Caso práctico de Auditoría en el mundo del Cloud


Como ya adelanté en el anterior post, este cuarto post lo centraré en exclusiva en analizar un caso práctico de auditoría aplicado al mundo del Cloud Computing [1]. Si que me gustaría destacar, que a pesar de que la resolución del caso es correcta, ISACA ha realizado una serie de cambios importantes en las últimas versiones de COBIT, la quinta en particular. Por lo tanto, este post ha sido elaborado con la información que ISACA ha publicado con fin divulgativo pero es necesario acceder a los manuales más recientes si se desea elaborar una auditoría de sistemas alojados en la nube completa y elaborada mediante los estándares más recientes.

En el caso que analizamos en este post, la compañía A, ofrece una solución de software llamada Business Express mediante un modelo de distribución **SaaS**, no obstante la compañía no cuenta con la infraestructura propia necesaria para ofrecer esta solución. Por lo tanto, ha decidido hospedar su infraestructura en la nube (**IaaS**) mediante un acuerdo entre esta empresa y un **CSP** (Cloud Service Provider).

En resúmen, el **CIO** de la compañía ha decidido encomendar a un auditor de sistemas la tarea de auditar los dos aspectos que he mencionado anteriormente: la solución que ofrece la compañía en forma de SaaS y los sistemas alojados en la nube(IaaS) del CSP para soportar esa solución.

Una vez el CIO le ha comunicado al auditor cuales son las dos cuestiones a auditar, el auditor ha decidido elaborar un plan de auditoría con el fin de identificar los riesgos existentes en ambos sistemas. Para la realización de dicha auditoría, en la actualidad existen multitud de frameworks distintos de los que hacer uso.

Por una parte se puede hacer uso de frameworks genéricos como el elaborado por **COSO** (Enterprise Risk Management-Integrated Framework), y por otra parte, se pueden utilizar los frameworks referentes a la parte IT como son el **ISO 27001** o el **ITIL**. Asimismo, diferentes organismos e instituciones como la **CSA** (Cloud Security Alliance), la **ENISA**, o el **NIST [2]** (US National Institute of Standards and Technology), ya han publicado diferentes guías referentes al tema que se trata en cuestión, las auditorías del cloud computing.

Finalmente, COBIT es un estándar que permite la realización de una auditoría holística que permita identificar los riesgos más relevantes de IT.

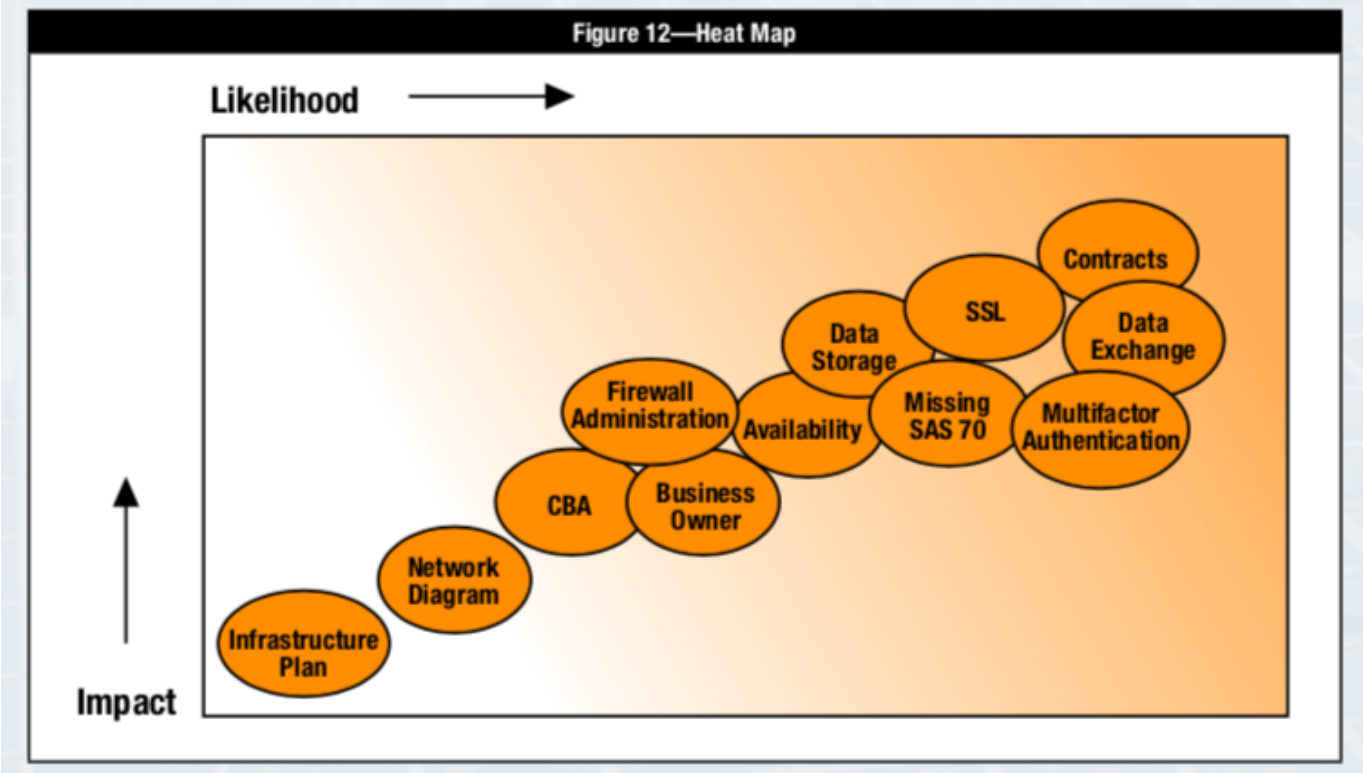
Por todo lo mencionado anteriormente, el auditor ha decidido hacer uso del framework Risk IT. Este framework se basa en los principios de COBIT pero complementandolo con todos aquellos riesgos no relacionados con IT que COBIT no contempla. Además, también hace uso de las distintas guías específicas sobre Cloud Computing que he mencionado antes para tener en cuenta también los riesgos propios de esta tecnología. Gracias a todo ello, el auditor consigue elaborar un listado de 36 escenarios distintos a analizar donde se relaciona cada riesgo IT con los objetivos de control propuestos por COBIT.

