Deloitte.

Blockchain & Ciberseguridad

Risk Advisory

Escrito por el laboratorio Blockchain de Deloitte EMEA en colaboración con Deloitte global cyber SMEs y sus firmas miembro, incluyendo Irlanda, Estados Unidos de América, China, Reino Unido, Argentina, Alemania, España, Portugal e Israel.

Autores:

Eric Piscini (Deloitte U.S.), David Dalton (Deloitte Irlanda) and Lory Kehoe (Deloitte Irlanda)

Reconocimiento especial:
Niamh O'Connell (Deloitte Irlanda) y

Guilherme Campos (Deloitte Portugal)

Introducción

Blockchain está ganando reconocimiento, pero hay todavía quienes cuestionan la escalabilidad, seguridad y sostenibilidad de la tecnología. Las oficinas miembro de Deloitte están colaborando continuamente para reforzar las capacidades de esta tecnología, desarrollando soluciones de primera clase y, ofrecer servicios a los clientes.

En el presente artículo los expertos en blockchain y ciberseguridad de Deloitte han unido esfuerzos para calificar específicamente la seguridad de la tecnología blockchain.

Más específicamente, desde una perspectiva global se revisará y abordará:

- El nivel actual de seguridad de blockchain desde una perspectiva del sistema y los datos, para los registros públicos y privados.
- El modelo de clasificación de seguridad CIA, compuesto por tres áreas: (1) Confidencialidad, (2) Integridad y (3) Disponibilidad, haciendo referencia a la valoración del nivel de madurez actual de la tecnología blockchain.
- Autenticación, Autorización y Auditoria (AAA), y no repudio, aspectos fundamentales de seguridad protegiendo la información y diseñando-gestionando nuevos sistemas y redes1.

Para el propósito de este artículo, blockchain públicos son definidos como no protegidos, donde los datos están disponibles y públicos para cualquier persona que desee participar en la red.

Mientras que, blockchain privado, se refiere a plataformas basadas en permisos establecidos generalmente por grupos o firmas, o divisiones entre una organización.

Contexto de Blockchain. La evolución de blockchain (o tecnología que se basa en una serie de registros distribuidos por medio de cadena de bloques) ha estado comparándose con el crecimiento exponencial del internet, con comentarios y argumentos de que esta tecnología potencial puede hacer disrupción en múltiples industrias como Salud, Sector Público, Energía, Manufactura y, particularmente la de Servicios Financieros, donde se prevé que sea el corazón palpitante de las finanzas2 y el proveedor de un nuevo tejido de la industria. De acuerdo con David Schatsky, Director General de Deloitte Estados Unidos, "*la tecnología proporciona una forma de registrar transacciones o cualquier integración digital de una forma que es segura, transparente, altamente resistente a interrupciones, auditable y, eficiente.*"[3] Tal es el interés en la tecnología que en 2016 fue invertido cerca de $1 billón de dólares en blockchain por firmas de servicios financieros y de tecnología,

1 http://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting
2 http://uk.businessinsider.com/world-economic-forum-potential-of-blockchain-in-financial-services-2016-8
3 https://dupress.deloitte.com/dup-us-en/focus/signals-for-strategists/trends-blockchain-bitcoin-security-transparency.html
4 https://www.bloomberg.com/news/articles/2016 06-23/finance-firms-seen-investing-1-billion-in-blockchain-this-year 5 http://wwwgartner.com/newsroom/id/3412017

cuyas inversiones se predice que pueden incrementar exponencialmente en los siguientes cinco años[4].Según un reporte de Gartner en 2016, la tecnología está en el pico de un hiper-ciclo y se ha convertido en prioridad para los líderes de la industria con el fin de entender cómo puede transformar sus modelos de negocio y alterar las cadenas de valor para ganar una ventaja competitiva, y quizás más fundamentalmente para seguir siendo relevante.

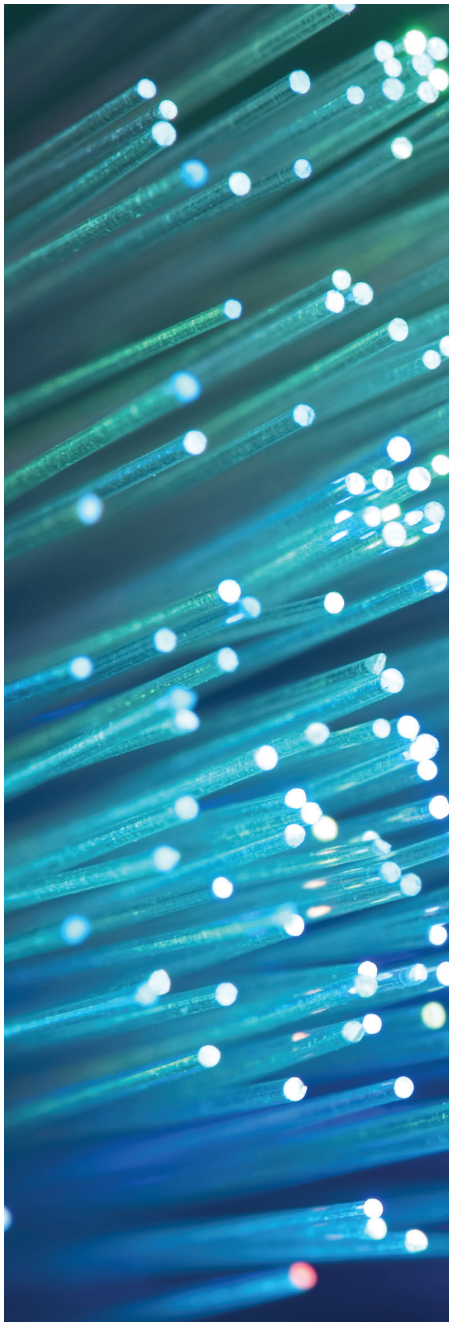
Sin embargo, hoy en día la tecnología permanece en el pico de una expectativa inflada y está a punto de sumergirse en un abismo de desilusión. Milan Sallaba, líder de tecnología de Deloitte Alemania señala que "*en alguno de los primeros casos de uso que hemos visto estaban desplegando blockchain por el simple hecho de hacerlo, sin centrarse suficientemente en los atributos centrales de la tecnología, que de hecho tiene el potencial de generar eficiencias sustanciales en los procesos a través de varias industrias y es probable que contribuya a modelos de negocios completamente nuevos*." Por esta razón la industria de blockchain se está moviendo más allá de la prueba de concepto a pilotos en producción con el establecimiento de casos de negocio para identificar que tan beneficiosa es la tecnología. Un componente fundamental de tales pruebas es enfocarse en la seguridad y privacidad que deben ser abordadas y probadas lo suficiente, en caso de que esta tecnología pueda llegar a convertirse en el verdadero catalizador del cambio social e industrial que muchos piensan que puede ser.

