FEDERACIÓN ARGENTINA DE CONSEJOS PROFESIONALES DE CIENCIAS ECONÓMICAS

CONSEJO ELABORADOR DE NORMAS DE CONTABILIDAD Y AUDITORÍA (CENCyA)

INFORME N° 25

APLICACIÓN DE NUEVAS TECNOLOGÍAS EN EL TRABAJO DEL AUDITOR

Contenido

1. Introducción

Esta publicación tiene por objetivo difundir entre los profesionales de ciencias económicas, y en especial entre los contadores que actúan como auditores de entidades de pequeña dimensión o menos complejas[1], las nuevas herramientas tecnológicas disponibles para su análisis e incorporación a la práctica y procesos de auditoría, lo que les permitirá mantenerse actualizados en relación con el presente que vive la profesión y convertir el rol del auditor mediante la incorporación de habilidades en el campo digital.

Los auditores deben ser capaces de utilizar la gran cantidad de datos disponibles de las organizaciones y efectuar un análisis de estos, lo que les posibilitará comprender mejor el negocio, identificar con más exactitud áreas de riesgo, ofrecer mayor cobertura y proporcionar mayor valor agregado. También les permitirá realizar procedimientos de auditoría de forma automatizada incrementando el testeo (100% de los datos en lugar de muestras), optimizando recursos, haciendo énfasis en el análisis de excepciones y mejorando el nivel de reporte. Podrán dedicar más tiempo a la planificación y elaboración de conclusiones, ya que los avances tecnológicos servirán de soporte para la realización de pruebas.

Para la adopción de estas nuevas herramientas tecnológicas es necesario reorientar el perfil de los auditores a fin de incorporar un mayor nivel de conocimiento y capacidades tecnológicas. Los auditores deben conocer y entender el uso de las nuevas tecnologías.

Existen múltiples tecnologías disponibles pero su grado de aplicación al proceso de auditoria es muy diverso, desde el uso muy difundido de análisis de datos (*Data Analytics*), pasando por la automatización de procesos hasta el uso incipiente de *Machine Learning* (aprendizaje automático) o realidad virtual. En esta publicación se proporcionará información sobre las principales herramientas tecnológicas disponibles y sus potenciales usos en la tarea de auditoría.

El objetivo de este trabajo consiste en brindar un análisis y conocimientos básicos sobre las herramientas tecnológicas incluidas. No crea una nueva norma, y solo proporciona orientaciones para su interpretación y eventual aplicación de criterios profesionales considerando el caso particular y tipo de encargo.

La identificación de alguna modalidad de uso puede darse al solo efecto descriptivo y no implica por parte de la FACPCE aceptación, recomendación o aprobación sobre sus cualidades o procedencia.

[1] Según definición del International Auditing and Assurance Standards Board (IAASB)

2. Las nuevas herramientas tecnológicas en Auditoría

La tecnología de la información y comunicaciones (TIC), omnipresente en cada aspecto de los negocios y la vida cotidiana se incrementa exponencialmente y su incidencia, por efecto de su evolución impredecible, transforma la vida de las organizaciones y sus procesos.

La utilización de servicios de nube es una tendencia irreversible en un ambiente global donde los avances técnicos sorprenden cada día. El dominio de *big data*, los registros distribuidos seguros -*blockchain*- y su extensión a otros usos, la vigencia de los contratos inteligentes (*smart-contracts)* y su no lejano complemento con la internet de las cosas, la información en poder de los administradores que permite integrar en procesos residentes actividades antes en poder de los administrados, son algunos integrantes de una lista infinita de eventos con fuerte impacto en la actividad de los profesionales en ciencias económicas.

Este es el medio en el que los responsables de preparar y emitir información financiera y no financiera soportan sus procesos, independientemente que se trate de una empresa de grandes dimensiones, complejidad o que cotice en la Bolsa o una entidad de pequeña dimensión o menos compleja. En consecuencia, los contadores que ejecuten los encargos previstos en las normas de auditoría, revisión, encargos de aseguramiento y servicios relacionados vigentes (Resolución Técnica N° 37[2]), verán afectada su tarea en forma integral, pero específicamente en lo referente a análisis y evaluación de riesgos, sistemas de control interno y procedimientos sustantivos, con el alcance que cada tipo de encargo requiera.

Las auditorías tienen que adaptarse a la era digital

Actualmente, tanto las compañías como los grupos de interés requieren de los auditores mejores niveles de reporte, que se incremente la frecuencia y efectividad en el testeo de los controles y, a su vez, que se optimicen los recursos. Los auditores deben poder usar y analizar los datos disponibles de las empresas para comprender mejor el negocio, identificar las áreas de riesgo y ofrecer mayor cobertura. Las metodologías y procedimientos de auditoría se deben ir adaptando a los nuevos riesgos lo que va a requerir un mayor uso de la tecnología.

La tecnología está cambiando la forma de enfocar y desarrollar la práctica de la auditoría, implica un cambio en los procesos y en la forma de analizar los trabajos, logrando más practicidad y eficiencia a través de la automatización de procesos, asegurando la misma calidad, reduciendo los costos y redefiniendo el papel del auditor.

El impacto de las nuevas tecnologías en el trabajo del auditor es un desafío que traerá cambios en la profesión y una oportunidad para repensar y mejorar los servicios ofrecidos a los clientes y mejorar la eficiencia. **Trabajar con herramientas digitales y contar con un equipo de profesionales que conozca estas herramientas es hoy una ventaja competitiva**, por lo cual iniciar el proceso de incorporar tecnología y capacitar a nuestros equipos es una necesidad que no puede esperar.

[2] Toda mención en este documento a la Resolución Técnica N°37 hace referencia a la Resolución Técnica N° 37 modificada por la Resolución Técnica N° 53 (FACPCE).

Los auditores deben centrarse en las oportunidades que ofrecen las nuevas tecnologías, teniendo presente que **el juicio profesional seguirá siendo esencial** para asesorar a los clientes y añadir valor.

En los capítulos siguientes se describirán las tecnologías más utilizadas para soportar el trabajo de auditoría de estados financieros, sus ventajas y potenciales usos. Definiremos cuáles son las nuevas herramientas tecnológicas disponibles y su adecuación al objetivo buscado y al tipo de tarea a realizar en el proceso de una auditoría.

3. Automatización Robótica de Procesos (RPA)

Automatización Robótica de Procesos (en inglés, *Robotic process automation*, abreviado *RPA*) se utiliza para describir una clase de aplicaciones de software -robots de software -que automatizan el trabajo mediante la emulación de tareas ejecutadas por operadores humanos. Es un programa informático que se ejecuta sobre bases de datos o documentos. Automatiza tareas repetitivas realizándolas de la misma manera que una persona trabajaría.

3.1. Implementación de RPA

En las empresas comerciales y/o industriales se pueden utilizar para apoyar la transformación de los procesos transaccionales de punta a punta. Las tareas individuales de estos procesos pueden ser completamente automatizadas con RPA, eliminando gran volumen de trabajo manual, generando ahorro de costos y mejoras en los reportes.

Para una implementación exitosa de RPA debemos considerar los siguientes aspectos:

1. Pensar en "transformación" antes de pensar en las herramientas

El cambio hacia RPA no es diferente al del outsourcing de procesos de negocios (BPO) de hace una década o dos, pero hay algunas diferencias importantes. Al igual que BPO, una fuerza de trabajo digital (o "virtual") es una alternativa de bajo costo. Pero en el caso de RPA, la reducción de costo es sólo uno de los objetivos; hay otros objetivos empresariales que generan interés en RPA, como se analiza a continuación. La diferencia mayor es que no hay solo un realojamiento (*lift and shift*[3]) en el RPA. BPO transfería puestos de trabajo completos a una nueva ubicación con salarios más bajos, en cambio los robots no suelen reemplazar el rol entero de una persona. Por el contrario, automatizan una parte del papel de alguien, como las pulsaciones de teclas realizadas en la herramienta en el proceso Caja a Saldos de Cuenta.

En consecuencia, para obtener valor, una organización debe estar preparada para rediseñar procesos y transformar su fuerza de trabajo actual, al mismo tiempo que está introduciendo nuevas herramientas de automatización. Esto requiere una visión y planificación.

El software en cualquier contexto -y RPA no es una excepción -es una herramienta para construir una solución, no la solución en sí. Una forma de establecer la actitud correcta desde el principio es no pensar en RPA como una automatización de procesos "rápida". Esto puede ayudar a cambiar el enfoque hacia los robots (las herramientas) a la automatización de procesos (la transformación). Este cambio en la actitud posiciona a las organizaciones para obtener un mayor valor en el uso de RPA, incluyendo las bases para las tecnologías de inteligencia artificial (AI) aún más transformadoras que vienen en el camino.

2. Definir objetivos de automatización

Antes de que las organizaciones salten a RPA, deben decidir por qué lo están haciendo. Muchos se sienten atraídos por la oportunidad de reducir costos al reducir el número de empleados a tiempo completo (*full-time equivalents o FTE*[4]) requeridos para realizar un

[3] Lift and shift: es un enfoque utilizado para migrar las aplicaciones a la nube. Implica mover la aplicación y todos los datos asociados a una plataforma en la nube sin tener que rediseñar la aplicación.

[4] Full-time equivalents o FTE: es una medida empleada en recursos humanos para conocer el número de trabajadores a jornada completa que son necesarios para llevar a cabo una actividad.

proceso o ejecutar una función. Pero la reducción de costos a menudo no es el único o incluso el enfoque principal para implementar RPA. Las estrategias de transformación corporativa y digital pueden dictar otros objetivos, como mejorar la productividad, acelerar los ciclos de reporte financiero, redistribuir recursos a actividades de mayor valor, permitir que la organización mantenga una estructura de costos eficiente o mejoran el cumplimiento y los controles.

Para una organización que crece rápidamente, RPA puede ofrecer una forma de administrar mayor volumen sin aumentar la escala de la gestión interna de la empresa. El uso de RPA también puede mejorar la calidad y el acceso a los datos previamente administrados a través de la actividad manual, lo que a su vez permite a la gerencia hacer una comparativa más eficaz y tomar mejores decisiones de negocios. También puede proporcionar una manera de mejorar la experiencia del cliente o de las partes interesadas proporcionando información más rápidamente o en un formato consolidado.

3. Identificar áreas de alto potencial

En términos generales, hay algunas características básicas del proceso que hacen buenos candidatos potenciales para aplicar RPA. Éstas incluyen:

- Actividades de alto volumen y alta frecuencia
- Actividades repetitivas y transaccionales
- Actividades intensivas en datos
- Actividades basadas en reglas
- Tareas que extraen datos de sistemas dispares, requiriendo así una actividad manual extensa
- Actividades que cuentan con oportunidades de estandarización; por ejemplo, donde cinco personas actualmente realizan el proceso de cinco maneras diferentes

Si bien estos son criterios simples, puede haber otras consideraciones. Por ejemplo, la automatización de una actividad simple que se reitera miles de veces al día y requiere de muchas personas, podría obtener un buen valor para la organización. Por otro lado, la organización también puede obtener un valor similar o mayor automatizando una actividad de menor volumen o menos frecuente donde la precisión es crítica y los errores humanos son costosos.

Por supuesto, una estructura adecuada de los datos y su integridad es un requisito previo para la automatización eficaz. De lo contrario, el ejercicio simplemente automatizará y exacerbará el uso de datos incorrectos.

Una vez que una organización ha identificado las áreas objetivo para la introducción de RPA, entonces tiene que "dimensionar el beneficio" y dar prioridad a las oportunidades.

4. Establecer el modelo de administración correcta

Para acelerar la transformación, una organización tendrá que ampliar su uso de la automatización de una manera gestionada y reflexiva y no como una serie de proyectos

separados. Con esto en mente, es útil planificar y trabajar en conjunto con las iniciativas de mejora de procesos punta a punta impulsadas por las organizaciones.

Si bien una de las características atractivas del software RPA es el hecho de que se puede implementar con poco o ningún soporte de TI, una colaboración adecuada con la función de TI sin embargo es crítica para el éxito de una iniciativa de RPA. Las aplicaciones RPA tocan y usan datos de otros sistemas centrales, por lo que el área de tecnología va a recibir solicitudes de asistencia con la integración. Esto será un reto si hay múltiples iniciativas en recursos humanos, finanzas, adquisiciones y otras áreas que involucran a diferentes proveedores y programas de automatización.

Dependiendo de las circunstancias de la organización, puede ser prudente establecer un área para supervisar y administrar el alcance, los costos, el calendario, la realización del caso de negocios y otras necesidades.

5. Plan para la transformación

La implementación de una herramienta que toma parte del trabajo de alguien requiere repensar cómo las personas dentro de la organización ejecutan el proceso; por lo tanto, no debe subestimarse el cambio involucrado. Las consideraciones clave incluirán cambios en el diseño del trabajo, roles, capacidades y habilidades requeridas. Por ejemplo, un proceso puede requerir menos personas para realizar un trabajo transaccional, pero requerirá nuevas habilidades para administrar la fuerza de trabajo virtual.

También es importante pensar en cómo preparar y apoyar a la organización, ya que da la bienvenida a la mano de obra digital. Por ejemplo, ¿cómo cambiará RPA las interacciones con las partes interesadas aguas arriba y aguas abajo de las actividades automatizadas? ¿Cómo cambiará la información o el calendario de la información que reciben? Una vez más, es fundamental pensar en estas áreas en conjunto con la implementación de RPA, no después de realizado.

Un plan de gestión del cambio formal debe incluir una hoja de ruta con actividades secuenciadas para facilitar los cambios y, a continuación, ampliar su uso de herramientas de RPA.

6. Realizar un piloto o prueba de concepto

Los pasos anteriores proporcionan una base para avanzar con una prueba de concepto de RPA o piloto. Una prueba de concepto es un pequeño proyecto de demostración que normalmente se lleva a cabo en un entorno de prueba que no interrumpe las operaciones en vivo. Esto puede ser útil para comprender el esfuerzo requerido para programar y ejecutar la herramienta y el impacto en los recursos.

En un piloto, por otro lado, la automatización está “dentro" e integrada con sistemas vivos y operaciones en vivo. Esto requiere un nivel diferente de rigor. También proporciona un indicador hacia la extensión de la automatización para abarcar actividades adicionales de una manera organizada; por ejemplo, un piloto de aplicación de pago en el proceso de compra a pago puede extenderse a la reconciliación del proveedor y luego a las actividades de establecimiento o set-up del proveedor.

Este es el punto en el que es prudente ver demostraciones de proveedores, evaluar capacidades y seleccionar el software basado en los objetivos y planes de transformación que se han establecido ahora.

A partir de aquí, la organización puede seguir el proceso habitual de implementación de tecnología, que incluye definir los requisitos técnicos y de negocio, diseñar la solución, documentar el proceso y finalmente implementar el software de RPA.

Los pasos descriptos anteriormente proporcionan un enfoque diseñado para maximizar el potencial y el valor de RPA introduciendo y luego expandiendo las capacidades de RPA de una manera estratégica y lógica. Si bien este enfoque requiere un cierto nivel de análisis y planificación, si se hace bien, no debe obstruir el camino hacia la implementación y obtención de valor de RPA en el corto plazo.

La clave es luchar contra el impulso de centrarse en la herramienta en lugar de centrarse en transformación y la visión. Con una visión bien definida, se seleccionarán las herramientas adecuadas, al igual que con el plano de la casa se seleccionarán de los materiales adecuados.

3.2. Aplicación en Auditoría

Muchos procedimientos o funciones relacionadas con el proceso de auditoría (que se repiten cliente por cliente) se pueden ejecutar mediante el uso de RPA. Es una oportunidad para redefinir y rediseñar los procesos de auditoría aplicados, utilizando RPA para la a ejecución de tareas repetitivas y que se ejecutan en base a reglas.

Para implementar RPA, como primera medida, se debe entender el proceso y desglosarlo en módulos: establecer una lista de tareas que se podrían automatizar con la RPA. Además, es necesario que los datos estén en un formato que el RPA pueda procesar. Una vez implementados los RPA, se debe tener en cuenta el uso y el mantenimiento de estos, ya que como cualquier software requerirá actualizaciones.

La RPA puede aumentar la eficiencia de la auditoría, ya que puede hacer las tareas repetitivas igual que los auditores, pero sin cansarse, en una fracción del tiempo en que un auditor puede hacerlo y por muchas horas y, al automatizar las tareas, se reducen los errores. Además, al realizar las pruebas sobre la totalidad de los registros contables, la RPA puede detectar más fácilmente las excepciones.

