Gestion de riesgos y Auditoria del Outsourcing de TI

En el último post se reflejaban los posibles riesgos y los diferentes tipos y clases de estos que podrían aparecer al realizar servicios de Outsourcing. Es fundamental el hecho de que una empresa tenga la habilidad para reducir esos riesgos de tal manera que sean insignificantes para la empresa. Para ello, en un proceso de Outsourcing, se debería de tener en cuenta las siguientes consideraciones [1]:

1. Revisar y evaluar los procesos de la compañía para monitorear la calidad de las actividades del Outsourcing. Habrá que determinar cómo se van a monitorear los cumplimientos de los SLA y otros requisitos fundamentales del contrato. Es primordial definir en el contrato las expectativas y los objetivos a cumplir, ya que serían afectadas tanto la disponibilidad, eficiencia y eficacia de las operaciones contratadas como la seguridad de los sistemas y de los datos.

Para evitar todo esto, será necesario revisar el contrato, y establecer métricas, cuadros de mando, etc. para comparar los requisitos estipulados con los resultados en tiempo real. Todo esto se hablará dentro de la administración interna para determinar los procesos que se irán a monitorear.

En caso de no plasmar en el contrato los requisitos, se tendrá que acordar como se supervisara la calidad de los servicios y de que manera se va ha responsabilizar el proveedor en caso de insatisfacción o errores. Por eso, hay que asegurarse de plasmar los siguientes temas en el contrato:

- Disponibilidad y tiempo de actividad esperado.
- Rendimiento esperado del servicio.
- Tiempo de respuesta del proveedor.
- Tiempo de resolución de problemas.
- Requisitos tanto de cumplimientos de los servicios como de seguridad.
- Métricas e indicadores de rendimiento.

2. Asegura de que haya procesos adecuados de recuperación de desastres para garantizar la continuidad del negocio en caso de un desastre en su proveedor.

La misma empresa deberá tener también procedimientos documentados sobre la forma en que se recuperarán sus datos en caso de desastre, donde se incluirán procesos de notificación y escalamiento, cualquier transferencia necesaria entre la empresa y el proveedor durante la recuperación, y posibles soluciones. También deberá especificarse un plan de contingencia. Por ello, se solicitará la información al proveedor sobre donde ubica sus datos, y si tiene cualquier replica de la arquitectura.

3. Revisar y evaluar los planes de la compañía en caso de una terminación esperada o inesperada de la relación de subcontratación. Para que esto no ocurra, la empresa debería exigir al proveedor que le entregue una copia de los datos periódicamente. Los sistemas desarrollados seran flexibles y fáciles de implementar en diferentes entornos.
4. Revisar los procesos del proveedor para garantizar la calidad del personal y minimizar el impacto de la rotación.

En caso de que los empleados de la empresa proveedora no estén calificados para desempeñar su trabajo de forma correcta o la proveedora tiene un índice alto de rotación, la calidad de los servicios desarrollados se ve afectada. Por ello, hay que revisar el contrato para asegurarse de que las descripciones tanto de los puestos de trabajo como las calificaciones necesarias para cada uno de ellos estén bien definidas y documentadas. En caso de que el proveedor realice cambios frecuentes en los puestos de trabajo, se deberá especificar y garantizar la continuidad de los servicios.

Relacionado con el tema de la auditoria de Outsourcing, cabe destacar que ISACA publico un programa de auditoria para optimizar las relaciones, selección de proveedores, la incorporación y los controles en los servicios de Outsourcing, el cual incluye [2]:

- Procesos de gobernabilidad y evaluación de riesgos.
- Análisis del costo-beneficio.
- Controles internos y requisitos para el proceso de selección de los proveedores.
- Los pasos apropiados para gestionar la transición de los proveedores internos de servicios a terceros.
- Monitoreo clave y los controles cuantitativos de la prestación de servicios del proveedor subcontratado.

La parte del proceso de selección del proveedor incluye pasos detallados como:

- Garantizar que el proveedor cumple con los requisitos reglamentarios de los clientes
- Que el proveedor es un líder de la industria en el espacio de Outsourcing
- El proveedor ha establecido un plan de continuidad comercial
- Los códigos de la conducta entre el cliente y el proveedor están alineada
- Que los términos del contrato son apropiados.

