APÉNDICE I: TEMAS DE INTERÉS ADICIONALES SOBRE AUDITORÍA DE TI

Este apéndice contiene una reseña de otros temas con los que los auditores de TI pueden encontrarse al realizar sus auditorías. Los temas analizados en este apéndice incluyen:

- Informática y Auditorías Forenses,
- Dispositivos Inteligentes,
- Telefonía móvil 5G,
- Minería de Datos,
- Big Data,
- Inteligencia Artificial (AI),
- Machine Learning (aprendizaje automático) y Algoritmos,
- Automatización de Procesos Robóticos (RPA), y
- Blockchain.

Muchas áreas emergentes en el ámbito de la TI podrían convertirse en temas de auditoría. Por lo tanto, los auditores deberían estar al corriente de estas áreas, y en condiciones de realizar auditoría vinculadas con los temas correspondientes, si fuese necesario.

Aunque es posible que entre estas áreas existan algunas diferencias técnicas o que se vinculen con aspectos específicos, estas pueden auditarse utilizando los mismos enfoques y técnicas que se exponen a lo largo de esta guía. También es posible que ellas requieran la formulación de algunas preguntas de auditoría adicionales, que los auditores podrían desarrollar por sí mismos al abordar estos temas, en función de los objetivos de auditoría.

I. Informática y Auditorías Forenses

La informática forense abarca el enfoque, las herramientas y las técnicas que se precisan para examinar información digital con el fin de identificar, preservar, recuperar, analizar y presentar hechos y opiniones acerca de la información almacenada. A menudo se considera que forma parte del programa de respuesta a incidentes de una organización, precisándose de análisis e investigación adicionales para identificar evidencia y comprender un incidente. La informática forense también se ha aplicado a una diversidad de áreas, por ejemplo, fraude, espionaje, homicidios, extorsión, uso indebido de computadoras, abuso de tecnologías, difamación, envío de correos maliciosos, fuga de información, hurto de propiedad intelectual, pornografía, envío de correos no deseados (*spam*), *hacking*, y transferencias ilícitas de fondos.[1]

La auditoría forense es una especialidad por la que se examinan medios digitales en procurad de evidencia relativa a una investigación o controversia. Estos tipos de auditoría involucran técnicas y principios similares a los de la recuperación de datos, pero con directrices y prácticas adicionales concebidas para generar una pista de auditoría legal mediante:

- La conservación de evidencia (por ejemplo, datos, accesos y registros) para su análisis;

[1]ISACA's IT Audit and Assurance Guideline G38 Computer Forensics.

- La captura y conservación de datos con tanta proximidad a la infracción o violación como sea posible;
- La recopilación de datos siguiendo normas adecuadas para su posible uso por parte de autoridades policiales;
- La utilización de un proceso de captura de datos mínimamente invasivo, sin la alteración de las operaciones del negocio o actividad; y
- La identificación de atacantes, de ser posible.

Referencias y lecturas adicionales

Electronic Crime Scene Investigation: A Good Practice Guide for Computer-Based Electronic Evidence.

International Organization for Standardization/International Electrotechnical Commission. *ISO/IEC 27035-2:2016, Information Technology— Security Techniques—Information Security Incident Management.* Geneva, Switzerland: International Organization for Standardization, November 11, 2016.

National Institute of Justice. *Forensic Examination of Digital Evidence: A Guide for Law Enforcement.* http://www.ncjrs.gov/pdffiles1/nij/199408.pdf. April 2004.

Wikipedia. "Computer Forensics." http://en.wikipedia.org/wiki/Computer_forensics.

II. Dispositivos Inteligentes

Los dispositivos inteligentes, como los teléfonos inteligentes, las *tablets* y otros dispositivos de Internet de las cosas (IoT)[2] están cambiando el panorama en cuanto al modo de utilización de los sistemas de información. Estos dispositivos brindan capacidades de computación portátil y ofrecen la posibilidad de conectarse a Internet toda vez que exista un servicio de *Wi-Fi* o celular. Los dispositivos inteligentes pueden variar significativamente en cuanto a su tipo, no obstante, existen algunas características que les son comunes, por ejemplo, el uso de sistemas operativos, la conexión de voz y datos en red, el almacenamiento de datos, y la utilización de sistemas de posicionamiento global, entre otros.[3]

Los dispositivos inteligentes también pueden brindar opciones convenientes para el teletrabajo. Tradicionalmente, esta modalidad laboral consistía en conectarse a la red de la organización mediante una *laptop* provista por ella. Sin embargo, los dispositivos inteligentes han permitido a los empleados utilizar aplicaciones y otros medios para trabajar de forma remota.