Esto ofrece a los auditores la posibilidad de medir con más precisión el riesgo de incorrecciones (que puede modificar su Informe) de manera oportuna. La aplicación de RPA a la realización de pruebas sustantivas, les permite a los auditores dedicar sus esfuerzos a tareas de mayor valor como la planificación, los intercambios con la Gerencia de los clientes y la evaluación de los resultados.

Cada estudio profesional deberá evaluar en función de la cantidad de clientes, complejidad de los sistemas sujetos a revisión, estadio de automatización propio, inversión requerida, recursos humanos disponibles y otros factores si le resulta conveniente efectuar un desarrollo propio o adquirir algún producto de automatización de procesos de auditoría de los existentes en el mercado, o eventualmente, profundizar el uso de herramientas actuales para el análisis de

datos (por ejemplo: tablas dinámicas, macros y automatizaciones en Excel, gestionar bases de datos con Access o servicios de análisis de datos como PowerBI).

Ejemplos de aplicación de RPA a pruebas de auditoría[5]

- Armado de Estados Contables de presentación en base a balance de sumas y saldos.
- Evaluación de controles internos y segregación de funciones (a aplicar sobre el ERP[6] del cliente)
- Automatización de KRI´s (*Key risk indicator* – Indicadores clave de riesgo) para el monitoreo de riesgos.
- Para una prueba de corte de ventas y utilizando la base de datos de los ingresos se puede diseñar un RPA que cruce los montos de las ventas de las facturas con los datos del envío y del pedido.
- Para el saldo de proveedores, se puede diseñar un RPA que identifique para cada compra que compone el saldo del proveedor, la fecha y el monto de los pagos realizados.
- Controlar si las presentaciones impositivas se hicieron en tiempo y forma: un RPA compara las declaraciones juradas con lo que se registró en el sistema de la empresa.
- RPA que realiza el proceso de **circularización** para verificar el saldo que un cliente, proveedor o banco tiene con la empresa auditada

[5] La revisión de RPA utilizados por el cliente en sus procesos y controles no forma parte del presente trabajo.

[6] ERP (*Enterprise Resource Planning*); sistemas de gestión utilizado por la empresa para automatizar y administrar sus procesos en distintas áreas: finanzas, fabricación, ventas, compras, recursos humanos, etc.

4. Internet de las cosas (IoT)

Internet de las cosas (en inglés, *Internet of things*, abreviado *IoT*) se refiere al proceso que permite conectar objetos cotidianos con internet. Hay disponibles cientos de productos que se pueden comandar a distancia (drones, autos sin conductor) o activar a distancia con nuestros celulares (encender la calefacción o el horno). IoT significa objetos conectados que tienen sensores, software y otras tecnologías que les permiten transmitir y recibir datos.

El objetivo es que estén conectados a Internet y que sean capaces de recopilar datos e información y transmitirla a otros dispositivos donde puede ser guardada y analizada. Es tanto el hardware como el software y los dispositivos para recoger y transmitir los datos.

El valor que aporta IoT reside en la información que crea. El objetivo no es solo recopilar datos sino utilizarlos. Los dispositivos de IoT recopilan y transmiten los datos que luego deben ser analizados, utilizando tecnologías como *data analytics* y *machine learning*.

Hay cuatro etapas clave en este proceso[7]:

1. **Capturar los datos**. A través de sensores, los dispositivos de IoT capturan datos de sus entornos. Esto podría ser tan simple como la temperatura o tan complejo como una transmisión de video en tiempo real.
2. **Compartir los datos**. Usando las conexiones de red disponibles, los dispositivos de IoT hacen que estos datos sean accesibles a través de una nube pública o privada, según se indique.
3. **Procesar los datos**. En este punto, el software se programa para que haga algo en base a esos datos –como encender un ventilador o enviar una advertencia–.
4. **Actuar según los datos**. Se analizan los datos acumulados de todos los dispositivos de una red de IoT. Esto brinda información estratégica poderosa para fundamentar acciones y decisiones de negocio confiables.

4.1. Implementación de IoT

El valor transformador de la estrategia de IoT conlleva un riesgo adicional o, al menos, nuevas vías de riesgo que exigen nuevas estrategias de protección del valor. Con más datos sensibles a través de internet, los riesgos son mayores para las empresas, por lo cual deberían determinar qué información es adecuada para IoT, que riesgos potenciales existen e implementar soluciones que sean seguras y resistentes. Los dispositivos con conectividad de red están permitiendo nuevos tipos de ataques y representan un nuevo conjunto de objetivos para la exposición potencial de datos y delitos.

El gran desafió de seguridad de IoT es la cantidad de puntos finales conectados. Cada nuevo dispositivo introducido en un ecosistema IoT añade un nuevo punto de ataque u oportunidad para un ataque malicioso, añadiendo así de amenazas adicionales para proteger los dispositivos, los datos y los usuarios. Además, cualquier fallo de hardware o software no debería crear vulnerabilidades.

[7] Fuente: https://www.sap.com/latinamerica/insights/what-is-iot-internet-of-things.html

Otros aspectos tecnológicos importantes para habilitar IoT es analizar los protocolos de comunicación (como se comunican los dispositivos entre ellos) y las redes de comunicación (la tecnología para comunicarse, por ejemplo: WiFi o 5G).

Para maximizar el valor, reducir el riesgo y aprender rápido se debería tener en cuenta:

1. **Planificar**: analizar las ideas y las posibilidades de uso en la industria, así como el impacto humano.
2. **Hacer un inventario**: antes de invertir en nuevos equipos, realizar un inventario de todos los sensores y dispositivos conectados que ya están en el negocio.
3. **Conocer los datos que ya se tienen**: muchas organizaciones tienen un montón de datos en bruto que nunca han aprovechado, hay que analizarlos para comprender mejor el valor actual de los mismos y las lagunas que tengan.
4. **Elegir socios probados**: para analizar rápidamente ideas, probar cosas nuevas y aprender rápidamente de los fracasos. Muchos aspectos de IoT no pueden probarse en laboratorios, sino sólo con usuarios reales de la empresa y clientes externos.
5. **Adoptar un enfoque ágil**: la tecnología en torno a IoT mejora constantemente a medida que los productos existentes evolucionan y surgen nuevas categorías. Considerar el uso de prototipos ligeros y la experimentación rápida. A medida que se avance podrá dar forma a la solución, perfeccionar el modelo y aplicarlo a escala.
6. **Mejorar el talento:** las empresas que persiguen estrategias de IoT también deben contar con el talento necesario para operar y mantener miles de dispositivos conectados. Considerar la posibilidad no solo de traer nuevos talentos sino también volver a capacitar a los empleados actuales.

Casos de aplicación de IoT en las empresas

- En procesos de fabricación: impulsar la automatización, analizar datos para prever y prevenir fallas de equipos y mejorar la seguridad laboral.
- En plantas industriales: permiten detectar desvíos y generar alarmas y mensajes a los usuarios para que realicen las acciones correctivas necesarias. En algunos casos pueden iniciar protocolos de actuación de forma automática para tratar dichas alarmas.
- En el sector ganadero: a través de la geolocalización ayuda a tener los animales siempre controlados.
- Transporte: uso de sensores en aviones, trenes, buques y vehículos para optimizar desde el rendimiento de motores y seguridad hasta logística y gestión de la cadena de suministros.

4.2. Aplicación en Auditoría

El uso de drones (vehículos aéreos no tripulados) combinados con sensores de IoT tienen el potencial de modernizar y hacer más eficientes algunos procesos de auditoría. Los drones permiten obtener imágenes cubriendo grandes distancias y espacios, mostrar el estado de los terrenos, materiales y productos e ingresar a ubicaciones de difícil acceso. Esta herramienta permite alcanzar una perspectiva única a relevar con gran nitidez y claridad los objetos, presentando los hallazgos en forma certera, segura y oportuna.

Estás imágenes sumadas a la capacidad de analizar las mismas y al conocimiento de la industria con que cuentan los auditores, proveen información relevante y de suma utilidad en el

caso de verificaciones de inventario de materias primas, productos y de activos fijos. La geolocalización y la información contenida en la metadata de las imágenes conforman un documento inalterable que asegura al auditor la validación de sus conclusiones con parámetros objetivos de tiempo y espacio.

Al utilizar drones para efectuar recuentos físicos de inventario, se ahorra tiempo a los auditores y costos en caso de tener que viajar a diferentes lugares, lo que aporta eficiencia al proceso.

5. Herramientas colaborativas

Las herramientas colaborativas son programas informáticos que permiten a los usuarios comunicarse y trabajar en equipo compartiendo información o produciendo conjuntamente nuevos documentos. Tienen como objetivo mejorar el proceso de trabajo y, en general, contienen funciones para planificar, organizar y analizar tareas.

En la actualidad, el uso de herramientas o sistemas colaborativos facilita a los equipos de auditoría comunicarse y trabajar conjuntamente sin la necesidad de estar reunidos en el mismo lugar. Las herramientas colaborativas generan grandes oportunidades para mejorar la comunicación, supervisión y control de los equipos de auditoría, e incluso en muchos casos, la comunicación e interacción con el cliente.

5.1. Tipos de herramientas

5.1.1. Documentos y planillas de uso colaborativo

El almacenamiento de documentos o planillas que forman parte de los papeles de trabajo[8] del auditor, en reservorios colaborativos en la nube, tales como Dropbox o Google Drive, permiten la interacción de todo el equipo sobre los papeles de trabajo.

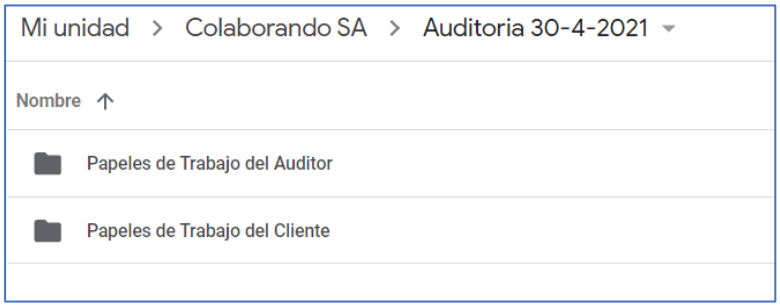
Ventajas de su uso:

- Permiten realizar cambios, revisiones o modificaciones en los papeles de trabajo.
- Todos los participantes cuentan con la última versión actualizada del documento o la planilla.
- Queda documentado quien sugiere cambios o hace comentarios sobre papeles de trabajo.
- Facilita la supervisión final antes del cierre de los papeles de trabajo.

Aplicación en la auditoría:

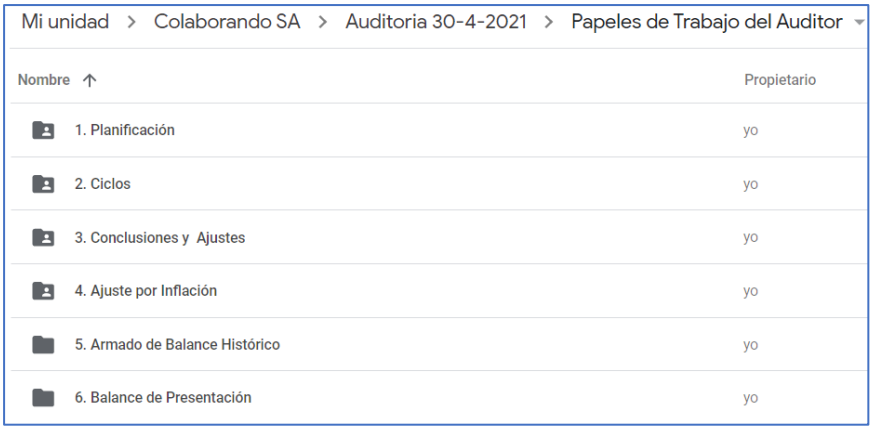
A continuación, se detallan algunos ejemplos del uso de carpetas de trabajo compartido que facilitan el trabajo de planificación, revisión y control del contador en un encargo de aseguramiento de estados contables.

- **Organización de papeles de trabajo:** El contador a cargo del encargo de auditoria puede abrir un directorio por cliente y por fecha de cierre de ejercicio, abriendo en ese directorio diferentes carpetas que le permitan organizar los papeles de trabajo.



Se podría organizar la carpeta abriendo una carpeta de papeles de trabajo del auditor y papeles de trabajo del cliente.

[8] Toda mención a Papeles de Trabajo hace referencia a la terminología utilizada en la RT N°37. Esta denominación fue reemplazada en la RT N°53 por Documentos del Encargo.



Dentro de la carpeta de trabajo del auditor se podrían, por ejemplo, generar carpetas que correspondan a cada una de las etapas del trabajo.

Compartiendo cada una de las carpetas y dando permiso de lectura y escritura en cada uno de los papeles de trabajo, otorga la posibilidad de visualizar rápidamente quien realizó la última modificación y fecha y hora en que el documento ha sido modificado por última vez:

- **Revisión de papeles de trabajo:** El uso compartido de documentos, formularios o planillas permite dejar plasmado en cado uno de los papeles de trabajo las referencias a la revisión de estos, o dejar comentarios al colaborador para completar o responder consultas que no han quedado claras en el papel de trabajo. Facilita la revisión en simultáneo y oportuna.

- **Revisión de estados contables:** Compartiendo el balance de presentación borrador directamente con el cliente, permite que el cliente también pueda realizar comentarios, sugerencias o cambios directamente, que luego podrán ser revisados o aceptados por el auditor.

5.1.2. Proyectos y tareas

Existen en el mercado plataformas de uso compartido, en versión gratuita o paga, que permiten realizar un seguimiento de cada uno de los encargos de auditoría, como si los mismos fuesen proyectos. Ejemplos de algunos de estos productos: Bitrix24, Trello.

Ventajas de su uso:

- Permite compartir el plan de trabajo asignándole tareas a cada miembro del equipo.
- Queda documentado el plan de trabajo y los participantes.

- Cada tarea finalizada puede pasar a una etapa de supervisión del gerente o socio a cargo del encargo.
- Permite asignar tiempos a cada tarea.

Aplicación en la auditoría:

El contador podría crear un proyecto por cada encargo de auditoría, compartiendo ese proyecto con el equipo de trabajo. Dentro de cada proyecto puede generar tareas y asignarlas a alguno de los miembros del equipo. En la asignación de tarea se describe el objetivo y se puede detallar el procedimiento, estableciendo fechas de inicio y finalización de la tarea. Adicionalmente se pueden adjuntar documentos o papeles de trabajo en cada tarea.

A efectos de la supervisión una vez que la tarea se encuentra finalizada cambia su estado a tarea para revisión, facilitando al contador el seguimiento y revisión de las tareas programadas. Al revisar cada tarea, se puede reasignar una subtarea o se pueden dejar comentarios a quien tenía la tarea a cargo.
Las plataformas existentes en el mercado permiten filtrar las tareas de cada proyecto por tareas vencidas o tareas a revisar. Adicionalmente se pueden visualizar en forma de GANTT, ordenando las tareas en secuencia, o en formato Kanban por estado.

5.1.3. Control de Tiempos

El uso de herramientas colaborativas también permite, aunque sea en un Excel compartido, llevar una base de datos del registro de horas de cada uno de los colaboradores.

Ventajas de su uso:

- Establecer desvíos respecto del presupuesto de horas por trabajo.
- Al asignarle una tarea a cada proyecto permite medir en que procedimiento o tarea se genera el desvío para poder reestimar correctamente las horas al renovar la contratación con el cliente, o fundamentar una facturación adicional por exceso de horas.
- Permite al rol de gerente o supervisor anticiparse al consumo en demasía de las horas.

Aplicación en la auditoría:

El contador podría crear una matriz o base de datos con los campos del nombre del cliente, nombre del colaborador, fecha, tipo de encargo (por ejemplo, auditoria de estados contables 2021), procedimiento (por ejemplo, toma de inventario, prueba de pasivos omitidos, etc.) y la cantidad de horas insumidas.

En otra tabla puede tener las horas presupuestadas por cliente, por encargo y por procedimiento y generar un cruce de datos entre las horas presupuestadas y las horas insumidas, por encargo y por tipo de procedimiento. Esta información se puede visualizar también a través de gráficos.

5.1.4. Comunicaciones

En la actualidad existen diferentes plataformas de comunicación que agilizan las conversaciones del contador con su equipo de trabajo. Algunas aplicaciones son solo para comunicarse, como puede ser el caso de WhatsApp, pero también existen plataformas integradas que permiten llevar proyectos y tareas y armar grupos de chat dentro de la misma plataforma por proyecto/cliente/ encargo.