Ciberseguridad en contexto

El alto nivel de dependencia en la tecnología y en el internet hoy día ha resultado en nuevos modelos de negocios y flujos de ingresos para las organizaciones, pero con nuevas brechas y oportunidades para quienes realizan ciberataques. Los ataques cibernéticos se han vuelto cada vez más específicos y complejos debido a la utilización de piezas de malware más sofisticado y la creciente amenaza de organizaciones cibernéticas profesionales[6]. Estos cibercriminales están robando información como propiedad intelectual, información del personal, registros médicos, datos financieros, y están recurriendo a estrategias rentables como la monetización al acceso de la información a través del uso de técnicas avanzadas de ransomware, o interrumpiendo las operaciones del negocio en general a través de ataques de Denegación Distribuida del Servicio, o DDoS por sus siglas en inglés[7]. En octubre de 2016, uno de los proveedores de servicios de dominio más grande, Dyn, experimentó la mayor Denegación Distribuida de Servicio en varios sitios web de alto tráfico como Twitter, Netflix y Spotify[8]. Los profesionales de Deloitte en riesgo cibernético sugieren que las organizaciones sigan un enfoque seguro, vigilante y resiliente cuando gestionen el ciberespacio independientemente de la tecnología que estas adopten[9].

Entonces, ¿qué pasa con blockchain? ¿será esta tecnología una ayuda cibernética o un obstáculo? Según Ed Powers, Líder de ciber-riesgo de Deloitte Estados Unidos, "*aunque todavía es incipiente, existe una innovación prometedora en blockchain encaminada a ayudar a las empresas a enfrentar desafíos inmutables de riesgo cibernético como lo son la identidad digital y mantener la integridad de los datos*." Blockchain podría ayudar a mejorar potencialmente la defensa cibernética ya que la plataforma pueda asegurar y prevenir actividades fraudulentas a través de mecanismos de consenso, y detectar la manipulación de datos debido a sus características subyacentes de inmutabilidad, transparencia, auditabilidad, encripción de datos y resiliencia operacional (incluyendo ningún punto de falla).

Sin embargo, como Cillian Leonowicz, Gerente Senior en Deloitte Irlanda opina "*las características de blockchain no proporcionan una panacea impenetrable a todos los males cibernéticos, pensarlo sería ingenuo en el mejor de los casos, como con otras tecnologías las Implementaciones de blockchain y roll outs debe incluir controles de ciber seguridad de sistema y red típicos, debida diligencia, prácticas y procedimientos*".



6 https://www.fireeye.com/offers/thank-you/mtrends2017-download-confirmation.html
7 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016
8 https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/
9 https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-gra-Changingthegameoncyberrisk.pdf

Confidencialidad

Según el Instituto Nacional de Estándares y Tecnología (NIST), confidencialidad se refiere a "*la propiedad de que la información confidencial no se divulgue a personas, entidades o procesos no autorizados*"[10].

Asegurar que solo las partes interesadas y autorizadas accedan a los datos correctos y apropiados es una preocupación común para las organizaciones que consideren utilizar blockchain hoy día. Proteger el acceso a la red de blockchain es fundamental en el aseguramiento del acceso a la información (particularmente en el blockchain privado). Si en un ciberataque se puede obtener acceso a la red de blockchain, es más probable que se tenga acceso a los datos, por ello, la importancia de los controles de autenticación y autorización que deben ser implementados[11], los mismo que con otras tecnologías.

Aunque la tecnología fue originalmente creada sin controles específicos de acceso (debido a su naturaleza pública) existen algunas implementaciones de blockchain que están empezando a asegurar la confidencialidad de la información y los desafíos en el control de accesos, proporcionando encripción de datos de bloque y capacidades AAA[12]. La encripción completa de los datos de la cadena de bloques garantiza que las partes no autorizadas no puedan acceder a los datos mientras estos datos se encuentren en tránsito (especialmente si los datos fluyen a través de redes no confiables).

Acceso a la red

En el blockchain público no existe la necesidad de controlar el acceso a la red, ya que los protocolos de las cadenas permiten que cualquiera pueda acceder y participar en la red, siempre y cuando descarguen primero un software. En contraste, el blockchain privado requiere de controles de seguridad apropiados para proteger el acceso a la red.

En un mundo perfecto sería tentador suponer que, debido a la naturaleza privada, las redes y sistemas locales ya están protegidos dentro del perímetro de la organización por varios anillos de seguridad a nivel interno (como firewalls, redes virtuales privadas, VLANs, sistemas de detección y prevención de intrusos, entre otros.), a través de una estrategia conocida como defensa de profundidad. No obstante, en un mundo perfecto los escenarios son una utopía, especialmente en seguridad, donde confiar solo en la efectividad de tales controles es insuficiente.

Por esta razón, las mejores prácticas de recomendaciones de controles de seguridad (como los controles de acceso) deberían también ser implementados directamente en el nivel de las aplicaciones siendo esta la primera y más importante línea de defensa, especialmente en escenarios de un ataque que obtiene acceso a una red local o donde existe ya un infiltrado. Las organizaciones, cuando consideren la arquitectura de red de blockchain, necesitarán también considerar cómo tratar los nodos no comunicados o intermitentemente activos, ya que las cadenas de bloques necesitarán continuar funcionando sin estos nodos, pero, también, deben ser capaces de restablecerse rápidamente cuando regresen a su función original[13].

"*Cada organización tiene que considerar la relación inherente entre rendimiento, innovación y ciber-riesgo, y analizar que proteger todo sería económicamente inviable, impidiendo las iniciativas estratégicas realmente importantes*" según Andrés Gil, líder de Ciberseguridad de Deloitte a nivel LATCO.