No obstante, los dispositivos inteligentes que se conectan con la red de una organización pueden introducir nuevos riesgos. Al considerar la postura de una organización en materia de seguridad, debería considerarse la utilización de dispositivos inteligentes. Los riesgos relacionados con el uso de dispositivos inteligentes incluyen aquellos asociados al cumplimiento normativo, la privacidad, la seguridad física y la seguridad de la información. Los riesgos específicos en estas áreas incluyen la utilización de múltiples versiones de hardware o software, el acceso no autorizado a información personalmente identificable o su eliminación, y los riesgos de que el dispositivo se extravíe o sea sustraído, entre otros. Para reducir el impacto de estos riesgos, las organizaciones pueden implementar controles de seguridad y políticas, por ejemplo, controles de autenticación, capacidades de supresión remota, encriptación de hardware, encriptación de software, copias de respaldo de datos, y gestión de dispositivos de la organización.

Al evaluar los riesgos y controles relacionados con dispositivos inteligentes, los auditores deberían, por ejemplo:

- Comprender la estrategia en materia de dispositivos inteligentes de la organización,
- Evaluar el efecto de los dispositivos inteligentes en la arquitectura tecnológica global de la organización,

---

[2]Global Technology Audit Guide, *Auditing Smart Devices*, https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG-Auditing-Smart-Devices-An-Internal-Auditors-Guide-to-Understanding-and-Auditing-Smart-Devices.aspx.

- Identificar y evaluar los riesgos incorporados por los dispositivos inteligentes, y
- Determinar la idoneidad de la gobernanza y los controles de gestión de riesgo relativos a los dispositivos inteligentes.

Referencias y lecturas adicionales

Global Technology Audit Guide. *Auditing Smart Devices*. https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG-Auditing-Smart-Devices-An-Internal-Auditors-Guide-to-Understanding-and-Auditing-Smart-Devices.aspx.

ISACA. *Mobile Computing Security Audit Program.* https://www.isaca.org/bookstore/audit-control-and-security-essentials/wapmcs. 2010.

Salman, Seyed. "Auditing the Internet of Things." *Internal Auditor Magazine*. October 29, 2015.

U.S. Government Accountability Office. *Internet of Things: Status and Implications of an Increasingly Connected World.* GAO-17-75. https://www.gao.gov/products/gao-17-75. May 15, 2017.

III. Tecnologías Inalámbricas 5G

Las tecnologías inalámbricas 5G, son un conjunto de tecnologías de quinta generación, que ofrecen la posibilidad de realizar conexiones más confiables y eficientes a redes inalámbricas. Estas redes prometen ofrecer un desempeño substancialmente mejor y con mayores capacidades, entre ellas, velocidades más altas, y la posibilidad de dar cabida a un número más elevado de dispositivos. Según los estudios de los beneficios socioeconómicos de las tecnologías 5G, los beneficios potenciales adicionales incluyen una mayor disponibilidad y acceso a servicios más avanzados de atención sanitaria y educación, menor contaminación, mayor eficiencia en el transporte, y una mejora de las capacidades de respuesta vinculadas con la seguridad pública. Se espera que, durante la próxima década, con el desarrollo de la tecnología, el desempeño de la red 5G supere de forma holgada el de anterior de cuarta generación. También se espera que la mejora del desempeño de las redes traiga aparejada la mejora de muchas aplicaciones móviles de banda ancha existentes, y también posibilite el surgimiento de nuevas aplicaciones transformadoras en diferentes industrias y en la sociedad.

Algunas mejoras tecnológicas que la tecnología 5G brinda son:

- **Mejora en las aplicaciones de banda ancha**. Conexiones más rápidas y mayores rendimientos podrían conllevar una mejora de aplicaciones asociadas a los servicios en la nube, *streaming* de video, juegos y realidad aumentada.
- **IoT**. Las tecnologías 5G podrían conectar enormes cantidades de dispositivos, como sensores en sistemas para transporte inteligente y logística, fábricas inteligentes, y ciudades inteligentes. Por ejemplo, los sensores en semáforos y caminos podrían reducir el número de accidentes automovilísticos.
- **Comunicaciones de importancia crítica**. Las comunicaciones ultra confiables, de baja latencia, podrían ayudar a una operación más confiable de vehículos autónomo, equipamiento industrial, robótica y drones.