Ventajas de su uso:

- Permite agilizar las conversaciones dentro del equipo de trabajo.
- Permite transferir documentos o papeles de trabajo a través del chat.
- Si se cuenta con una plataforma integrada en la nube quedan documentadas las discusiones que se generan dentro del equipo de trabajo sobre determinado asunto del encargo.

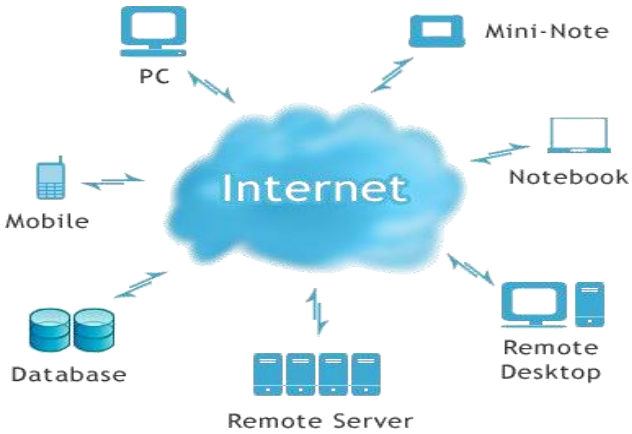
5.2. Resguardo de la documentación

Con respecto al soporte de las tareas que debe realizar el profesional actuante, sobre la documentación del encargo:

- Definir un diseño adecuado de los resguardos de los documentos de trabajo (por ejemplo, una estructura de árbol conformada por carpetas y archivos) que guarde relación con los programas de trabajo que surjan de la planificación de la tarea, agrupándolos por tipo de legajo y procedimiento, en el que incluirán las copias activas de trabajo.
- Tener en cuenta que la documentación a resguardar se conformará con “toda” la documentación correspondiente al encargo. Sin ánimo de agotar el listado: documentación referida a los procesos mediante los cuales la información se genera, datos y documentos referidos al encargo, información obtenida de terceros, los documentos generados por el revisor y sus informes, las afirmaciones del responsable en caso de tratarse de un encargo de constatación, inclusive, la carta convenio si se firmara digitalmente.
- Para el acceso a los documentos, aplicar el principio de saber-hacer, cada integrante del equipo de trabajo debe acceder a los recursos necesarios para la ejecución de su tarea exclusivamente.
- Realizar copias de seguridad (*backups)* de los documentos de trabajo en forma rutinaria.

6. Computación en la nube (Cloud Computing)

Cloud Computing es un modelo que, mediante una petición de red, permite el acceso a un conjunto compartido de recursos informáticos configurables, por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios, que pueden ser rápidamente aprovisionados y puestos en producción con un esfuerzo mínimo de administración o de interacción con el proveedor de servicios.[9]



Fuente: Imágenes de Google

La computación en la nube se está convirtiendo en el estilo de diseño dominante para nuevas aplicaciones y para la adecuación de una gran cantidad de aplicaciones ya existentes, facilitando y flexibilizando los despliegues tanto de infraestructuras, como de herramientas y componentes para el desarrollo ágil de aplicaciones y servicios. Su adopción otorga, entre otras ventajas, la posibilidad de transformar los costos fijos que implica una estructura de TI en variables (accediendo a los servicios a través de la red y mediante un SLA[10]).

Estos servicios se realizan cuando un usuario, mediante un acuerdo de nivel de servicios (SLA) contrata a un proveedor de servicios u organización de servicios (OS) para la realización de determinados procesos de IT.

La computación en la nube permite el acceso a los datos en tiempo real desde cualquier parte en cualquier momento. Las ventajas son mayor eficiencia, mayor disponibilidad, escalabilidad, rápida aplicación y bajos costos iniciales. Los proveedores de nube (organizaciones de servicios) ofrecen sus servicios por alguno de los tres tipos principales de servicios de informática en la nube:

- **Infraestructura como servicio (IaaS):** acceso a almacenamiento y capacidad de cómputo. Es la categoría más básica y permite "alquilar" infraestructura de TI de un proveedor de servicios en la nube (servidores y máquinas virtuales, almacenamiento, redes y sistemas operativos). El cliente asume los riesgos sobre datos y seguridad de las aplicaciones.

[9] Definición según NIST- National Institute of Standards and Technology.
[10] SLA- *Service Level Agreement*: Acuerdo de nivel de servicios.

- **Plataforma como servicio (PaaS):** ofrece a los desarrolladores herramientas para crear y hospedar aplicaciones web. Está diseñado para dar acceso a los usuarios a los componentes que necesitan para desarrollar y utilizar con rapidez aplicaciones web o móviles, sin preocuparse por configurar y administrar la infraestructura de servidores, almacenamiento, redes y bases de datos subyacentes (por ejemplo: *App´s de Google*).

- **Software como servicio (SaaS):** método de entrega de aplicaciones de software donde los proveedores de servicios en la nube hospedan y administran de forma integral las aplicaciones. Facilita tener la misma aplicación en todos sus dispositivos a la vez porque toda la inteligencia y datos de aplicación están alojados en la nube (por ejemplo: Gmail, etc.)

Inicialmente todos estos servicios de computación en la nube eran ofrecidos por sus fabricantes a través de internet (nube pública), si bien los proveedores empezaron a ofrecer su tecnología de nube de forma que pudiese ser instalada sobre infraestructura física privada para que los clientes pudiesen optar por desplegar su propia nube privada facturándolos bien en modalidad pago por uso, o bien mediante costes fijos en función de la capacidad asignada.

6.1. Implementación de Computación en la nube

Antes de iniciar un proceso de migración a la nube, se deben considerar estos cuatro aspectos:

1. **Antes de implementar**
   - Evaluar los costos y beneficios relacionados al cambio a un proveedor en la nube.
   - Identificar y clasificar todos los activos de información (datos, aplicación, procesos) dentro del alcance.
   - Preparar una lista de posibles candidatos a proveedores de nube y realizar una verificación sobre ellos (situación económica, referencias, autenticidad, etc.).
   - Involucrar a las áreas de control (legal, cumplimiento, finanzas, etc.) durante el proceso de decisión de migrar a servicios en la nube.
   - Evaluar el diseño y los requisitos de los proveedores (organización de servicios) para mudarse a la nube y/o solicitar un período de prueba.

2. **Una vez elegido el proveedor (organización de servicio**s) solicitar y verificar, entre otros aspectos:
   - La política de seguridad para verificar que este alineada con sus propias políticas.
   - La lista de ubicaciones de infraestructura y las medidas técnicas de seguridad en lugar (IDF/IPS, cortafuegos o *firewall*s, etc.).
   - Los detalles técnicos y controles que aplica para garantizar la privacidad de los datos.
   - El proceso de gestión de incidentes de seguridad para asegurarse que esté alineado con sus propias políticas de seguridad.
   - Información sobre la gestión de vulnerabilidades, gestión de parches y gestión de versiones.

3. **Acordar los términos y condiciones, entre otros, asegurarse de:**
   - Seguir siendo el único propietario de cualquier activo migrado.
   - Que la capacidad contratada esté siempre disponible y no ser dirigido a otros proveedores sin aprobación.

- Que le proporcionen informes periódicos sobre seguridad (informes de incidentes, Registros IDS / IPS, etc.) para su análisis.
- Que el proveedor aplique un borrado de datos obligatorio bajo su aprobación al vencimiento del contrato.
- Acordar una estrategia de salida, especificando los términos que desencadenan la recuperación de los activos de la empresa en el plazo requerido.

4. Establecer medidas preventivas:

- Cifrar todos los activos sensibles antes de la migración para evitar la divulgación y garantizar que se lleve a cabo una gestión adecuada de las claves.
- Utilizar sistemas de gestión de acceso e identidad corporativa en lugar de los sistemas de gestión de acceso del proveedor. Requerir la implementación de un canal seguro entre la infraestructura y el sistema de gestión de acceso corporativo.
- Asegurarse de que se aplique una política de seguridad global que especifique los requisitos mínimos aplicado a todas las entidades que comparten una nube comunitaria.
- Implementar un plan de recuperación ante desastres (*Disaster Recovery Plan* o DRP) teniendo en cuenta la posibilidad de una interrupción completa del proveedor**.**

6.2. Aplicación en Auditoria

El uso de la nube posibilita que los auditores puedan atender a los clientes desde cualquier lugar y que varios profesionales trabajen en el mismo cliente simultáneamente. También elimina algunos costos relacionados con actualizaciones de software y back-up de seguridad (los servicios en línea se actualizan y hace back-ups automáticamente).

Otras ventajas son que se requiere una infraestructura tecnológica simple (se utilizan tabletas, computadoras portátiles, teléfonos inteligentes y una conexión a internet). En general no se debe realizar una instalación de software en los dispositivos, solo una aplicación de acceso. Las principales desventajas con la protección de los datos y el acceso o descarga de los mismos cuando el usuario quiere descontinuar el servicio o si el proveedore deja de operar.

El acceso a través de la nube puede solucionar problemas como información incompleta o modificaciones posteriores, y evita el inconveniente del traslado de información. Dado que funcionan *on line* el auditor y el cliente pueden tener acceso a los mismos datos al mismo tiempo, por lo que ante cualquier cambio o ajuste realizado se tendrá la información actualizada. Además, es posible incorporar sistemas de alerta para verificar tendencias o irregularidades en tiempo real y solucionarlas a tiempo.

La computación en la nube permite a las firmas contables ampliarse y reducirse rápidamente sin incurrir en costos de red y hardware.

Informes sobre los controles en una Organización de servicio[11]

El objetivo de estos *encargos* es que el contador emita un informe sobre los controles vigentes en una *organización de servicios* que se presumen relevantes para el control interno de las

[11] Más información en: Resolución Técnica N° 37 (modificada por la RT N°53) – Capítulo V. NORMAS SOBRE OTROS ENCARGOS DE ASEGURAMIENTO. Apartado A, Otros Encargos de Aseguramiento en General. Punto 14 y Apartado C INFORMES SOBRE LOS CONTROLES DE UNA *ORGANIZACIÓN DE SERVICIOS* y en NIEA 3402 Informes de Aseguramiento sobre los Controles en las Organizaciones de Servicios.

empresas usuarias de esos servicios, en cuanto se relacionan con la preparación de su información contable. El informe que emita el contador será utilizado por las empresas usuarias de tales servicios y por sus auditores.

Las empresas que contraten a una organización de servicios pueden solicitarle un Reporte SOC, a fin de asegurarse que han implementado controles para administrar la información de manera segura. El reporte SOC evalúa los controles internos de la organización de servicios en términos de seguridad, disponibilidad, integridad del procesamiento, confidencialidad y privacidad.

Los informes de control de organización de servicio (SOC), conocidos como SOC 1, SOC 2 o SOC 3, son marcos establecidos por el Instituto Estadounidense de Contadores Públicos Certificados (AICPA) para informar los controles internos implementados en una organización de servicios. Son informes de aseguramiento que los contadores pueden emitir en relación con el control de estas organizaciones.

SOC 1: Informe sobre controles en una empresa de servicios, relevantes para evaluar control interno de empresas usuarias para estados financieros.

SOC 2: Informe sobre controles internos en una empresa de servicios, relevantes para la Seguridad, Continuidad, Procesamiento, Integridad, Confidencialidad. Son una auditoría de los procedimientos de control en las organizaciones de TI que ofrecen servicios. En resumen, se trata de un estándar internacional de generación de informes sobre los sistemas de gestión de los riesgos de ciberseguridad. El encargo será firmado por un contador público, pero será necesaria la colaboración interdisciplinaria de profesionales con conocimientos de IT y procesos.

SOC 3: Informes de Confianza, para empresas de servicios. Distribución pública. Al igual que el informe SOC 2 este informe también será firmado por un contador público, pero será necesaria la colaboración interdisciplinaria de profesionales con conocimientos de IT y procesos

7. Big Data y Data Analytics

El **Big Data** es un término que se utiliza para describir volúmenes grandes de datos. En esta terminología comprende los datos estructurados y no estructurados que son producidos y gestionados todos los días. En ellos puede encontrarse cualquier cantidad de información vital para desarrollar y optimizar empresas, modelos de negocios y cualquier proceso inclusive la auditoría de estados financieros.

Lo interesante de la actualidad del Big Data no es solo su volumen, sino la funcionalidad que se obtiene de ellos al analizarlos. Las organizaciones actualmente utilizan herramientas tecnológicas muy potentes para navegar entre estos conjuntos gigantescos de información y encontrar formas más eficientes de realizar procesos, descubrir gustos y preferencias de los usuarios y potenciar los procesos estratégicos de toma de decisiones.

Para entender por qué este tipo de datos es tan importante es necesario explorar sus principales fuentes u orígenes. Es posible obtener datos directamente de la conexión a internet o del internet de las cosas e incluso conseguir información valiosa en datos experimentales.

Es importante destacar que puede obtenerse diferentes tipos de datos y que estos dependerán de los formatos de archivos. Estos datos pueden ser no estructurados si son documentos, vídeos, audios entre otros. En cambio, los datos semi estructurados se tratan con diferentes tipos de software. Los datos estructurados constituyen la menor cantidad de datos que hay en el mundo digital, por lo que obtener información correctamente analizada puede representar un reto. Aquí es donde entran a jugar un rol fundamental los grafos.

El Rol de los grafos

Los grafos son estructuras de especial importancia en la que es posible almacenar cantidades grandes de información. Pero lo mejor de estas maravillas que empezaron a idearse cientos de años atrás, es que permiten entender las conexiones entre los datos que albergan. Los grafos están compuestos por nodos en los que podemos encontrar diferentes tipos de datos y estos pueden estar relacionados o conectados a otros nodos a través de aristas.
Al poder hacer un seguimiento detallado y con el apoyo de poderosas herramientas, darle rango visual para el ojo humano, es posible entender de mejor manera los datos para tomar decisiones correctas y ajustadas a la realidad.

Los grafos permiten estudiar y determinar las interrelaciones entre unidades de datos, siendo de especial importancia en los análisis de *big data*. El *Big Data* concentra, analiza o gestiona cantidades gigantescas de datos y los grafos favorecen su entendimiento para tener un diagnóstico acertado y de calidad de ellos. Los grafos pueden ayudar, si son desarrollados de forma acertada, a atender las principales dificultades del *big data*.

En instancias de gran volumen de datos, los diferentes métodos de análisis pueden ayudar a recolectar, limpiar, integrar y obtener datos de calidad en tiempos cortos de análisis. Además, esta reducción de tiempo en procesos de estudio permite que la toma de decisiones pueda ser desarrollada a tiempo, disminuyendo el porcentaje de probabilidad de ejecutar tareas cuando los datos ya caducaran.

Lo más importante en la vinculación de estas dos áreas tan potentes del desarrollo tecnológico es que pueden ser extrapoladas a diferentes áreas y ser aprovechadas de forma rápida para solucionar problemas. Esta área está en pleno desarrollo y crecimiento.

Los grafos y las bases de datos de grafos proporcionan modelos de grafos para representar las relaciones. Permiten a los usuarios aplicar el reconocimiento de patrones, la clasificación, el análisis estadístico y el aprendizaje automático a estos modelos, lo que posibilita un análisis más eficiente a escala de grandes volúmenes de datos.

Como las bases de datos de grafos almacenan explícitamente las relaciones, las consultas y los algoritmos utilizando la conectividad entre vértices, pueden ejecutarse en subsegundos en lugar de horas o días. Los usuarios no necesitan realizar innumerables combinaciones y los datos se pueden utilizar más fácilmente para el análisis y el aprendizaje automático, para descubrir más sobre el mundo que nos rodea.

Dimensiones del Big Data

Son las características que deben cumplir los conjuntos de datos para ser considerados como Big Data. Actualmente se clasifican las dimensiones en 5V:

- Volumen: continuo incremento en los datos día a día,
- Variedad: los datos provienen de distintos canales (transacciones, sensores, ERP, etc.), fuentes (interna o externa) y formatos (imágenes, vídeo, voz y texto)
- Veracidad: es necesarios filtrar los datos que pueden ser falsos y controlar su integridad
- Velocidad: Los datos se generan a una gran velocidad. Se deben almacenar y analizar antes de que pierdan valor.
- Valor: que se pueda extraer información útil de los datos, de manera rentable y eficiente

7.1. Implementación de Big Data y Data Analytics

La automatización de procesos, el uso de ERP, los cambios tecnológicos y el incremento de transacciones generan una gran cantidad de datos en las empresas (**Big Data**). Esta información para que resulte útil debe ser revisada y analizada.