Las organizaciones deben evaluar su perfil de riesgo dinámico y determinar qué nivel y qué tipos de ciber-riesgos son aceptables, considerando cuáles son más importantes y la justificación en cuáles se deben invertir en controles de seguridad ´para proteger los activos más importantes. Es esencial evaluar los puntos débiles a lo largo del proceso de extremo a extremo, con la conciencia de que los miembros, proveedores y socios de confianza en cualquier momento pueden ser la fuente de errores o acciones intencionales que pueden dar aperturas a incidentes.

Las organizaciones deberían implementar todo un programa de ciberseguridad para evaluar estos desafíos incluyendo un marco de gobierno que incluya roles, procesos, medidas de responsabilidad,

10 http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
11 http://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting
12 https://media.readthedocs.org/pdf/hyperledger-fabric/latest/hyperledger-fabric.pdf
13 https://hbr.org/2017/03/how-safe-are-blockchains-it-depends
14 http://searchsecurity.techtarget.com/definition/PKI

indicadores de rendimiento bien definidos y, sobretodo, un cambio de mentalidad en toda la organización.

En línea con estos requerimientos, blockchain puede proporcionar controles de seguridad avanzada, por ejemplo, aprovechando la seguridad de la infraestructura clave pública (KPI por sus siglas en inglés) para autenticar y autorizar a las partes, y encriptar sus comunicaciones (KPI es un conjunto de roles, políticas y procedimientos requeridos para crear, gestionar, usar, almacenar, y revocar certificados digitales y gestionar una clave pública de cifrado[14].

El blockchain público podría ser potencialmente comparado con la internet, donde las organizaciones podrían intercambiar y recuperar información con cualquiera que tenga acceso a un proveedor de servicios, mientras que el blockchain privado podría ser comparado con las páginas de intranet de las organizaciones, donde la información es compartida e intercambiada únicamente con quien ha sido autorizado para acceder al sitio. Si blockchain llegara a ser mundialmente adoptado, las organizaciones necesitarían asegurar la implementación de controles de seguridad para proporcionar autenticación, autorización y cifrado de datos con el fin de proteger adecuadamente el acceso a la información. "*Los ciberataques siempre buscan puntos débiles de un punto a otro, y la información confidencial almacenada en una cadena de bloques probablemente se convertirá en una prioridad de alto nivel si dichos controles son inadecuados*", según Eva Yee Ngar Kwok, Socia de la línea de Tecnología de Risk Advisory en Deloitte China, Hong Kong.

Acceso y Divulgación de la información

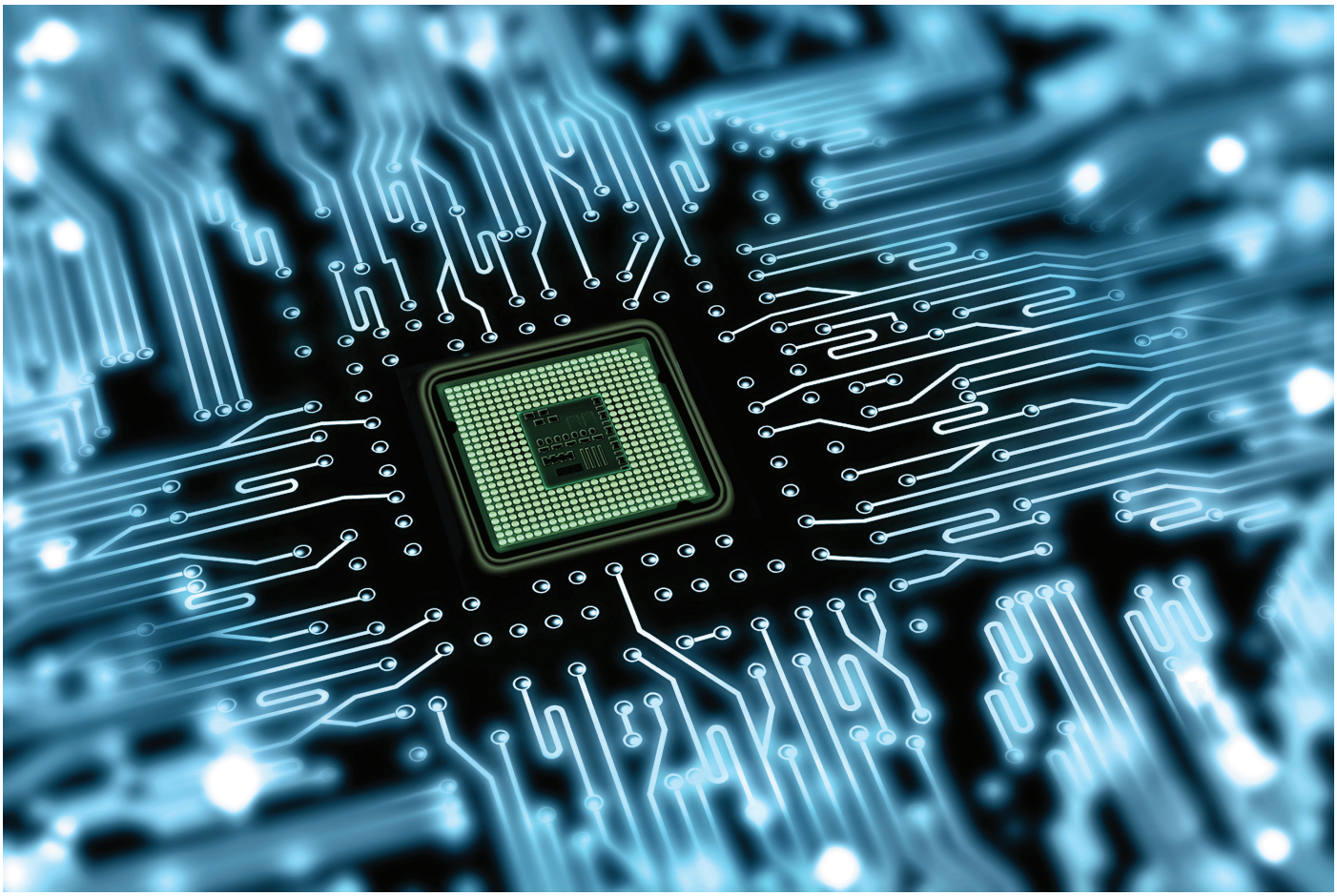
Hoy, si un ciberataque logra acceder a una red de blockchain y los datos, no significa necesariamente que el hacker pueda leer o recuperar la información. La encripción completa de los bloques de datos se puede aplicar a los datos que están en circulación en la red, garantizando efectivamente su confidencialidad, considerando que se siguen los lineamientos más recientes de encripción. El uso del cifrado de extremo a extremo, que se ha convertido en un importante tema de discusión en años recientes[15], donde solo quienes tienen la autorización de acceder a la información cifrada, por ejemplo, a través de su clave privada, pueden descifrar y ver la información. Emplear claves de encripción en conjunto con KPI puede proporcionar a las organizaciones un alto nivel de seguridad. La información cifrada en una cadena de bloques puede proporcionar a las organizaciones un nivel de protección de la información confidencial, y una perspectiva del control al acceso de la información.

