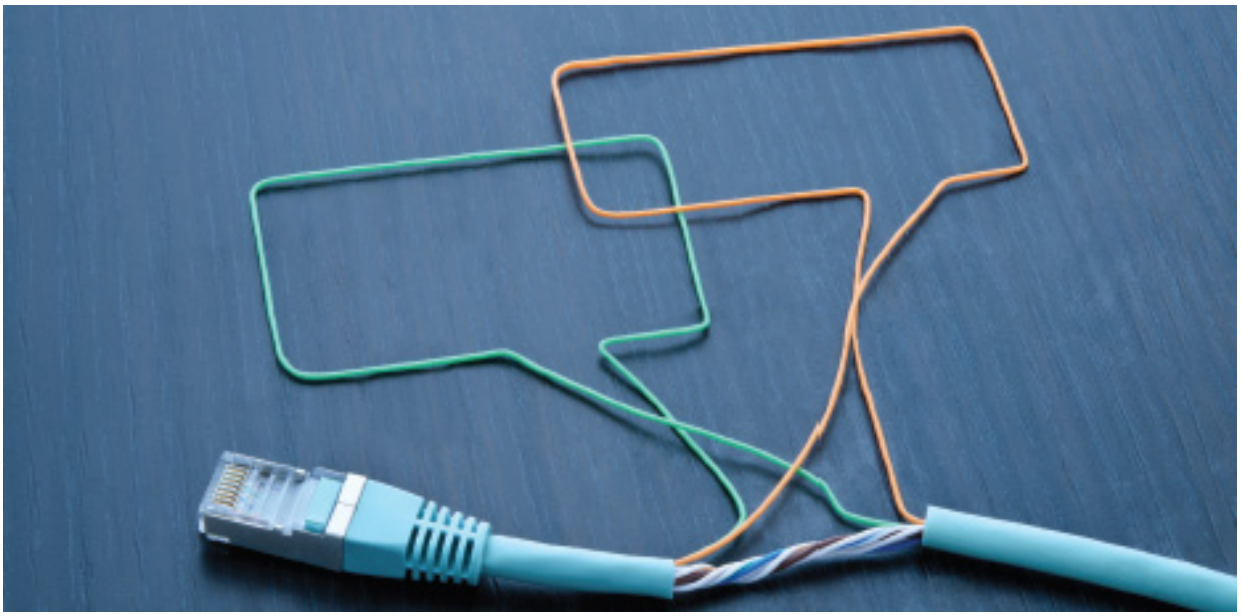
Deloitte.

Los riesgos de la tecnología de la información en los servicios financieros: Lo que los miembros de junta necesitan saber – y hacer

En las compañías de servicios financieros las responsabilidades de la Junta relacionadas con el riesgo se han intensificado, con el riesgo de la tecnología de la información (TI) volviéndose crecientemente crítico. Aun así, el riesgo de TI puede ser el riesgo que el miembro típico de la junta de servicios financieros pueda ser el que menos esté preparado para vigilarlo. Después de todo, pocos directores son escogidos por su experticia el TI, y de alguna manera muchos piensan de manera estrecha acerca del riesgo de TI – esto es, en términos de ataques cibernéticos y disponibilidad del sistema – cuando de hecho los riesgos de TI permean la compañía.

Considere que en el corazón de una institución financiera radica, en esencia, una compañía de tecnología. La tecnología permite virtualmente cada actividad en los servicios financieros y consume una porción enorme de las inversiones de capital y de los gastos operacionales. El desempeño de la institución financiera depende de la confiabilidad y seguridad de su tecnología. La caída del sistema puede maniatar a la institución y a sus clientes. El negocio se basa en datos exactos y oportunos. El panorama cambiante de la tecnología requiere que las instituciones tomen decisiones estratégicas sobre cuáles tecnologías adoptar, y cuáles evitar. Los controles débiles en la tecnología pueden llevar a errores de procesamiento o a transacciones no autorizadas. Y los reguladores en todo el mundo continúan centrándose no solo en la seguridad y la solidez sino también en el cumplimiento con las leyes y regulaciones específicas del país.

Las juntas son responsables por vigilar el riesgo de TI así como también los otros riesgos. En últimas, la administración y el gobierno efectivos del riesgo de TI dependen tanto del equipo ejecutivo senior, que incluye al director de información jefe [chief information officer (CIO)], al director de riesgos jefe [chief risk officer (CRO)] y al director de tecnología jefe [chief technology officer (CTO)], así como también al conjunto amplio de administradores responsables en toda la compañía. Todos los líderes de la organización financiera tienen que entender al riesgo de TI y las palancas disponibles para asegurar que esté siendo abordado de la manera adecuada. Este documento resalta riesgos de TI seleccionados para que las juntas de las instituciones financieras los consideren, y sugiere estrategias que pueden emplear para vigilarlos de mejor manera.



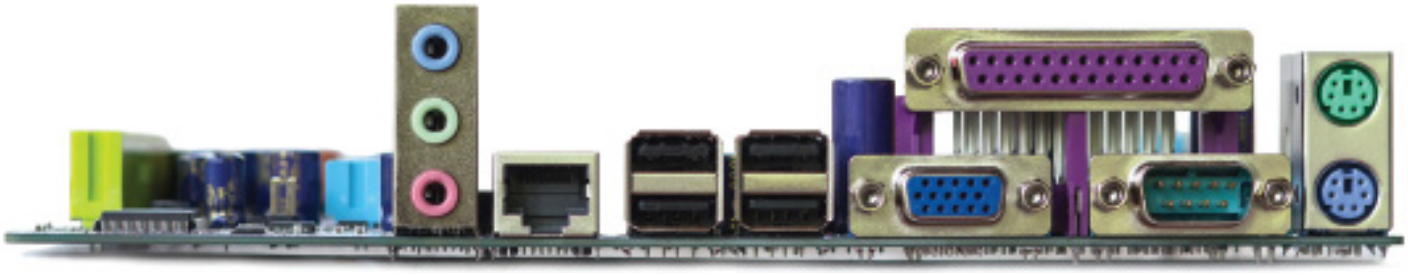
La junta y el riesgo de TI

La tecnología es el gran facilitador, pero también presenta riesgo generalizado, potencialmente de impacto alto. El riesgo cibernético en la forma de robo de datos, cuentas comprometidas, archivos destruidos, sistemas deshabilitados o degradados en estos día está en “la parte superior del pensamiento.” Sin embargo, ese no es el único riesgo de TI por el cual la junta y la administración deben estar preocupados.