Mientras que las tecnologías 5G ofrecen nuevas oportunidades en múltiples sectores, también existen inquietudes acerca de los riesgos asociados a la ciberseguridad y otros desafíos: Por ejemplo:

- **Implementación de infraestructura.** Las aplicaciones que precisan una baja latencia y un ancho de banda substancial requieren una infraestructura significativa, lo que incluye cables de fibra óptica y celdas pequeñas. La instrumentación de esta infraestructura podría ser onerosa, y supondrá el empleo

de mano de obra calificada, además de tiempo para la planificación, realización de compras y contrataciones, y obtención de permisos en el ámbito local.

- **Ciberseguridad.** La gran cantidad de componentes que integran la red 5G conlleva un aumento de los riesgos de que algunos de esos componentes no se configuren y aseguren de forma adecuada.
- **Privacidad.** Las redes 5G posibilitarían la existencia de datos de localización mucho más precisos, porque se espera que los dispositivos que utilizan estas tecnologías se conecten a celdas mucho más próximas entre sí. La mayor precisión de los datos de localización podría aumentar el riesgo de que la privacidad de los usuarios se vea comprometida.

Referencias y lecturas adicionales

Fraunhofer Institute for Production Technology IPT. *5G-Audit.* https://www.ipt.fraunhofer.de/en/Competencies/Productionqualityandmetrology/Productionmetrology/5g-audit.html.

ISACA. *ISACA Outlines Risks and Benefits of 5G Technology.* https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2021/isaca-outlines-risks-and-benefits-of-5g-technology. February 9, 2021.

U.S. Government Accountability Office. *Science & Tech Spotlight: 5G Wireless.* GAO-20-412SP. https://www.gao.gov/products/gao-20-412sp. March 27, 2020.

U.S. Government Accountability Office. *5G Wireless: Capabilities and Challenges for an Evolving Network.* GAO-21-26SP. https://www.gao.gov/products/gao-21-26sp. November 24, 2020.

IV. Minería de datos

La minería de datos es el proceso que consiste en descubrir patrones y demás información valiosa de grandes conjuntos de datos. En relación con los avances en áreas relacionadas, como el almacenamiento de datos y Big Data, las técnicas de minería de datos han experimentado una rápida mejora. La minería de datos permite a las organizaciones transformar datos no procesados en conocimientos útiles mediante la búsqueda de tendencias o anomalías. La minería de datos puede mejorar la toma de decisiones organizacionales mediante análisis minucioso de datos, por ejemplo, a través de la descripción de conjuntos de datos de destino o la predicción de resultados utilizando algoritmos de aprendizaje automático (*machine learning*).

La minería de datos habitualmente consta de cuatro pasos principales: establecimiento de objetivos, recopilación y preparación de los datos, aplicación de algoritmos de minería de datos, y evaluación de los resultados. A continuación, se describe cada uno de estos pasos:

- **Establecimiento de objetivos.** Es necesario que las partes interesadas trabajen en conjunto para definir el problema del negocio o actividad, lo que ayuda a determinar las preguntas relacionadas con datos que es preciso responder.
- **Preparación de los datos.** Una vez definido el alcance, pueden recopilarse y depurarse los datos pertinentes para maximizar el desempeño.
- **Algoritmos de minería.** Los datos son analizados para detectar relaciones, patrones y correlaciones. Además, pueden aplicarse algoritmos para clasificar datos, dependiendo de que los datos se hayan etiquetado previamente.
- **Evaluación.** Una vez analizados los datos, se puede proceder a la evaluación e interpretación de los resultados. De ese modo, las organizaciones pueden utilizar los conocimientos obtenidos para lograr los objetivos propuestos.

Los acontecimientos recientes en materia de *machine learning* han permitido al campo de la minería de datos expandirse al análisis textual. Esto es importante, puesto que casi el 90 por ciento de toda la información se estructura en formatos tales como documentos, mensajes de correo electrónico, redes sociales, y otros tipos de archivos. La realización de análisis sobre estos datos utilizando técnicas de minería de datos no es factible, dado que la minería de datos solamente funciona para datos estructurados.

La minería de texto supone el uso de técnicas estadísticas, lingüísticas y de *machine learning* que permiten el análisis de información no estructurada. Tal como sucede con las técnicas de minería de datos, se están desarrollando nuevos métodos de minería textual para ayudar a los auditores a procesar lenguajes naturales. Estas herramientas serán críticas para asistir a los auditores a evaluar los volúmenes en constante crecimiento de información electrónica.