Se conoce como **Data Analytics** (Análisis de Datos) a los procesos que permiten obtener información a través de la interpretación de patrones relevantes sobre una base de datos. Se buscan resultados a partir del análisis y transformación de datos (cualitativos y cuantitativos) para resaltar información útil, brindar conclusiones y apoyar la toma de decisiones.

Para ello es necesario:

1. Definir qué se medirá y/o analizará, y cómo se hará dicha medición
2. Recolectar y extraer los datos
3. Organizar y analizar los datos
4. Interpretar los resultados
5. Utilizar los resultados

Debido a la gran demanda en la gestión de los datos que surgen del Big Data empresas como Microsoft, Google, Apache, etc., han desarrollado productos para almacenar, clasificar, analizar y gestionar los grandes conjuntos de datos.

Antes de tomar la decisión de implementar Big Data/Data Analytics se debería:

- Evaluar si se cuenta con un conjunto de datos lo suficientemente grande y verificar si son datos estructurados, semiestructurados y no estructurados.
- Analizar si los resultados a obtener de los datos son relevantes para la organización
- Contar con los recursos de hardware y software necesarios
- Contar con el personal capacitado
- Definir costos, resultados esperados y el tiempo planificado para su implementación.

Ventajas de su aplicación

La principal ventaja es la mejora en la toma de decisiones, ya que se analiza un universo mayor de información, mejorando la calidad y confianza en los resultados y generando información oportuna y en tiempo real que permite reducir riesgos.

Limitaciones en la implementación

- Falta de infraestructura tecnológica
- Falta de habilidades y conocimientos en los recursos humanos
- Deficiente definición de objetivos, metodologías y políticas de seguridad

7.2. Aplicación en Auditoría

La aplicación de Big Data/Data Analytics es una oportunidad para mejorar la eficiencia y la asignación de recursos en el trabajo de auditoría, pero su impacto dependerá de la estructura del estudio. Las grandes firmas podrán desarrollar sistemas de análisis de datos aplicado en los ERP de los clientes y, además, podrán utilizarlos para varios trabajos de auditoría por su volumen de negocio y la magnitud de las empresas que auditan. Es decir, podrán hacer estos desarrollos rentables más fácilmente.

Para las firmas de menos tamaño será difícil desarrollar un sistema de análisis que pueda aplicar a varios clientes y que sea rentable. Para superar esto existen aplicaciones en el mercado que pueden ser utilizadas en múltiples clientes y trabajos de auditoría, así como para varias firmas.

Principales ventajas en el proceso de auditoría:

- Mayor confianza en el resultado de las pruebas al aumentar la muestra o aplicar sobre la totalidad del universo.
- Reduce costos y tiempos de ejecución.
- Se pueden crear, consultar y visualizar informes usando diferentes fuentes de datos de manera fácil, ágil y rápida.
- La información está disponible 24/7 con acceso desde cualquier dispositivo con conexión a internet.
- Mejora la evaluación de riesgos de las empresas clientes identificando anomalías y patrones de alto riesgo para intensificar las pruebas de auditoría.
- Se obtiene un conocimiento más profundo de los clientes para ayudar en la planificación de la auditoría.

- Con la aplicación conjunta de IA o “machine learning” se pueden detectar incongruencias o situaciones irregulares cuyo origen puede ser la manipulación de información o el fraude (auditoría continua sobre los procesos).

Ejemplos de aplicación a pruebas de auditoría

- Cuentas por Pagar: buscar duplicados en pagos y facturas. Resumir movimientos por proveedor para verificar los saldos individuales. Conciliar los pagos con las facturas del proveedor. Identificar datos incorrectos o inusuales
- Cuentas por Cobrar: Efectuar un análisis de deudas por vencimiento. Detectar saltos en la secuencia de facturas. Identificar facturas duplicadas. Identificar diferencias entre nota de pedido, remitos y facturas.
- Activos Fijos: Identificar activos totalmente amortizados. Comparar el valor contable con el valor recuperable. Identificar activos con vida útil o tasas de amortización superiores a las establecidas.
- Nómina: Comparar la nómina al inicio y al cierre de ejercicio para identificar nuevos empleados y las bajas. Verificar si los cambios en la remuneración son los esperados. Totalizar remuneraciones, pagos netos, retenciones y cualquier otro dato con valores.

7.3. El futuro de Big Data: IA y Machine Learnig[12]

La inteligencia artificial (IA) y el aprendizaje automático (*machine learning*) se ven comúnmente como áreas de gran interés debido a su promesa de mejorar los resultados comerciales y crear un nuevo impacto. Los grafos pueden utilizarse para potenciar la ciencia de datos de algunas maneras clave.

Cuando se trata de aprendizaje automático, los modelos se basan en datos. Cuanto mejores sean esos datos, cuanto más ricos, profundos y completos sean, generalmente, mejor será el modelo de aprendizaje automático. Hay un paso completo para crear un modelo de aprendizaje automático, llamado **ingeniería de características**[13], que implica enriquecer los datos.

Hay ciertos tipos de **ingeniería de características** que pueden ser más complicados de lograr, especialmente cuando se trata de observar las relaciones con los datos y colocar esas relaciones en primer plano. Tratar de hacerlo puede requerir demasiadas combinaciones y el proceso puede ser lento y engorroso. La solución con grafos, más comúnmente, las características para el aprendizaje automático se pueden crear a través de grafos ejecutando algoritmos de grafos en un conjunto de datos que se ha cargado en una base de datos de grafos y creando datos enriquecidos, que luego se pueden utilizar para el aprendizaje automático. Este paso de la ingeniería de características proporciona al modelo de aprendizaje automático información más completa y útil.

Por ejemplo, un modelo de aprendizaje automático ya podría tener información sobre un nuevo cliente, en base a la información suministrada respecto a la organización y los riesgos

[12] Machine learning es un subconjunto de inteligencia artificial (IA): consiste en enseñar a las computadoras a aprender de los datos y mejorar con su uso. Los algoritmos se capacitan para encontrar patrones y correlaciones en grandes conjuntos de datos y para tomar las mejores decisiones y predicciones basadas en ese análisis (fuente: https://www.sap.com/latinamerica/insights/what-is-machine-learning.htm).

[13] La ingeniería de características en el proceso de tomar un conjunto de datos y construir variables explicativas - **características**- que se pueden usar para entrenar un modelo de machine learning para un problema de predicción.

asociados con su cliente potencial y la clase de servicio por presupuestar, de forma de arribar a la respuesta de auditoría adecuada al nivel de riesgo evaluado para el trabajo incluyendo las características que debería tener el equipo de trabajo por seleccionar para cumplir los requerimientos del compromiso incluyendo la confección de la carta de contratación. De esta forma cualquier proceso de evaluación de riesgos es pasible de ser llevado a un modelo que clasifique y evalúe el riesgo y, en base a eso permita formular predicciones para minimizar dichos riesgos. Al incluir características derivadas de los grafos, los modelos de aprendizaje automático pueden volverse más potentes y precisos. Alternativamente, los algoritmos de grafos se pueden ejecutar en datos para generar nuevos conocimientos, como el uso de *clustering*[14] para encontrar nuevos riesgos potenciales similares en función de los que contrataron.

[14] El *clustering* es un proceso que consiste en agrupar ítems en grupos con características similares y se utiliza para determinar patrones.

8. Ciberseguridad

La **ciberseguridad** o seguridad informática es un conjunto de procedimientos y herramientas que se implementan para proteger los datos e información que se genera y procesa a través de la infraestructura de sistemas.

El auditor debería considerar el riesgo cibernético. Una forma eficaz y eficiente para gestionar dichos riesgos es partiendo de la consideración del enfoque proporcionado por el Marco Integrado de Control Interno del COSO Marco 2013 (en adelante Marco 2013), como el Marco Integrado de Gestión de Riesgos Empresariales (2004).

En primer lugar, se debe partir del conocimiento sobre los efectos que podría conllevar una gestión organizacional reactiva y tener en cuenta que un daño de un ciberataque podría ser tan grave que la organización podría dejar de existir y operar.

Por ello la primera recomendación en materia de seguridad informática debiera ser la de ubicar como objetivo estratégico para la organización al riesgo cibernético, ya que, con el paso del tiempo, la evolución de las tecnologías y la mayor sofisticación de los hackers, el riesgo cibernético cobrará cada vez mayor relevancia. En tal sentido, la organización debería tener en cuenta los siguientes aspectos:

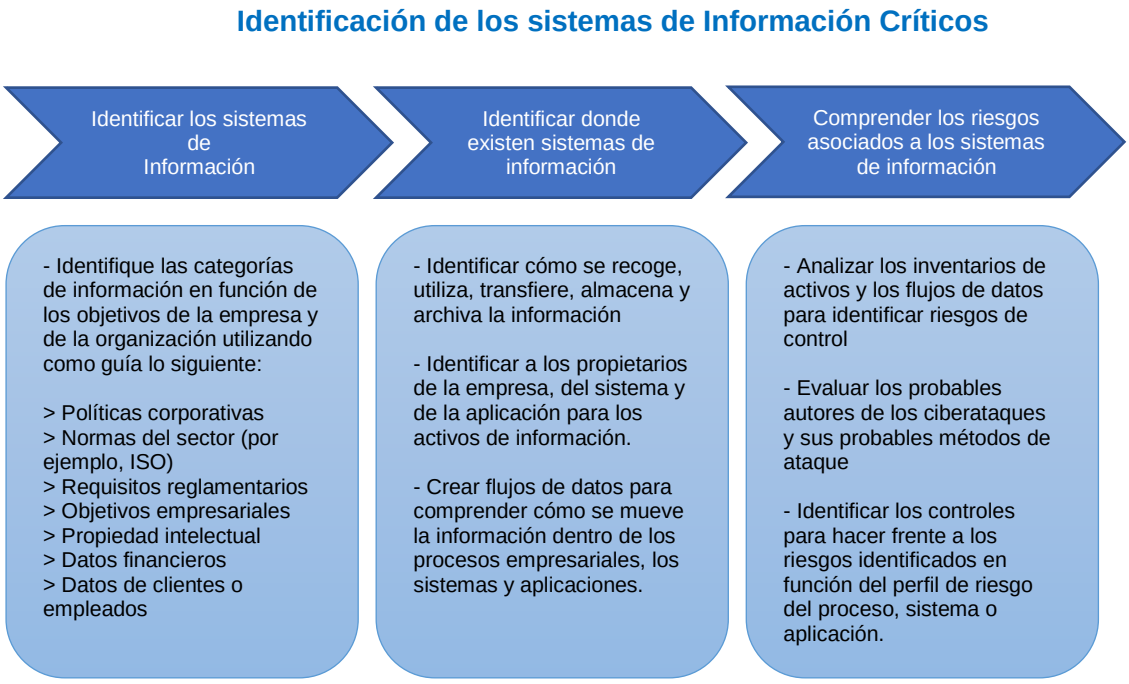
- Las actividades de control son las acciones realizadas por los individuos dentro de la organización que ayudan a garantizar el cumplimiento de las directrices de la Dirección para mitigar los riesgos que afectan a la consecución de los objetivos.
- Los ataques cibernéticos son inevitables y algunos tienen éxito.
- Las estructuras de control deben desplegarse en forma de capas.
- Los ataques pueden tener origen interno como externo.
- El objetivo es mantener a los intrusos fuera del entorno informático, y si ingresan, detectarlos a tiempo y corregir.
- La organización desplegará controles preventivos, detectivos y correctivos.

El Marco 2013 puede ser utilizado como guía para que la organización logre una transformación que les permita diseñar, evaluar y mantener un entorno de seguridad, vigilancia y resistencia en un mundo que cada vez más será impulsado por la cibernética.

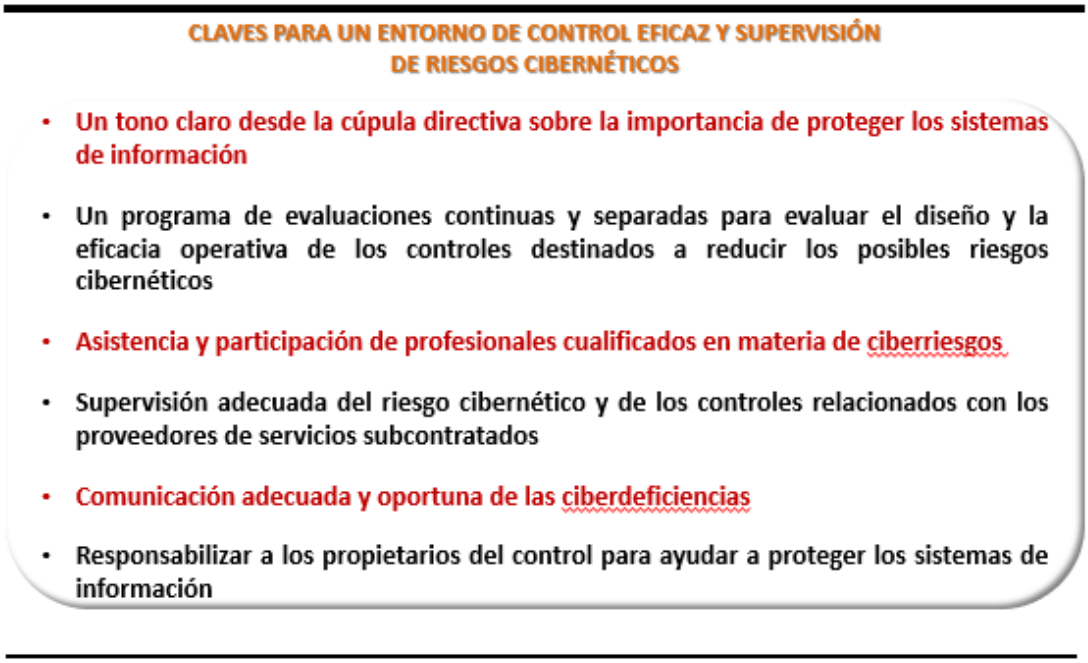
A continuación, se presentan algunas preguntas que podrían resultar clave para guiar a la organización en este proceso:

Fuente: Coso in the Cyber Age – COSO (traducción propia)

Una parte clave de la utilización del Marco de 2013 para gestionar el riesgo cibernético es identificar los sistemas de información de valor y llevar a cabo las evaluaciones de riesgo para esos activos. A continuación, se presenta un enfoque de alto nivel para crear el inventario de sistemas de información y la evaluación de riesgos (según lo identificado por el Principio 6 de COSO). El resultado (output) será un inventario de activos de información, un análisis de brechas y controles priorizados para ser implementados en la organización.



Fuente: Coso in the Cyber Age – COSO (traducción propia)



Fuente: Coso in the Cyber Age – COSO (traducción propia)

Adicionalmente a lo descripto precedentemente, hacer uso de las tecnologías aplicadas a la reducción de riesgos resulta fundamental. El problema de la seguridad cibernética involucra

áreas complicadas, como la detección de tráfico no válido, la caza de amenazas cibernéticas y la detección de *malware*.

Para proteger los sistemas informáticos se deben adoptar políticas de seguridad integrales y aplicables a todos los equipos conectados a la red. Las soluciones van más allá de contar con un antivirus, algunas medidas a implementar son:

1. **Establecer políticas de seguridad**: Con el objetivo de mitigar el riesgo de pérdidas o accesos no autorizados, proteger la información y garantizar la confidencialidad de los datos. Se suelen incluir planes de acción antes fallas o ataques. También se incluyen reglas sobre el uso para ayudar a los empleados a prevenir brechas de seguridad (prohibición de acceder a web sospechosas, no insertar unidades USB sin autorización, etc.).
2. **Respaldar la información**: Se deben realizar copias de seguridad automáticas y periódicas de la información (respaldos físicos o en la nube) a fin de recuperarse más rápido de cualquier ataque. Adicionalmente, se pueden encriptar los backups con contraseña.
3. **Cifrar las comunicaciones**: Se deben proteger las comunicaciones en donde se transmiten datos sensibles (cifrar contraseñas de usuarios, datos personales, datos financieros, acceso a correo electrónico, etc). El cifrado consiste en "alterar" la información para que no sea legible para terceros que puedan acceder.
4. **Utilizar Antivirus**: Tanto para los equipos fijos como móviles (incluyendo tabletas y teléfonos inteligentes). Los antivirus deben tener actualizaciones periódicas, servicio técnico y ser fáciles de instalar
5. **Proteger todos los equipos conectados a la red:** como impresoras o televisores inteligentes. No existen antivirus para estos aparatos, pero se puede limitar el riesgo. Como primera medida, se deben mantener actualizados los softwares de cada producto. En el caso de las impresoras, utilizar cortafuego o *firewall*, no mantener conexión abierta a Internet, cifrar el disco duro y utilizar contraseñas para su uso.
6. **Adquirir herramientas de seguridad**: instalar cortafuegos o *firewalls* o cortafuegos para analizar y filtrar el tráfico que entra y sale y bloquear posibles amenazas. Puede ser hardware (dispositivos que se añaden a la red) o software (una aplicación que se instala en el computador), el primero protege a todos los dispositivos conectados a la red, mientras que el segundo solo protege el dispositivo en el que está instalado.