Las instituciones financieras enfrentan el riesgo de desalineación entre las estrategias de negocio y de TI, las decisiones de la administración que incrementan el costo y la complejidad del entorno de TI, y el talento insuficiente o no coincidente. La tecnología de las compañías financieras puede volverse obsoleta, sometida a disrupción, o no-competitiva, con los sistemas heredados obstaculizando la agilidad. Las fusiones y adquisiciones pueden de manera irremediable complicar el entorno de TI de la organización – un hecho que muchos equipos de administración fallan en presupuestar y abordar. Mientras tanto, las empresas nuevas [startups] orientadas-a-la-tecnología, así como también las soluciones con tecnología financiera disruptiva (“FinTech”) están desafiando los modelos y procesos de negocio en el corazón de muchas instituciones, haciendo de la rapidez de respuesta un requerimiento para la relevancia y la viabilidad continuas.

El riesgo de tecnología tiene implicaciones estratégicas, financieras, operacionales, regulatorias, y reputacionales. Para abordarlo, los miembros de junta no necesitan volverse expertos en TI, pero necesitan entender suficientemente bien el panorama de la TI para vigilar y cuestionar a la administración.

Para abordar los riesgos de la tecnología, los miembros de junta no necesitan volverse expertos en TI, pero necesitan entender suficientemente bien el panorama de la TI para vigilar y cuestionar a la administración.



Estructura de la administración del riesgo de TI, de Deloitte

Un buen punto de partida para la junta es entender la estructura que la administración usa para administrar al riesgo de TI. Si bien las estructuras varían de institución a institución, una que sea efectiva ayuda a orientar un modelo de operación práctico y consistente a través de todos los dominios de TI para identificar, administrar, y abordar los riesgos. Como ejemplo, en la Exhibición 1 se muestra la estructura, de Deloitte, para la administración del riesgo de TI.

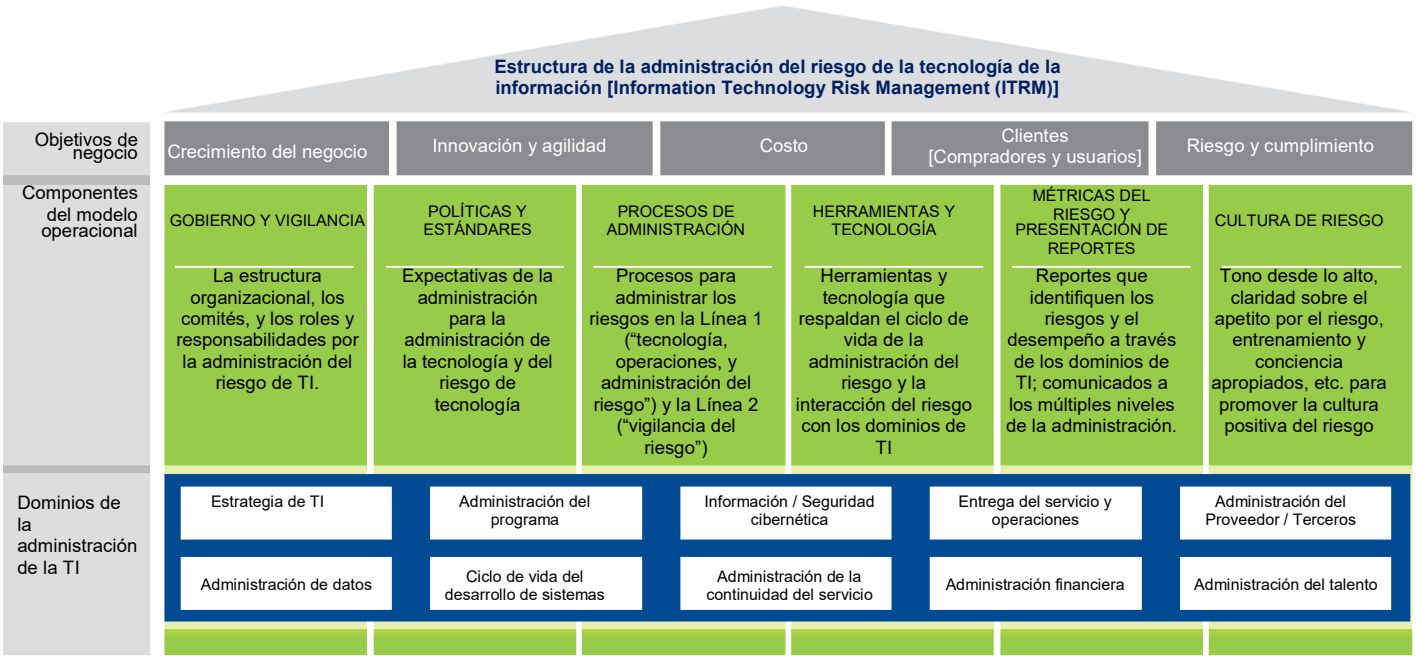
Esta estructura describe – a lo largo del nivel superior – los orientadores clave y los objetivos de la TI en los servicios financieros: facilitar el crecimiento del negocio, lograr innovación y agilidad tecnológica, promover la reducción del costo, respaldar al cliente y al centro de atención puesto en el cliente, y solidificar la administración efectiva del riesgo y el cumplimiento.