Dado que el documento cuenta con información abundante acerca de la realización de los controles, he decidido centrarme en las conclusiones del informe y destacar aquellas cuestiones más relevantes.

Por ejemplo, el riesgo número 34 hace referencia a la los riesgos relacionados con los acuerdos contractuales, los referentes de los distintos proveedores de servicios en particular. El auditor al analizar el acuerdo percibe la carencia de una auditoría externa al CSP, una cuestión trascendental antes de entablar cualquier tipo de relación con este tercero.

Este ejemplo, demuestra cómo COBIT no solo permite auditar riesgos tecnológicos sino que además, también analiza y estudia un amplio espectro de riesgos que van más lejos de la propia tecnología como es en este caso son los acuerdos contractuales. Es decir, una análisis holística de los riesgos.

El informe elaborado por el auditor también destaca como la integridad de los datos se ve comprometida por la carencia de un sistema seguro de comunicación entre la empresa A y los sistemas alojados en el CSP (punto 28). Además, en lo referente a los Service Level Agreements (**SLA**), estos presentan un nivel de detalle escaso y la calidad del servicio (**QoS**) también se ha visto comprometida.



En resúmen y como demuestra esta infografía teniendo en cuenta los criterios de probabilidad e impacto, hay dos cuestiones a destacar: los aspectos asociados a los **acuerdos contractuales** y los aspectos referentes a la **seguridad en la comunicación** entre ambas entidades (Empresa A y los sistemas alojados en el CSP).

Para concluir, el objetivo final de este post ha sido el mostrar un framework metodológico para identificar, clasificar y priorizar los riesgos más relevantes en la implantación de esta tecnología. Al fin y al cabo, la clave del éxito radica en saber destinar los recursos en función de las prioridades de cada riesgo (prioridades alineadas con la estrategia del negocio). Por otra parte, los controles son importantes y resultan cruciales pero siempre se debe tener en cuenta una simple cuestión ¿Este nuevo control me va a suponer un coste superior al riesgo que intento evitar?, de ser así el implantar el control no es una opción viable.

En definitiva, cualquier control que se realice tiene un claro objetivo: identificar el impacto de los riesgos en el negocio. Por consiguiente, toda esta gestión de riesgos IT debe ir alineada con la estrategia de la empresa.

[1] «SP 800-144, Guidelines on Security and Privacy in … – NIST CSRC.» https://csrc.nist.gov/publications/detail/sp/800-144/final. Se consultó el 29 noviembre 2018.

[2] «Cloud Computing Risk Assessment A Case Study – isaca.» https://m.isaca.org/Journal/archives/2011/Volume-4/Documents/jpdf11v4-Cloud-Computing.pdf. Se consultó el 29 noviembre 2018.

Blockchain: Riesgos asociados (3/5)

Buenas de nuevo! Si eres un nuevo lector y no has leído mis anteriores entradas, te invito a que te acerques a las anteriores entradas. En la primera entrada [enlace], hablé de qué era Blockchain; la arquitectura que tenía, cómo funcionaba y sus respectivos beneficios. Después, en el segundo artículo [enlace] (anterior a este) realicé una reflexión para primeramente comprender los riesgos y después ver qué directivas e iniciativas regulativas existían para proteger y guiar a toda organización que estuviera interesada en incluir estas "cadenas de bloques"; además hice un pequeño análisis donde ya identificábamos algunas cuestiones que planteaban si realmente existía una compatibilidad con la ley RGPD.

Volviendo al presente, el objetivo de este post será identificar los riesgos potenciales asociados a Blockchain. Pero antes de nada, veamos qué es un riesgo:

"Contingencia o posibilidad de un daño" [1]

Entonces, todo aquello que pudiera ser un problema por el daño que supone se define como eso mismo. Dentro del contexto empresarial, más concretamente en Sistemas de Información, me gustaría hacer especial hincapié en que los riesgos no sólo están en la tecnología como buenamente se suele pensar.
Es obvio asumir que utilizar una tecnología concreta debes aceptar que esta puede fallar. Sin embargo, existen más actores rodeando no sólo a las tecnologías sino que también a las propias organizaciones y sociedades a las que forman y donde están. Por otra parte, ya en 2016 ISACA había identificado riesgos potenciales, de los que hablaré a continuación. Muestra de ello, se expone la figura 1[2], que básicamente es un Heatmap donde en función de la probabilidad y el impacto se muestran los riesgos para Blockchain:

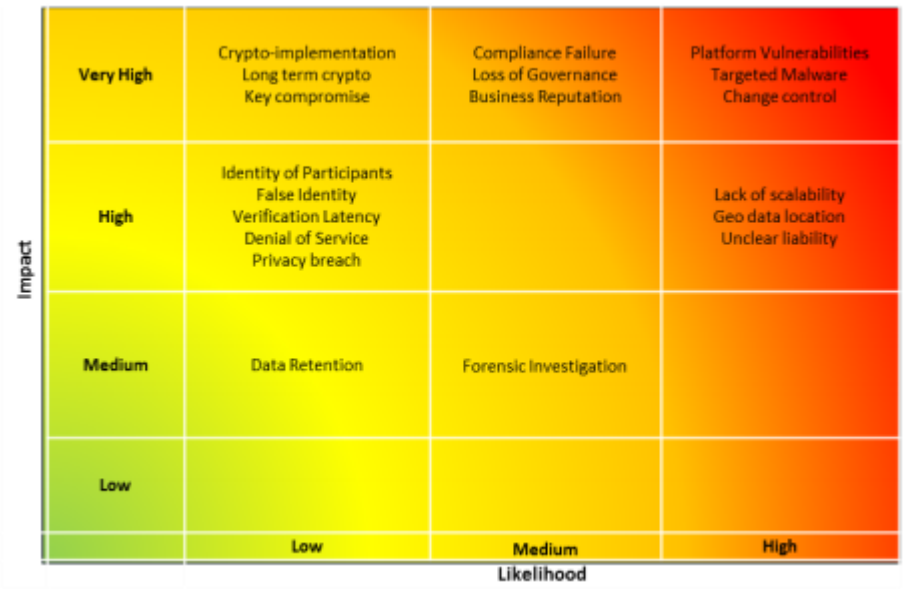


Figura 1: Tabla de riesgos para Blockchain en función de la probabilidad e

impacto.