8.1. Tipos de herramientas de seguridad informática

La seguridad informática se construye formando a los empleados para que sepan tratar los datos de la empresa, creando protocolos de actuación y reacción frente a ataques y con el uso de software y otras herramientas. Entre las principales podemos encontrar:

- **Software antivirus**: aportan protección ante *malware* u otros elementos maliciosos, frenan posibles amenazas y pueden poner el dispositivo en cuarentena. Lo importante es que todos los dispositivos conectados a la res de trabajo cuenten con un antivirus de calidad, fiable y actualizado
- **Cortafuego o *firewall* de red**: inspeccionan el tráfico web, identifica a los usuarios habilitados, bloquea accesos no autorizados, de acuerdo con las reglas previamente definidas.

- **Servidor proxy**: es un dispositivo que actúa de intermediario entre internet y las conexiones del navegador y filtra lo que circula entre ambos. Puede bloquear sitios web peligrosos o aquellos que no se permita el acceso dentro del ámbito laboral.
- ***End Point Disk Encryption*** (cifrado de punto final): es un proceso de codificación de datos que protege los sistemas operativos de la instalación de archivos corruptos.
- **Escáner de vulnerabilidades:** es un software que detecta, analiza y gestiona los puntos débiles de un sistema, enviando alertas en tiempo real.

8.2. Aplicación en Auditoría[15]

Reforzar la ciberseguridad es indispensable para los auditores ya que trabajan y tienen acceso a datos altamente confidenciales. Los auditores son custodios de su propia información e inclusive de sus clientes, por lo que tienen la responsabilidad de que las medidas de protección estén activas y vigentes. Además, adquiere especial importancia cuando se trabaje en forma remota debido al abundante intercambio de información por medio de dispositivos informáticos. Se deben adoptar medidas más eficientes de seguridad para mitigar la ocurrencia de ataques informáticos.

Es necesario apoyarnos de tres factores importantes:

- la tecnología, con la utilización de herramientas de protección para las redes de comunicación, equipos móviles, servidores, desarrollos de software, etc.
- las personas, formándolas y sensibilizándolas en el uso adecuados de los perfiles de acceso y el uso de los datos e información del estudio y de los clientes
- los procesos, implementando políticas de seguridad, planes de recuperación de desastres y de continuidad de negocio, entre otros.

Algunas medidas a implementar:

1. Establecer y comunicar políticas de seguridad.
2. Enviar comunicaciones simples y eficaces a los colaboradores sobre los riesgos de seguridad informática.
3. Implementar la realización de copias de seguridad frecuentes y la actualización de los softwares.
4. Revisar el funcionamiento de los sistemas, de las plataformas y de las redes de manera periódica.
5. Establecer políticas de contraseña seguras y de mecanismos de autenticación
6. Aplicar herramientas tecnológicas de seguridad informática (antivirus, cortafuego o *firewall*, encriptado de datos, etc.).

[15] La realización de auditorías de ciberseguridad en clientes excede el alcance de este trabajo.

9. Blockchain y Smart Contracts

Blockchain o cadena de bloques, es un sistema de registro digital que se implementa en forma distribuida, inmutable y sin un repositorio único ni una autoridad central.

Básicamente permite a una comunicad de usuarios, registrar sus transacciones en un *ledger*[16] que es público para esa comunidad, dado que cada participante mantiene un registro completo de ellas, sin que ninguna pueda ser modificada una vez validada, de modo que proporciona *una única versión de la verdad.*

Si bien las cadenas de bloques se difunden con más intensidad desde el año 2008 por la utilización de ciertas tecnologías y conceptos informáticos, con la novedad de incorporarles un valor a través de Bitcoin dando así origen a las monedas digitales, sus antecedentes se remontan a la década del 70´ con los primeros conceptos de clave asimétrica[17] y la estructura del árbol de Merkle.[18]

La tecnología basada en cadenas de bloques está en constante evolución. Si bien su aplicación a las criptomonedas es la más difundida, también pueden utilizarse para representar otros activos digitales, desplegar en ella el software de contratos inteligentes –*smart contracts*- o para almacenar otro tipo de transacciones, según el caso de uso para mejorar la eficiencia y la eficacia operativa y el control sobre sistemas existentes.

¿Cómo funciona? ¿Por qué los registros no pueden ser modificados?

Blockchain utiliza una estructura de árbol de Merkle para crear un resumen de las transacciones dentro de la cadena de bloques. Esta metodología, proporciona desde la raíz, una huella digital única y permanente de los registros de las transacciones en el bloque. Es un artefacto verificable y las transacciones se almacenan en texto simple.

Los componentes básicos para describir la tecnología blockchain son:

1. Las funciones hash criptográficas

Una función hash consiste en un algoritmo que, aplicado a una entrada, generará como salida un compendio único y de tamaño fijo, independientemente de la extensión de la entrada, aunque esta sea de un solo bit. Cualquier cambio que se produzca en los datos de la entrada generará como resultado un compendio distinto del original, de modo que cualquiera puede verificar la integridad del registro aplicando la misma función hash sobre la entrada, si el compendio obtenido es diferente, significa que la entrada fue modificada.

Las funciones hash son además unidireccionales, es decir, desde la entrada se obtiene el compendio, pero desde el compendio es inviable reconstruir la entrada.

El más utilizado en las cadenas de bloques es el Algoritmo de Hash Seguro –SHA- por sus siglas en inglés, con una extensión fija de 256 bit. Como el compendio se expresa en hexadecimal, su extensión siempre será de 64 caracteres.

El siguiente cuadro muestra ejemplos de aplicación de SHA 256:

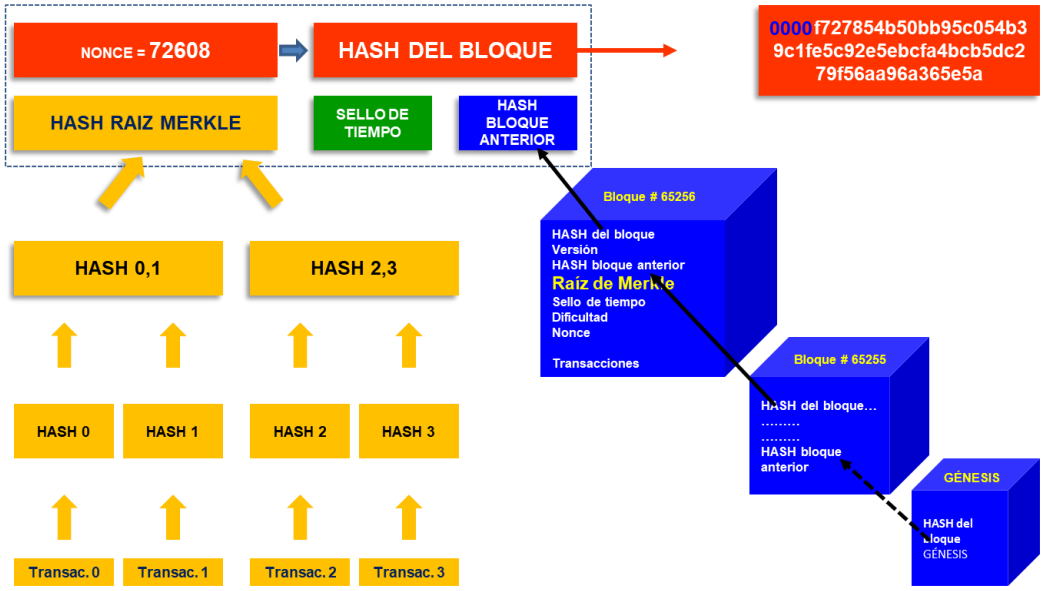
[16] Ledger (Libro mayor): Es el registro de todas las transacciones realizadas por la *blockchain* desde su bloque génesis.
[17] Whitfield Diffie y Martin Hellman. Algoritmo Diffie-Hellman.
[18] Ralph Merkle: investigador estadounidense, uno de los inventores de la criptografía asimétrica y hash criptográficos.

ENTRADA	COMPENDIO
1	6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
FACPCE	189a33cfed522934476ed8f82770ee98e7a0d0f68c2a662f0e16a6eb37a813a6

2. El árbol de Merkle

Es una estructura de registro que permite obtener un resumen de las transacciones registradas en el bloque, generando a través de las sucesivas aplicaciones de un hash criptográfico una huella digital única.

El cuadro siguiente grafica su estructura.



Fuente: Elaboración propia

Por cada transacción (verlas en la base del gráfico) se genera un hash individual, luego se agrupan de a dos, y por cada par se genera otro hash, y así sucesivamente hasta el obtener el hash raíz de cada árbol. Ahora bien, para obtener el hash del bloque además del hash raíz se requiere integrar:

- El hash del bloque anterior, para así conformar la ***cadena de bloques.*** De este modo, la huella digital incluye a todos los registros de transacciones de la cadena, dotándolos de inmutabilidad, dado que cualquier alteración no importa en qué bloque, generaría la inconsistencia inmediata de todos los registros siguientes.
- El sello de tiempo –*timestamping*- determina la fecha con precisión y será también inmutable.
- Un nivel de dificultad para el ***minado,*** que se explica en el párrafo siguiente.

El minado del bloque en este caso se explica aplicando la metodología de prueba de fuerza (o de trabajo, Proof of Work). Esto requiere generar el hash del bloque, aplicando sobre el hash raíz, el sello de tiempo y el hash del bloque anterior[19] el algoritmo SHA 256 para generar el compendio de 64 caracteres que corresponde al bloque, pero tal como se observa en el gráfico que antecede, se requerirá vencer una dificultad, que consiste que un número de caracteres

[19] A los efectos de este ejemplo, podría incluir otros elementos.

iniciales del hash sean ceros, en el ejemplo se requieren 4. Esto impone que el minero realice pruebas de cálculo al azar, incorporando un número como auxiliar de cálculo –el nonce[20]- hasta que el compendio obtenido cumpla con el nivel de complejidad requerido. En ese punto, el bloque se acepta y cierra y se distribuye a la red para ser validado por cada nodo y así integrar definitivamente la blockchain. Validar no es lo mismo que minar, simplemente es recalcular para verificar la integridad, muchísimo más sencillo y rápido.

Al no existir un propietario de la blockchain, el minado es un mecanismo de confianza que permite a los usuarios confiar en las transacciones.

Cabe resaltar que cualquier corrección sobre los datos históricos de transacciones registrados en la cadena de bloques no es posible realizarla en forma retroactiva, solo puede subsanarse por registros de ajuste posteriores. Esto a la vez que fortalece algunas cuestiones de control, puede obstaculizar en materia operativa o dificultar el cumplimiento de algunas normas legales como se expondrá más adelante.

3. Redes Peer to Peer –o redes entre pares, P2P-

Son redes cuya arquitectura está definida para que todos los nodos[21] tengan la misma jerarquía e igual comportamiento[22]. Sus características principales se describen a continuación:

- No tienen ninguna estructura definida. Las conexiones entre nodos son directas y cada uno de ellos cumple un doble papel de cliente y servidor.
- Los nodos se reconocen entre sí y si se produce un problema, pueden solicitar a los nodos adyacentes la información faltante o actualizaciones.
- Es robusta y soporta una alta rotación de nodos. Puede resistir a los cambios por nuevas conexiones de nodos a la red y desconexión de antiguos.

Fuente: Elaboración propia

En el gráfico anterior se puede observar claramente la topografía de la red completa en (1), la continuidad de la operabilidad ante la desconexión del nodo 5 (2) y la adaptabilidad posterior de la red (3).

También se puede deducir, que al contener todos los nodos toda la información de la cadena de bloques, una alteración a la integridad de los datos por cualquier motivo en un nodo implicaría su inconsistencia y por lo tanto su validación por toda la red resultaría imposible. Esto es parte sustancial también de la seguridad en cuanto a la inmutabilidad del registro de las transacciones que otorga.

[20] Nonce: *Number that can be only used once.* Número que solo se puede usar una vez.
[21] Integrantes de la red.
[22] Puede haber alguna excepción como el caso de los mineros.

Sobre estas redes se soportan los *ledgers* o libros de contabilidad (también llamados mayores) distribuidos, es decir, el total de los registros se encuentra en cada nodo.

4. Criptografía de clave pública/privada (o asimétrica)

Se utiliza en par de claves, una pública *(KPi)* y una privada *(Kpi)* relacionadas aritméticamente entre sí. La KPi se hace conocida, de ahí su nombre, sin alterar la seguridad de los procesos, dado que a través de ella no puede determinarse la Kpi que debe permanecer siempre a resguardo por el titular.

En el esquema blockchain, la Kpi se utiliza para firmar digitalmente los datos de cada transacción, y la KPi para verificar esos registros. Esto permite una relación 1 a "n", dado que quien esté en poder de la KPi puede verificar más de un registro firmado con la Kpi.

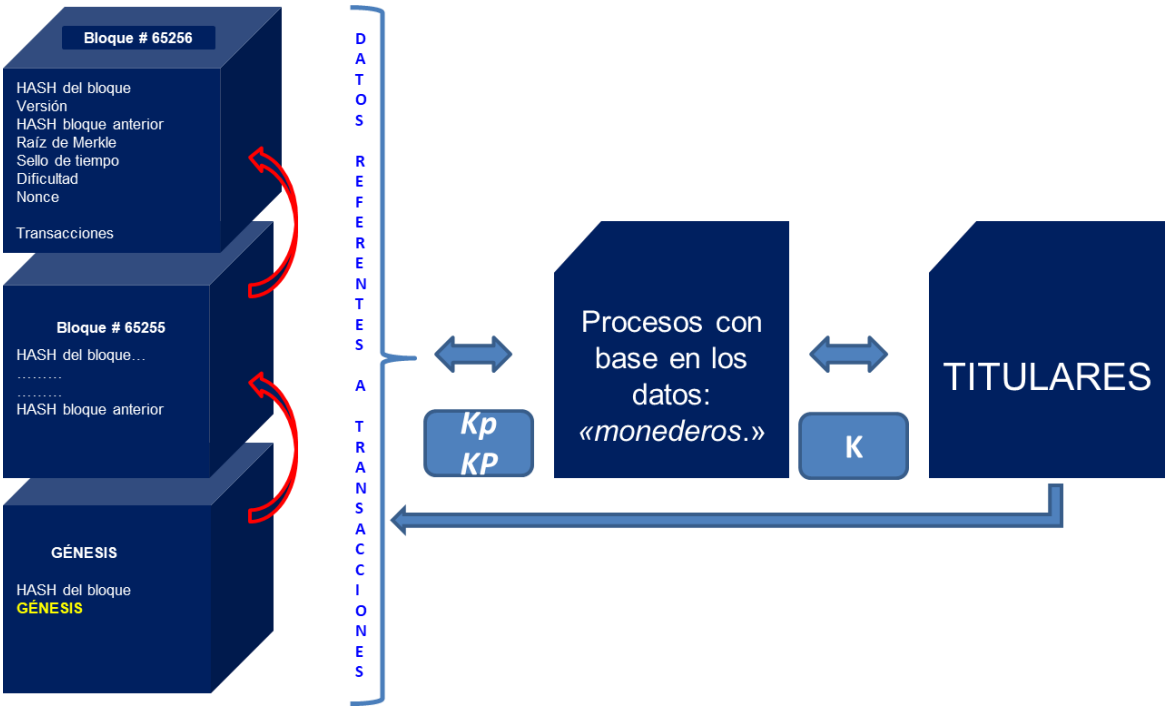
La KPi de cada usuario, luego de una transformación digital generada por una sucesión de hash, se transforma en una cadena corta de caracteres que constituye su *dirección,* mediante la que accede a sus registros en la cadena de bloques. Esto permite que los usuarios sean *seudónimos.*

Resumiendo, un usuario de la cadena firma cada transacción con su Kpi (lo que puede constituir una adquisición o disposición de activos) y accede al registro de sus transacciones identificándose mediante su *dirección.* Los sistemas blockchain, utilizan las direcciones para definir los *puntos finales* de una transacción, es decir *"de…" – "para…"*

Ahora bien, las KPi, Kpi y las *direcciones* generalmente se almacenan a través de un software denominado *monedero billetera*[23], que, a su vez, puede calcular al número total de activos de un usuario dado que los "saldos" habitualmente no están incluidos como registros en los bloques.