A continuación, reflejare un modelo de checklist elaborado para los procesos de Outsourcing de IT:

Checklist para Auditar operaciones y servicios de Outsourcing

1. Revisar los contratos aplicables para asegurar que identifiquen adecuadamente todos los productos entregables, requisitos y responsabilidades pertinentes al compromiso de su empresa.

2. Revisar y evaluar el proceso utilizado para seleccionar el proveedor de outsourcing.

3. Determine cómo sus datos se segregan de los datos de otros clientes.

4. Revisar y evaluar el uso de la encriptación para proteger los datos almacenados de la compañía

5. Determinar cómo los empleados y los proveedores acceden a sus sistemas y cómo se controlan los datos.

6. Revisar y evaluar los procesos para controlar el acceso lógico de los no empleados a su red y sistemas internos.

7. Asegúrese de que los datos almacenados en las ubicaciones del proveedor estén protegidos de acuerdo con sus políticas internas.

8. Revisar y evaluar los controles para prevenir, detectar y reaccionar ante los ataques.

9. Determinar cómo se realiza la gestión de la identidad para los hosts basados en Cloud Computing.

10. Determinar cómo el cumplimiento de las leyes de privacidad aplicables y otras regulaciones es asegurado.

11. Revisar y evaluar los procesos para asegurar que la empresa cumple con licencias de software aplicables para cualquier software.

12. Garantizar que las prácticas de retención y destrucción para los datos almacenados fuera del sitio cumplen con la política interna.

13. Revisar y evaluar la seguridad física del proveedor.

14. Revisar y evaluar los procesos de su empresa para monitorear la calidad de operaciones externalizadas. Determinar cómo se monitorea el cumplimiento de los SLAs.

15. Asegurar que existan procesos adecuados de recuperación ante desastres.

16. Determinar si los procesos de gobernanza apropiados están en marcha

17. Revisar y evaluar los planes de su empresa en caso de espera o inesperada terminación de la relación de outsourcing.

18. Si los servicios de TI se han obtenido mediante Outsourcing, revise los procesos del proveedor de servicios para garantizar la calidad del personal y minimizar el impacto del volumen de negocios.

19. Revisar y evaluar el derecho y la capacidad de su empresa de obtener información de la empresa proveedora.

20. Revisar los requisitos para la notificación de violación de seguridad. Garantizar que los requisitos están claramente definidos respecto a Cuándo y cómo el proveedor debe notificar a su empresa en caso de una brecha de seguridad y que su empresa tenga una respuesta claramente definida procedimientos cuando reciban dicha notificación.

Como conclusión, es imprescindible realizar un buen proceso de auditoría para evitar posibles problemas para la empresa, tales como gastos innecesarios, entorpecer o romper la confianza en la relación empresa-cliente, etc.

Importantísimo un plan de gestión de riesgos antes de cualquier proceso de vinculación con el proveedor y establecer métricas para medir el rendimiento de los servicios y actividades proporcionadas por la parte proveedora de forma periódica, y dejar plasmado en el contrato todos los requisitos y objetivos al más mínimo detalle

REFERENCIAS:

[1] Chris Davis, Mike Sheller y Kevin Wheeler (IT Auditing Using Controls To Protect Information Assets 2nd edition, 2011), edicion PDF, Capitulo 14

[2] https://oceano.biblioteca.deusto.es/primo-explore/fulldisplay?docid=TN_proquest1905430789&context=PC&vid=deusto&lang=es_ES&search_scope=default_scope&adaptor=primo_central_multiple_fe&tab=default_tab&query=any,contains,OUTSOURCING%20AUDIT&sortby=rank&offset=0

Controles en la propiedad intelectual

En el post anterior hable sobre los riesgos relacionados con la propiedad intelectual, concretamente sobre las fuentes de las que pueden surgir estos riesgos. El objetivo de este post es comentar los controles que un auditor tendría que implementar para tratar los diferentes tipos de riesgos.

Como mencionamos en el post anterior los riesgos pueden proceder de varias fuentes diferentes que suelen ser internas o externas a la organización. En función de esto aplicaremos unos controles u otros.