Referencias y lecturas adicionales

IBM. *Data Mining*, https://www.ibm.com/cloud/learn/data-mining. January 15, 2021.

Scholtes, Jan. *Text Mining and eDiscovery for Big Data Audits*. https://medium.com/ecajournal/text-mining-and-ediscovery-for-big-data-audits-82a1592cac91. March 6, 2020.

V. Big Data

Big data es un término que se asigna a conjuntos de datos amplios y complejos que se procesan en grandes volúmenes y que a menudo se gestionan como tipos de datos no estructurados o semiestructurados. Las metodologías asociadas a Big Data pueden utilizarse para resolver problemas relacionados con un negocio o actividad que se encontraban ocultos. Algunas de las principales actividades que Big Data puede ayudar a optimizar son:

- **Desarrollo de productos.** Los modelos predictivos pueden ayudar a las organizaciones a anticipar la demanda de los clientes y sugerir productos futuros.
- **Mantenimiento predictivo.** Big Data también puede ayudar a predecir fallas mecánicas mediante entradas en registros y datos de sensores, lo que ayudaría a las organizaciones a maximizar las tareas de mantenimiento.
- **Fraude y cumplimiento.** Big Data puede ayudar a las organizaciones a identificar patrones de datos que indicarían la comisión de fraude o la perpetración de otras actividades maliciosas.
- **Experiencia del cliente.** Big Data permite a las organizaciones recopilar datos de redes sociales, visitas a sitios web, registros de llamadas y otras fuentes para personalizar la experiencia del cliente.
- **Machine learning.** Big Data ha dado la posibilidad de brindar capacitación a máquinas y enseñarles, en lugar de programarlas.

El gran volumen de Big Data demanda una solución de almacenamiento en condiciones de ofrecer accesibilidad y seguridad. Big Data exige la capacidad de procesar datos no estructurados, entre ellos, datos originados en redes sociales, datos de sensores de equipos, y datos de optimización para equipamiento mecánico. Muchas organizaciones a menudo utilizan proveedores de servicios externalizados para proveer la capacidad de cómputo y satisfacer las necesidades de almacenamiento que se requieren para el análisis de Big Data.

Los riesgos asociados con Big Data incluyen una baja calidad de datos, el uso de tecnologías inadecuadas, deficiencias en términos de seguridad, y prácticas de gobernanza de datos carentes de madurez. El auditor debería involucrar al director general de información y a otros líderes de la organización para comprender mejor los riesgos de Big Data en lo relativo a la recopilación de datos, su almacenamiento, análisis, seguridad y privacidad.

Al evaluar herramientas y técnicas de Big Data, el auditor debería considerar los siguientes elementos:

- **Almacenamiento.** ¿De qué modo la organización almacena una cantidad de datos constantemente creciente y cómo el almacenamiento actual se integra con nuevas fuentes de datos?
- **Localmente o en la nube.** ¿La organización, mantiene los entornos de Big Data localmente o los externaliza a proveedores en la nube?
- **Herramientas de descubrimiento de datos.** ¿Qué nivel de madurez ha alcanzado la organización en términos de comprensión y adquisición de los datos y aprendizaje a partir de ellos?
- **Herramientas de monitoreo.** ¿Qué indicadores clave de desempeño ha definido la organización para monitorear la eficacia y el desempeño de los sistemas de Big Data?
- **Adquisición de software.** La comprensión de las diferencias entre los sistemas de Big Data y los sistemas tradicionales será esencial para seleccionar el software adecuado.

Referencias y lecturas adicionales

Colombo, Pierro, and Elena Ferrari. "Access Control Technologies for Big Data Management Systems: Literature Review and Future Trends." *Cybersecurity*, Vol. 2, no. 3 https://doi.org/10.1186/s42400-018-0020-9. 2019.

Global Technology Audit Guide. *Understanding and Auditing Big Data.* https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG-Understanding-and-Auditing-Big-Data.aspx.

Murphy, Maria L. and Journal of Accountancy, "How to Prepare for Auditing in a Digital World of Big Data." *Journal of Accountancy*. https://www.journalofaccountancy.com/news/2014/oct/201411104.html. October. 16, 2014.

Oracle. *What is Big Data?* https://www.oracle.com/big-data/what-is-big-data/.

