos del proceso, sin esperar a que los proyectos culminen para mapear los riesgos. Esto implica no dejar de lado a los equipos de ciberseguridad en los procesos de planeación, ejecución y pruebas de los procesos digitales o de la transformación digital; sino asegurar que participan en la implementación y que su validación será indispensable para la liberación y cambios de procesos.

Los ataques de *ransomware*, los ataques de *phishing* y las vulnerabilidades en los sistemas son solo algunos ejemplos de las distintas formas en las que podemos ser víctimas de ataques cibernéticos.

Los ataques de ***ransomware***, los ataques de ***phishing*** y las vulnerabilidades en los sistemas son solo algunos ejemplos de las distintas formas en las que podemos ser víctimas de ataques cibernéticos, los cuales pueden modificarse al momento de cambiar los procesos y/o implementar nuevas plataformas digitales en las organizaciones.

Las consecuencias de un ataque cibernético son diversas pero todas ellas pueden ser devastadoras para cualquier compañía, siendo algunas de las más comunes: interrupciones operativas, multas o sanciones económicas, pérdida de información y daños a la marca o reputación de la organización.

Si bien las medidas para prevenir un ataque cibernético son diversas y dependen de las operaciones, infraestructura y presupuesto de cada compañía, éstas pudieran dividirse en tres grupos:

- **Implementación de medidas de seguridad**.
- **Capacitación del personal** para concientizar sobre el tema y aumentar las capacidades de prevención.
- **Robustecimiento de los procesos operativos**.

Es responsabilidad, tanto del Director General como de todo el equipo directivo, además del CISO (***Chief Information Security Officer***), garantizar que se cuidan estos riesgos de ciberseguridad al establecer procesos de transformación digital. Asimismo, es responsabilidad del Consejo de Administración y de los Comités de Riesgos, Auditoría o Ciberseguridad, el monitorear el cambio en los mapas de riesgos y supervisar la adecuada gestión conforme a las modificaciones en los procesos digitales.

02. **Seguridad de la información:** Otro de los puntos importantes asociados con la transformación digital es la creciente disponibilidad e importancia de los datos como activos estratégicos. La gran cantidad de datos que circulan en el entorno digital aumenta la necesidad de proteger la información confidencial y personal de los ***stakeholders*** (empleados, accionistas, clientes, proveedores, entre otros).

La gestión eficaz de datos ha tomado un papel que es esencial para el éxito empresarial por el impacto que éstos pueden tener, permitiendo la toma de decisiones informada y sustentada. Sin embargo, esto también requiere que las organizaciones aborden los riesgos asociados con la recopilación, almacenamiento, procesamiento y depuración de la información.

Al igual que en el riesgo de ciberseguridad, una afectación a la seguridad de la información puede tener como consecuencia multas o sanciones económicas y daños a la marca o reputación.

La gestión de riesgos en este contexto implica no sólo la seguridad técnica, sino también el cumplimiento normativo, a partir de un análisis proactivo de los eventos que pudieran amenazar la integridad y confidencialidad de los datos y su dimensionamiento, para el diseño y la adopción de medidas preventivas y correctivas.

Para fortalecer el proceso e incrementar la seguridad, es importante que las compañías revisen la forma en que el cambio en los procesos digitales está incluyendo la captación, administración y control de nuevos datos, así como su gestión y aseguramiento de privacidad, debiendo analizar y adoptar medidas como:

- **Adopción de un enfoque proactivo para la privacidad de datos**, estableciendo procesos claros y transparentes acerca del tratamiento que la compañía dará a la información de sus terceros interesados (***stakeholders***).

La transformación digital alienta el incremento y la sofisticación de los modelos, entre ellos los utilizados para la medición y administración de riesgos, lo cual puede conducir a un incremento en el riesgo de modelo, si este no se encuentra adecuadamente identificado y gestionado.

- **Implementación de acciones preventivas** como puede ser el control de accesos, encriptación, depuración de información, entre otras.

03. **Marca y reputación:** Estamos hablando probablemente del activo más importante de cualquier compañía y, si bien siempre ha sido importante su cuidado, en la era digital las compañías se encuentran más expuestas debido al alcance y a la velocidad de propagación de la información a través de redes sociales.

    Por esta razón, es importante contar con estrategias que consideren el monitoreo de medios, comunicación efectiva e incluso la gestión de crisis de forma que se proteja la marca y la reputación de la empresa.

04. **Fraude digital:** Con el aumento en la utilización de herramientas tecnológicas también se has incrementado el uso de tecnologías digitales para cometer fraudes mediante robos de identidad, robo de información (por ejemplo, tarjetas bancarias) y estafas.

    El fraude digital puede causar pérdidas financieras a las compañías y/o a sus clientes, daños a la reputación y afectar la confianza de los clientes. Por esta razón, es importante implementar medidas como autenticación multifactor, uso de contraseñas robustas, análisis de comportamiento de los usuarios, así como la concientización de terceros interesados sobre este tema.