La tabla se interpreta de la siguiente manera: “cuanto más rojo, mayor cuidado” hay que tener, mayor riesgo e impacto implican. Como si fuera un semáforo de riesgos.

Según ISACA, podríamos ponderar en varios niveles estos riesgos. En un primer nivel (en color rojo), se encuentran el control de cambios, las vulnerabilidades y la gestión y control del cambio. En un segundo nivel (en color “ámbar”), se encuentran los riesgos asociados a la pérdida de control y cumplimiento legislativo. En un tercer nivel, riesgos asociados a la privacidad y retención de la información además de la encriptación, entre otros.

Es algo lógico; primeramente, hay que gestionar el cambio de paradigma que implicaría dentro de una organización. Después, ¿Sirve para toda la infraestructura de la que se nutre la organización?¿O sólo en parte? Desde luego, son preguntas que al menos, deben ser planteadas. Después, al ser una tecnología tan vanguardista, desconocemos por donde flaquea. ¿Y si se detectase una vulnerabilidad? ¿Estaríamos dispuestos a asumir este riesgo?

Desde un punto de vista legislativo, se deben tener en cuenta las directivas y leyes. Las tecnologías, pertenecientes a corporaciones, deben cumplir sus responsabilidades legales. Ejemplo de reglamento lo es la RGPD (por nombrar una, no por ello única). Si esta cambia, la manera en la que Blockchain está diseñada para nuestro caso de uso debe ser al menos analizada y ver si realmente no tiene implicaciones; en caso contrario, se debería abordar todo un proyecto de adecuación (como ya se ha ido viendo con el boom de los cookies). La incorporación de Blockchain ya tendrá un ROI bastante alto y la Empresa deberá tener especial interés en mantenerlo en producción, esto es, mucho valor tendrá que aportar BlockChain para asumir este riesgo tan alto.

Por último, discutamos los riesgos de color verde. Es evidente que habría que plantearse la generación de claves y cómo gestionarlos. ¿Quien se responsabilizará de eso?¿Cada cuanto se generarían nuevas claves, si es que se hacen?¿Qué pasaría si la clave pública se fuga?[3] Además, ¿Quienes serían los agentes verificadores?¿Por qué ellos?¿Tendrían más responsabilidades?¿Serían personas o sólo máquinas, de manera automática? A todo esto, habría que añadirle una serie de cuestiones en torno a la capa de persistencia: ¿De qué manera persistimos esta información?¿Bajo qué condiciones validamos? En definitiva, existen muchísimos riesgos que, desde luego, hay que tratar de abordarlos antes de dar pie a la implantación de esta tecnología. Hay que valorar si realmente merece la pena invertir en esto mismo, si realmente aporta valor y utilidad directa. Hay que mantener la prudencia, no vaya a ser que demos un paso en falso.

En el próximo post hablaré de los controles que se pueden aplicar para los

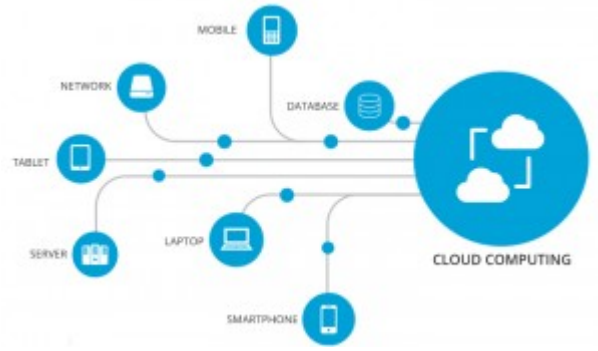
riesgos en esta tecnología. Hemos identificado varias cuestiones que deberán ser abordadas, intentaremos minimizar o al menos mitigar los mismos.

1. Real Academia de España, Buscador de RAE, http://dle.rae.es/?id=WT8tAMI, acceso el 22 de noviembre de 2018.

2. Blockchain and Risk (Mike Small CEng, abril 2016), https://m.isaca.org/chapters8/Northern-England/Events/Documents/blockchain.pdf., acceso el 22 de noviembre de 2018.

3. «Seguridad de contactos inteligentes basados en Blockchain II – Vulnerabilidades y riesgos» (Stefan Beyer, marzo de 2018), https://www.securityartwork.es/2018/03/20/seguridad-de-contratos-inteligentes-basados-en-blockchain-ii-vulnerabilidades-y-riesgos/, acceso el 22 de noviembre de 2018.

Riesgos en el entorno Cloud. Una perspectiva holística de los riesgos



El pasado lunes, se celebró en Bilbao uno de los eventos más importantes relacionados con la ciberseguridad (Basque Cybersecurity Day) y como no era de extrañar, en prácticamente todas las conferencias se citó de una forma u otra los posibles riesgos asociados a las tecnologías emergentes (entre las cuales se incluye, el Cloud Computing) . No obstante, el enfoque que se le dio a los riesgos tecnológicos era radicalmente distinto a la opinión que tenía acerca del tema.