Salijeni, George, Anna Samsonova-Taddie, and Stuart Turley. "Understanding How Big Data Technologies Reconfigure the Nature and Organization of Financial Statement Audits: A Sociomaterial Analysis." *European Accounting Review, vol. 30, no. 3.* https://www.tandfonline.com/doi/full/10.1080/09638180.2021.1882320. 2021.

VI. Inteligencia artificial

La inteligencia artificial (AI) es una tecnología transformadora con aplicaciones en medicina, agricultura, fabricación, transporte, defensa y otras áreas. El campo de la AI se fundó sobre la base de la idea de que las máquinas podrían utilizarse para simular la inteligencia humana. Se he conceptualizado a la AI como un concepto que ha tenido tres oleadas diferenciadas de desarrollo. La primera oleada de tecnologías basadas en AI incluye sistemas expertos o basados en reglas, en los que una computadora se programa sobre la base de conocimientos o criterios especializados. La segunda oleada de sistemas de AI incluye el aprendizaje estadístico o automático (*machine learning*) basado en la utilización de datos, y permite inferir normas o procedimientos decisorios mediante los que se predice con exactitud los resultados especificados. La tercera oleada de desarrollo de AI incluye aspectos de las dos primeras oleadas, y conlleva capacidades relacionadas con la sofisticación, abstracción y explicación contextual.

La AI trae aparejada una promesa substancial de mejoramiento de la vida humana y la competitividad económica, de diversas maneras. Algunos ejemplos de áreas substancialmente importantes con aplicaciones potenciales para la AI son:

- **Ciberseguridad**—Los sistemas automatizados y los algoritmos avanzados permiten reducir el tiempo y los esfuerzos destinados a la detección de vulnerabilidades, aplicación de parches a esas vulnerabilidades, la detección de ataques, y la instrumentación de defensas frente a ataques activos.
- **Vehículos automatizados**—Las empresas dedicadas a la producción de vehículos y tecnología utilizan herramientas de AI para evaluar una situación, formular un plan, y ejecutar decisiones sobre controles a vehículos.
- **Justicia penal**—Los algoritmos están automatizando parte de la labor analítica, cuyos insumos se utilizan para la toma de decisiones por parte de seres humanos.
- **Servicios financieros**—Las herramientas de AI pueden ayudar a acrecentar el volumen de las operaciones de servicios al cliente, la gestión la patrimonial de clientes, la determinación de perfiles de riesgo de clientes, y los controles internos.

Mientras que la AI ofrece numerosos beneficios a muchas industrias, también plantea nuevos riesgos y podría desplazar a trabajadores y ampliar las desigualdades socioeconómicas. Los desafíos relacionados con la adopción de la AI incluyen:

- la recopilación y el intercambio de datos confiables y de alta calidad necesarios para brindar capacitación en materia de AI.
- el acceso a recursos de informáticos adecuados y disponer de una fuerza de trabajo idónea dotada de los conocimientos, habilidades y capacitación necesarios para su empleo;
- asegurarse de que las leyes y reglamentos que rigen los sistemas facilitados por la AI sean adecuados y que la aplicación de la AI no infrinja libertades civiles; y
- Desarrollar un marco ético que rija el uso de la AI y asegurarse de que las acciones y decisiones vinculadas con sistemas de AI puedan ser adecuadamente explicadas y aceptadas por aquellos que interactúan con tales sistemas.

El evaluar la utilización de la AI por parte de las organizaciones gubernamentales y demás entidades, los auditores deberían considerar la evaluación de prácticas clave en áreas tales como la gobernanza, datos, desempeño y monitoreo. Algunos ejemplos de procedimientos auditables de estas áreas a nivel organizacional son:

- **Gobernanza**—Las organizaciones deberían definir objetivos, roles y responsabilidades claros, demostrar valores y principios que fomenten la confianza, desarrollar una fuerza laboral competente, involucrar a partes interesadas con perspectivas diversas para mitigar los riesgos, e implementar un plan de gestión de riesgos específico de la AI.
- **Datos**—Las organizaciones deberían documentar las fuentes y orígenes de los datos para, de ese modo, corroborar su confiabilidad, y evaluar sus atributos, variables, y aumento/mejoramiento en términos de idoneidad.
- **Desempeño**—Las organizaciones deberían catalogar los componentes modelizados y no modelizados que constituyen el sistema de AI, definir parámetros, y evaluar el desempeño y los productos de cada componente.
- **Monitoreo**—Las organizaciones deberían desarrollar planes para el monitoreo continuo rutinario del sistema de AI y documentar los resultados y las medidas correctivas que han de tomarse para asegurarse de que el sistema produzca los resultados deseados.