05. **Riesgo de Modelo:** Este tipo de riesgo está asociado a la potencial pérdida en la que una institución puede incurrir, como consecuencia de decisiones basadas principalmente en la producción y el mantenimiento de modelos analíticos de todo tipo, a causa de errores en el desarrollo, implementación o ejecución de esos modelos.

    La transformación digital alienta el incremento y la sofisticación de los modelos, entre ellos los utilizados para la medición y administración de riesgos, lo cual puede conducir a un incremento en el riesgo de modelo, si este no se encuentra adecuadamente identificado y gestionado. En toda organización que utilice modelos analíticos para la generación de información y la toma de decisiones, debería existir un marco de gestión del riesgo de modelo bien definido e implementado, para evitar o mitigar los impactos operacionales y económicos que pueden derivar de su manifestación.

Beneficios de la transformación digital en la gestión de riesgos:
Resulta, asimismo, fundamental identificar los beneficios de la adopción de las nuevas herramientas digitales traen a las organizaciones. A continuación, se mencionan algunos de ellos:

01. **Disponibilidad de datos en tiempo real:** La digitalización permite que las organizaciones recopilen y analicen grandes cantidades de

La digitalización y/o automatización de los procesos permite a las organizaciones adaptarse más rápidamente a los cambios en el entorno empresarial y responder de manera proactiva a nuevos riesgos emergentes.

información y datos en tiempo real, facilitando la identificación oportuna de oportunidades de mercado e identificación de posibles riesgos, facilitando la toma de decisiones con información más precisa y con la capacidad de hacer modelos predictivos.

02. **Precisión y eficiencia:** Las herramientas digitales, como la inteligencia artificial (IA), pueden ayudar a identificar patrones y/o tendencias en la información, cuyos datos podrían no ser identificados con el uso de métodos tradicionales, mejorando así su precisión, tanto para la estrategia como para la gestión de riegos, y para permitir una asignación más eficiente de los recursos.

03. **Disminución de materialización de riesgos:** Hoy en día existen herramientas tecnológicas y digitales, que permiten la automatización de tareas rutinarias, disminuyendo la ocurrencia de errores humanos y/o manuales y, por lo tanto, disminuyendo la probabilidad de que un riesgo se materialice.

04. **Agilidad y capacidad de respuesta:** La digitalización y/o automatización de los procesos (operativos y de gestión de riesgos) permite a las organizaciones adaptarse más rápidamente a los cambios en el entorno empresarial y responder de manera proactiva a nuevos riesgos emergentes.

En conclusión, la transformación digital está dando forma a una nueva era en la gestión de riesgos empresariales. Las organizaciones, en todos sus niveles de la estructura organizacional -desde accionistas, directores, gerentes, analistas, entre otros deben ser conscientes de las nuevas capacidades habilitadas por el gran avance de la tecnología, así como también de la evolución constante de las amenazas digitales, y adaptar sus modelos de gestión de riesgos para abordar estos desafíos emergentes.

Aquellas compañías que logren integrar estrategias de gestión de riesgos efectivas en este nuevo entorno, no sólo se protegerán contra amenazas potenciales, sino que también estarán mejor posicionadas para capitalizar las oportunidades que la transformación digital trae consigo.

La gestión de riesgos ya no es sólo un componente de la estrategia empresarial, se ha convertido en un pilar fundamental para el éxito sostenible en la era digital.

Contacto:

Daniel Aguiñaga
Socio Líder de Gobierno Corporativo
daguinaga@deloittemx.com
Tel. +52 55 5080 6000

Raúl Malvestiti
Socio Asesoría en Riesgos
ramalvestiti@deloittemx.com
Tel. +52 55 50806619 ext: 6619

Deloitte.

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

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

Tal y como se usa en este documento, Galaz, Yamazaki, Ruiz Urquiza, S.C., tiene el derecho legal exclusivo de involucrarse en, y limita sus negocios a, la prestación de servicios de auditoría y otros servicios profesionales bajo el nombre de “Deloitte”. Deloitte Impuestos y Servicios Legales, S.C., tiene el derecho legal exclusivo de involucrarse en, y limita sus negocios a, la prestación de servicios de consultoría fiscal, asesoría legal y otros servicios profesionales bajo el nombre de “Deloitte”. Deloitte Audit Delivery Center, S.C. (antes Deloitte Auditoría, S.C.), tiene el derecho legal exclusivo de involucrarse en, y limita sus negocios a, la prestación de servicios de auditoría y otros servicios profesionales bajo el nombre de “Deloitte”. Deloitte Asesoría en Riesgos, S.C., tiene el derecho legal exclusivo de involucrarse en, y limita sus negocios a, la prestación de servicios de asesoría en riesgos y otros servicios profesionales bajo el nombre de “Deloitte”. Deloitte Asesoría Financiera, S.C., tiene el derecho legal exclusivo de involucrarse en, y limita sus negocios a, la prestación de servicios de asesoría financiera y otros servicios profesionales bajo el nombre de “Deloitte”. Y Deloitte Consulting Group, S.C., tiene el derecho legal exclusivo de involucrarse en, y limita sus negocios a, la prestación de servicios de consultoría y otros servicios profesionales bajo el nombre de “Deloitte”.

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

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

.