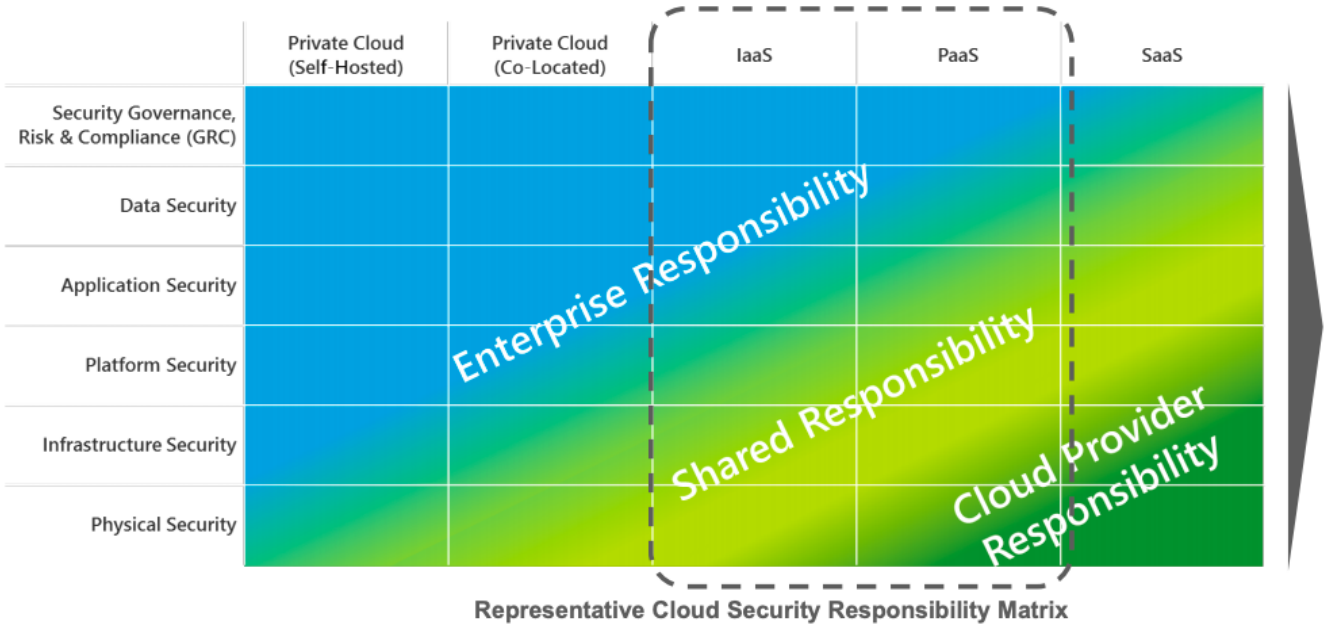
Por lo tanto, el post que tenía pensado escribir la semana pasada ha sido totalmente reescrito, y he decidido explicar el framework propuesto por ISACA [1] para abordar los riesgos de la tecnología del Cloud Computing pero enriquecido con todas las aportaciones de relevancia que escuché en el ciclo de conferencias.

Entre todas las conferencias hubo una que me llamó la atención en particular, la realizada por la actual CEO de Siemens España, Rosa García [2]. En esta conferencia se abordó la gestión de los riesgos desde un punto de vista holístico y destacaba como en el punto en el que nos encontramos hoy en día los riesgos IT se deben entender como una parte más de la estrategia

empresarial. En pocas palabras, cuando se habla de seguridad en estos términos, no solo nos referimos a la parte de la tecnología o la parte “ciber”, sino a todo el entorno que compone la seguridad (la seguridad de los datos y la información, el plan de gobernanza IT, los modelos de fallo y de contingencia, la gestión del cambio, etc …).

Por otra parte, otro de los puntos relevantes (especialmente para entender el mundo de los riesgos del Cloud Computing), es el referido al papel de los proveedores. La robustez de la seguridad de una organización, viene marcado por el eslabón más débil de la cadena y muchas veces este eslabón ni siquiera es parte central de la organización como es el caso de los proveedores (en los cuales se incluyen los proveedores de servicios cloud). En este punto, son destacables los datos de la encuesta elaborada por KPMG [3] donde cita como el 44% (12 puntos más que en el año 2017) de los encuestados no posee ningún tipo de instrumento para el control del framework de seguridad con los proveedores. Además el 34% de los encuestados, tampoco poseen ningún tipo de control de ciberseguridad en los contratos de terceros y finalmente, el 59% ni siquiera tienen el derecho contractual a la realización de una auditoría del proveedor.

En definitiva, la adopción del cloud computing muchas veces va ligada a contratos con terceros, los proveedores de servicios. No obstante, muchas de las empresas no realizan ningún tipo de supervisión o control de estos y ello supone un claro riesgo para la seguridad de sus empresas. Para explicarlo mejor, me valdré de la siguiente infografía elaborada por Deloitte.[4]



Representative Cloud Security Responsibility Matrix

La infografía representa el nivel de responsabilidad que debe adquirir una compañía en función de su grado de dependencia de terceros. Es decir, una empresa cuyos sistemas estén totalmente gestionados a nivel interno, es totalmente responsable del sistema pero una empresa cuyo entorno está totalmente alojado en la nube, debe ceder esa responsabilidad al tercero.se

Pero siempre hay que tener en cuenta un hecho crucial, aunque cedas la responsabilidad de tu sistema a un tercero, la responsabilidad de los datos

que se gestionan en él siempre va a seguir siendo tuya. Pongamos como ejemplo la seguridad de un teléfono móvil: la seguridad del terminal es responsabilidad del fabricante. Sin embargo, el usuario sigue siendo responsable de la forma en la que use este terminal y en el mundo Cloud sigue siendo igual.

Por otra parte y siguiendo con lo planteado inicialmente, me gustaría listar cuales son los riesgos más comunes que deben afrontar las empresas en el mundo del Cloud. El próximo listado de riesgos se extrajo de un informe de ISACA donde se mencionaba una encuesta elaborada por la Cloud Security Alliance [5].

En primer lugar, los CSP (Cloud Service Providers) suelen ofrecer APIs públicas para el acceso a los sistemas en la nube, desde la autenticación y gestión de credenciales hasta la monitorización del uso de recursos. No obstante, estas APIs pueden suponer una puerta de entrada a posibles vulnerabilidades.

En segundo lugar, el documento destaca un problema que mi compañero Pablo ya ha tratado en sus respectivos posts con mucho más detalle, los Insiders Threads. En este caso, el problema se extiende no solo al personal propio de la organización sino al personal perteneciente por ejemplo a los CSP. Este elemento resulta crucial para entender la importancia que tienen los controles al personal implicado de la organización, especialmente a las relaciones con terceros.

Por otro lado, en la mayoría de servicios en la nube los recursos computacionales son compartidos por diferentes usuarios y organizaciones. A pesar de poder contar con elementos de seguridad que permiten aislar el acceso a estos recursos, siempre pueden ser un foco de conflicto.