Referencias y lecturas adicionales

Raji, Inioluwa Deborah, and Andrew Smart, Rebecca N. White, Margaret Mitchell, Timnit Gebru, Ben Hutchinson, Jamila Smith-Loud, Daniel Theron, and Parker Barnes. “Closing the AI Accountability Gap: Defining an End-to-End Framework for Internal Algorithmic Auditing.” Presented at the 2020 *Conference*

on Fairness, Accountability, and Transparency in Barcelona, Spain. https://arxiv.org/abs/2001.00973. January 28, 2020.

UK Information Commissioner's Office. *Big data, Artificial Intelligence, Machine Learning and Data Protection*. Version: 2.2. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf. September 4, 2017.

U.S. Government Accountability Office. *Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities*. GAO-21-519SP. https://www.gao.gov/products/gao-21-519sp. June 2021.

U.S. Government Accountability Office. *Artificial Intelligence: Emerging Opportunities, Challenges, and Implications*. GAO-18-142SP. https://www.gao.gov/products/gao-18-142sp. March 28, 2018.

VII. Aprendizaje automático (*machine learning*) y algoritmos

El aprendizaje automático (*machine learning*) es un campo de la informática que se ocupa de métodos para el desarrollo de modelos a partir de datos de entrada para formular predicciones relacionadas con datos. En este campo se utilizan algoritmos programados para predecir valores de salida dentro de un margen aceptable y, a medida que a estos algoritmos se les agregan nuevos datos, ellos 'aprenden' y optimizan el desempeño. Un algoritmo es un conjunto de reglas o instrucciones que una computadora sigue de forma automática al realizar cálculos para resolver un problema o responder una pregunta. Los algoritmos pueden presentarse de muchas formas, por ejemplo, modelos computacionales, árboles de decisión, y otros modelos de datos complejos y aplicaciones de autoaprendizaje.

En general, existe la percepción de que los algoritmos se están volviendo cada vez más inteligentes. Esto obedece al hecho de que, a medida que el volumen de datos aumenta y es posible acceder a nuevo hardware, los algoritmos están en condiciones de procesar más datos, a una velocidad mayor. Esto lleva a que los algoritmos se tornen más innovadores y su alcance se amplíe. Los algoritmos pueden apoyar y mejorar la gestión operativa y la prestación de servicios para las organizaciones. Además, están concebidos para acrecentar la eficiencia de procesos que utilizan datos complejos. Los algoritmos formulan predicciones o realizan análisis, que luego los expertos utilizan para respaldar su labor.

Sin embargo, la utilización de algoritmos puede plantear un conjunto de riesgos para las organizaciones, entre ellos:

- El impacto del algoritmo puede no ser lo suficientemente claro para el público.
- El algoritmo o conjunto de datos utilizado por el algoritmo puede contener determinados sesgos.
- El programador o científico de datos tal vez carezca de los conocimientos o el contexto específicos para permitir al algoritmo alcanzar decisiones informadas.
- El algoritmo puede realizar un aprendizaje no previsto.
- Es posible que solamente el proveedor tenga conocimiento de los detalles subyacentes al algoritmo.

Una auditoría de aprendizaje automático (*machine learning*) puede incluir la auditoría de componentes de TI que utilizan algoritmos relacionados con esta actividad. La auditoría siempre debería incluir una evaluación de riesgos de sistemas de TI relacionados, dado que habitualmente los algoritmos no se utilizan como software independiente. Al evaluar o analizar algoritmos, el auditor debería considerar las siguientes áreas:

- **Gobernanza y rendición de cuentas.** Esto incluye los roles, responsabilidades, conocimientos especializados, gestión del ciclo de vida de los algoritmos, factores de riesgo vinculados con la utilización de los algoritmos, y acuerdos con las partes interesadas externas. Es posible formular

modelos de evaluación de la gobernanza y rendición de cuentas de acuerdo con las normas de gobernanza establecidas en COBIT. [4]

- **Modelo y datos.** Esto incluye la calidad y el desarrollo de los datos, su uso, y el mantenimiento del modelo subyacente para el algoritmo. Esto también podría incluir preguntas acerca de los datos y posibles sesgos contenidos en ellos, la minimización de datos, y la forma en que el modelo se pone prueba.
- **Privacidad.** Es posible que los algoritmos utilicen datos personales. Dado lo cual, los algoritmos deben cumplir con las normas legales relativas al procesamiento de datos personales.
- **Controles generales de TI.** Estos incluyen los controles convencionales de TI, como los relativos al acceso, la gestión de la continuidad, y la gestión del cambio.

Referencias y lecturas adicionales

ISACA. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. 2012.

Netherlands Court of Audit. *Understanding Algorithms*. https://english.rekenkamer.nl/publications/reports/2021/01/26/understanding-algorithms. 2021.

Supreme Audit Institutions of Finland, Germany, the Netherlands, Norway, and the United Kingdom. *Auditing Machine Learning Algorithms*. https://www.auditingalgorithms.net/. November 24, 2020.

VIII. Automatización de Procesos Robóticos

La automatización de procesos robóticos (RPA) consiste en la automatización de las tareas de rutina de un negocio o actividad, regidas por una lógica de negocio y el ingreso de datos estructurados. Las tareas vinculadas con la RPA incluyen transacciones de procesamiento, el accionamiento de respuestas, y la comunicación con otros sistemas digitales. Esto a menudo abarca funciones tales como el copiado y pegado, el *scraping* de datos en la Web, la realización de cálculos, la apertura y traslado de archivos, el análisis de correos electrónicos, y la extracción de datos.

De implementarse eficazmente, la RPA puede brindar a las organizaciones la capacidad de reducir gastos de personal y errores humanos. Asimismo, la RPA puede mejorar resultados de negocios, como los vinculados con la satisfacción del cliente, y liberar personal para resolver problemas, realizar análisis y efectuar otras tareas de agregado de valor. La RPA habitualmente conlleva una implementación de bajo costo y a menudo no precisa de software a medida para su integración. En ocasiones, las organizaciones pueden recurrir al aprendizaje automático (*machine learning*) u otras tecnologías de inteligencia artificial para mejorar su RPA.

Tal como sucede con cualquier otra tecnología de automatización, la RPA tiene el potencial de eliminar empleos, lo que puede plantear desafíos para la gestión de talentos en una organización. Además, la RPA puede incrementar la exposición al riesgo en comparación con las aplicaciones típicas de TI. Por ejemplo, los cambios en los roles laborales, la seguridad del acceso, la gestión de cambios en aplicaciones y la gobernanza del entorno RPA son aspectos que es necesario considerar al implementar la RPA. La automatización de un proceso relacionado con el negocio o actividad puede derivar en modificaciones de los requisitos del control del proceso. Esto lleva a que los entornos automatizados sean críticos para que los auditores tengan la seguridad de que se produzca el resultado deseado.

[4]COBIT es una norma de control de la gobernanza de TI diseñada para satisfacer la necesidad de evaluar riesgos relacionados con información y TI.

Al auditar el entorno del RPA, es necesario evaluar varias etapas diferentes del entorno, además de considerar pasos específicos en estas etapas:

- **Planificación**—En la etapa de planificación, para comprender claramente las áreas en las que el RPA se implementa, es necesario que el auditor defina el nivel de automatización, analice los flujos de trabajo, y determine qué otros sistemas integrados deberían incluirse.
- **Examen paso a paso**—Una vez que el auditor identifica las automatizaciones presentes en un entorno, es importante poner a prueba los riesgos asociados con cada automatización en el proceso. Es esencial realizar un examen paso a paso del código para comprender los riesgos, controles y sistemas involucrados en la automatización.
- **Diseño**—Es necesario considerar a las automatizaciones como elementos de TI, y el auditor debería incluir las automatizaciones más importantes en el alcance del diseño. Esto debería incluir todas las automatizaciones que generen informes u otros productos utilizados por la dirección. Además, el auditor debería evaluar la idoneidad de los controles aplicados para mitigar y eliminar los riesgos asociados con cada automatización en el proceso.
- **Elaboración de informes**—Si se utilizase la automatización para generar informes, será necesario que el auditor determine la completitud y exactitud de los informes mediante la evaluación del código, la lógica y los parámetros aplicados para generar los informes.

Referencias y lecturas adicionales

Automation Anywhere. *What is Robotic Process Automation (RPA)?* https://www.automationanywhere.com/rpa/robotic-process-automation.