Como ejemplo, implementar un protocolo de comunicación seguro en blockchain (siguiendo los recientes estándares de seguridad y lineamientos de implementación), garantizando que incluso en una situación en donde un hacker intente realizar un ataque al dispositivo de un profesional de la organización, éste no podrá falsificar la identidad ni divulgar cualquier dato, así éste se encuentre en tránsito en la red. Incluso en una situación extrema en la que las claves privadas estáticas se ven comprometidas, las sesiones pasadas se mantienen confidenciales debido a las propiedades perfectas de secreto de envío de los protocolos de seguridad[16].

A pesar de que los usuarios de blockchain generalmente realizan una copia de su clave de seguridad en un sitio privado, el robo de claves privadas sigue siendo un riesgo alto. Es importante anotar que las claves son usadas para múltiples propósitos en el ecosistema de blockchain: protección del usuario de la información, confidencialidad de la información, y autenticación y autorización de la red. Según Lior Kalev, Director de servicios de Ciber Riesgos de Deloitte Israel, "Las personas buscan y necesitan estar conectadas con sus datos todo el tiempo desde cualquier lugar, y cualquier dispositivo lo que genera riesgos cibernéticos, y hace que la gestión al acceso a la red en las organizaciones sea un desafío". Las organizaciones necesitan ser conscientes que acceder a su cuenta de blockchain desde varios dispositivos puede ponerlos en un nivel alto de riesgo de perder el control de sus claves privadas. Considerando esto, es importante que las entidades sigan procedimientos adecuados en la gestión de claves (como el IETF o las directrices en la gestión de claves criptográficas RFC 4107)17 y desarrollar internamente prácticas seguras de gobierno en la gestión de claves, ya que esto será fundamental para la seguridad de la red de blockchain. Según Artur D'Assumpção, Director de Riesgo Cibernético y Ciberseguridad de Deloitte Portugal "*En un ambiente empresarial será fundamental asegurar adecuadamente el material de la clave privada para no poner en peligro la integridad y los registros. Un ejemplo de una protección adecuada es el uso de "key vaults" especiales que implementan tecnologías como Módulos de Seguridad de Hardware para asegurar información secreta, proporcionando un entorno altamente seguro y resistente a la manipulación.*"

Actualmente los algoritmos criptográficos, utilizados para la generación de claves públicas y privadas, se basan en problemas de factorización de enteros, que son difíciles de descifrar con la capacidad de un computador actual. Según Jacky Fox, Líder Cyber de Deloitte Irlanda, "*Los avances en la computación cuántica serán importantes para la seguridad de blockchain debido a su impacto en la práctica de la criptografía actual.*" Por ejemplo, Bitcoin

utiliza algoritmos criptográficos para producir un par de claves públicas y privadas y una dirección la cual se deriva utilizando operaciones de hash y suma de comprobación en la clave pública.
La exposición de la dirección por sí sola no es de alto riesgo. Sin embargo, la exposición de la dirección y la clave pública requerida para realizar transacciones potencialmente, dados los avances suficientes en la computación cuántica, permitirá la derivación de la clave privada. Jacky Fox destaca que "*mientras que la computación cuántica comercial no está disponible como una realidad a gran escala, tiene sentido planificar ahora el cambio a la criptografía resistente cuántica. NIST se encuentra actualmente en el proceso de desarrollar estándares de criptografía resistentes a la cuántica y la NSA está recomendando a sus proveedores el plan de implementar SHA-384 en lugar de SHA-25*."



15 https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/
16 https://www.wired.com/2016/11/what-is-perfect-forward-secrecy/)
17 https://tools.ietf.org/html/rfc4107

Integridad

La integridad es definida como el "protegerse en contra de la modificación o destrucción inadecuada de la información, e incluye asegurar el no repudio y autenticidad de la información" según NIST"[18].

Mantener la consistencia de la información, y garantizar la integridad durante todo el ciclo de vida es crucial en los sistemas de información. Encripción de datos, comparación hash (valor enviado vs. valor recibido), o el uso de firma digital, son algunos ejemplos de cómo los propietarios de los sistemas pueden asegurar la integridad de la información, independientemente de la etapa en la que se encuentre (en tránsito, en reposo y en almacenamiento). Las características, inmutabilidad y trazabilidad ya proporcionan a las organizaciones un medio para garantizar la integridad de la información.

Inmutabilidad

La tecnología Blockchain puede considerarse como una tecnología segura, desde el punto de vista que permite a los usuarios confiar en que las transacciones almacenadas en el libro de contabilidad contra falsificaciones son válidas. La combinación de hashing y criptografía secuencial, a lo largo de una estructura descentralizada, hace que sea muy difícil para cualquier parte manipular la información a comparación de una base de datos estándar[19]. Esto proporciona a las organizaciones el usar las tecnologías con seguridad sobre la integridad y la veracidad de la información. Los protocolos basados en modelo de consenso asociados a la tecnología también presentan en las organizaciones un mayor de nivel de aseguramiento sobre la seguridad de los datos, ya que grosso modo el 51% [20] de los usuarios en cadenas de bloques públicas y privadas necesitan estar de acuerdo en que una transacción es válida antes de ser agregada a la plataforma. Las organizaciones pueden implementar otros mecanismos para prevenir y controlar la división del bloque mayor en caso de que ocurra un ataque de control cibernético del 51%, por ejemplo, controlar si uno de los nodos aumenta la potencia de procesamiento y está ejecutando un número significativamente mayor de transacciones[21].