El gráfico siguiente describe la situación:

[23] Esta denominación es propia de las criptomonedas, pero no tratándose de ellas, igual sería un software complementario que opera generando información (reportes que *blockchain* no elabora) sobre las transacciones registradas en *blockchain* y resguardando las claves y direcciones.



Fuente: Elaboración propia

En este esquema, la pérdida de una Kpi implica la pérdida de los activos dada su imposibilidad de reconstrucción, así como si un atacante accede al *punto final* (resguardo de las claves, por ejemplo, una billetera) y se apodera de la Kpi, dispondrá de los activos.
En el caso que intervenga un Exchange, el titular tiene una dirección de acceso, pero la Kpi la conserva el Exchange, con los riesgos que implica.

El sistema de clave pública/privada en la forma en que se implementa en las blockchain es el soporte del *pseudoanonimato,* dado que la titularidad es anónima sobre registros identificados por medio del sistema de claves.

¿Qué es un *Smart Contract?*

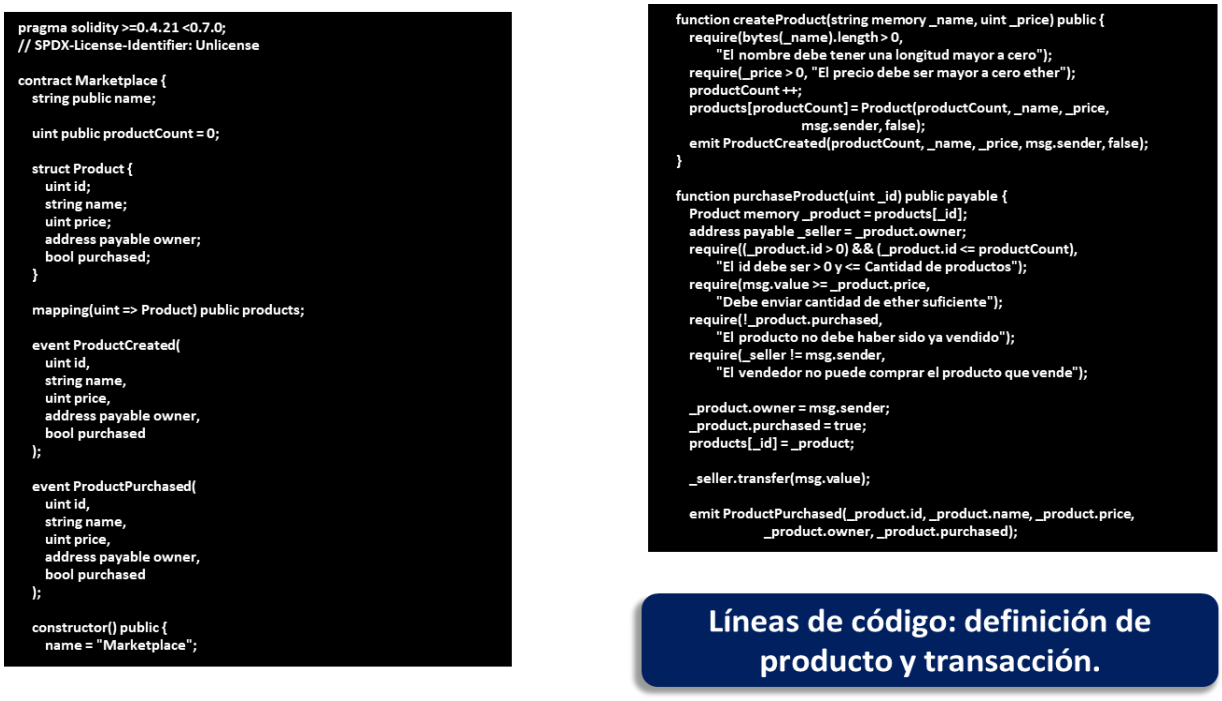
Un contrato inteligente (*Smart Contract)* es una colección de códigos y datos que se despliega en una cadena de bloques. Son programas informáticos (escritos en lenguaje de programación) que con los datos proporcionados pueden realizar cálculos, almacenar información, ejecutar funciones y transferir activos sin intervención humana por ejecutarse de forma automática. No necesariamente se trata de que cumplan funciones financieras, pero pueden impulsar transacciones e intercambio de activos. Las cláusulas registradas en blockchain garantizan su inmutabilidad.

El cuadro que sigue permite una comparación entre un contrato tradicional y un contrato inteligente[24]:

[24] Elaborado por el grupo de investigación sobre los efectos de las nuevas tecnologías en el ejercicio profesional de los contadores públicos del Instituto de Investigaciones y Estudios Contables de la Facultad de Ciencias Económicas de la UNLP.

COMPARACIÓN	
CONTRATOS TRADICIONALES	**CONTRATOS INTELIGENTES**
Escrito en lenguaje natural	Son programas informáticos escritos en lenguaje de programación
Las partes firman para asegurar su compromiso	Lleva a cabo una serie de tareas determinadas según las instrucciones programadas
Tiene costo	Reduce tiempos y costos
Puede requerir la intervención de un tercero de confianza	No requiere la intervención de un tercero de confianza.
Sus cláusulas están sujetas a la interpretación de las partes	Su cumplimiento no está sujeto a interpretación. Si ocurre una determinada condición, se ejecutará una acción en forma automática.

Una imagen para la "lectura" de un contrato inteligente se vería como se muestra en un sencillo ejemplo del gráfico siguiente. Para leerlo hay que interpretar las líneas de código[25]:



9.1. Implementación de Blockchain

A continuación, se listan en forma sintética y no taxativa generalidades, ventajas y riesgos que trae aparejado el uso de blockchain y algunas medidas para facilitar su implementación y mitigar los riesgos de acuerdo con las posibilidades. Estos comentarios pueden tenerse en cuenta tanto para el asesoramiento profesional a terceros como para el uso en el ejercicio propio de blockchain.

[25] Elaborado por el grupo de investigación sobre los efectos de las nuevas tecnologías en el ejercicio profesional de los contadores públicos del Instituto de Investigaciones y Estudios Contables de la Facultad de Ciencias Económicas de la UNLP.

Generalidades

1. Blockchain puede implementarse **para uso interno exclusivo de la organización** o **para uso de un consorcio** por ejemplo de un grupo **utilizando un desarrollo propio**[26], o se puede implementar tanto para uso propio o un consorcio **utilizando un motor de blockchain público**[27].
2. Es mucho más que un soporte para criptomonedas, aunque trascendió por ellas. Su utilización es muy amplia, como, por ejemplo: cadenas de suministros, contratos, seguros, historias clínicas, registros de la propiedad entre otras.
3. La inmutabilidad de los registros **no permite que sean corregidos** en caso de error, sin embargo, esto puede realizarse por un nuevo registro de **"ajuste" que será incluido en un bloque posterior** al que contiene el registro erróneo.
4. No hay una única blockchain[28], de hecho, existen un sinnúmero de ellas que no se comunican entre sí. Esta cuestión de origen técnico aún no está resuelta.
5. No brinda soluciones mágicas. La tecnología está en permanente evolución y se requiere un conocimiento acabado sobre su funcionamiento antes de tomar la decisión de su implementación. La funcionalidad adecuada de la cadena depende del motor de blockchain, los procesos empresariales y los controles generales de TI.
6. Impacta en la forma en que la Dirección, la administración y los auditores desempeñarán su tarea, **seguirá siendo necesaria y relevante, aunque se ejecute en forma distinta**.

Ventajas que otorga y/o mejoras en el control interno

1. La ejecución y registro de transacciones con mínimo de intervención humana. Puede "aislar" los procesos evitando los sesgos posibles como resultado de su participación, como así también los riesgos de fraude tradicional.
2. Los registros tienen inmutabilidad e irreversibilidad comprobables criptográficamente. Si la blockchain está diseñada en forma adecuada, impedirá el agregado, modificación o eliminación de datos históricos, brindando un alto nivel de seguridad a los registros.
3. El sistema libro mayor compartido proporciona visibilidad de los registros porque están en texto simple, esto posibilita su lectura y beneficia al entorno de control.
4. Una blockchain de consorcio puede resultar eficaz cuando la organización es descentralizada.
5. Puede integrarse con otras tecnologías emergentes como IA, IoT y motores de reglas estandarizados. Esto permite entre otras cuestiones, la ejecución de los contratos inteligentes, además pueden proporcionar información sobre desvíos en tiempo real.
6. Los contratos inteligentes mediante un diseño adecuado pueden prevenir y evitar las oportunidades de fraude, al no requerir la intervención humana para su ejecución. Sin embargo, no están libres de que se manipule la información proveniente de los oráculos[29] que requieren para su ejecución.
7. Si el conocimiento sobre el funcionamiento de la cadena de bloques es adecuado, puede facilitar la evaluación de riesgos sobre captura, registro y conservación de datos.

[26] Son códigos libres y abiertos.
[27] Por ejemplo, Ethereum.
[28] Más conocidas Bitcoin, Ethereum
[29] Fuentes de información externas a la cadena a los cuales el Smart consulta (o recibe) datos que impulsan su ejecución.

8. Las ***pruebas de consenso***[30] permiten la probabilidad de detección de fraude por la mayor intervención en la validación.
9. La existencia de nodos que conservan ***todos toda*** **la información**, minimiza la pérdida de datos. Puede incidir en los requisitos sobre las copias de seguridad (*backups)* y en las posibilidades para recuperación de desastres.

Riesgos propios del uso de blockchain

1. Si bien blockchain no requiere la intervención humana, no cambia su naturaleza, voluntad o comportamiento con respecto al control interno.
2. El pseudoanonimato descripto, impide la identificación de quienes realizan transacciones en la cadena de bloques en el caso en que esta no requiera permisos o identificaciones para su acceso.
3. En ciertas circunstancias, la descentralización y la falta de un "tercero de confianza", puede ocasionar que, ante una discrepancia o inconsistencia, no exista el "árbitro" adecuado produciendo una demora en su resolución. Si se trata de una debilidad en la seguridad de la cadena, esto puede tornarse crítico. Cuando no existe una autoridad central que administre, es muy difícil establecer actividades de control.
4. La reputación de la cadena de bloques es una de las cuestiones de mayor riesgo. Su utilización para operaciones de lavado de dinero o financiamiento de actividades delictivas ha generado ya manifestaciones de los organismos internacionales de control y de algunos países.
5. El motor de blockchain, del que depende una parte de la fiabilidad de sus registros, puede definirse por consenso en el que no necesariamente participan todos los usuarios. Esto implica que los cambios consensuados, pueden estar fuera del control de la organización y admitir niveles de riesgos que exceden los umbrales definidos por la dirección de un componente si se tratara de un grupo. Si se adhiere a una blockchain pública, es altamente probable que la situación descripta se verifique.
6. Esta tecnología aún es novedosa y evoluciona a un ritmo que torna difícil la disponibilidad de personal especializado, que es imprescindible si se pretende implementarla en la organización. De no contarse con un soporte técnico adecuado, blockchain puede no ser una solución recomendable, resultando crítico si se trata de una blockchain privada o de consorcio sobre base de desarrollo propio.
7. Las nuevas tecnologías pueden proporcionar una altísima disponibilidad de datos. Sin embargo, esto no siempre es una ventaja dado que pude producir sobrecarga que resulta nociva desde el punto de vista de su gobernanza.
8. Las ventajas que proporcionan los contratos inteligentes con respecto a su ejecución automática y libre de interpretaciones pueden a su vez exacerbar los riesgos. Si el evento disparador de una acción está viciado o tiene un error de diseño, la ejecución se disparará en forma automática y probablemente en tiempo real, resultando muy difícil detenerla. La inmediatez, la automaticidad y la irreversibilidad son una ventaja sólo si el diseño del contrato está probado y adecuadamente implementado.
9. La blockchain trae desafíos con respecto a la ciberseguridad. Si bien los datos permanecen inmutables en sus registros en las cadenas, pueden quedar expuestos por accesos indebidos a su disponibilidad. Esto ha sucedido en varias oportunidades y con

[30] Un algoritmo de **consenso** es la forma en que los participantes acuerdan en que la participación es válida (Definición según NIST- National Institute of Standards and Technology).

altos costos para los titulares mediante los denominados ataques de punto final. Consisten en que los ciberatacantes traspasan los resguardos de los sitios donde se almacenan las claves que es externo a la cadena, por ejemplo, un monedero, u otras vulnerabilidades[31] con el mismo fin.

10. Otro riesgo existe cuando el minado no es por prueba de fuerza sino por "consenso"[32]. En este caso, un protocolo de consenso mal diseñado o implementado compromete la validación por distribución del poder de cómputo.

Algunas medidas que ayudan a mitigar riesgos y/o facilitan su implementación

1. Blockchain trae aparejados riesgos específicos sin embargo no son independientes del ERM[33] general de la organización, por lo tanto, debería considerarse en ese contexto.
2. Crear competencias adecuadas en torno a las nuevas tecnologías para garantizar su uso es una decisión apropiada. Esto implica la formación de equipos interdisciplinarios en cada una de las etapas de los procesos. Seguramente resultará necesario requerir la participación de expertos en blockchain y de controles generales de TI además de soporte jurídico, contable y de gestión, dependiendo del uso a dar a la cadena, así como sensibilizar a las partes intervinientes con respecto a las ventajas y riesgos que trae aparejado su uso.
3. La inmediatez, automaticidad e irreversibilidad de las transacciones requiere una supervisión permanente y que se evalúe en forma continua la vigencia de los controles informáticos, tanto preventivos como detectivos incluyendo protocolos de consenso, códigos en los contratos inteligentes, resguardos de claves, en general, la fiabilidad de la cadena de bloques.
4. Es recomendable implementar para todas las aplicaciones, pero en especial para los contratos inteligentes, una metodología que documente el control de cambios para garantizar la trazabilidad.
5. Si se trata de una blockchain privada o de un consorcio es recomendable: tener definido el procedimiento para resolver disputas, umbrales de riesgo dado que pueden ser distintos, responsables de control y rendiciones de cuentas, comunicación de alertas, control de cambios y recuperación de desastres, políticas para resguardo de claves, criterios para contratación de servicios de terceros, entro otros controles.
6. Para evitar la saturación de datos, es aconsejable el análisis de datos de cada proceso para seleccionar cuales resultan útiles para su ejecución, gestión y supervisión.
7. Con respecto a la información que se espera extraer de la blockchain y para que esta resulte acorde a los fines, es necesario que intervengan las partes apropiadas de acuerdo con sus intereses, incluyendo a auditoría interna y externa por cuestiones de auditabilidad del sistema.
8. Con respecto a las organizaciones de servicios que proporcionan datos que ingresan a la blockchain, es recomendable evaluar permanentemente su calidad, la vigencia de los acuerdos de servicios y requerir informes SOC.

[31] Conocidas como *Backdoors* o *puertas traseras.*
[32] Existen diferentes metodologías para consensuar por mayoría que exceden el marco de este trabajo.
[33] ERM: Enterprise Risk Management o gestión de riesgos empresariales.

9.2. Aplicación en Auditoría

¿Qué proporciona blockchain y qué no?

La Dirección puede otorgarle distintos fines a la información obtenida de una cadena de bloques, operativos, financieros de supervisión, u otros.

Si se trata de fines financieros, es decir para la preparación y presentación de información financiera, determinados datos pueden representar tanto transacciones que generan derechos y obligaciones, (presentes, futuras o contingentes como podrían surgir de un contrato inteligente) o representar la tenencia de algún activo financiero, incluyendo una cantidad como presunto valor de este.

El hecho que la información provenga de una cadena de bloques puede brindar seguridad con respecto a la existencia del registro y que este no ha sido alterado, pero no proporciona en principio evidencia suficiente y adecuada de auditoría.

Una aclaración previa es que la información que el auditor utilizará como evidencia puede adoptar distintas formas, requiriendo procedimientos específicos a aplicar. Puede existir información cuyo origen ha sido digital y se conserva en ese medio digital (*Smart Contracts,* por ejemplo) en cuyo caso la evidencia será absolutamente digital, o soportes en papel que luego se digitalizarán, conformando evidencia digitalizada. También, estos datos obtenidos en forma digital pueden provenir de la entidad o de un tercero como podría ser una interfaz con una organización de servicios u otro componente del grupo.

Como se anticipó, refiriéndonos a información para uso financiero, la única seguridad que otorga blockchain es en cuanto a la inalterabilidad del registro y que este efectivamente ha ocurrido en una fecha determinada. Aun así, esta seguridad depende de la fiabilidad que otorguen los controles probados de la cadena.