El cuarto y último aspecto a tratar entre los principales riesgos asociados está relacionado con la pérdida de datos e información. En este punto, hay dos riesgos que hay que tener en cuenta con los datos que se alojan en la nube: la posible pérdida de datos y la aún peor posible filtración de los mismos. Actualmente, las organizaciones y sus estrategias de negocio están completamente orientadas a los datos y por ende, este punto debe ser supervisado y auditado con especial atención.

En definitiva, los servicios alojados en la nube suponen un nuevo reto a las organizaciones que lo incorporan. Además, a pesar de que los riesgos relacionados con la tecnología no son nuevos, el paradigma del cloud computing acrecienta estos riesgos de una forma u otra como ya he mencionado anteriormente.

Por último, me gustaría adelantar el contenido del próximo post donde expondré un caso práctico elaborado por ISACA explicando las medidas y controles que se deben tomar en las organizaciones que decidan adoptar esta tecnología.

Fuente consultadas:

[1] «IT Control Objectives for Cloud Computing – Information Security ….» https://www.isaca.org/chapters2/kampala/newsandannouncements/Documents/IT%20contro%20objectives%20for%20Cloud%20computing.pdf. Se consultó el 10 noviembre del 2018.

[2] García, R. (2018). *Perspectiva del CEO en la gestión del Riesgo Empresarial*. Conferencia realizada en el Basque Cybersecurity Day.

[3] «Clarity on Cyber Security – KPMG.» 25 mayo 2018, https://assets.kpmg.com/content/dam/kpmg/ch/pdf/clarity-on-cyber-security-2018.pdf. Se consultó el 10 noviembre del 2018.

[4] «Cloud Cyber Risk Management – Deloitte.» https://www2.deloitte.com/content/dam/Deloitte/us/Documents/about-deloitte/us-allian-deloitte-cloud-cyber-risk-considerations-amazon-web-services.pdf. Se consultó el 10 nov.. 2018.

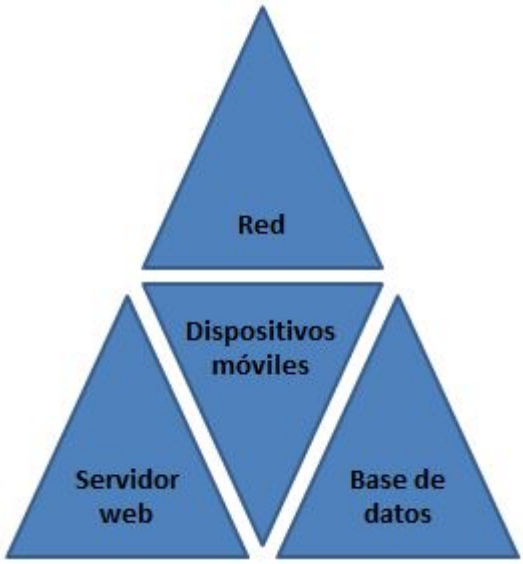
[5] «Top Threats Cloud Computing V1.0 – Cloud Security Alliance.» https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf. Se consultó el 10 noviembre del 2018.

[6] «Risk Landscape of Cloud Computing – isaca.» https://www.isaca.org/Journal/archives/2010/Volume-1/Pages/Risk-Landscape-of-Cloud-Computing1.aspx. Se consultó el 10 noviembre del 2018.

Factores de riesgo en las aplicaciones móviles y algunos controles básicos con los que abordarlos

Con la continua evolución tecnológica, especialmente en el ámbito empresarial, la auditoría del TI y los profesionales de seguridad deben adaptarse al escenario de las amenazas cambiante creado por las aplicaciones móviles adelantándose al riesgo. Para ello deben poner controles apropiados y probar las aplicaciones móviles desde su concepción hasta su lanzamiento. Es por ello que he seguido leyendo sobre la **Gestión del Riesgo Institucional en el Mundo Móvil**, y esta vez he investigado acerca de los **factores de riesgo** en las aplicaciones móviles y algunos **controles básicos** con los que abordarlos. En este Post he utilizado como fuente un artículo de una revista llamada **"ISACA Journal: mobile apps"**.

Los riesgos en las aplicaciones móviles se pueden dividir en cuatro categorías:



Riesgos y controles en la categoría de Dispositivos móviles:

1. **Almacenamiento de datos:**
    - **Riesgo:** Pérdida y divulgación de datos.
    - **Control:** El cifrado de los datos en reposo en el dispositivo móvil se establece en el Estándar de Cifrado Avanzado (Advanced Encryption Standard: AES) de 128, 192 o 256. Mediante este control los datos se almacenan de forma segura para evitar la extracción maliciosa de la aplicación cuando los datos están en reposo.
2. **Transmisión de datos:**
    - **Riesgo:** Pérdida y divulgación de datos.
    - **Control:** El cifrado de datos se aplica para los datos en transmisión a través de la Capa de Puertos Seguros (Secure Sockets Layer: SSL) y fuertes protocolos de seguridad tales como:
        - Acceso Web – HTTPS vs. HTTP
        - Transferencia de archivos – FTPS, SFTP, SCP, WebDAV sobre HTTPS vs. FTP, RCP
        - Protocolos de seguridad – Seguridad en la Capa de Transporte (Transport Layer Security: TLS)

      Mediante este control la transmisión datos de la aplicación móvil está cifrada cuando no se dispone de datos en reposo.

IMPORTANTE: Estos dos primeros riesgos tratan sobre la pérdida y la divulgación de datos, tema que hace referencia a la **DLP** y a la gestión de contenido móvil (**MCM**).

3. **Aplicación de gestión de acceso y seguridad:**
    - **Riesgo:** Acceso no autorizado y fraude.
    - **Control:** La gestión de aplicaciones móviles (**MAM**) se utiliza para gestionar el acceso y el despliegue de la aplicación. Además, se mantienen unas adecuadas listas blancas y listas negras. Mediante este control la aplicación está configurada para limitar el acceso y configurada adecuadamente para uso autorizado limitado.

4. **Llevar dispositivos móviles fuera del perímetro empresarial:**
    - **Riesgo:** Pérdida o robo del dispositivo móvil, haciendo posible el acceso no autorizado a las aplicaciones móviles del dispositivo y al fraude de los datos de éstas.
    - **Control:** (**MAM**) *Leer el control 3.2 de esta categoría.

Riesgos y controles en la categoría de Red:

1. **Conectividad inalámbrica:**
    - **Riesgo:** Pérdida y divulgación de datos (**DLP & MCM**).
    - **Control:** La transmisión de datos utiliza, como mínimo, SSL o TLS. Ambos protocolos criptográficos para la transmisión segura de datos. Mediante este control el cifrado se aplica cuando se activa la conexión Wi-Fi.
2. **Secuestro de sesión (Session hijacking):**
    - **Riesgo:** Pérdida y divulgación de datos y acceso no autorizado (**DLP & MCM**).
    - **Control:** Los protocolos de conexión para el Localizador Uniforme de Recursos (Uniform Resource Locator: URL) a través de TLS son a través de HTTPS en lugar de HTTP para conectarse de forma segura a una URL. Mediante este control se evita el secuestro de una sesión debido a un protocolo de conexión inseguro.

Riesgos y controles en la categoría de Servidor web:

1. **Gestión de acceso:**
    - **Riesgo:** Pérdida y divulgación de datos y acceso no autorizado (**DLP & MCM**).
    - **Control:** Todos los servidores web aplicables se asignan a los propietarios de sistemas técnicos y empresariales. Los roles y responsabilidades definidos son adecuados, especialmente para el personal interno y de terceros. Mediante este control los roles y responsabilidades de la propiedad son establecidos, documentados y comunicados.
2. **Ataque de fuerza bruta:**
    - **Riesgo:** Acceso no autorizado y fraude, disponibilidad de la aplicación.
    - **Control:** Los protocolos de bloqueo están habilitados para cuentas con varios intentos de contraseña incorrectos. Se recomienda la utilización de CAPTCHA (programa que distingue entre seres humanos y ordenadores) para evitar DoS (Denegación de Servicio). Mediante este control la gestión de la estrategia de DoS abarca programas adecuados para bloquear los protocolos no autorizados.

Riesgos y controles en la categoría de Base de datos:

1. **Acceso privilegiado:**

    - **Riesgo:** Acceso no autorizado y fraude.
    - **Control:** El acceso a la BD está limitado a las personas apropiadas, y las revisiones de acceso adecuadas y las cuentas del sistema documentadas se mantienen archivadas. Todas las cuentas y contraseñas predeterminadas se deshabilitan al aplicar controles de contraseña estrictos. Mediante este control el acceso elevado a las BBDD se asegura adecuadamente utilizando las mejores prácticas.
2. **Inyección SQL (SQL injection):**
    - **Riesgo:** Acceso no autorizado y fraude.
    - **Control:** Se da lugar a la técnica de validación de entrada; existen reglas específicamente definidas para el tipo y la sintaxis contra las reglas clave de negocio. Mediante este control el acceso a la BD del Back-end está protegido adecuadamente de vulnerabilidades utilizando técnicas de validación de entrada apropiadas.
3. **Validación de la entrada de la aplicación (cliente):**
    - **Riesgo:** Acceso no autorizado y fraude.
    - **Control:** La limpieza de los datos de usuario de la aplicación procedentes de la aplicación móvil se protege adecuadamente mediante comprobaciones de lógica incorporada dentro de la aplicación. La correcta implementación de las comprobaciones lógicas está habilitada en el lado del servidor. Mediante este control los datos procedentes de aplicaciones móviles son examinados antes de confiar en ellos para extraerlos o enviarlos a la capa de BD.
4. **Servicios de BD de aplicaciones.**
    - **Riesgo:** Acceso no autorizado y fraude.
    - **Control:** El servidor de BD se prueba adecuadamente y se protege contra ataques maliciosos. Los formularios de inicio de sesión requieren HTTPS. Las conexiones SSL son obligatorias.

¿Y el último post?:

No se han tratado amenazas como el **Phishing**. Puesto que considero que es fundamental tener ciernas nociones de esta amenaza, mi último post, tratará sobre ésta.

Referencia:

Revista de ISACA:

J. Khan, Mohammed «Mobile App Security Audit Framework», *ISACA Journal: mobile apps,* nº 4 (2016): 14-17.

BYOD: ¿Es posible controlar algo que no es tuyo?

En el anterior post redacté algunos de los riesgos que nos podemos encontrar al utilizar las tendencias BYOD y COPE que estoy tratando en esta serie de entradas. En aquel momento finalicé diciendo que la próxima vez iba a hablar única y exclusivamente de los controles que se les podían aplicar a esos problemas y, como no puede ser de otra manera, así va a ser. Os preguntaréis, ¿Es realmente necesario aplicar controles?, pues sí. Una sociedad que se toma a la ligera lo que ocurra sin tener en cuenta si existen problemas, tarde o temprano terminará en desastre. Y esto se puede aplicar a todos los ámbitos de la vida, eso sí, sin llegar a tener que vivir, como decía uno de mis compañeros en uno de sus posts, vigilados por el "gran hermano".

Lo primero de todo será identificar la persona encargada de hacer estos controles. En este punto es donde entra en juego la figura del Auditor, que en este caso tendrá el rol de hacer que se cumplan las políticas adoptadas para la empresa, identificar los controles internos y deficiencias que puedan afectar a la organización y detectar cualquier problema de seguridad de la información que esté relacionado con la poca seguridad de los dispositivos móviles. Recientemente, desde ISACA ha sido lanzado un programa para la auditoría de BYOD [1]. Este, se centra en los dispositivos BYOD que se conectan a la red de la organización o contienen su información, incluyendo todas las variedades de Smartphone, Tablet, Ordenadores portátiles y todos sus sistemas operativos. Además, los propios auditores tendrán que adaptar esta guía para sus organizaciones, ya que, se plantea como un punto de partida para la realización de su trabajo.

Una de las prácticas más recomendables para una empresa o incluso nosotros mismos, es la de crear una política de uso de los dispositivos. Para ello, podemos tener en cuenta el estándar ISO 27001 [2], el cual se refiere a la seguridad de la información. Sin embargo, aunque parezca increíble en la sociedad en la vivimos, en ningún momento se nombra la palabra BYOD en el estándar, pero sí que existen numerosos controles [3] de esta que son imprescindibles en cualquier compañía moderna y que los podríamos adoptar para este caso.

El primero de ellos, **la política de dispositivos móviles** (6.2.1), que requiere el desarrollo de una política de uso de dispositivos móviles para reducir los riesgos. El segundo, el correspondiente al **teletrabajo** (6.2.2), ya que los dispositivos son usados no solo en las oficinas. Este, está formado por controles para el acceso, procesamiento y almacenamiento de información. El tercero, **las políticas y procedimientos de intercambio de información** (13.2.1), se centra en la protección de la información que se transfiere mediante cualquier modo de comunicación, incluyendo en este caso los dispositivos móviles. Finalmente, el último control que se podría incorporar, el de **mensajería electrónica** (13.2.3) que recogerá la forma en la que los mensajes electrónicos serán protegidos. Pero no nos podemos limitar solo a estos, otros como **el uso aceptable de los activos** (8.2.3) y **el control**

de acceso a redes y servicios asociados (9.1.2) serían igual de relevantes para una compañía que utilice el *BYOD* en su día a día.

Además de los controles relacionados con los estándares ISO, también pueden ser planteados otros muchos en relación a los riesgos que pueden surgir en las tendencias BYOD y COPE. Teniendo en cuenta los mencionados en la anterior entrada, voy a comentar algunos controles que se pueden aplicar.

Comenzando por la seguridad [4], para la pérdida de información sensible habría que implementar políticas y procedimientos que comunicasen los límites para el uso de los dispositivos y que ocurrirá si eso es ignorado. Para prevenir las vulnerabilidades, es recomendable el uso de una VPN y así verificar que la información que se transmite se encuentra encriptada y es la correcta, por parte del administrador, la existencia de perfiles únicos de seguridad permitiría adaptar la infraestructura a cada usuario. Así mismo, para evitar que se mezcle la información personal con la de negocio, se puede invertir en software EMM o *Enterprise Mobility Management* que monitoriza y detecta los riesgos antes de que estos ocurran. Otro de los riesgos comentados se refería a la pérdida de los dispositivos, para esto, una política de seguridad aplicada mediante una solución MDM o *Mobile Device Management* sería la ideal al permitir al administrador bloquearlo remotamente. Finalmente, para poder combatir las infraestructuras no preparadas para BYOD, se debería hacer una auditoría de todo el entorno TI de la empresa para revisar si puede ser usada con dispositivos móviles y documentar los usos de la red permitidos para evitar el exceso en su uso (descargas, etc…).

Además de todo esto, se debe controlar que los propios dispositivos tienen la seguridad adecuada como, por ejemplo, no permitir dispositivos con ‘jailbreak’ [5], y asegurarse de que los empleados conocen la política de empresa para este uso de los dispositivos, así como, que están concienciados de los riesgos que puede haber en ella. El auditor debería asegurarse de que esto se está realizando por medio de la firma de un contrato confirmando que conocen sus libertades y limitaciones. Otro de los problemas es la posible pérdida de las contraseñas de la empresa [6], por lo que debe existir una política de guardado de las mismas y asegurarse que se encuentran encriptadas.

Todos estaremos de acuerdo en que muchas veces a pesar de tener estos controles no se les hace demasiado caso. En numerosas ocasiones, son hojas y hojas incomprensibles que pasan desapercibidas. Por ello, nuestro objetivo no tiene que ser el de rellenar documentos, esos carecen de importancia y cuanto más cortos y simples sean mejor será (Adoptando el ya conocido principio KISS “*keep it simple stupid*”). Lo importante siempre deben ser las personas, por lo que lo más relevante debe ser cambiar su comportamiento y hacer que trabajen de una forma segura sin cambiar ninguna de las libertades de las que disponían hasta ahora.

[1] BYOD Audit/Assurance Program, ISACA, http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/byo

d-audit-assurance-program.aspx, Visitado el 21 de noviembre de 2016

[2] How to write an easy-to-use BYOD policy compliant with ISO 27001, Advisera, http://advisera.com/27001academy/blog/2015/09/07/how-to-write-an-easy-to-use-byod-policy-compliant-with-iso-27001/ , Visitado el 21 de noviembre de 2016

[3] Controles ISO 27002-2013, iso27000, http://www.iso27000.es/download/ControlesISO27002-2013.pdf, Visitado el 21 de noviembre de 2016

[4] 5 BYOD security implications and how to overcome them, Edel Creely, Trilogy Technologies, http://trilogytechnologies.com/5-byod-security-implications/, Visitado el 21 de noviembre de 2016

[5] BYOD: How your business can address the 5 biggest vulnerabilities, Scott Anderson, Ccb Technology, http://ccbtechnology.com/byod-5-biggest-security-risks/, Visitado el 22 de noviembre de 2016

[6] 10 worst-case BYOD scenarios (and how to prevent them), Jack Wallen, Techrepublic, http://www.techrepublic.com/blog/10-things/10-worst-case-byod-scenarios-and-how-to-prevent-them/, Visitado el 22 de noviembre de 2016

¿Qué impacto produce el Mundo Móvil en la Auditoría Interna? ¿Qué hacemos? (BYOD)

He estado leyendo sobre la **Gestión del Riesgo Institucional en el Mundo Móvil**, ya que el uso de aplicaciones móviles es muy frecuente dentro de una empresa y en la actualidad existe una variedad inmensa de amenazas contra estos dispositivos. Aprovecho ahora para remarcar que el Mundo Móvil hace referencia a los dispositivos móviles, por lo que no está única y exclusivamente compuesto por teléfonos móviles o Smartphones, también están incluidas las Tablets y las PDAs, al igual que otros muchos dispositivos portátiles que puedan ser utilizados para desempeñar una función dentro de una empresa. Una vez asimilado esto, el siguiente paso es preguntarse:

¿Qué impacto produce el Mundo Móvil en la Auditoría Interna?:

Es un hecho que las aplicaciones móviles evolucionan rápida y

constantemente, por lo que la auditoría interna debe asegurarse de que está al día con la tecnología móvil que está siendo utilizada por sus organizaciones y que estas están considerando todas las posibles exposiciones de riesgo en todo momento. Para entender mejor el impacto, he consultado el **Top 10 de Principales Prioridades de la Auditoría Interna en Organizaciones de Servicios Financieros** y he descubierto que las aplicaciones móviles se encuentran en este top, concretamente en el séptimo puesto. En la explicación del top, justifican que las aplicaciones móviles tienen lugar en el top por los riesgos que suponen las aplicaciones móviles para las empresas, en especial en relación a la autentificación del usuario.

Entonces, una vez asumido que las aplicaciones móviles pueden suponer un problema en algunas organizaciones, queda preguntarse cuáles podrían ser unas buenas medidas a tomar dentro de las organizaciones para evitar los problemas. En algún post siguiente a este, trabajaré los riesgos más importantes, así como los controles a tomar para cada uno de ellos, pero de momento, en este post solo pondré, según la explicación del top, los puntos de acción que los auditores jefes ejecutivos y las funciones de auditoría interna necesitan considerar:

1. Garantizar que las **aplicaciones móviles** y la banca están completamente cubiertas en el universo de auditoría (todos los productos / servicios, plataformas, proveedores, etc.).
2. Asegurarse de que los terceros son tenidos en cuenta en las políticas y procedimientos de gestión de proveedores.
3. Considerar la posibilidad de riesgo de fraude en relación con las **transacciones móviles** dentro de los procesos de cara al cliente (orígenes y servicio).
4. Entender el enfoque de la seguridad por tener una **presencia móvil**.
5. Considerar el proceso de extremo a extremo de cara al servicio. Los **móviles** son la típica puerta de entrada a otros servicios y plataformas.
6. Entender los planes y controles de gestión del cambio de **aplicaciones móviles**.
7. Considerar todas las **plataformas móviles** compatibles aplicables (iOS, Android, Windows, etc.) en los planes de auditoría.
8. Si procede, tener en cuenta los controles necesarios para apoyar un modelo de entrega de software ágil.
9. Considerar la posibilidad de la gestión del servicio multiplataforma, incluyendo los componentes de otros fabricantes.
10. Tener en cuenta las responsabilidades de las empresas, las políticas y procedimientos en relación al aprovisionamiento de cuentas en los **dispositivos móviles**.

Y entonces, viendo los riesgos e impacto: ¿Todo está perdido? ¿Qué hacemos?

Llegados a este punto la solución es tomar una decisión estratégica. ¿Pero cuál?

¿Qué hacemos? (BYOD):

Según **un documento de ISACA** existen varias posibles decisiones estratégicas, cada una con sus respectivas ventajas y desventajas. A continuación, enumero algunas de las decisiones estratégicas que ISACA propone:

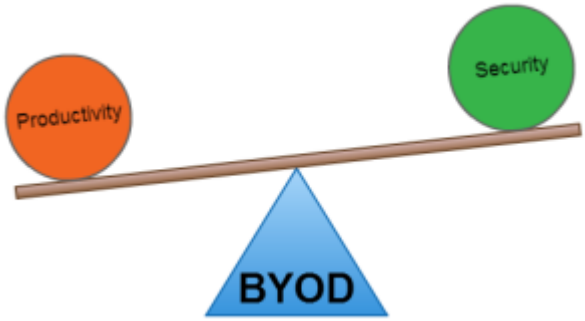
- Solución de plataformas estandarizadas.
- BYOD "Puro".
- Estrategia combinada.

Aquí algo llamó mi atención. ¿BYOD? ¿Seguro? Para quienes no sepan muy bien que es esto del BYOD: BYOD significa Bring Your Own Device y es una estrategia que permite a los empleados, proveedores y otros usuarios el utilizar dispositivos seleccionados y comprados por ellos para ejecutar aplicaciones de la empresa (Típicamente Smartphones y Tablets, pero también se pueden usar en PCs).

BYOD, provocó la tendencia BYOx, o Bring Your Own "Everything":

Entonces, ¿qué implica ofrecer a todos los empleados la posibilidad de utilizar su propio material para trabajar? A priori, una gran comodidad para el empleado, lo que le mantiene motivado en su trabajo, con lo que aumenta considerablemente la productividad de la organización. ¿Pero a qué precio? ¿Dónde reside la seguridad en este caso? En el empleado, que no

necesariamente va a controlar el uso que va a hacer de sus dispositivos. Esto es una fuente de incidencias de seguridad.



Y yo me pregunto, ¿dónde está el punto a favor de introducir BYOD en una empresa? Lo que en realidad se propone con el BYOD "Puro" es el cambio de migrar los datos a otro sitio y que no se almacenen en el dispositivo desde el que se accede a ellos. El objetivo es crear un sistema de acceso remoto a los recursos que los empleados necesitan para realizar su trabajo. De esta forma, se evita que un problema de seguridad en el equipo local se pueda transmitir a la red de la empresa. Aun así es necesario que las comunicaciones entre el equipo BYOD y los recursos se realicen de forma segura, sobre todo cuando el empleado no se encuentre dentro de las instalaciones de la empresa.

Por último y para concluir este post, el BYOD se vende como un ahorro y aunque ISACA propone el BYOD "Puro" como una decisión estratégica de cara a minimizar el riesgo, yo considero que el cambio de no tener BYOD a tenerlo se debe hacer si el objetivo es aumentar la productividad de la empresa, no la seguridad.

Referencias:

KnowledgeLeader:

Ed Page y Jason Goldberg, «Coping With the Pace of Change in Mobile

Applications», *Top Priorities for Internal Audit in Financial Services Organizations,* nº 1 (2016): 31-34.

ISACA:

«La información se mueve, ¿tu seguridad también?», ISACA, acceso el 14 de octubre de 2016, http://www.isaca.org/chapters7/Monterrey/Events/Documents/20140409%20La%20Informacion%20se%20Mueve.pdf.

Otros:

«El BYOD la pesadilla del responsable de seguridad», EOI, acceso el 14 de octubre de 2016, http://www.eoi.es/blogs/ciberseguridad/2016/04/19/el-byod-la-pesadilla-del-responsable-de-seguridad/.

«Cómo implementar una política segura de BYOD en la empresa», BBVA con tu empresa, acceso el 14 de octubre de 2016, http://www.bbvacontuempresa.es/como-implantar-una-politica-segura-de-byod-en-la-empresa.