"Derecho a ser olvidado"

Respecto a la inmutabilidad de los datos es importante considerar cómo las cadenas de bloques y blockchain en general, encajarán con las leyes de privacidad de la información. Cómo implementar el derecho "a ser olvidado" en una tecnología que garantiza que nada se borrara es un desafío, para el cual, existen múltiples soluciones. Una solución es cifrar la información en el sistema, para asegurar que, cuando llegue el momento, el "olvido" de las claves garantiza que la información confidencial ya no es accesible.

Otra posibilidad es centrarse en el valor de blockchain para proporcionar evidencia inalterable de hechos escribiendo el hash de las transacciones en él, mientras que las transacciones en sí mismas se almacenan fuera del sistema. Esto mantiene la integridad de las transacciones, al tiempo que permite la capacidad de borrar las transacciones, dejando información restante, "olvidada" en la cadena de bloques.

18 http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
19 https://techcrunch.com/2016/12/05/how-blockchain-can-help-fight-cyberattacks/
20 https://learncryptography.com/cryptocurrency/51-attack
21 https://learncryptography.com/cryptocurrency/51-attack

Trazabilidad

Cada transacción agregada a una cadena de bloques pública o privada está firmada digitalmente y con marca de tiempo, lo que significa que las organizaciones pueden rastrear hasta un periodo de tiempo específico cada transacción e identificar la parte correspondiente (vía su dirección IP pública) en la cadena de bloques. Esta característica detalla una prioridad importante en seguridad de la información: el no repudio[22], que es la garantía que alguien no pueda duplicar la autenticidad de su firma en un archivo o la autoría de una transacción que originó. Esta funcionalidad inmediata de blockchain aumenta la confiabilidad en el sistema (detección de intentos de manipulación o transacciones fraudulentas), ya que cada transacción está asociada criptográficamente a un usuario.

Cualquier nueva transacción agregada a una cadena de bloques resultará en el cambio del estado global del bloque mayor. La implicación de esto es que, con cada nueva iteración en el sistema, el estado previo será almacenado, dando como resultado un registro de historial completamente rastreable. La capacidad de auditar la tecnología proporciona a las organizaciones un nivel de transparencia y seguridad de cada interacción. Desde una perspectiva de ciberseguridad, esto proporciona a las entidades un nivel adicional de seguridad de que los datos son auténticos y no se han manipulado.

Contratos Inteligentes

Los "smart contracts", siendo programas de computación que se ejecutan en el bloque mayor, se han convertido en una característica de blockchain[23]. Este tipo de programa puede ser usado para facilitar, verificar, o reforzar las reglas entre las partes, permitiendo el procesamiento directo e interacción con otros contratos inteligentes. Dicho software proporciona una gran área que puede ser atacada, por lo que un ataque a un contrato inteligente podría tener un efecto dominó en otras partes de la plataforma, es decir, el lenguaje por sí mismo o la implementación de los contratos. Durante el evento DevCon 2 en Shanghái, un ataque DDoS explorando la vulnerabilidad en un contrato inteligente basado en Ethereum, previno a los hackers seguir atacando otros bloques en la cadena.[24].

Blockchain da a conocer un nuevo paradigma en el desarrollo de software, con buenas prácticas seguras en el desarrollo (como la implementación de codificación segura y pruebas de seguridad) que necesitan ser implementadas (y actualizadas) para supervisar el ciclo de vida de los contratos inteligentes (como la creación, pruebas, despliegue y gestión). Según Diego Rodriguez Roldan, Director la práctica de Asesoramiento de Deloitte España, "será necesario aplicar metodologías como el Ciclo de Vida Seguro del Desarrollo del Software (S-SDLC) con el fin de minimizar la amenaza de un error crítico durante el ciclo de vida de un contrato inteligente". El ataque a la entidad DAO, una organización descentralizada construida sobre Ethereum, es un ejemplo donde los contratos inteligentes pueden ser atacados. Un hacker llevó a cabo un error de contagio inteligente que resultó en el robo de 60M de Ethereum's[25].

Calidad de los datos

La tecnología blockchain no garantiza o mejora la calidad de los datos. El blockchain tanto privado como público solo tiene la responsabilidad por la exactitud y calidad de la información una vez que esta ha sido introducida en la cadena de bloques, lo que significa que debe confiar en que los datos que se obtienen de los sistemas fuente existentes de las organizaciones son de buena calidad, como sucede con todos los demás sistemas de tecnología. Según Prakash Santhana, Director General de la práctica de Asesoramiento en Deloitte Estados Unidos. "*la mayor vulnerabilidad del marco blockchain está fuera del marco en las fuentes "de confianza". Una fuente de confianza corrupta podría potencialmente causar un efecto domino en toda la red. Un ataque en la fuente de confianza podría incluso ser a través de las partes conectas por vía directa o indirecta*". La fuente de confianza genera datos no confiables que entran a un ambiente confiable, por lo tanto, las organizaciones deben considerar el uso de múltiples fuentes de confianza para aumentar la seguridad en la integridad de los datos que ingresan al blockchain desde fuentes de confianza.

Si los datos ingresados son precisos, la tecnología de blockchain puede desempeñar un papel importante en la transformación de la salida de datos a medida que las tecnologías se aproximan a las capacidades en tiempo real, permitiendo a las organizaciones que verifiquen los datos transaccionales más rápido que cualquier otro sistema y facilita que las organizaciones tomen medidas más proactivas. Dado que los datos se transmitirán inevitablemente de un sistema origen de las organizaciones a una cadena de bloques, las entidades deben garantizar que los canales de intercambio sean seguros, ya que este es sin duda un punto de ataque y entrada para los atacantes.

22 http://searchsecurity.techtarget.com/definition/nonrepudiation
23 http://www.coindesk.com/making-sense-smart-contracts/
24 https://www.ethnews.com/looking-back-at-ethereum-in-2016
25 http://www.coindesk.com/dao-attacked-code-issue-leads-60-million-ether-theft/

Disponibilidad

El NIST define la disponibilidad como "*asegurar el acceso y uso oportuno y confiable de la información*"[26].