¿Qué NO otorga necesariamente blockchain?

Son varias cuestiones para considerar y pueden requerir que el auditor de estados contables deba aplicar procedimientos complementarios para obtener evidencia de auditoría suficiente y adecuada. Por ejemplo:

1. **Existencia.** Si se trata de un activo digital, su existencia puede depender exclusivamente de la fiabilidad y de las pruebas que puedan obtenerse de la cadena de bloques, que a su vez depende de la tecnología subyacente y de la eficacia de los controles implementados, por lo tanto, no cumple el requisito de existencia por el mero registro. Es probable que se requiera probar los controles y verificar la seguridad de las claves privadas.
2. **Propiedad.** La asignación de un activo en la cadena de bloques puede no brindar evidencia sobre su propiedad, atento el carácter pseudoanónimo de las transacciones. Esta puede ser limitante difícil de sortear cuando se transan activos en forma directa en la blockchain.
3. **Integridad.** La fiabilidad de los controles implementados por la entidad, aplicables para garantizar que todas las transacciones que deben ser incluidas se capturan por la blockchain en forma completa, exacta y oportuna. El resultado de esta verificación es lo que finalmente brindará evidencia suficiente y adecuada con respecto al principio de

integridad. Una vez capturados, si la blockchain funciona en forma adecuada, la integridad se mantendrá inalterable.

4. **Ocurrencia:** La información obtenida de la blockchain puede proporcionar evidencia suficiente y adecuada en cuanto a su registro e inalterabilidad, pero no es extensiva por si sola para respaldar que el hecho efectivamente haya ocurrido en la realidad. El pseudoanonimato contribuye a que puedan fraguarse operaciones con actores ficticios o partes relacionadas.
5. **Valoración.** Algunos registros de la blockchain son de naturaleza financiera y pueden incluir un "valor" asignado al momento de la transacción. No necesariamente ese valor representa su valoración de acuerdo con el marco de información aplicable al momento de preparar y presentar la información financiera. El auditor deberá aplicar procedimientos adicionales para obtener evidencia suficiente y adecuada con respecto a las afirmaciones de la Dirección al respecto. Con respecto al marco de información aplicable, se remite a lo expuesto en el párrafo siguiente *in fine*.
6. **Exposición:** Con respecto a este fin, el auditor debe tener presente que las cadenas de bloques no contemplan por sí mismas el armado de informes, se realizan por aplicaciones complementarias que extraen los datos de la cadena y los agrupan y/o clasifican de acuerdo con ciertos parámetros. Por lo tanto, deberá incluir en sus procedimientos los relativos a evaluar y obtener evidencias de auditoría al respecto. El otro punto no menor, es la dificultad en clasificar un activo digital dado que las normas al respecto se encuentran en la actualidad en constante evolución sin definiciones concretas a este momento. Deberá evaluar al respecto la finalidad y uso de esos activos según la Dirección, la aplicabilidad del marco de información financiera aplicable y normativas vigentes en cada jurisdicción en el caso que existan.

El auditor externo deberá aplicar –con las adecuaciones y su juicio profesional- los enfoques y procedimientos que surgen de las normas de auditoría vigentes, dado que aún no existe un juego normas específicas al respecto.

10. Evidencia Digitales

La Resolución Técnica N°37 modificada por la Resolución Técnica N°53 (FACPCE) consigna en el Capítulo II Sección B.3 *"El contador, a través del desarrollo de su tarea, debe reunir elementos de juicio válidos y suficientes que permitan respaldar las aseveraciones formuladas en su informe.*

Esta afirmación es concordante con el marco internacional[34], que define a la evidencia de auditoría como la: *"…**información** (elementos de juicio)[35] utilizada por el **auditor** para alcanzar las conclusiones en las que basa su opinión. La evidencia de auditoría incluye tanto la **información contenida en los registros contables** de los que se obtienen los estados financieros, **como otra información**"[36].*

En el marco digital, una evidencia digital no difiere conceptualmente de lo señalado, sino que reúne características particulares, podría afirmarse que son: ***los elementos de juicio generados, almacenados o transmitidos por medios digitales,* entendiéndose por digital *"…un dispositivo o sistema que crea, presenta, transporta o almacena información mediante la combinación de bits*[37].**

La ***información contenida en registros contables*** se refiere a **datos***.* Los datos pueden ser una abstracción –representación cuantitativa de un elemento o hecho- pero también pueden materializar en los registros la aplicación de un criterio o, constituir el elemento base que proporciona la información sobre la que la Dirección decidirá, con respecto a la aplicación de sus estimaciones contables.

Los datos se transforman en información cuando mediante algún método se los somete –*procesa*- de acuerdo con principios, normas, criterios.

La ***otra información,*** es un concepto significativamente más amplio, significa adquirir o ampliar conocimiento sobre una materia, y su "forma" puede ser extremadamente variada a la vez que cuantitativa o cualitativa, tanto tratándose de evidencia en soporte físico como digital.

Los ejemplos que siguen podrían constituir evidencias del medio digital:

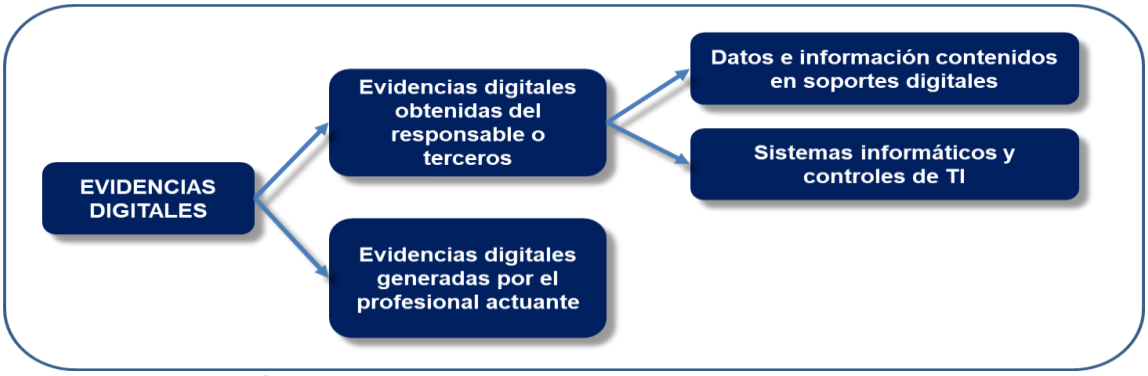
1. Los datos contenidos en una base.
2. Las sentencias sobre control de autorización de transacciones incluidas en una aplicación para emisión de facturas, necesarias para evaluar el control de aplicaciones como parte del sistema de control interno en general, o,
3. La filmación obtenida por un dron durante la toma de un inventario.

Claramente, las evidencias digitales no solo consisten en *datos*, sino que pueden adoptar distintas formas de acuerdo con su naturaleza.

[34] Manual de Pronunciamientos Internacionales de Control de Calidad, Auditoría, Revisión, otros Encargos de Aseguramiento y Servicios Relacionados - GLOSARIO
[35] El agregado en paréntesis es nuestro,
[36] La referencia a *estados financieros* obedece a la letra de la norma, pero se entiende extensiva a todos los encargos que ejecuta el contador público.
[37] Real Academia Española.

10.1. Tipos de evidencias digitales

El siguiente gráfico sintetiza un esquema sobre los elementos que constituyen las evidencias digitales de acuerdo **con su origen**. Como se observa, pueden provenir de fuentes externas al contador actuante, tanto desde el responsable de la materia objeto del encargo, de terceros, como así también las elaboradas por el propio contador.



Fuente: Elaboración propia.

Esta clasificación no significa una escisión ni su concepción en forma independiente, sino que una es parte y a menudo consecuencia de la otra, de modo que deben tratarse e interpretarse como un todo orgánico.

En la tabla siguiente se describe sintéticamente que integra cada componente:

Evidencias Digitales Obtenidas del responsable	**Datos e Información contenidos en soportes digitales**	Constituyen la representación digital –intangible- de hechos, transacciones, relaciones, procesos, criterios, que se obtienen de bases de datos y todo tipo de documentos, tanto en formato numérico como de texto, imágenes, sonidos, videos, comunicaciones digitales u otros. Las evidencias digitales si bien son un intangible, **sólo existen en la medida que se aloje en un soporte físico.**[38]
	Sistemas Informáticos y controles de TI	**Es esencial para el contador actuante relevar, evaluar y documentar los procesos mediante los cuales la información se genera**, desde la captura y registro del dato origen hasta la "salida" que constituye la materia del encargo, así como el control interno –particularmente de TI- aplicado. Esta condición toma relevancia en forma más que proporcional en la medida que se incrementa la complejidad de los procesos. Cabe destacar que el control interno específico de TI no está sesgado del control interno en general, sino que en estos momentos es una parte relevante del mismo.
Evidencias Digitales	**Datos e Información contenidos en soportes digitales**	Elementos obtenidos a través de requerimientos a terceros o información disponible en medios a los que puede acceder el contador actuante. Por ejemplo, una circularización o una consulta a los letrados del responsable.

[38] Ver en este documento, conservación de las evidencias digitales.

Obtenidas de terceros	**Sistemas Informáticos y controles de TI**	Particularmente se requieren estos elementos de juicio cuando el responsable utiliza servicios de nube, por ejemplo, a través de un informe sobre los controles de una organización de servicios.
Evidencias Digitales Generadas por el contador actuante	**Documentación del encargo**	El contador actuante generará sus programas de trabajo con la indicación de su cumplimiento, que incluirán también los elementos de juicio válidos y suficientes utilizando medio digitales o mixtos. Difícilmente en la actualidad utilice sólo soporte papel.

Otra visión del tipo de evidencias, también relacionadas con su origen y procesos posteriores, indican que: las evidencias pueden originarse a través de contenidos exclusivamente digitales y permanecer en ese estado durante su ciclo de vida –*evidencia digital*- u originarse en documentos soportados en papel y luego digitalizarse –*evidencias digitalizadas*- u originarse en documentos digitales y luego transferirse a papel. En todos estos casos, los métodos y objetivos para su legitimación varían sustancialmente.

Naturaleza de las evidencias digitales

El hecho que las evidencias *tradicionales*[39] evolucionan al formato digital, **no significa que modifiquen su fin principal** que es proporcionar la información necesaria al contador actuante para arribar y sustentar sus conclusiones según el tipo de encargo. Tampoco se modifican los requisitos de legitimidad, relevancia, validez y suficiencia, ni la necesidad de cumplir con ciertos requerimientos para garantizar su valor probatorio en caso de resultar necesario. Simplemente, tienen distintas características atentas a su condición de intangibilidad.

Las principales son:

- **Modificables.** Se parte de la premisa que un registro electrónico es modificable por medios e intenciones, legítimas o no. Esta condición de ***volatilidad*** impacta en la subsistencia de la fuente de la evidencia recolectada por el contador, particularmente las que quedan en custodia de terceros. Parte significativa y relevante de la información se obtiene de tablas que conforman bases de datos transaccionales. Estas bases por su naturaleza son *dinámicas*, de modo que se modifican a medida que suceden las transacciones.
- **Ilegibles:** Para acceder a su *vista* se requieren medios adecuados de acceso.
- **Perdurables:** Si bien un registro electrónico no tiene los mismos riesgos que uno soportado en papel en cuanto a su exposición y posibilidad de degradación, el soporte físico del registro está sujeto a riesgos propios de deterioro de los soportes y además la obsolescencia en la tecnología utilizada.
- **Sensibles:** La fiabilidad de las evidencias digitales depende o se ve altamente influenciada por la sofisticación del sistema, la tecnología subyacente y las prácticas de controles de TI.

Al momento de identificar y evaluar las evidencias digitales, estas características deben considerarse en conjunto dado su interdependencia y relación.

[39] Que siguen las formas, ideas o costumbres del pasado (RAE), por ejemplo, el soporte papel.

10.2. Aplicación en Auditoría

A continuación, detallamos las cuestiones claves a considerar al momento de obtener, procesar y conservar las evidencias digitales que proporcionen información necesaria al contador actuante para arribar y sustentar sus conclusiones según el tipo de encargo.

10.2.1 Obtención de evidencias digitales

Los requisitos de legitimidad[40], relevancia, validez y suficiencia que imponen las normas vigentes[41] con respecto a las evidencias, están condicionados o dependen en este caso de sus características específicas en el medio digital: la modificabilidad, ilegibilidad, sensibilidad y perdurabilidad. Es decir, el cumplimiento de los requisitos se garantizará sólo mediante una adecuada metodología en su obtención y tratamiento durante todo el proceso, teniendo en cuenta que todas las características citadas configuran factores de riesgo relevantes.

Particularmente, la etapa de obtención es clave, por ser una de las iniciales y determinante en consecuencia de la confiabilidad de las siguientes etapas del proceso.

Una guía (simplificada) para su obtención podría indicar las siguientes premisas:

1. ¿Qué compone la evidencia digital y que se debe relevar cuando esta tiene su origen en el responsable de la materia objeto del encargo o de un tercero vinculado?

Como ya se anticipó, en ambos casos son dos los componentes:

- ***Como primera medida los procesos mediante los cuales la información se genera.*** Esto incluye: la infraestructura sobre la que el sistema de información opera, la evaluación de riesgos y las políticas de control interno y las específicas aplicadas a TI y el diseño e implementación de las aplicaciones mediante las cuales los datos se originan, modifican, procesan y almacenan.[42] Su complejidad variará de acuerdo con el grado de sofisticación del ambiente analizado y sus procesos.
- ***La información involucrada en el encargo.*** Datos y otra información.

La revisión de los procesos mediante los cuales la información se genera pondrá de manifiesto los riesgos de generación incorrecta, pérdida o alteración indebida y los controles en ellos involucrados y el grado de confiabilidad que los mismos otorgan.

Los datos y la otra información relevada, proporcionará la información sobre la que se ejecutarán algunos procedimientos, como por ejemplo el análisis de datos.

2. ¿Cuáles son los controles de TI que deben ser evaluados?

En el marco digital, el contador actuante debe tener presente que existen dos tipos de controles que deben ser evaluados: los generales y los de aplicación de TI.

Los controles generales son los que definen la seguridad y confiabilidad de la plataforma sobre las cuales las aplicaciones operan. La siguiente lista -no taxativa- brinda ejemplos sobre los básicos esenciales:

- Políticas de resguardo
- Segregación de funciones de TI

[40] Se ha explicitado el término legitimidad a los efectos de esta guía, no lo mencionan la Resolución Técnica N°37 de la FACPCE ni la NIA 500 del IAASB de la IFAC.
[41] Resolución Técnica N°37 de la FACPCE y NIA 500 del IAASB de la IFAC.
[42] Resolución Técnica N°37 de la FACPCE (ejemplo III.A.i.3.1) y NIA 500 del IAASB de la IFAC (párrafo 18 y vinculados).

- Estándares y metodologías de desarrollo.
- Control de seguridad de redes y accesos.
- Control de cambios
- Plan de contingencias y política de continuidad de negocio.

Los controles de aplicación son los que operan sobre el flujo de datos en las etapas de entrada, proceso y salida y su objetivo es proporcionar un nivel de seguridad acerca de que los requisitos de integridad, exactitud y validez de la información cumplen con ciertos criterios, que pueden estar establecidos por estándares específicos[43], definidos por la Dirección o lo que es más habitual, una combinación de ambos.

Una lista no taxativa de controles a evaluar se observa en la siguiente tabla:

Controles de entrada	**Controles de proceso**	**Controles de salida**
• Captura del dato exacto en el momento oportuno. • Controles de acceso mediante claves, terminales, horarios. • Validación de datos • Corrección de errores y procedimientos ante rechazos • Niveles de autorización.	• Verificación de uso de las versiones vigentes • Procedimientos de recupero ante interrupciones • Verificaciones de integridad de proceso a proceso.	• Disponibilidad, integridad y confidencialidad de la información. • Vigencia de las opciones de recupero. • Metodología para detección de errores no superados durante el proceso o para información “inusual”.

Cabe resaltar, que una organización voluminosa y/o sofisticada, seguramente requiera la aplicación de procedimientos también sofisticados, inclusive debe tenerse presente la intervención del trabajo de un experto, dado que la exponencial incidencia de la TI requieren cada vez una mayor experticia.

Esto no significa presuponer de ningún modo que las evidencias digitales solo son posibles en un ambiente de TI sofisticado o con requisitos tales, que en una organización pequeña donde los medios pueden resultar limitados, el contador actuante deba resignar su obtención. No existen hoy organizaciones qué, por lo menos parte de su información no se procese en un medio digital, por lo tanto, la obtención de evidencias digitales resulta no solo posible sino necesaria. Sólo se requiere adaptar los procedimientos a las circunstancias y tomar los recaudos del caso.