El siguiente nivel ilustra los seis componentes del modelo de operación requeridos para respaldar la administración del riesgo de TI a través de la compañía: gobierno y vigilancia, políticas y estándares, procesos de administración, herramientas y tecnología, métricas del riesgo y presentación de reportes sobre el riesgo, y cultura de riesgo.

El nivel inferior identifica los dominios típicos de la administración del riesgo, tales como estrategia de TI, administración de datos, y entrega de servicio y operaciones. Si bien los nombres o la configuración de esos dominios pueden variar de compañía a compañía, son típicos de las actividades requeridas para implementar las capacidades de TI en una organización.

Los riesgos de TI pueden surgir de cualquier nivel dentro de la estructura. Primero, los riesgos pueden surgir de las prioridades que compiten entre los objetivos de lograr crecimiento del negocio, reducir costos, respaldar el centro de atención puesto en el cliente, y similares. Segundo, los riesgos de TI pueden persistir dentro de o ser amplificados por un modelo inadecuado de operación de la administración del riesgo, i.e., inefectivos gobierno y vigilancia, políticas y estándares, procesos de administración, herramientas y tecnología, métricas del riesgo, o cultura del riesgo. Tercero, los riesgos pueden surgir de entrega no sólida de cualquiera de los 10 dominios de administración de la TI aquí descritos, incluyendo estrategia de TI, administración del programa, seguridad cibernética, y similares.

Exhibición 1



Riesgos principales en la tecnología de la información

Para vigilar el riesgo de TI, las juntas tienen que entender los riesgos que la tecnología presenta para la institución, y tienen que preguntar a la administración qué orienta el entendimiento real del panorama del riesgo y establecer dirección y expectativas claras.

Algunos de los riesgos más importantes en tecnología en servicios financieros incluyen:

1. **Riesgo estratégico de TI**
2. **Riesgo de seguridad cibernética y respuesta ante incidentes**
3. **Capacidad de recuperación de TI y riesgo de continuidad**
4. **Riesgo de proveedor de tecnología y de terceros**
5. **Riesgo de administración de datos**
6. **Riesgo de ejecución del programa de TI**
7. **Riesgo de operaciones de tecnología**
8. **Riesgo de administración inefectiva del riesgo**

Lo que sigue sirve como cartilla sobre cada uno de esos riesgos y puede ser usado para orientar conversaciones más significativas con los *stakeholders* clave sobre el riesgo de TI.

1. Riesgo estratégico de TI

En un mundo rápidamente cambiante, el riesgo que emana de una estrategia inefectiva de TI se encuentra entre las principales amenazas que una institución financiera enfrenta. Los ejemplos de riesgos que emanan de la estrategia de TI incluyen:

Acoger versus esperar la nueva tecnología: Las instituciones tienen que balancear el riesgo de adoptar tecnología nueva contra el de ignorarla u esperar que las cosas se resuelvan. Las soluciones en la nube tienen tanto una promesa inmensa como riesgo importante. Las soluciones de FinTech – un centro de mucha innovación en servicios financieros – están generando disrupción en el *status quo*, orientando la competencia incrementada y decisiones importantes sobre asociaciones y adopción de tecnología.

Operar versus construir: TI y el negocio tienen que llegar a un acuerdo sobre el portafolio apropiado de inversiones, de manera específica en que tanto gastar para "mantener las luces puestas en" versus invertir en nueva tecnología y capacidades. Gastar excesivamente en mantenimiento puede desplazar oportunidades para adoptar nueva tecnología y desarrollar nuevas capacidades.

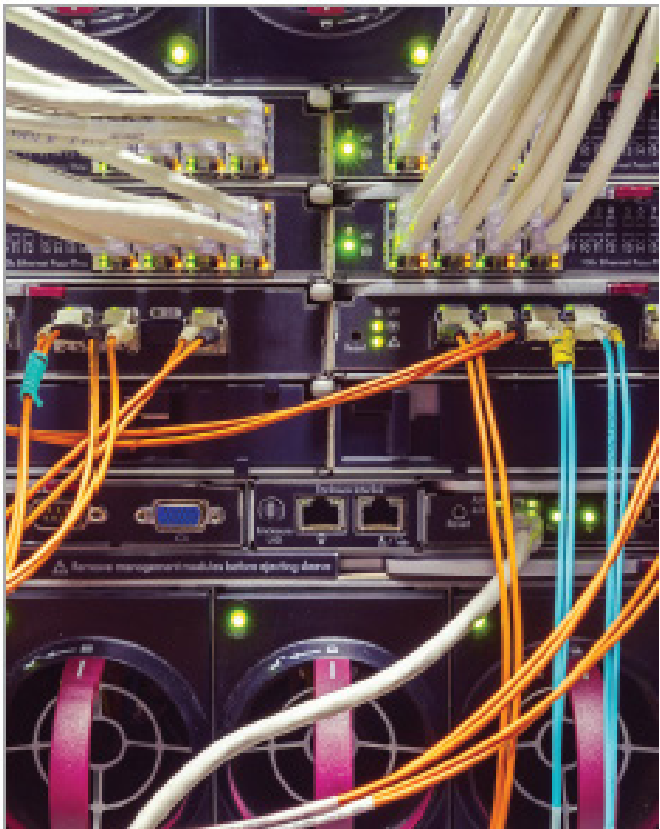
Carencia de integración entre las estrategias de TI y las estrategias de negocio: La falla en integrar las estrategias de negocio con las estrategias de tecnología pueden llevar a inversiones inapropiadas y a expectativas desalineadas. La estrategia de TI tiene que respaldar las prioridades de negocio en evolución y los modelos de operación también en evolución, y permitir respuestas ágiles ante los desarrollos del mercado.

Tecnología heredada: Las instituciones financieras continúan esforzándose en inutilizar o eliminar las tecnologías desactualizadas que incluyen centros de datos, plataformas y aplicaciones. A menudo la tecnología retenida para respaldar geografías seleccionadas, productos personalizados, o procesos únicos generan complejidad incrementada y costos más altos. Cuando esto ocurre sobre cientos o incluso miles de aplicaciones, la organización puede encontrarse paralizada por su propia tecnología.

Evitar las verdades duras: Las fusiones y adquisiciones multiplican las aplicaciones en portafolios de tecnología cuando la administración se centra en ahorros de costos de corto plazo más que en simplificar y actualizar el entorno de TI. En muchos casos, pueden requerirse fuertes inversiones para abordar años de haber evitado los desembolsos requeridos para un entorno sólido y eficiente.

Preguntas para que la junta plantee:

- ¿Cuál es la estrategia de TI de nuestra organización, particularmente en lo que se relaciona con respaldar nuestros negocios, ofertas, y clientes y otros *stakeholders*?
- ¿En general, como organización deseamos ser un innovador en servicios financieros facilitados por TI o tomar la ruta más conservadora y ser adoptadores tardíos? ¿Qué necesitamos tener en funcionamiento para administrar los riesgos inherentes en cada estrategia?
- ¿Nosotros monitoreamos el mercado por los desarrollos que podrían ofrecer oportunidades o riesgos para nuestro negocio?



2. Riesgo de seguridad cibernética y respuesta ante incidentes

Muchos reportes de ataques cibernéticos, rupturas de la privacidad de los datos, y mala conducta de compañías importantes han colocado la seguridad cibernética en lo alto de las agendas de las juntas. Los directores necesitan entender el punto de vista que la administración tiene de los ataques cibernéticos, la potencial probabilidad y los impactos de los eventos de riesgo, y los pasos dados para abordar los riesgos. Ni es práctico ni es posible proteger igualmente todos los activos digitales; además de tener capacidades cibernéticas fundamentales a través de la institución, las "joyas de la corona" deben ser identificadas y protegidas adicionalmente. La administración tiene que estar vigilante en la identificación de las amenazas emergentes y en la implementación de mecanismos efectivos para mitigarlas. Finalmente, la vigilancia en la seguridad cibernética – controles de acceso, protocolos de seguridad, y similares – no deben ocultar el objetivo de la institución de ser fácil hacer negocios con ella. Ello puede ser un balance difícil de lograr.

La respuesta ante el incidente cibernético [Cyber incident response (CIR)] golpea cuando la seguridad cibernética falla, lo cual casi seguramente se dará de tiempo en tiempo. La probabilidad alta de un incidente cibernético señala que la administración tiene que tener un plan de CIR sólido, bien probado, listo para ser lanzado cuando se detecte un incidente. Las respuestas deben ser proporcionales al incidente y cubrir protocolos técnicos, forenses, de comunicación, y de cumplimiento. Las prioridades pueden incluir asegurar la evidencia digital, restaurar operaciones, y notificar a la administración senior, a los *stakeholders* afectados, y quizás, a quienes hacen forzoso el cumplimiento de la ley y a las autoridades regulatorias.

Preguntas para que la junta plantee:

- ¿Tenemos en funcionamiento el modelo correcto de *accountability* para la seguridad cibernética? ¿Tenemos la financiación y el talento correctos?
- ¿Hemos identificado las "joyas de nuestra corona"? ¿Qué hemos hecho para protegerlas?
- Conociendo el panorama en evolución del riesgo cibernético, ¿cuáles son nuestras mayores exposiciones y qué inversiones se requieren?
- ¿Para cuáles escenarios cibernéticos tenemos en funcionamiento controles?
- ¿Hemos probado nuestro plan de respuesta ante el incidente cibernético?
- ¿Estamos bien ensayados?
- ¿Qué inversiones son requeridas para remediar y actualizar nuestro entorno de TI heredado?

3. Capacidad de recuperación de TI y riesgo de continuidad

Con la tecnología facilitando virtualmente cada actividad en los servicios financieros, la TI de la organización tiene que tener capacidad de recuperación ante disrupciones y cortes. La organización debe tener estándares de capacidad de recuperación de manera que las inversiones en capacidad de recuperación se dirijan a la tecnología que respalde sus procesos de negocio más críticos. La prueba de la recuperación, especialmente para la tecnología crítica, tiene que ser rigurosa y tiene que verificar que los planes de recuperación funcionarán.

Las instituciones necesitarán un punto de vista de extremo-a-extremo de toda la tecnología requerida para respaldar un producto o proceso particular para validar que todos los componentes se puedan recuperar de una disrupción. A veces, las instituciones realizan la prueba de una sola vez de una aplicación particular de tecnología, más que probar de manera comprensiva toda la tecnología requerida para respaldar procesos de extremo-a-extremo tales como compensación o liquidación. Finalmente, las instituciones que para servicios críticos de tecnología confíen en proveedores externos tienen que entender la capacidad de recuperación de esos terceros como si la tecnología fuera propia y operada por la institución.

Preguntas para que la junta plantee:

- ¿Hemos definido nuestros procesos de negocio críticos y hemos identificado los activos de tecnología – aplicaciones, infraestructura, y terceros – más esenciales para respaldarlos?
- ¿Qué escenarios hemos planeado y probado? ¿Hemos planeado por cortes de tecnología extendidos y/o recurrentes?
- ¿Hemos entendido los puntos de falla individuales [single points of failure (SPOFs)] en nuestro entorno de tecnología?
- ¿Hemos experimentado cualesquiera situaciones en que éramos incapaces de responder a un corte de tecnología dentro de nuestras franjas de tiempo planeadas? ¿Nuestros procesos de prueba no identificaron esta debilidad?
- ¿Qué pasos necesitan darse para reducir el número y el tiempo medio de los cortes?
- ¿Estamos preparados si múltiples sistemas fallan al mismo tiempo y sabemos qué sistemas dependen unos de otros?

4. Riesgo de proveedor de tecnología y de terceros

Como los acuerdos con vendedores y proveedores de servicio, socios de negocios conjuntos, y otras partes que son terceros proliferan en los servicios financieros, así también los riesgos. Además, el propio riesgo de tecnología de terceros puede generar riesgos operacionales, financieros, de reputación, y otros riesgos para las instituciones que usan sus servicios. El entendimiento claro de esos riesgos puede ser oscurecido por imperativos de negocio y por el entusiasmo de la relación, por formas estándar de aseguramiento proporcionadas por vendedores, y por procesos de debida diligencia que consisten en verificar-la-caja.

La institución financiera como un todo tiene que desarrollar e implementar procedimientos adecuados de debida diligencia, contratación, y monitoreo para todas las partes, incluyendo los proveedores de tecnología contratados por TI. Debida diligencia tiene que ser realizada sobre la reputación, la alineación estratégica, la viabilidad financiera, el cumplimiento, y otros atributos del tercero.

Además, TI tiene que asumir el liderazgo en las valoraciones de las capacidades de TI de terceros, si el tercero apoya TI o el negocio. Si bien muchas instituciones tienen capacidades maduras para valorar el riesgo cibernético y de continuidad de negocios del tercero, también deben entender la efectividad de los procesos de administración de tecnología del tercero. Por ejemplo, procedimientos inefectivos de administración del cambio en un tercero pueden incrementar el riesgo de disrupción del servicio.

Preguntas para que la junta plantee:

- ¿Cuáles son los principales riesgos de TI asociados con proveedores de servicio, socios de negocio, vendedores, y otros terceros de la institución?
- ¿Cuáles son nuestros procesos para la diligencia debida – y el monitoreo subsiguiente – de los riesgos de TI de terceros?
- ¿Tenemos adecuada vigilancia de los proveedores con relación a sus capacidades de recuperación?

5. Riesgo de administración de datos

La administración inefectiva de los datos en una institución financiera puede abrir la puerta al fraude financiero, a problemas de presentación de reportes de contabilidad y regulatorios, y a pérdida de la confianza de los *stakeholders*. Las agencias reguladoras están expresando fuerte interés en las capacidades de administración de datos, dado que la administración del riesgo y del capital dependen de datos confiables, exactos, y oportunos. Además, las instituciones financieras de manera creciente están combinando datos externos con datos internos, adicionando nuevos niveles de complejidad a la administración de los datos y, potencialmente, nuevos riesgos.

Las capacidades rigurosas de administración de los datos recaen en el gobierno de los datos, la política, y los procedimientos que respaldan la exactitud, confiabilidad, y oportunidad de los datos, y aclaran la propiedad de los datos, el uso y la alteración. La creación, transformación, almacenamiento, y disposición controlados de los datos es central al concepto de integridad de los datos.

Cuando las instituciones retienen datos innecesarios, enfrentan adicionales costo, complejidad, y riesgo que podrían de que podrían ser violados. Las instituciones deben tener política y estándares que respalden la disposición sólida de datos, y aseguramiento de que esa política está siendo puesta en práctica.

Preguntas para que la junta plantee:

- ¿Qué tan efectivos son nuestra política y nuestros estándares de administración de los datos?
- ¿Los elementos críticos de los datos están identificados en las aplicaciones clave?
- ¿Cómo la calidad de los datos es medida en los servicios clave y en las aplicaciones asociadas?
- ¿Cómo el gobierno de los datos está integrado en procesos de TI tales como ciclo de vida del desarrollo de sistemas, revisiones de arquitectura, y similares?

6. Riesgo de ejecución del programa de TI

En cualquier momento, una institución financiera grande tendrá en desarrollo múltiples programas de TI a través de las funciones organizacionales y las regiones geográficas. Los ejemplos incluyen los sistemas de planeación de recursos de la empresa [enterprise resource planning (ERP)], administración del riesgo de la empresa [Enterprise risk management (ERM)], y administración de relaciones con el cliente [customer relationship management (CRM)]. Esos programas presentan riesgos, tales como sobrecostos en relación con el presupuesto, demoras, y falla en entregar los resultados de negocio que se tienen como objetivo. Los generadores del riesgo incluyen programas desalineados con los objetivos estratégicos, reglamentos del programa que fallan en abordar los riesgos, carencia de gobierno del programa, ejecución irregular, mala asignación de recursos, y carencia de comunicación formal. La administración del programa de TI también es crítica para el éxito de cualquier fusión o adquisición que combinará sistemas de TI.

La administración necesita centrarse en la administración del cambio, así como también en los aspectos técnicos del proyecto y minimizar los supuestos optimistas contenidos en los planes del proyecto. El uso de analíticas para identificar y administrar los riesgos, el pronóstico de los resultados del proyecto, y el identificar las correcciones del curso en la medida en que los proyectos avances constituyen el enfoque emergente. Los métodos de toma de decisiones orientada-por-datos pueden complementar o reemplazar el enfoque orientado-por-la-anécdota que a menudo prevalece en la planeación del proyecto. Probar las aguas con un proyecto piloto puede revelar cómo las analíticas pueden funcionar y si implementar ese enfoque en una escala más amplia.

Preguntas para que la junta plantee:

- ¿Qué programas clave de TI (compras, proyectos, implementaciones) actualmente tenemos en consideración o en curso?
- ¿Nuestra estructura de administración del programa tiene inmerso un conjunto consistente de procesos y herramientas de gobierno a través del programa – y presenta alarmas tempranas ante los riesgos de demoras del proyecto, sobrecostos por encima del presupuesto, y fallas de entrega de manera que puedan ser abordados?
- ¿Nuestro programa de TI coordina objetivos estratégicos, procesos de negocio, y desarrollo del sistema sobre múltiples franjas de tiempo? ¿Qué tan rigurosos son nuestros esfuerzos de planeación, comunicación y control?
- ¿Hemos considerado el uso de analíticas para administrar y coordinar nuestros programas de TI?

7. Riesgo de operaciones de tecnología

La administración debe asegurar que estén en funcionamiento procesos operacionales rigurosos para proteger la integridad del entorno de la tecnología. La TI necesita entregar los servicios en los niveles acordados con el negocio, administrar la capacidad, entender y administrar sus activos, cumplir con los acuerdos de licencia de software, y administrar de manera efectiva los incidentes y los problemas. Las arquitecturas que no son-estándar y complejas pueden menoscabar la capacidad para satisfacer los objetivos del desempeño del servicio. Un proceso débil de administración de incidentes conduce a la solución inoportuna e inconsistente de los problemas, y a oportunidades perdidas para fortalecer los procesos.

Los entornos de tecnología no son estáticos sino que continuamente están evolucionando. Uno de los riesgos más importantes es la liberación del cambio en el entorno que hace que la tecnología sea inutilizable. La administración tiene que asegurar que los cambios a la tecnología sean probados y liberados de la manera apropiada, y manejados con gran cuidado.

Preguntas para que la junta plantee:

- ¿Cuándos cambios de tecnología causaron un corte cuando fueron liberados o necesitaron ser reversados/vueltos atrás? ¿Qué aspectos de nuestros procesos actuales facilitaron esta situación?
- ¿En qué áreas carecemos de acuerdos adecuados sobre el nivel de servicio entre tecnología y el negocio, y por consiguiente hay el riesgo de desconexión entre las expectativas del servicio y el desempeño del servicio?
- ¿Cuáles son nuestras estadísticas de tiempo de actividad / tiempo de inactividad para nuestras tecnologías críticas? ¿Cómo podríamos mejorar nuestro desempeño?

8. Riesgo de administración inefectiva del riesgo

Para abordar el riesgo tradicionalmente las instituciones financieras siguen el modelo de las tres líneas de defensa. La primera línea de defensa, propietarios de producto y procesos, identifica y administra el riesgo. La segunda línea, frecuentemente ejecutada por las funciones de riesgo y cumplimiento, proporciona la estructura de administración del riesgo y la vigilancia independiente de la primera línea. La tercera línea, usualmente auditoría interna, proporciona a la junta y a la administración senior aseguramiento independiente sobre la efectividad de las primeras dos líneas de defensa.

Encontrar el modelo operacional correcto para permitir la administración efectiva del riesgo de tecnología ofrece retos. La función del riesgo puede tener la experticia en administración del riesgo, pero carencia de conocimiento sobre la tecnología que le permitiría ofrecer luces sólidas sobre el entorno de TI. Inversamente, la función de TI tiene el conocimiento de la tecnología, pero carece de la independencia necesaria para proporcionar un punto de vista no sesgado sobre el riesgo.

Considerando la importancia que hoy tiene el riesgo de tecnología, las organizaciones necesitan mejorar el desarrollo de habilidades y de patrones de carrera en la administración del riesgo de tecnología. De hecho, la demostración de las habilidades tanto en tecnología como en administración del riesgo podrían ser criterios adicionales para posiciones de administración tales como el CIO o el CRO.

Preguntas para que la junta plantee:

- ¿Cómo hemos estructurado el balancear la necesidad de personas técnicas que puedan identificar los riesgos de tecnología con la necesidad de que sean independientes y objetivas?
- ¿Qué prácticas tenemos en funcionamiento para monitorear los principales riesgos estratégicos en la tecnología?
- ¿Cómo podemos impedir que la función de administración del riesgo se desarrolle en una función de prueba del control?
- ¿Hemos creado patrones para las posiciones de nivel de administración para quienes sirven en nuestra función de administración del riesgo de tecnología?

Principales acciones que las juntas pueden realizar para vigilar de mejor manera al riesgo de TI

La junta puede dar una serie de pasos para mejorar su conocimiento de – y su visibilidad en – los riesgos de TI que la institución enfrenta y los métodos que la administración usa para abordarlos. Las siguientes prácticas han surgido de la experiencia e investigación de Deloitte, e incluyen enfoques y mecanismos para permitir que las juntas de servicios financieros vigilen de mejor manera al riesgo de TI:

1. **Constituya un comité de la junta para el riesgo de TI**: Considere formar un comité, a nivel de la junta, para el riesgo de TI, un sub-comité de un comité existente para el riesgo, o un comité asesor para promover el entendimiento del riesgo de TI. Este comité interactuaría con las funciones de TI y de riesgo, el CRO y otros ejecutivos senior, el comité de riesgo a nivel de la junta, y el comité de auditoría. Más allá de los beneficios de la vigilancia, tal comité enviaría un mensaje fuerte a los *stakeholders* de que la organización establece una prioridad alta en la administración del riesgo de TI.

   Un comité de este tipo podría incluir miembros de fuera de la junta y miembros de la administración con experticia en TI y riesgo de TI. Las juntas pueden considerar incluir en este comité al menos uno o dos directores con experiencia práctica, profunda, en IT y administración del riesgo cibernético. El comité le reportaría a la junta en pleno en sus reuniones regularmente programadas. A este comité se le podría asignar la tarea de examinar los riesgos de TI futuros, así como también los actuales, y que sirva de enlace con otros comités a nivel de la junta según sea necesario.

   Si la junta y la administración actualmente no ven que sea factible un comité o un sub-comité de riesgo de TI a nivel de la junta, pueden considerar establecer un comité asesor en lo que se refiere al riesgo de TI. Este comité asesor incluiría miembros de la administración con experticia en TI, y quizás uno o dos expertos externos, para proporcionarle orientación a la junta, al comité de la junta sobre el riesgo, y al comité de auditoría, así como también a la administración, en relación con los proyectos, inversiones, y riesgos relacionados con TI.

2. **Requiera experticia en TI en la junta**: Considere ampliar la experticia de la junta mediante adicionar un director con fuertes habilidades de administración de tecnología y experiencia de liderazgo. Este requerimiento podría ser adicionado cuando surja una vacante en la junta, durante el siguiente proceso de nominación de director, o incluso mediante adicionar un director a la junta actual.

3. **Comprometa a auditoría interna**: Pida a auditoría interna que fortalezca su centro de atención puesto en el riesgo de TI, y que reporte sobre el riesgo de TI independientemente a la junta a través del comité de auditoría. Auditoría interna puede reportar sobre el panorama y las capacidades de la administración del riesgo de TI de la organización, así como también sobre las oportunidades para el mejoramiento del programa de riesgo de TI. La junta debe asegurar que auditoría interna tiene el talento y los conjuntos de habilidades requeridos para de manera independiente retar la TI. Además, partes externas pueden llamarse para que aumenten las capacidades de la auditoría interna y realicen revisiones independientes de áreas seleccionadas de tecnología.

4. **Incremente la transparencia**: Fomente que la administración mejore la calidad de la presentación de reportes sobre TI para la junta, centrándose menos en los proyectos tradicionales de TI y más en los eventos de riesgo de TI, capacidad de recuperación, y riesgo clave e indicadores de desempeño, la junta necesita reportes de la administración que sean perspicaces y estén basados-en-hechos, con el fin de asegurar que la institución verdaderamente está administrando el riesgo de TI y no simplemente prestando un “servicio marginal” sobre el problema.

5. **Establezca umbrales de notificación a / aprobación de la junta**: Defina umbrales para las situaciones de riesgo de TI que tengan que llevarse a la atención de la junta, incluyendo inversiones importantes en TI, contratos propuestos por proveedores con riesgos importantes de TI, y ciertos eventos de riesgo, tales como violaciones cibernéticas, caídas del sistema, o elementos que originan notificación regulatoria.

6. **Defina la agenda**: La junta debe asegurar que el riesgo de TI tiene un espacio permanente en la agenda de la junta. Los temas podrían incluir los principales riesgos y vulnerabilidades de TI,

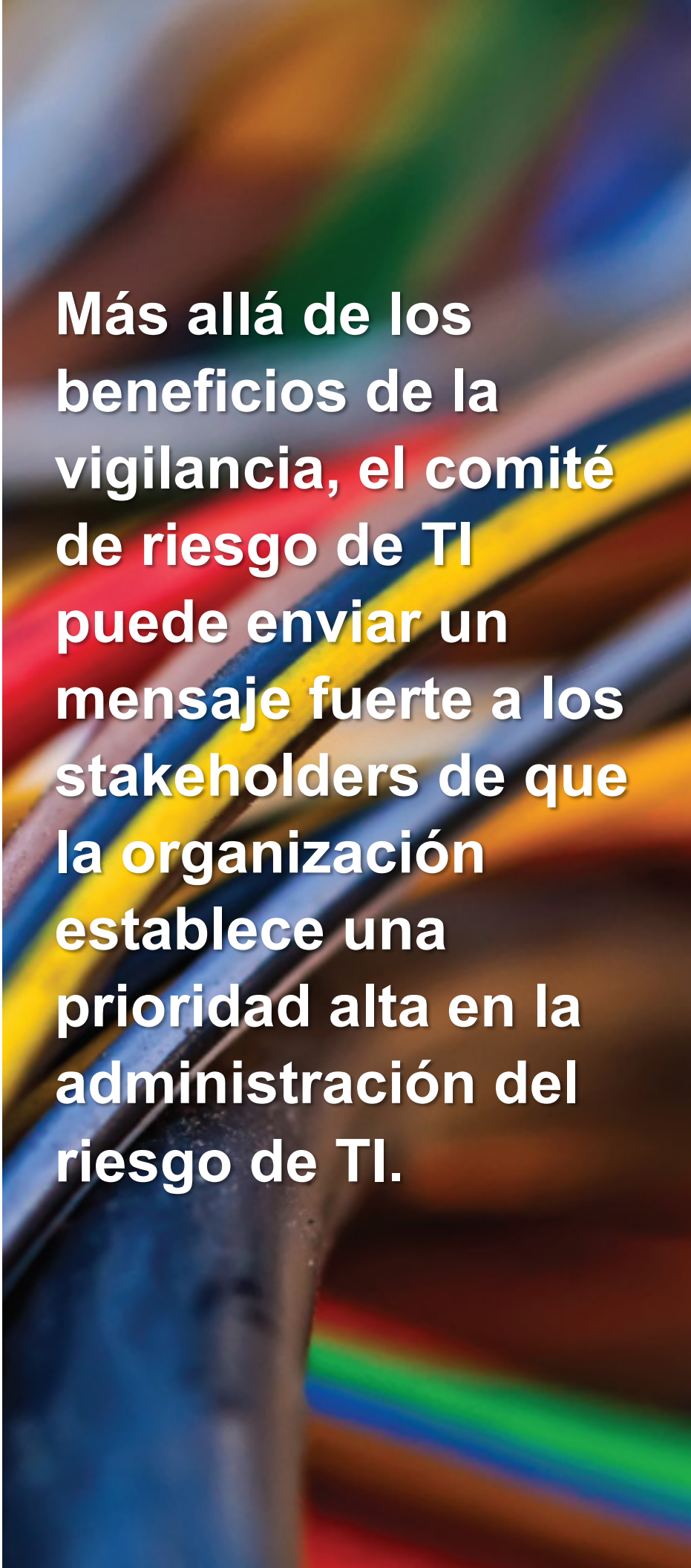
riesgos emergentes, cultura de administración del riesgo, inversiones en administración del riesgo de TI, iniciativas de administración del programa de TI, y patrón de carrera y desarrollo del talento.

Además, algunas juntas pueden designar que directores específicos asuman un mayor rol en la TI y se reúnan por separado con la administración de tecnología. En esas conversaciones, los directores pueden hacer preguntas de prueba, obtener más detalle, y ganar un mayor nivel de entendimiento que subsiguientemente puedan compartir con los compañeros de la junta.

7. **Prohíba la jerga**: Enfatice a la administración que no se debe esperar que la junta traduzca e interprete la jerga de la tecnología. Establezca una expectativa firme de que la administración tiene que informar a la junta o a un comité de la junta sobre los riesgos, programas, y problemas de TI de una manera clara, concisa.

8. **Haga preguntas y busque educación**: La junta debe hacer a la administración n preguntas relacionadas con tecnología y riesgo, tales como las que se sugieren en los recuadros contenidos en este documento y calibrar qué áreas están siendo fortalecidas por la administración para respaldar seguridad y solidez versus simplemente satisfacer requerimientos de cumplimiento. Considere invitar a las reuniones de la junta conferencistas, tales como funcionarios que hacen forzoso el cumplimiento de la ley, académicos, reguladores, consultores administrativos, y expertos en tecnología. Los expertos externos pueden ofrecer un punto de vista independiente sobre el panorama del riesgo de TI, así como también luces respecto de lo que otras compañías están haciendo, cómo la organización se compara con sus pares, y dónde se pueden necesitar nuevas capacidades o inversiones.

9. **Participe en ejercicios de crisis**: Los miembros de junta deben tener un lugar en la mesa para la preparación y respuesta ante una crisis de tecnología. Mediante participar en simulaciones de crisis y juegos de guerra, la junta puede ganar un mayor entendimiento de las capacidades reales de las instituciones, comunicar cómo se comprometería en una crisis, y evaluar sus propias capacidades para ayudar a “mantener a flote el barco” en el caso de un evento importante.



Una prioridad alta para las juntas de instituciones financieras

En medio de todos los desafíos y riesgos a ser abordados, los ejecutivos senior de servicios financieros pueden pasar por alto los riesgos de TI. Ellos viven principalmente en el mundo del riesgo financiero y regulatorio y tienden a ver la TI como un facilitador de las operaciones y al riesgo de TI principalmente en términos de ataques cibernéticos y disponibilidad del sistema.

La junta puede ampliar ese punto de vista. Si bien primero tiene que ampliar su propio punto de vista respecto del riesgo de TI, la junta puede comprometerse inmediatamente en vigorizar el gobierno del riesgo de TI en la organización.

Estar cómodo en las conversaciones acerca del riesgo de TI puede llevar tiempo para los directores que carecen de experiencia en TI. Aun así el sentido común es una excelente guía así como también una herramienta para cortar a través de la jerga. Las lecturas y resúmenes de expertos externos también pueden ayudar. Sin embargo la junta va con ello, el gobierno y la vigilancia del riesgo de TI están entre las responsabilidades clave relacionadas con el riesgo, tanto ahora como en el futuro previsible.

Además, en los servicios financieros los desafíos relacionados con el riesgo de TI seguramente crecerán en número e importancia en los próximos años. Conseguir estar a la vanguardia en esos riesgos en el futuro pagará dividendos para la junta, sus equipos ejecutivos, y sus instituciones.


e="text/javascript">
lmage = "bigImage1";
= Math.ceil(photos.length / 9);
ges();
lmages();
ent.getElementById('bigImage0').src =
ent.getElementById('bigImage0').style.display
PhotoDescription('1');
updatePages() {
= 0;
html = '<table style="width: 330px;" cellspacing=
page != 0) {
html = html + '<a href="#" onclick="page=0; upd
ml += '</td><td style="text-align: center;">';

Contactos

Edward Appert
Cyber Risk Services
Deloitte & Touche LLP
eappert@deloitte.com
+1 212 436 7511

Vikram Bhat
Cyber Risk Services
Deloitte & Touche LLP
vbhat@deloitte.com
+1 973 602 4270

Adel Melek
Risk Advisory
Deloitte Touche Tohmatsu Limited
amelek@deloitte.ca
+1 416 601 6524

Michael Rossen
Global Center for Corporate Governance
Deloitte Touche Tohmatsu Limited
mrossen@deloitte.com
+1 212 492 4531

Dan Konigsburg
Global Center for Corporate Governance
Deloitte Touche Tohmatsu Limited
dkonigsburg@deloitte.com
+1 212 492 4691

Acerca del Deloitte Global Center for Corporate Governance
El Global Center reúne el conocimiento y la experiencia de las firmas miembros de Deloitte de todo el mundo en el área crítica de gobierno corporativo. Nuestra misión es promover el diálogo en el gobierno corporativo entre las firmas miembro, las corporaciones y sus juntas de directores, inversionistas, la profesión contable, la academia, y el gobierno. El Global Center también coordina el liderazgo en el pensamiento sobre los problemas de gobierno corporativo desarrollado por las firmas miembros para avanzar el pensamiento en los problemas de gobierno corporativo en todo el mundo. Encuéntrenos en línea en www.global.corpgov.deloitte.com.

Esta es una traducción al español de la versión oficial en inglés del **Information technology risks in financial services: What board members need to know – and do – 2016 – http://www2.deloitte.com/global/en/pages/risk/articles/a-crisis-of-confidence.html -** Traducción realizada por Samuel A. Mantilla, asesor de investigación contable de Deloitte &Touche Ltda., Colombia, con la revisión técnica de César Cheng, Socio Director General de Deloitte & Touche Ltda., Colombia