Boulton, Clint. *What is RPA? A Revolution in Business Process Automation.* https://www.cio.com/article/3236451/what-is-rpa-robotic-process-automation-explained.html.

Deloitte. *Auditing the RPA environment, https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-auditing-the-rpa-environment-noexp.pdf*. March 2018.

IX. Blockchain

El blockchain es una suerte de 'libro mayor' distribuido, que permite realizar transacciones de activos digitales en tiempo real. Específicamente, en ese libro mayor se registran acontecimientos digitales organizados en bloques cronológicos que se encuentran encriptados y distribuidos entre muchas entidades diferentes. Los bloques solamente pueden actualizarse cuando una mayoría de las entidades prestan manifiestan su acuerdo con la transacción. La blockchain utiliza un marco peer-to-peer en el que cada nodo tiene una copia idéntica de los datos y un protocolo de consenso sincroniza los datos entre nodos.

Esto da como resultado de una actualización de los datos en tiempo real sin la necesidad de una autoridad central o un tercero que valide las transacciones. Dichas transacciones pueden escribirse en la blockchain solamente una vez, y no es posible revertir tales transacciones. Las tecnologías de blockchain son:

- **Descentralizadas**: Pueden operar independientemente de cualquier intermediario o autoridad que les permita funcionar de acuerdo con relaciones peer-to-peer.
- **Distribuidas:** El libro mayor de blockchain se distribuye y replica entre todos los nodos de la red.

- **Rastreables**: Todo registro en el blockchain se vincula con la transacción previa de manera tal que exista una pista de auditoría completa y rastreable de las transacciones subyacentes.
- **Validadas**: Las transacciones son validadas por los nodos participantes en relación con los mecanismos de consenso previamente a incorporarse a la blockchain.
- **Inmutable**s: Las transacciones en el blockchain son inmutables, lo que significa que no pueden reemplazarse, revertirse o alterarse una vez que han sido validadas.
- **Verificables**: Las transacciones en el blockchain se transmiten a todos los nodos de la red, donde cada nodo puede verificar el historial de transacciones.

Mientras que el blockchain brinda capacidades como las mencionadas precedentemente, podrían surgir varias cuestiones derivadas de la implementación de las que le son propias, entre ellas:

- **Bifurcaciones duras de blockchain**: Se trata de situaciones en las que se han creado dos copias divergentes del blockchain. Estoy habitualmente ocurre cuando existe un desacuerdo entre nodos respecto a las reglas que rigen el blockchain.
- **Duplicaciones de gastos**: Esto sucede principalmente con las criptomonedas, cuando un activo puede transferirse a múltiples entidades.
- **Dominancia del 51 por ciento**: Esta es una cuestión que podría surgir cuando una entidad controla la mayoría de la red, lo cual le otorga a esta entidad la capacidad de actuar maliciosamente.
- **Desempeño deficiente**: Los mecanismos de consenso a menudo generan una compensación de factores entre la velocidad de rendimiento y la confiabilidad de las transacciones.

Una consideración importante al auditar tecnologías blockchain es la confiabilidad de los datos. Específicamente, es necesario que los auditores estén al corriente de la posibilidad de que el blockchain sea manipulado o alterado. El algoritmo de consenso utilizado por blockchains específicos podría ser manipulado, de modo tal que se incorporen transacciones el blockchain sin la debida autorización.

Otras consideraciones al auditar el blockchain incluyen inquietudes vinculadas con la seguridad, como el almacenamiento de datos de identificación digital, que podría dar lugar a la divulgación de información personal si en el futuro se quebrase la encriptación.

Referencias y lecturas adicionales

Deloitte. *An Internal Auditor's Guide to Blockchain: Blurring the Line between Physical and Digital*. https://www2.deloitte.com/us/en/pages/risk/articles/internal-auditing-guide-to-blockchain.html. 2019.

KPMG. *Auditing Blockchain Solutions.* https://assets.kpmg/content/dam/kpmg/in/pdf/2018/10/Auditing_Blockchain_Solutions.pdf. October 2018.

RSM US. *How Blockchain Technology Will Affect the Audit.* https://rsmus.com/what-we-do/services/assurance/how-blockchain-technology-will-affect-the-audit.html. November 13, 2019.

U.S. Government Accountability Office. *Blockchain: Emerging Technology Offers Benefits for Some Applications but Faces Challenges.* GAO-22-104625. *https://www.gao.gov/products/gao-22-104625.* March 23, 2022.