3. ¿Cuál es el alcance de la información a obtener?

El objetivo del contador es obtener elementos de juicio válidos y suficientes que permitan respaldar las aseveraciones de su informe según el tipo de encargo. El término *validez*, implica analizar los conceptos de *relevancia y fiabilidad.*

*La **relevancia** se refiere a la conexión lógica con la finalidad del procedimiento de auditoría, o su pertenencia al respecto, y, en su caso, con la afirmación que se somete a comprobación, en tanto que por **fiabilidad*** se entiende confianza, seguridad. La condición requiere que la información *sea suficientemente completa y exacta[44] (Íntegra)*

[43] ISO serie 27000, COBIT, ITIL, COSO, entre otros.
[44] NIA 500 de IAASB de la IFAC párrafos #A27 y #A49, respectivamente.

Se resaltan dos cuestiones a considerar:

En relación con la **relevancia,** el medio digital se caracteriza por la posibilidad de almacenar gran cantidad de datos que pueden encontrarse en estado "disponible" mediante el acceso debido. En la actualidad, el desarrollo del Big Data, el bajísimo costo de almacenamiento unido a la fácil accesibilidad a la nube, la potencia de cálculo disponible y las comunicaciones, **ha generado en las organizaciones una –a veces- excesiva acumulación de datos, que puede provocar efectos adversos**, tanto para la organización como para el contador al momento de obtener sus evidencias digitales.

El requisito de **integridad** en los datos de un proceso se verifica, en términos informáticos, cuando en ese proceso se incluye la totalidad de los datos que deben ser incluidos (considerando su relación lógica con el proceso), son exactos, se actualizan (alta, baja o modificación) en forma oportuna mediante una transacción autorizada, y se almacenan en ambiente seguro. **La calidad de las conclusiones que se obtengan de todo análisis de datos posterior que se ejecute sobre una población, dependerá inexorablemente de la integridad de los datos de origen que conforman esa población y de la lógica definida por el contador actuante para su análisis**

Posteriormente y cumplidos estos requisitos, el *análisis de datos* es una herramienta potente a la hora de aplicar procedimientos, pero no reemplaza el escepticismo ni el juicio profesional. En efecto, un dato o un conjunto de ellos pueden representar:

- La existencia de un activo. Por ejemplo, una participación societaria, un título de propiedad, un certificado de tenencia de bonos u otros sustentados en documentos digitales, sin embargo, no necesariamente otorgan información o garantías acerca de su valoración o en su caso existencia física.
- La existencia de una transacción, pero no necesariamente que esta haya sido debidamente autorizada, o que se encuentre libre de incorrecciones por fraude o error. Esto se verifica aún si los datos son extraídos de una cadena de datos[45] considerada fiable.
- La existencia de un activo, pero no necesariamente su propiedad.
- El registro de los resultados de las estimaciones contables que la Dirección realice, o los datos de base que utilizó para su valoración, pero no necesariamente representan los fundamentos técnicos que las sustentan.

En estas circunstancias, seguramente el contador actuante deberá aplicar procedimientos analíticos sustantivos adicionales para complementar, verificar u obtener los elementos de juicio necesarios que los registros electrónicos no otorgan, a través de la documentación de origen, sea esta física o digital.

En el cuadro que sigue se exponen requisitos que hacen a la fiabilidad y oponibilidad de la evidencia de acuerdo con su soporte:

[45] Consulte el capítulo 2.7 *Blockchain* y *Smart Contracts.*

EVIDENCIAS SEGÚN SU SOPORTE		
Soporte de origen:	**Transferido o conservado en:**	**Fiabilidad y oponibilidad**: Dependerá de:
Digital	Digital	-Metodología de captura y mantenimiento. -Relación unívoca entre registros de origen y copia. -Legitimación de la copia.
Digital	Papel	-Controles aplicados al proceso de transformación. -Legitimación de la copia.
Papel	Digital	-Controles aplicados al proceso de transformación y mantenimiento. -Legitimación de la copia.

Fuente: Elaboración propia

Consideraciones al momento de obtener evidencias digitales

Se describen a continuación algunas pautas básicas y cuestiones a considerar al momento de obtener evidencias digitales

¿Los datos a requerir sólo están disponibles en formato electrónico?	**SI:** Deberá verificarse si el proceso que originó el dato solo tiene soporte electrónico, es decir, tanto la transacción o documento de origen como el dato resultante son intangibles. La volatilidad de la fuente potencia el factor de riesgo con respecto a la verificabilidad de la evidencia. La alteración de la fuente dejaría sin sustento a la evidencia, pero puede tomar garantías al respecto, asegurando la correspondencia entre su documentación y la obrante en base al momento de su obtención. **SI:** Pero tienen fuente documental tangible, el contador evaluará previamente la fiabilidad del dato con respecto a su fuente, considerando la fiabilidad resultante.
¿Se requieren herramientas específicas para la obtención y análisis de los datos?	Existe una variedad de software de aplicación específico de auditoría de alta calidad que ordena y facilita en forma significativa la tarea, independientemente del volumen de los datos a explotar. Sin embargo, su utilización no es excluyente para que el revisor obtenga y procese evidencias digitales, incluida la documentación de su labor, y esto es inclusivo para estudios medianos y pequeños con ejecución de encargos en PyMES. Con respecto a la explotación de los datos obtenidos, existen aplicaciones como Excel, sql o access, con suficiente potencia como para ejecutar la tarea de análisis de datos, dependiendo para el volumen a procesar, de la potencia de cálculo que dispone el revisor más que de la herramienta que utiliza. Si el contador dispone de la asistencia de un experto o tiene la experticia suficiente, desarrolle sus propias bases con los datos obtenidos del responsable y sobre ella genere y aplique sus consultas (*queries*).
¿Cómo garantizar que los datos obtenidos son	• Por garantías propias de la aplicación utilizada por el contador. • Por la entrega por parte del responsable de archivos firmados digitalmente[46]. Tiene estatus legal.

[46] Ley 25.506. Presunción de: autoría, integridad, validez y remitente, aunque admite prueba en contrario.

copia legítima y exacta de los obrantes en base del responsable?	• Por la entrega por parte del responsable de archivos firmados electrónicamente. Tiene estatus contractual. • Por la entrega por parte del responsable de archivos acompañados por un HASH, con el mismo estatus que cuando se utiliza firma electrónica. La inclusión de la metodología adoptada se fortalece con su inclusión en la carta convenio. Puede resultar excluyente, salvo el caso de firma digital.
¿Cuál es el alcance real de las medidas de protección descriptas en el ítem anterior?	El cifrado de los datos no garantiza su inalterabilidad, sino que permite detectar si esta se produjo. Para asegurar su inalterabilidad es necesario limitar la edición del archivo a solo lectura. Esto es importante porque requiere precauciones sobre su resguardo, por ejemplo, un archivo firmado digitalmente, aún con la mayor garantía, podría quedar inutilizado por una modificación no debida.
¿Cómo prever la posibilidad de repetir la prueba?	El contador actuante debe tener en cuenta la política de resguardo de datos del responsable. Los datos pueden modificarse o sanitizarse en las bases origen**. Esta situación resalta la importancia que tiene la legitimación al momento de obtener la evidencia digital**, debido a que el revisor solo puede adoptar medidas preventivas sobre este hecho, a través de la inclusión de cláusulas que establezcan tiempos y/o formas de resguardo en la carta convenio. Sin embargo, no dejan de ser declaraciones de intenciones, pero no garantiza su cumplimiento por parte del responsable.
Información requerida a terceros por procesos de circularización.	Se aplican los recaudos previstos para circularizaciones, sólo que con los recaudos por la transmisión electrónica. La amplitud de circunstancias excede la extensión de esta guía, por ejemplo: una comunicación electrónica puede ser un e-mail, un “sms”, un “mms”, un “WhatsApp” o cualquier tipo de transmisión que tenga un emisor y uno o varios destinatarios. Puede ponerse a disposición en un soporte (que puede ser digital, magnético, sólido o la nube), todos tienen distintas características, por lo tanto, es necesario recurrir a la aplicación del juicio del contador actuante para evaluar, aplicando el escepticismo profesional, la validez de cada una de las alternativas.

10.2.2 Procesamiento de la evidencia digital

Los riesgos de modificación o destrucción de la información obtenida, es decir ya en poder del revisor, se pueden producir en dos momentos: durante la explotación de los datos y el análisis de documentos digitales obtenidos, o luego de finalizada la tarea, durante el plazo de conservación. En este último (Ver **punto 10.2.3**. siguiente), además de alteraciones en la documentación del proceso, debe considerarse la accesibilidad en el tiempo.

La cuestión clave para tener en cuenta en este apartado es que los archivos originales *nunca deben ser alterados*, asegurando su resguardo desde el momento de su captura y trabajando siempre sobre copias. Las razones son varias, entre ellas, si se alteraran los datos originales seguramente se arribaría luego a conclusiones incorrectas, pero fundamentalmente se alterarían las garantías de oponibilidad de los documentos de trabajo.

Las garantías de oponibilidad de los documentos de trabajo dependen de la *cadena de custodia*[47], consistente en un procedimiento que permite la trazabilidad de la evidencia desde el momento de su obtención, análisis y conservación, identificando a todos los intervinientes o que accedieron a ella, sus acciones y garantizando su conservación y no alteración. Este procedimiento es aplicable a todo tipo la evidencia.

La no alteración de los archivos de origen está más garantizada cuando se utiliza un software de auditoría que prevé estas cuestiones junto con el ordenamiento de la documentación del proceso (papeles de trabajo[48]), pero requiere recaudos adicionales si no se lo dispone y se utilizan herramientas de difusión masiva como Excel, SQL o similares, por ejemplo:

- Crear una carpeta de acceso restringido y resguardar en ella los archivos originales en formato solo lectura y bloqueando su acceso a personas no autorizadas del equipo de trabajo.
- Definir un diseño adecuado de los resguardos de los documentos de trabajo[49] (por ejemplo, una estructura de árbol conformada por carpetas y archivos) que guarde relación con los programas de trabajo que surjan de la planificación de la tarea, agrupándolos por tipo de legajo y procedimiento, en el que incluirán las copias activas de trabajo[50]
- Resguardar copia de la carpeta fuera del servidor, siguiendo algún estándar de seguridad aplicable a backups.

10.2.3 Conservación, perdurabilidad una vez finalizada la tarea

Son dos los riesgos que corre el contador con respecto a la evidencia digital en este punto: riesgo de destrucción, alteración o acceso indebido; o riesgo de inaccesibilidad posterior.

Las normas de auditoría establecen que el *contador debe conservar, en un soporte adecuado a las circunstancias y por el plazo que fijen las normas legales o **por diez años**, el que fuera mayor.*

Con respecto a la destrucción, alteración o acceso, indebido, independientemente que se utilice un software de auditoría, un software propio o aplicaciones estándar, el riesgo de destrucción o alteración existe en la medida en que se acceda a la información, cuestión que puede resultar bastante frecuente por consultas si se trata de un encargo recurrente.

En otro orden, el acceso de intrusos puede comprometer la integridad de los archivos (destrucción, modificación) o su disponibilidad (*Ramsonware*)[51] y si bien es técnicamente imposible un resguardo 100% efectivo, nada libera la responsabilidad del contador por omisión, por no haber tomado los recaudos razonables en las circunstancias para impedirlo. El contador deberá aplicar las medidas que al respecto definen los estándares de seguridad, consultando a un experto cuando lo considere necesario.

---

[47] Este precepto requiere un desarrollo jurídico extenso que excede este marco. Se recomienda su observación y en su caso, recurrir a asesoramiento jurídico especializado, particularmente en actuación forense.
[48] La mención a “papeles de trabajo” se ha sustituido en la Resolución Técnica 37 por “documentación del encargo”
[49] Se utiliza la expresión ***documentos de trabajo*** en el sentido amplio del término documento, incluye datos estructurados, no estructurados o mixtos (archivos de datos, documentos de texto, imágenes entre otros).
[50] Remitimos al Capítulo 2.3. Herramientas colaborativas.
[51] “Secuestro de datos”. Es un *malware* mediante el cual un sujeto atacante puede producir bloqueos y cifrados que impiden el acceso a los datos, con eventual destrucción y/o publicación si no se abona un “rescate”. Políticas de prevención de “desastre” y “continuidad” brindan herramientas para prevenir, intentar evitar o recuperarse de ataques con este *malware*.

Con respecto a la **inaccesibilidad posterior**, puede producirse por los siguientes motivos:

- **Obsolescencia técnica**: Los ciclos evolutivos de la tecnología son cada vez más cortos y los recursos técnicos se renuevan más de una vez dentro del plazo de conservación exigido por las distintas normativas. Inexorablemente, la obsolescencia técnica del resguardo se producirá dentro de los diez años. Esto debe contemplarse al momento de decidir sobre la política de copias de seguridad (*backups)* que aplicará el contador, incluida la herramienta soporte que utilizará para el mismo, porque no solamente será necesario resguardar los datos, sino también las aplicaciones para su lectura.
- **Deterioro de los soportes:** Como ya se indicó, las evidencias digitales si bien son un intangible, sólo existe en la medida que se aloje en un soporte físico y estos, por su propia naturaleza se desgastan o están sujetos a condiciones, agentes o cuestiones físicas que los deterioran. Frente a la amplia gama de soportes disponibles en el mercado, el contador decidirá aplicando su criterio y en función a los requerimientos de la situación, que soporte resulta adecuado en las circunstancias. Para esta decisión, se recomienda tener especialmente en cuenta las especificaciones del fabricante con respecto a su producto.
- **Resguardo en la nube:** Utilizar estos servicios implica una ***transferencia de confianza*** por parte del contador hacia el proveedor del servicio, dado que sus datos quedarán en poder de un tercero en un ambiente de seguridad sobre el que no tiene ningún tipo de injerencia.

Los avances tecnológicos determinan la necesidad de la participación del contador púbico en los procesos de generación y verificación de información, atento a su competencia y experticia, sin embargo, la aplicación del juicio profesional puede requerir el asesoramiento de un experto, tanto en cuestiones de seguridad de TI como en derecho informático.

Bibliografía consultada

1. Examining Automation in Audit - IFAC (International Federation of Accountants) – Autores: Dr. Andrea M. Rozario, CPA, Abigail Zhang, Dr. Miklos A. Vasarhelyi - . Abril 2019. https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/examining-automation-audit

2. La Transformación Digital en el Sector de la Auditoria – Instituto de Censores Jurados de Cuentas de España – Marzo/2019

3. Tech Trends 2016 – Innovating in the digital era – Internet of Thing: From sensing to doing - Deloitte University Press - 2016 https://www2.deloitte.com/co/es/pages/technology/articles/el-internet-de-las-cosas.html

4. The 'Practice Transformation Action Plan - A Roadmap to the Future' – IFAC (International Federation of Accountants) - 2020

5. Guide to Practice Managemente for SPMs – Module 5 - IFAC (International Federation of Accountants)- 2018

6. Ventajas de la utilización del Big Data en el proceso auditor - OLACEFS (Organización Latinoameticana y del Caribe de Entidades Fiscalizadoras Superiores) – Autores: Hamlet Abel Morales Carcamo y Rodrigo José Berrios Mendoza - 2018 https://www.olacefs.com/wp-content/uploads/2018/10/2%C2%B0-Premio-Nicaragua.pdf

7. Activos Digitales. Aspectos técnicos, normativos, legales y contables de los bitcoins – Autores: Catani, María Laura; Rumitti, Carlos Alberto; Castiglioni, Gabriela Inés; Champredonde, Raúl Eduardo; Cóccaro, ,Ana María; Lofeudo, Ismael; Martires, Lorena María; Mercapidez, María Guillermina; Rosso, Hernán Pablo; Villar, José - Simposio Regional de Investigación Contable – UNLP - Diciembre/2020 http://sedici.unlp.edu.ar/handle/10915/111588

8. Impacto de la Economía Digital en la Profesión Contable – CILEA (Comité de Integración Latino Europa – América) – Estudios Internacionales CILEA 2018/2 – Agosto/2018

9. Technology – Audit Documentation – Non-Authoritative Support Material Related to Technology: Audit Documentation when Using Automated Tools and Techniques -IAASB (International Auditing and Assurance Standards Board) – Abril/2020

10. COSO in the Cyber Age. Committee of Sponsoring Organizations of the Treadway Commission (COSO) – 2015 https://www.coso.org/Pages/guidance.aspx