Los ataques cibernéticos que intentan impactar la disponibilidad de los servicios de tecnología continúan aumentando[27]. DDoS, siendo uno de los tipos más comunes de ataques[28], puede también causar la mayor disrupción de los servicios de internet, y, por lo tanto, afectar las soluciones basadas en blockchain. Las implicaciones resultantes son que los sitios web se interrumpan, las aplicaciones móviles no respondan, y esto puede generar pérdidas y costos cada vez mayores para las empresas[29]. Dado que las cadenas de bloques son plataformas distribuidas, los ataques DDoS en las cadenas de bloques no son como los ataques comunes. Estos ataques son costosos ya que intentan infiltrarse y dominar la red con grandes volúmenes de transacciones pequeñas. La descentralización y las características P2P, o peer-to-peer, de la tecnología hace a esta más difícil de destruir que arquitecturas distribuidas de aplicaciones convencionales (como el de cliente-servidor), aunque seguramente se está sujeto a ataques DDoS y, por lo tanto, aún sigue siendo necesario implementar medidas de protección, tanto a nivel de red como a nivel de aplicación[31]. La red de Bitcoin resistió un ataque DDoS en 2014[32], donde los hackers intentaron controlar la red mediante peticiones.

Según Peter Goch, Socio de Risk Advisory en Deloitte Reino Unido, "*esto es probable que vuelva a suceder, y se estima que los ataques DDoS se incrementen en tamaño y en escala, con ataques regulares de terabyte por segundo, que restringen la capacidad de la infraestructura de internet regional e incluso, global*". Este aumento se debe en gran medida a la creciente base instalada de dispositivos inseguros de tecnología Internet de las Cosas (IoT), la disponibilidad en línea del malware DDoS y la disponibilidad de velocidades de ancho de banda cada vez mayores. Aunque las soluciones de cadena de bloques descentralizadas y resistentes dependen de la alta disponibilidad, los ataques DDoS seguirán siendo una amenaza persistente.

26 http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf, pg. 21
27 http://www.zdnet.com/article/ddos-attacks-increase-over-125-percent-year-over-year/
28 https://techcrunch.com/2016/12/05/how-blockchain-can-help-fight-cyberattacks/
29 https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf
30 http://www.coindesk.com/so-ethereums-blockchain-is-still-under-attack/
31 https://techcrunch.com/2016/12/05/how-blockchain-can-help-fight-cyberattacks/
32 https://www.forbes.com/sites/leoking/2014/02/12/bitcoin-hit-by-massive-ddos-attack-as-tensions-rise/#2442aa4246ad

No existe un único punto de falla

La tecnología Blockchain no tiene un único punto de falla, lo que reduce considerablemente las posibilidades de que un ataque DDoS basado en IP interrumpa el funcionamiento normal [33]. Si se quita un nodo, los datos siguen siendo accesibles a través de otros nodos dentro de la red, ya que todos ellos mantienen una copia completa del bloque mayor en todo momento. La naturaleza distribuida de la tecnología resuelve el problema de falso consenso.

Bitcoin a la fecha, es la plataforma más probada en el mercado, que ha resistido con éxito los ataques cibernéticos durante más de 7 años[35]. La infraestructura de blockchain evidentemente proporciona un nivel adicional de accesibilidad a los datos, dado que los datos son accesibles a través de cualquiera de los nodos de la red, incluso en el caso de que un ataque DDoS interrumpa algunos de los nodos.

Aunque se considere que una red blockchain no tienen un único punto de falla, las organizaciones podrían enfrentarse a riesgos de eventos externos fuera de su control. Por ejemplo, una interrupción global de la red de internet interrumpiría incluso una red pública blockchain distribuida como Bitcoin o Ethereum, creando interrupciones que afectarían las operaciones de una organización como con cualquier otra tecnología. Las redes privadas de blockchain con un número menor de nodos necesitarían garantizar que su red esté lo suficientemente distribuida globalmente y resiliente, sin puntos únicos de falla en una organización o plataforma para garantizar una operación continua, incluso en caso de un desastre natural o un ataque coordinado.

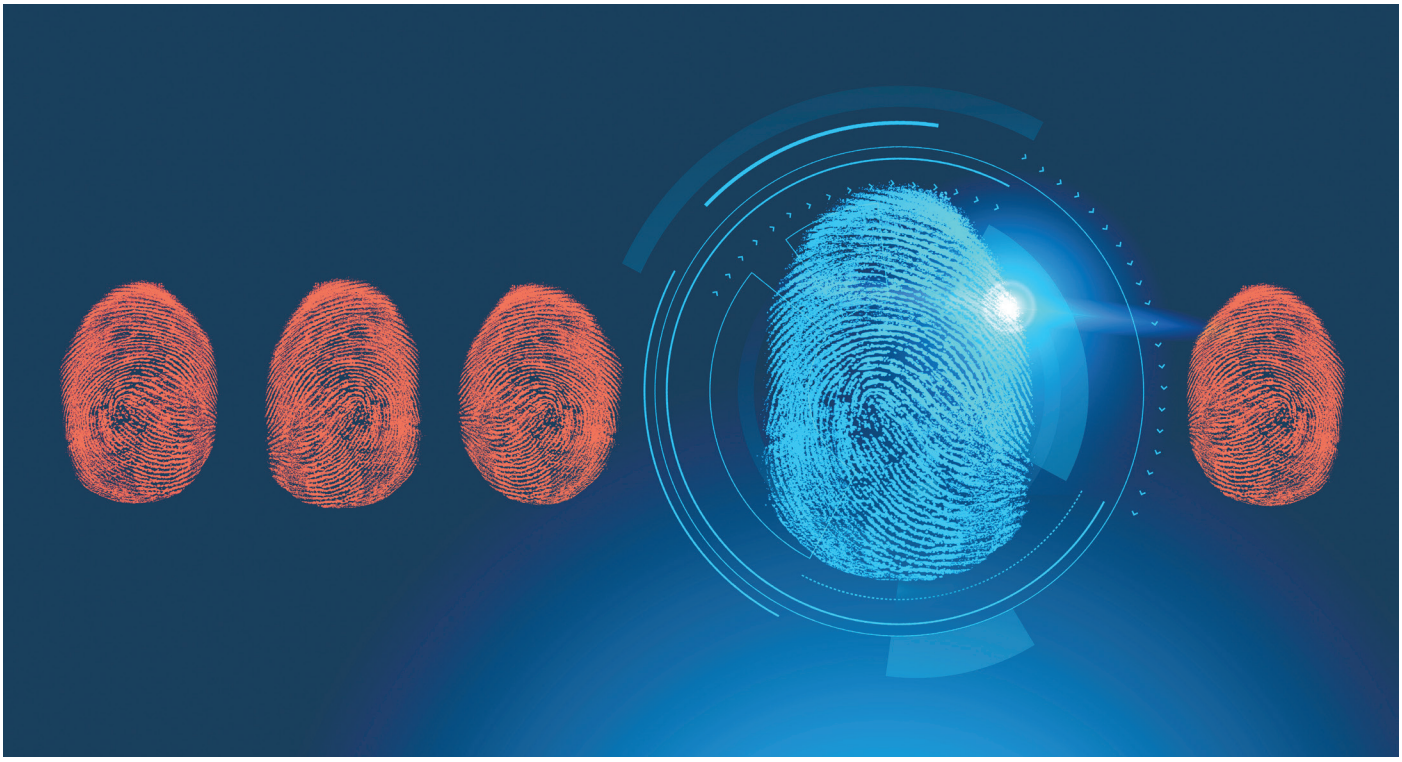
Resiliencia Operacional

La combinación de la naturaleza P2P y el número de nodos en una red, operando de una forma distribuida 7x24, hace que la plataforma sea operacionalmente resiliente. Dado que tanto el blockchain público como privado consiste en múltiples nodos, las organizaciones pueden hacer que un nodo bajo ataque sea redundante y, que funcione común y corriente. Entonces, incluso si una gran parte de la red de blockchain es atacada, continuará operando debido a la naturaleza distribuida de la tecnología.

Esto no significa que la red es completamente "a prueba de balas"". Desde el principio de blockchain en 2008, las plataformas han enfrentado amenazas donde los hackers han intentado poner en peligro su estabilidad, utilizando diferentes fuentes de ataque. La docilidad de las transacciones, un error que se detectó cuando las transacciones se encontraban en un estado de validación pendiente, dio como resultado un ataque a la red Bitcoin en 2014[36], lo que afectó la experiencia de los usuarios. En 2016, un hacker aprovechó los contratos inteligentes en Ethereum, y la forma en que se pueden utilizar, para crear un desbordamiento en la red, hasta el punto en que la creación de bloques y la validación de las transacciones se vieron gravemente afectadas, lo que desaceleró la red[37]. Esto se ha abordado con la creación de un hardfork (divergencia permanente de la versión anterior de blockchain)[38]. Según Suchitra Nair, Director de Risk Advisory en Deloitte Reino Unido *"La resiliencia operacional de blockchain será un área clave para los reguladores, y necesitarán ser rigurosos en las pruebas y evidencias con el fin de obtener una garantía regulatoria. La alta gerencia debe poder articular los riesgos clave que sustentan la tecnología blockchain y el marco y control del Gobierno Corporativo establecido por la alta dirección".* La importancia de la participación de los reguladores para facilitar el desarrollo y la adopción de blockchain es abordada por la Líder de Gestión de Inversiones de Asia Pacífico de Deloitte, Jennifer Qin, quien señala que "*para hacer que blockchain sea comercialmente viable y ser totalmente adoptada por las empresas y los gobiernos, debe cumplir con los requisitos regulatorios, y diversos entornos empresariales.*"

33 https://blog.ethereum.org/2016/09/22/transaction-spam-attack-next-steps/
34 https://ice3x.co.za/byzantine-generals-problem/
35 http://performermag.com/band-management/contracts-law/dot-blockchain-music-project/
36 http://www.coindesk.com/bitcoin-bug-guide-transaction-malleability/
37 http://www.coindesk.com/so-ethereums-blockchain-is-still-under-attack/
38 https://blog.ethereum.org/2016/11/18/hard-fork-no-4-spurious-dragon/

Seguro, Vigilante y Resiliente Programa de Ciber-Riesgo



39 https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-gra-Changingthegameoncyberrisk.pdf

Ningún sistema de información o defensa cibernética puede considerarse 100% seguro. Lo que hoy se considera seguro no lo será mañana, esto debido a la naturaleza lucrativa del delito cibernético y el ingenio del delincuente para buscar nuevos métodos de ataque. Aunque algunas de las capacidades subyacentes de blockchain proporcionan confidencialidad, integridad y disponibilidad de datos, al igual que otros sistemas, es necesario adoptar controles y estándares de seguridad cibernética para las organizaciones que usan blockchain dentro de su infraestructura técnica para proteger a sus organizaciones de ataques externos.

Los profesionales ciber de Deloitte en todo el mundo sugieren que las entidades sigan nuestro enfoque cibernético seguro, vigilante y resiliente (SVR) que no solo apoyará a las entidades para que permanezcan seguras, sino que también se vuelvan más vigilantes y resilientes a las amenazas cibernéticas en desarrollo. Creemos que la adopción de este enfoque seguro, vigilante y resiliente al ciberespacio es un paso clave para ayudar a los líderes a continuar impulsando el desempeño en sus organizaciones[39].

Eric Piscini, líder global de Deloitte Estados Unidos en Blockchain, Destaca que "mientras que la seguridad cibernética es fundamental para la gran adopción de blockchain, las operaciones, la arquitectura tecnológica, la creación de subsidiarias, el talento y las regulaciones globales son componentes clave que también deben considerarse". Para obtener más información sobre cómo proteger su blockchain o, más generalmente, su negocio contra los ataques cibernéticos, comuníquese con nuestros expertos en ciber seguridad y blockchain en su región.

Estrategia y Gobierno

Seguro

Seguridad significa tener priorizados los controles por el riesgo para defenderse de las amenazas conocidas y emergentes

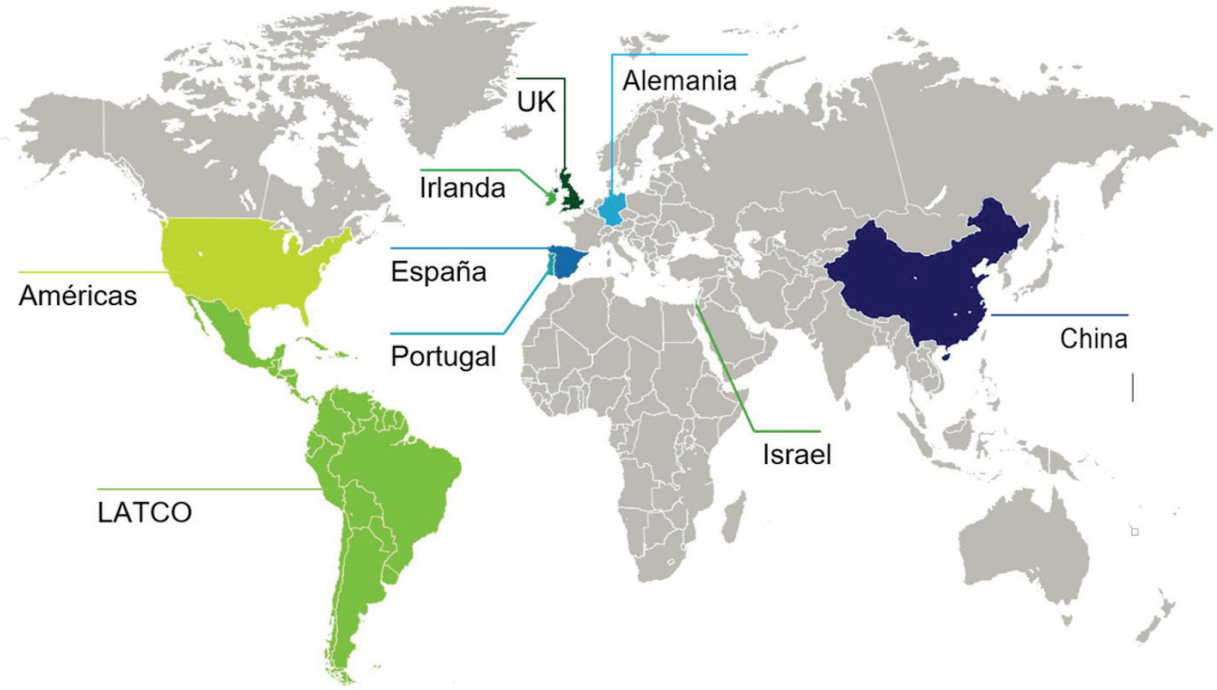
Vigilante

Supervisión significa tener inteligencia de amenazas y conocimiento de la situación para identificar conductas perjudiciales

Resiliente

Resiliencia significa tener la capacidad de recuperarse y minimizar el impacto de los incidentes cibernéticos

Lista Global de profesionales de Deloitte que contribuyeron a este artículo



Abhishek Biswas (abiswas@deloitte.com) – Deloitte US Advisory Senior
Manager Andres Gil (angil@deloitte.com) – Deloitte LATCO Cyber Risk Lead
Artur D'Assumpção (adassumpcao@deloitte.pt) – Deloitte Portugal Cyber Risk / Cyber Security Lead
Charles Ho Lam Low (clow@deloitte.com.hk) – Deloitte China Risk Advisory Technology Risk
Manager Cillian Leonowicz (cleonowicz@deloitte.ie) – Deloitte Ireland Senior Manager
Dave Clemente (daclemente@deloitte.co.uk) – Deloitte UK Risk Advisory Senior Manager
Diego Roldan Rodriguez (drodriguezroldan@deloitte.es) – Deloitte Spain Advisory
Director Edward Powers (episcini@deloitte.com) – Deloitte U.S Cyber Risk Lead
Eva Yee Ngar Kwok (evakwok@deloitte.com.hk) – Deloitte China Risk Advisory Technology Risk
Partner Fernando Picatoste (fpicatoste@deloitte.es) – Deloitte Spain Risk Advisory
Partner Irfan Saif (isaif@deloitte.com) – Deloitte US Advisory Principal
Jacky Fox (jacfox@deloitte.ie) – Deloitte Ireland Cyber Lead
Jennifer Yi Qin (jqin@deloitte.com.cn) – Deloitte Asia Pacific Investment Management
Lead Lior Kalev (lkalev@deloitte.co.il) – Deloitte Israel Cyber Risk Services Lead
Luciana Gaspari (lgaspari@deloitte.com) – Deloitte Latin America Risk Advisory Senior
Manager Milan Sallaba, Deloitte Germany's Technology-Sector Lead
Pablo Cabellos Rodríguez (prodriguezcabellos@deloitte.es) – Deloitte Spain Risk Advisory
Manager Peter Gooch (pgooch@deloitte.co.uk) – Deloitte UK Risk Advisory
Partner Prakash Santhana (psanthana@deloitte.com) – Deloitte US Advisory
Managing Director Suchitra Nair (snair@deloitte.co.uk) – Deloitte UK Risk Advisory
Director Vikram Bhat (vbhat@deloitte.com) – Deloitte US Advisory Principal
Yang Chu (yangchu@deloitte.com) – Deloitte US Advisory Senior Manager

Deloitte.

www.deloitte.com/co

Deloitte se refiere a una o más firmas de Deloitte Touche Tohmatsu Limited (“DTTL”), y su red global de firmas miembro y de entidades relacionadas. DTTL (también denominada “Deloitte Global”) y cada una de sus firmas miembro son entidades legalmente separadas e independientes. DTTL no presta servicios a clientes. Por favor revise www.deloitte.com/about para conocer más.

Deloitte es líder global en Servicios de auditoría y aseguramiento, consultoría, asesoramiento financiero, asesoramiento en riesgos, impuestos y servicios relacionados. Nuestra red de firmas miembro presente en más de 150 países y territorios atiende a cuatro de cada cinco compañías listadas en Fortune Global 500®. Conoce cómo aproximadamente 264.000 profesionales de Deloitte generan un impacto que trasciende en www.deloitte.com

Esta comunicación contiene únicamente información general, ni Deloitte Touche Tohmatsu Limited, ni sus firmas miembro o sus entidades relacionadas (colectivamente, la "Red Deloitte") están, por medio de la presente comunicación, prestando asesoría o servicios profesionales. Previo a la toma de cualquier decisión o ejecución de acciones que puedan afectar sus finanzas o negocios, usted deberá consultar un asesor profesional cualificado. Ninguna entidad de la Red Deloitte se hace responsable por pérdidas que pueda sufrir cualquier persona que tome como base el contenido de esta comunicación.

© 2018. Para información, contacte a Deloitte Touche Tohmatsu Limited.