Entre los riesgos externos encontramos como más importantes (mayor probabilidad de que ocurran y mayor impacto para la empresa) los relacionados con temas de robo de información como puede ocurrir a través de ataques cibernéticos. Para tratar estos riesgos se recomienda usar los controles del estándar ISO 27002 [1] que se encarga de temas relacionados con la protección de datos. Algunos que podemos implementar son:

- **10.1 Controles criptográficos:** asegurar el uso apropiado y efectivo para proteger la confidencialidad, autenticación y integridad de la información.
- **11.2.4 Mantenimiento de los equipos:** asegurarse de que los equipos tienen todas las ultimas actualizaciones para evitar brechas de seguridad.
- **12.2.1 Controles contra el código malicioso:** implementar controles para la detección, prevención y recuperación ante afectaciones de malware.

- **13.1 Gestión de la seguridad en las redes:** implantar estándares, directrices y procedimientos de seguridad técnicos para redes y herramientas de seguridad de red como IDS/IPS (detección y prevención de intrusiones).
- **13.2.1 Políticas y procedimientos de intercambio de información**: Deberían existir políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de comunicación.
- **15.1 Seguridad de la información en las relaciones con suministradores:** se debe controlar el acceso de terceros a los sistemas de información de la organización.

Otro conjunto de riesgos bastante importante son los que pueden provenir de dentro de la organización. Los riesgos más comunes aquí se producen simplemente por descuido y debido a la poca educación de los propios empleados en materia de seguridad. En este caso podemos implementar los siguientes controles del ISO 27002 [1]:

- **7.1.1 Investigación de antecedentes:** asegurarse al contratar que la persona contratada no es un posible espía de otra organización como el caso Ferrari comentado en el post anterior. [2]
- 7.2.2 Concienciación, **educación** y **capacitación** en seguridad de la información: es importante presentar a los trabajadores una guía de buenas prácticas que deben lleven a cabo para asegurarnos la protección de la información.
- **9.1 Requisitos de negocio para el control de accesos:** establecer políticas de acceso a la información para evitar que nadie que no deba acceda a información confidencial.
- **11.1.2 Controles físicos de entrada:** evitar que personas no autorizadas accedan a lugares de acceso restringido.
- **11.2.9 Política de puesta de trabajo despejado y bloqueo de pantalla:** evita que personas sin acceso autorizado puedan visualizar en el ordenador información confidencial cuando el responsable del ordenador no está en su puesto de trabajo.
- **12.3 Copias de seguridad:** asegurar de tener siempre disponibles copias de la información en caso de que alguien borre de forma voluntaria o por accidente información.
- **12.6.2 Restricciones en la instalación del software:** evitar que los usuarios puedan instalar software malintencionado con el que puedan robar información.
- **13.2.4 Acuerdos de confidencialidad y secreto:** firmar acuerdos de confidencialidad con los empleados para evitar que puedan divulgar en el futuro información confidencial. En caso de hacerlo se podría denunciar.

Por último siempre es importante actuar de acuerdo a lo que la ley establece. En caso de empresas internacionales será necesario cumplir con la ley vigente en cada uno de los países en los que se opera, que en temas de propiedad intelectual suele variar de unos a otros. En caso de que el país está englobado dentro de una organización superior como puede ser la UE también será necesario tener en cuenta su legislación. Para este caso se pueden

implementar los siguientes controles del punto 18.1 que se encarga de cumplir con los requisitos legales:

- **18.1.1 Identificación de la legislación aplicable: se deberá estar al corriente de todos los cambios que se pudieran producir en la legislación.**
- **18.1.2 Derechos de propiedad intelectual (DPI):** se deberían implementar procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar productos software originales.
- **18.1.5 Regulación de los controles criptográficos.**

Referencias:

[1]http://www.iso27000.es/

[2]https://lat.motorsport.com/f1/news/analisis-nace-un-nuevo-caso-de-spygate-en-la-f1/1594861/

Gestión de riesgos en propiedad intelectual

En este tercer post hablaré sobre los diferentes riesgos relacionados con la propiedad intelectual que pueden surgir dentro de un entorno empresarial. Un riesgo es la probabilidad de que un peligro ocurra y tengan consecuencias negativas para la organización. Para llevar a cabo una buena gestión de riesgos como auditores, es importante conocer las diferentes fuentes de las que pueden surgir para posteriormente listar una serie de riesgos potenciales y poder actuar en consecuencia para intentar evitarlos. Algunas de las fuentes más importantes a tener en cuenta a la hora de buscar riesgos son [1]:

- **Dentro de la propia organización:** esta es una de las principales fuentes de riesgo. En algunos casos es debido a la falta de educación de los empleados de la empresa en cuanto a propiedad intelectual se refiere. En otros casos es debido a actos deliberados de los propios empleados. Este último caso es el más común y suele darse al abandonar un empleado la empresa. Esto es debido a que la propiedad intelectual está en muchas ocasiones en el propio conocimiento de la gente y cuando se va hay que tener en cuenta que se puede transmitir a gente externa a la organización. Si esto ocurre, se pueden tomar acciones legales como hizo Mercedes Benz hace unos años al enterarse de que un ex-ingeniero suyo estaba transmitiendo información confidencial a un equipo de la

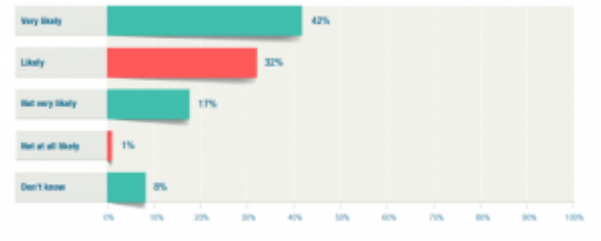
competencia que en este caso era Ferrari. [2]

- **Entidades cercanas a la organización:** en este apartado están incluidas todas aquellas entidades que tienen alguna relación con la organización pero que no pertenecen a la misma. Algunos ejemplos pueden ser distribuidores, proveedor, clientes, partners o personas subcontratadas. Todas estas entidades presentan un riesgo siempre y cuando tengan a acceso a aquello que esté protegido.
- **Competidores:** cualquier empresa que se encarga de manufacturar, crear y distribuir productos o servicios similares a nuestra empresa presenta un riesgo potencial. Un claro ejemplo de este tipo de riesgos está presente en la industria de los teléfonos móviles, donde hasta la simple forma de interactuar con la pantalla está protegido por patente en algunos países. Esto suele provocar múltiples demandas por infringir la propiedad intelectual entre empresas pioneras como sucedió hace unos años entre Apple y Samsung. [3]
- **“3rd parties” independientes:** en este apartado se encuentran las conocidas entidades no practicantes (NPE) [4] que se dedican a amasar una gran cantidad de patentes pero no a llevar a cabo su desarrollo. El objetivo de la mayoría de estas entidades es buscar posibles infringimientos contra la propiedad intelectual y poner demandas para así poder obtener beneficios económicos. A este tipo de patentes se las conoce como “patentes troll”. [5]
- **Entidades de gobierno:** es importante tener en cuenta que la ley de propiedad intelectual no es la misma en todos los países y que esta puede cambiar. Por lo tanto hay que estar al corriente de estos cambios para evitar posibles infracciones.
- **Entidades ilegales:** en este apartado se encuentra principalmente la piratería y los hackers informáticos. Un hacker puede ser una persona individual, una organización criminal o incluso entidades patrocinadas por un gobiernos con el objetivo de obtener información de rivales u otros países. Es un aspecto a tener bastante en cuenta ya que en España el 32 % de las empresas admite que ha sufrido algún ataque por hackers. [6] Como piratería nos referimos a toda copia falsa de un producto que tenga derechos de propiedad intelectual. Se estima que alrededor del 8% de productos que se obtienen en el mundo son copias falsas lo que supone una pérdida estimada de unos 512 millones de dólares en pérdidas para las entidades propietarias del producto original.
- **Proveedores de servicios y soluciones IP:** en muchas ocasiones las empresas deciden subcontratar empresas especializadas para llevar a cabo la gestión de su propiedad intelectual. Hay que tener en cuenta que siempre que la propiedad intelectual pasa a entidades externas supone un potencial riesgo para la empresa.

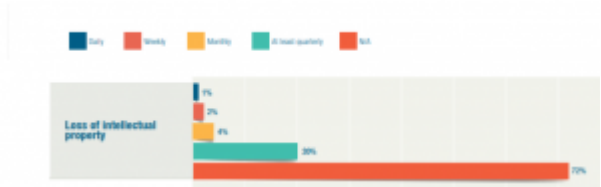
Una vez que sabemos donde buscar los riesgos, debemos hacer un listado de todos los riesgos posibles y analizarlos en función de varias variables como pueden ser:

- