Deloitte.

Auditoría de los riesgos de las tecnologías disruptivas♦

♦ Documento original: "***Auditing the risks of disruptive technologies. Internal Audit in the age of digitalization,***" Deloitte, 2018.
https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-rfa-auditing-the-risks-of-disruptive-technologies.pdf.
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.

La era de la digitalización

Estamos en medio de una emocionante convergencia. Los avances tecnológicos y las tendencias en analíticas avanzadas, automatización robótica de procesos [robotic process automation (RPA)], e inteligencia cognitiva [cognitive intelligence (CI)] rápidamente están remodelando los modelos de negocio, mejorando la productividad, y permitiendo la innovación en la manera como las organizaciones conectan productos y servicios para sus consumidores. La adopción generalizada de esos avances ahora comúnmente se le refiere como Industria 4.0 o la Cuarta revolución industrial (vea figura 1).

Esto crea una coordinación intricada. Como las compañías continúan adoptando tecnologías emergentes, auditoría interna (AI) proactivamente tiene que valorar y ganar perspectiva sobre los nuevos riesgos asociados con esas tecnologías. Hacerlo le permitirá a AI valorar si están siendo implementados los controles apropiados para prevenir y detectar los riesgos nuevos y emergentes.

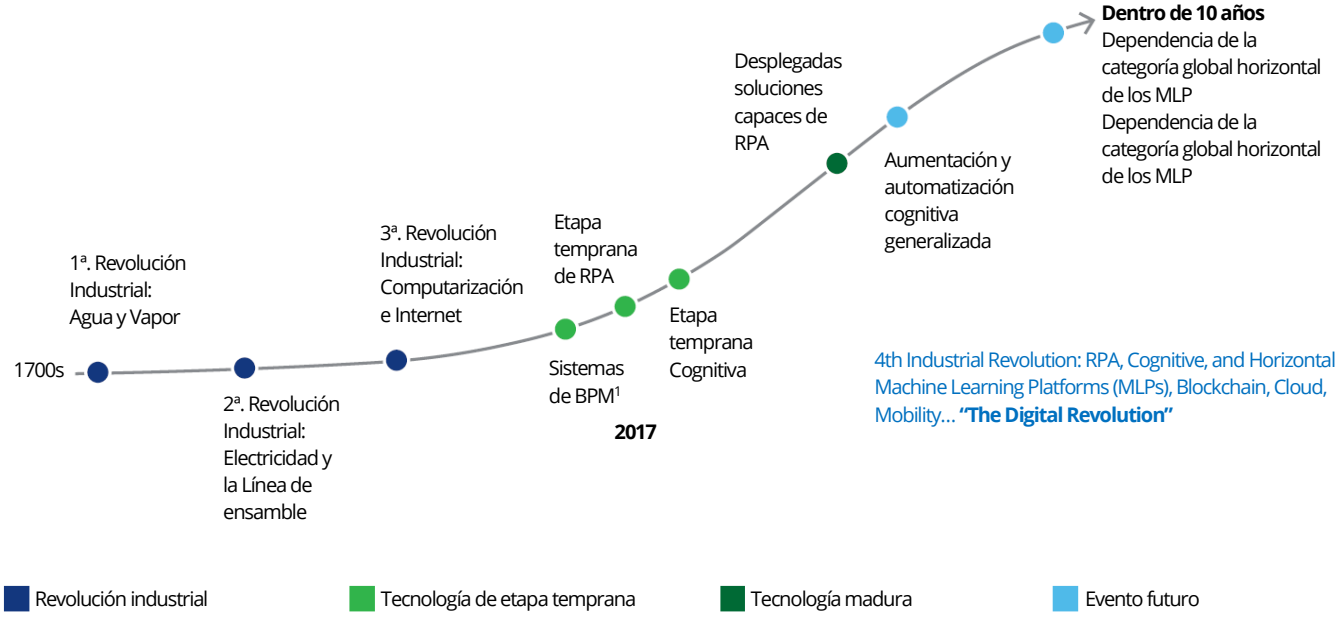
Muchos departamentos de AI han tenido avances en el abordaje de esas disrupciones. Si bien algunos pueden estar más maduros con su enfoque que otros, la mayoría de departamentos están en las fases tempranas del viaje. Además, ellos esperan aprovechar las tecnologías avanzadas para adicionalmente modernizar y mejorar la efectividad de sus programas, creando por lo tanto la necesidad de administrar los riesgos asociados.

Actualmente, una gran cantidad de tecnologías rápidamente están avanzando en Industria 4.0, incluyendo más redes interconectadas y poderosas, computación de alto desempeño, y el advenimiento de herramientas digitales, incluyendo analíticas de datos, RPA, y CI. Combinadas, esas tecnologías están cambiando los negocios de maneras profundas.

El centro de atención de este documento está en la digitalización. En las siguientes páginas, daremos una mirada cercana a los riesgos específicos asociados con las tecnologías digitales y ofreceremos sugerencias para ayudar a que los departamentos de AI valoren esos riesgos.

Figura 1. Industria 4.0

Los avances en ciencia de datos, capacidades de procesamiento, y las más nuevas tecnologías han provocado la 4ª Revolución Industria, cambiando nuestro mundo hacia lo digital.

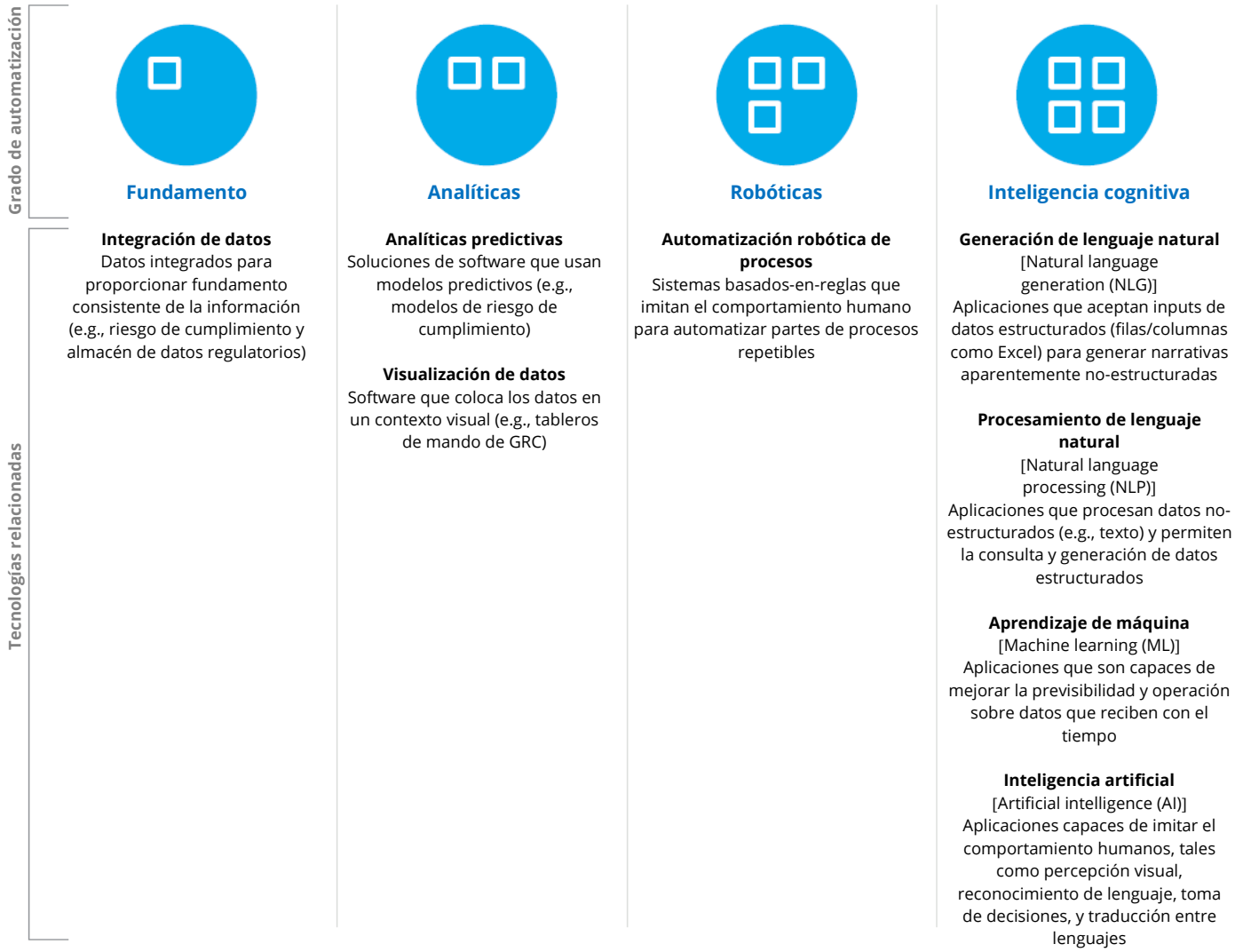


Fuente: Industry 4.0: Challenges and Solutions for the Digital Transformation of Exponential Technologies, Deloitte AG, 2015 and Deloitte proprietary research.

Digitalización disruptiva

Las tecnologías digitales disruptivas se construyen – y extienden – a partir de tecnologías fundamentales y analíticas. Mediante introducir nuevas capacidades de automatización mediante RPA, y CI, las tecnologías digitales disruptivas pueden ofrecer a AI grandes ganancias en eficiencia y efectividad. Muchas compañías líderes han adoptado una o todas las tecnologías que se muestran en la figura 2 para administrar sus operaciones del día-a-día. Por consiguiente, los departamentos de AI de esas organizaciones deben mantenerse en el paso.

Figura 2. El espectro de la digitalización



Vista de conjunto de la AI – pasado, presente, y futuro

Dónde comenzó todo: integración de datos

Las compañías tienen que ser capaces de analizar datos rápida y consistentemente en orden a orientar los mejoramientos a través de la empresa en tiempo real. Este requerimiento ha creado un fuerte entorno para el crecimiento innovador, con la integración de datos como la base de la automatización exitosa.

Qué se ha hecho recientemente: analíticas

Las compañías crecientemente están aprovechando las analíticas para iluminar patrones, perspectivas, y oportunidades ocultas en sus cada vez crecientes almacenes de datos. La exploración puede ocurrir para entender las tendencias futuras y los riesgos mediante el uso de analíticas predictivas. Las organizaciones también pueden desplegar visualización de datos para el contexto visual significativo y comprensivo.

Dónde estamos ahora: automatización

RPA es el uso de software para desempeñar tareas basadas-en-reglas en un entorno virtual mediante imitar la acción del usuario en la interfaz, a menudo trabajando en sistemas múltiples. Las compañías están mostrando importante interés en la adopción de RPA, dado que la automatización de las actividades que consumen tiempo pueden llevar a mayor eficiencia, permitiendo que el personal se centre en actividades que recompensan más y son de valor más alto. Otro beneficio es la escalabilidad, la cual puede mejorar la respuesta a los picos y valles en la demanda y en el volumen.

Qué sigue: CI

Las tecnologías avanzadas de CI, tales como procesamiento de lenguaje natural y aprendizaje de máquina, emplean algoritmos para:

- Extraer conceptos y relaciones a partir de datos
- “Entender” su significado
- Aprender a partir de patrones de datos y experiencia anterior, extendiendo lo que los humanos y las máquinas podrían hacer por sí mismos

Cuando las compañías adoptan iniciativas de automatización, introducen nuevas tecnologías en el entorno de la empresa. Esas nuevas tecnologías, a su vez, presentan nuevos riesgos para el ambiente de control. Si no son administradas de la manera apropiada a través de las tres líneas de defensa, esos riesgos pueden erosionar o eliminar el valor.

Abordando el entorno actual de digitalización

Riesgos asociados con la automatización

Cuando se introducen estas tecnologías de RPA y CI en el ecosistema, las empresas se están exponiendo a sí misma ante riesgos exponenciales que necesitan ser abordados. Nosotros clasificamos esos riesgos en cinco categorías clave (ver figura 3):

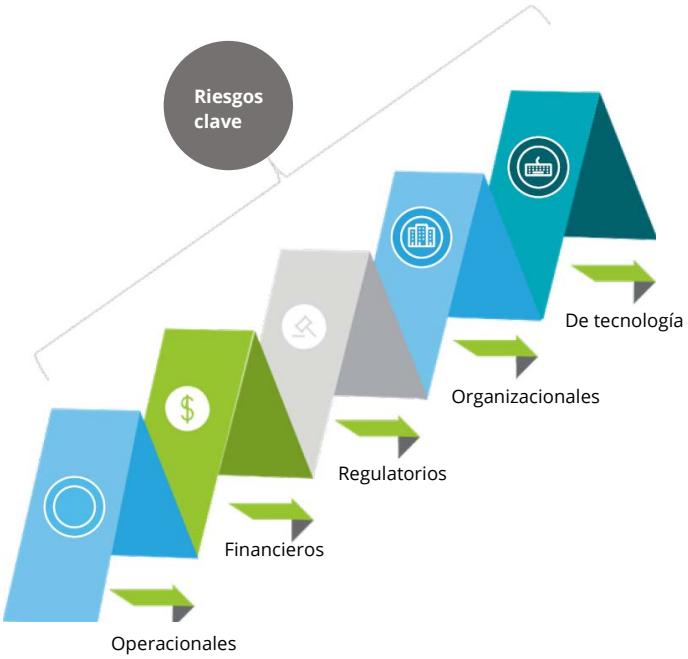
Riesgos operacionales:

- Las tecnologías de RPA y CI pobremente diseñadas, unidas con la velocidad alta de los robots*, pueden multiplicar los errores de procesamiento.
- Los procedimientos inefectivos de vigilancia del robot pueden llevar a errores operacionales de impacto alto.
- Enfoques desiguales para la aplicación de las tecnologías de RPA y CI a los problemas de negocio pueden llevar a un entorno no-estandarizado e incrementar la complejidad de la vigilancia de los robots.
- Los datos de input proporcionados por desarrollados para entrenar los algoritmos usados por las tecnologías de CI pueden ser incompletos, desactualizados, o sesgados. O pueden tener un tamaño de muestra insuficientemente grande y diverso. Además, los métodos inapropiados de recolección de datos pueden resultar en un desajuste entre los datos usados para entrenar el algoritmo y los inputs actuales de datos usados para las operaciones.
- Supuestos defectuosos, técnicas inapropiadas de modelación, errores de codificación, y el sobre ajuste de los algoritmos de automatización para entrenar datos pueden presentar más riesgo operacional.
- Muchos vendedores de tecnología de RPA y de CI son bastante nuevos y no plenamente maduros, presentando riesgo de tercero y financiero.

Riesgos financieros:

- La implementación incorrecta de las tecnologías de RPA y de CI puede resultar en pérdidas financieras y reputacionales para la organización.
- La declaración financiera equivocada debida a desalineación o mala configuración de las tecnologías de RPA y de CI puede resultar en importantes deficiencias o debilidades materiales en los controles internos sobre la presentación de reportes financieros.

Figura 3. Cinco riesgos clave asociados con la automatización



Riesgos regulatorios:

- Un cambio en la ley o en la regulación puede impactar las tecnologías de RPA y de CI de quienes adopten temprano.
- Algunos procesos altamente regulados (e.g., privacidad de los datos) pueden estar "fuera de los límites" para la automatización del robot.
- Los reportes regulatorios incorrectos y/o incompletos generados a través de RPA y CI pueden resultar en problemas regulatorios y multas costosas.
- Los robots pueden actuar de maneras que contravienen leyes existentes (e.g., los algoritmos de aprendizaje pueden resultar en discriminación ilegal contra las minorías).
- Los estándares y las regulaciones de privacidad de los datos pueden estar en riesgo de no-cumplimiento si los robots usados para recaudar información confidencial o restringida no están implementados con estrictos controles de protección.

* La expresión original es 'bot'. Se trata de software robótico, a diferencia de los robots mecánicos. Aquí se le traduce como 'robots.' (N del t).

Riesgos organizacionales:

- El reemplazo o la readaptación de empleados de tiempo completo [full-time employees (FTEs)] puede impactar negativamente la moral del empleado.
- La desalineación a través de grupos puede llevar a brechas en roles y *accountability*.
- Los estándares faltantes alrededor de la ejecución de cambios a los robots pueden obstaculizar los procesos de administración del cambio.
- Un solo robot puede ser equivalente a múltiples FTE, resultando en riesgo de concentración.
- El naciente despliegue de robots puede introducir desafíos de entrenamiento entre los stakeholders.

Riesgos de tecnología:

- El impacto de los cambios rutinarios de mantenimiento a la plataforma existente de TI puede necesitar una prueba de regresión por las implementaciones que dependen de la robótica.
- La realidad de la "caja negra" de los algoritmos de la automatización limita la transparencia en el funcionamiento de la tecnología.
- El software robótico requerirá credenciales para acceso a datos, sistemas, y aplicaciones. Y al igual que con cualquier otro usuario del sistema, el robot puede presentar desafíos de seguridad de la información y de control del acceso.
- Los robots pueden ser usados de manera inapropiada para desempeñar tareas o arrastrar datos de las aplicaciones. Ellos también son más susceptibles a una serie de ataques cibernéticos a nivel de hardware, firmware,* o aplicación.
- Los programas de continuidad del negocio y recuperación del desastre [Business continuity and disaster recovery (BCDR)] tienen que tener en cuenta los riesgos que presenta la implementación de las tecnologías analíticas avanzadas, RPA, y CI.
- Los datos proporcionados para entrenar un robot pueden ser incompletos, desactualizados, o irrelevantes, resultando en un resultado incorrecto.
- Los robots diseñados de manera inapropiada que trabajan más rápido que los SLA de acuerdo convenido pueden agobiar los sistemas existentes de TI.

* Firmware = software permanente programado en la memoria de solo lectura (N del t).

Maestría en el arte de auditar los riesgos debidos a la digitalización

Valorar el impacto de las tecnologías RPA y CI en el ambiente existente de los controles, incluyendo los nuevos riesgos, es imperativo para la adopción exitosa de esas tecnologías de nueva era. Pero no hay necesidad de reinventar la rueda. Esos riesgos pueden ser abordados mediante extender los enfoques existentes para la administración del riesgo de la empresa. Cuando valora esas tecnologías, AI debe encontrar un balance entre sus responsabilidades para:

Asegurar: proporcionar el aseguramiento tradicional

Asesorar: actuar como un asesor de confianza

Anticipar: preparar para los nuevos riesgos en el horizonte

Este balance depende tanto del nivel de madurez de la adopción de la entidad, como de las metas estratégicas del departamento de AI.

Vaya más allá de los controles y el cumplimiento. Ofrezca perspectivas que se puedan llevar a la acción, a fin de construir capacidad de recuperación y crear valor-

+ Asegure	**+ Anticipe**	**+ Asesore**
Confianza	Previsión	Perspectiva

Asegure

Los riesgos presentados durante el ciclo de vida de desarrollo del robot (tal y como se muestra en la figura 4) no necesariamente son nuevos. Solamente son una extensión de una estructura típica de administración del riesgo de TI. En la medida en que la segunda línea de defensa (e.g., departamentos de cumplimiento y riesgo de operación) presiona para modernizar su enfoque para la prueba de los controles, y en la medida en que muchas organizaciones se mueven hacia el modelo combinado de aseguramiento para ganar eficiencias, es imperativo que AI se involucre tempranamente en el camino. Esto le ayudará a la AI a proporcionar aseguramiento efectivo y valioso que no sea duplicativo.

Algunas consideraciones prácticas para que AI agregue valor al proporcionar aseguramiento incluyen:

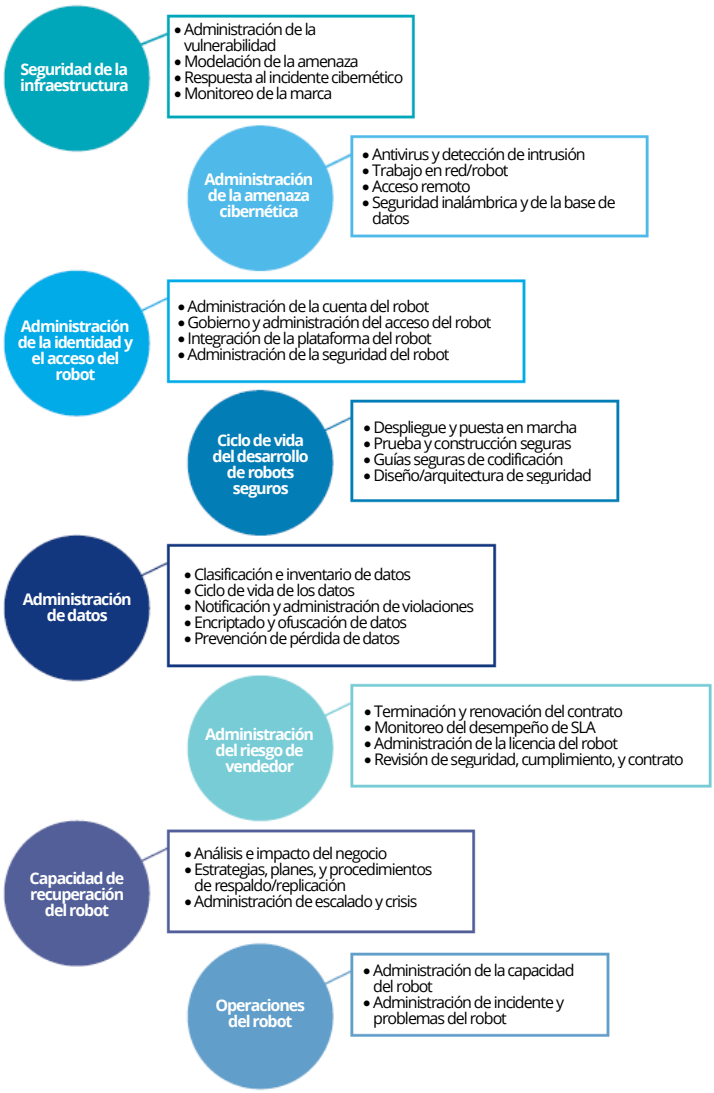
Prueba: Los departamentos de AI deben tener acceso a la documentación de los procedimientos de prueba y deben revisar de manera independiente la prueba desempeñada mediante casos documentados de muestreo de la prueba, los resultados generados, y los problemas registrados.

Manejo y monitoreo de la excepción: Deben ser diseñados una estructura y un proceso para monitorear los robots en los entornos de prueba y producción, así como los problemas de triaje que puedan surgir. AI puede considerar los siguientes elementos de la estructura cuando procede a proporcionar aseguramiento sobre el diseño y la efectividad de la operación de los robots:

- **Identificación y solución del problema del robot:** ¿Hay herramientas y procesos usados por el negocio para monitorear la calidad de los resultados del robot, notificar al personal sobre las excepciones, y crear planes de acción predefinidos para resolver y restaurar los servicios en el evento de que falle la ejecución del robot?
- **Administración del cambio del robot:** ¿Hay un proceso estándar para la ejecución de los cambios a los robots existentes, incluyendo notificar a los *stakeholders* y actualizar los procedimientos y las configuraciones del robot?
- **Administración del riesgo de terceros**: ¿Los contratos con el vendedor del software de automatización están alineados con los protocolos existentes para los terceros que son vendedores de tecnología?
- **Continuidad del negocio**: ¿El plan mejorado de continuidad del negocio y de recuperación de desastres de TI incluyen los pasos requeridos para reanudar las operaciones orientadas por la fuerza de trabajo digital basada-en-el-robot?
- **Supervisión y cumplimiento del robot**: ¿Cómo los propietarios y el personal de cumplimiento que vigilan el trabajo desempeñado por los robots aseguran que los robots se adhieren a los requerimientos regulatorios y a las políticas de la firma?

Proceso de recertificación: AI debe fomentar que los *stakeholders* del negocio y de la tecnología desempeñen una recertificación anual del diseño y la implementación de las tecnologías inteligentes de automatización de RPA y CI. Si es necesario, el proceso también debe ser probado para proporcionar aseguramiento objetivo de si se están ejecutando tal y como se tiene la intención que lo hagan.

Figura 4. Eventos y sub-actividades representativas de la administración del ciclo de vida del robot[2]



[2] Para información acerca de riesgos adicionales del algoritmo, lea "Managing algorithmic risks: Safeguarding the use of complex algorithms and machine learning," Deloitte Development LLC, 2017 https://www2.deloitte.com/us/en/pages/risk/articles/algorithmic-machine-learning-risk-management.html.

Asesore

Si las organizaciones están en las fases exploratorias de la adopción de las tecnologías de RPA y CI, los departamentos de AI deben involucrarse durante la fase previa a la implementación de la automatización de RPA y CI. Unas pocas consideraciones para que los departamentos de AI lleven a la mesa incluyen:

- Asesore a la organización sobre su capacidad para tener en cuenta los factores de riesgo involucrados.
- Proporcione orientación sobre las prácticas líderes para orientar mayores desempeño y valor.
- Eleve el perfil de AI, demostrando conocimiento acerca del tema al tiempo que mantiene la objetividad.

Algunas consideraciones prácticas para ayudar a que AI eleve su rol como asesor de confianza incluyen:

Documente el proceso: AI debe fomentar que las unidades de negocio creen y mantengan documentación de la pre-implementación que pueda ser fácilmente auditada. Ejemplos de documentación del proceso incluyen:

- **Estrategia de automatización**: Propuesta general de valor del negocio, alcance, racionalización de recursos (costos, personal), y métricas para medir el ROI y el valor.
- **Documentación del proceso de automatización**: Procedimientos detallados, desde muestreo hasta presentación de reportes, para ayudar a completar la codificación para el proceso de automatización.
- **Flujo del proceso de automatización**: Una representación visual del proceso robótico general.
- **Codificación de RPA para automatización**: Guiones detallados de codificación que cubran RPA de principio a fin para cada prueba.
- **Pruebas de papeles de trabajo**: Esto incluye muestra de la población, presentación de reportes sobre excepciones, resultados de la prueba, y resultados/resumen de la prueba final.

Disemine los cambios en el proceso de valoración del riesgo: AI debe adaptar un proceso continuo de valoración del riesgo para ser capaz de evaluar oportunamente el impacto de la innovación. Para ese fin, AI debe considerar e integrar los cambios tecnológicos en el proceso de valoración del riesgo.

Ejecute procedimientos dinámicos de auditoría: AI debe prepararse para ejecutar más frecuentemente auditorías dinámicas y efectivas, especialmente cuando los robots sean desplegados en gran escala a través de una variedad de casos de uso. AI puede considerar realizar auditorías usando una estructura ágil. Si es adoptada correctamente, la estructura de Auditoría Interna Ágil [Agile Internal Audit] promueve realizar trabajo en incrementos pequeños, tiempo ajustado para corta duración, y centrada en la colaboración para incorporar retroalimentación frecuente y mejorar las auditorías iterativamente.

Considere actualizaciones a la presentación de reportes: AI debe identificar el nivel y la estructura de la presentación de reportes requerida para las auditorías de la automatización de RPA y CI (e.g., nivel de tecnología versus nivel de función de negocios u orientado-a-aseguramiento versus consultivo).

Anticipe

Sin importar cuál sea el nivel de madurez de la organización con relación a la adopción de la digitalización disruptiva, es imperativo que los departamentos de AI anticipen y alineen los esfuerzos para monitorear riesgos emergentes, desarrollar estrategias, e implementar estrategias de remediación del riesgo. Las analíticas y las nuevas tecnologías les permiten a los departamentos de AI desarrollar perspectivas perspicaces, proactivas, y centradas-en-el-futuro.

Además de asesorar y proporcionar aseguramiento, AI se debe centrar en anticipar los riesgos emergentes asociados con las tecnologías de automatización de RPA y CI.

Un balance entre empujar las fronteras y el apetito por el riesgo: En orden a tener una silla en la mesa y tener un punto de vista en la definición de la estrategia de riesgo para las tecnologías disruptivas, AI debe proactivamente entender el caso de uso de cada solución automatizada de RPA y CI. AI debe establecer una estructura de priorización para la auditoría de los riesgos clave, tales como riesgo cibernético y riesgo de terceros, planteados por la implementación de las tecnologías disruptivas.

Detección del riesgo y analíticas: En anticipación de la implementación de las tecnologías de RPA y CI, los departamentos de AI deben incorporar herramientas de analíticas de datos y de detección del riesgo para proactivamente identificar los riesgos emergentes y ganar perspectivas sobre el mejor enfoque para la auditoría de esas nuevas tecnologías.

Simulaciones de crisis y sistemas de alarmas tempranas: Operar una simulación usando escenarios orquestados de crisis donde la implementación del software robótico pueda ir mal puede ayudarles a los departamentos de AI a sumergirse en sus roles en tiempo real. También puede permitirles revelar lapsos en la capacidad de respuesta de la organización en múltiples niveles: estratégico, comportamental, y táctico.

AI debe mantener el ritmo

En la medida en que las compañías continúen adoptando tecnologías disruptivas para ganar eficiencias operacionales tangibles, los departamentos de AI necesitan mantener el ritmo. Aquí hay algunas consideraciones prácticas sobre cómo los departamentos de AI pueden contribuir:

Planeación y alineación estratégicas: Los departamentos de AI deben crear la visión estratégica, las metas, y la hoja de ruta sobre cómo planean auditar los procesos que serán automatizados vías las tecnologías de RPA y CI y las analíticas avanzadas. Su enfoque debe definir la tecnología de selección de la auditoría de esos procesos (riesgo alto, frecuencia), método de muestreo, plantillas de los papeles de trabajo, y procedimientos de solución de problemas. Además, la visión debe estar alineada e integrada con la estructura existente de administración del riesgo de la empresa [enterprise risk management (ERM)] e incorporar la visión estratégica general de la organización.

Valoraciones del riesgo: Los departamentos de AI deben comenzar la valoración del riesgo de la automatización de RPA y CI tan pronto como sea posible. Con base en la valoración realizada, los departamentos de AI serán más capaces de evaluar las vulnerabilidades y especificar las áreas para la priorización de las auditorías. Debido a la tasa de avances tecnológicos y adaptación, es crítico que AI continuamente valore el riesgo asociado con la digitalización (vea la figura 5).

Analíticas y tableros de mando: Aprovechar las analíticas para diseñar tableros de mando que les proporcionen a los departamentos de AI una descripción detallada de los factores de salud de las tecnologías de RPA y CI le ayudará a AI a estar por delante de la curva.

Entrenamiento y reclutamiento: Los profesionales de AI tienen que adoptar y adaptarse al inminente cambio de la automatización. Entender los matices de esas tecnologías de automatización puede equipar a los auditores con herramientas para desempeñar más efectivamente sus trabajos.

Además, la administración senior debe inyectar perspectivas y conocimientos frescos mediante reclutar especialistas temáticos provenientes de otros departamentos u otras compañías. Es importante que los recursos de AI tengan conocimiento técnico con relación a las tecnologías que estén valorando, así como también entendimiento general de la metodología de AI que será requerida a aplicar.

El poder de la automatización: Lo último, pero no lo menos importante, los departamentos de AI deben considerar las oportunidades para aprovechar las analíticas avanzadas y las tecnologías de RPA y CI para automatizar el ciclo de vida de la auditoría, incluyendo valoraciones del riesgo de auditoría, planeación de la auditoría, trabajo de campo de auditoría, documentación de papeles de trabajo, y presentación de reportes. Esto no solo permite que los departamentos de AI modernicen sus enfoques para realizar las auditorías, sino que también ofrece perspectivas clave sobre los desafíos y riesgos presentados por la adopción de esas tecnologías disruptivas.

Figura 5. Valoración continua del riesgo de digitalización

Continuamente AI debe
- Monitorear y actualizar los datos provenientes de fuentes informativas clave.
- Valorar los riesgos e identificar las amenazas emergentes relacionados con los siguientes dominios clave de riesgo: cibernético, regulatorio, privacidad, financiero, reputacional, falla en adoptar.
- Evaluar el impacto de RPA en la organización, procesos, recursos, panorama regulatorio, vigilancia cibernética y de terceros, etc.

Valoración inicial del riesgo
- Realícela tan pronto como sea posible
- Identifique riesgo inicial asociado con nuevas tecnologías
- Desarrolle un mapeo inicial del riesgo clave y de las metas estratégicas relacionadas con la digitalización

Proceso de "refrescar" el riesgo
- Considere los cambios a la estructura de la organización de la empresa para adaptarla a las necesidades dinámicas del negocio.
- Valore la priorización del riesgo con base en los criterios de impacto y vulnerabilidad según sea necesario

Mantenga el ritmo de la disrupción

La tasa de adopción de las tecnologías de digitalización disruptivas puede ser diferente para cada compañía. Por consiguiente, variará el nivel de preparación de cada departamento de AI para responder a los riesgos enfrentados. Pero el desafío general permanece siendo el mismo: estar cómodo con la incomodidad. Y repasar qué puede hacer AI para entregar aseguramiento y asesoría en la era de la digitalización.

La práctica globalmente reconocida de Deloitte Risk and Financial Advisory puede ayudarle a usted a manejar y prepararse para la disrupción. Nuestras personas, herramientas, y procesos ofrecen soluciones estratégicas para ayudarle a usted en el entendimiento y la auditoría de los riesgos asociados con las tecnologías de RPA y CI, así como también con las analíticas de datos predictivas. La disrupción está aquí para quedarse – aprovechar nuestra experiencia puede ayudarle a usted a mantener el ritmo.

Contactos

Para más información sobre la auditoría de los riesgos de las tecnologías disruptivas, por favor contacte a nuestro equipo de Deloitte Risk and Financial Advisory.

Sandy Pundmann
US Managing Partner, Internal Audit
Deloitte & Touche LLP
+1 312 486 3790
spundmann@deloitte.com

Michael Schor
Partner, Internal Audit Innovation and Automation
Deloitte & Touche LLP
+1 212 436 6208
mschor@deloitte.com

Neil White
Principal, Global IA Analytics Leader
Deloitte & Touche LLP
+1 212 436 5822
nwhite@deloitte.com

Geoffrey Kovesdy
Senior Manager, Internal Audit
Deloitte & Touche LLP
+1 212 436 5149
gkovesdy@deloitte.com

Deloitte.

Acerca de Deloitte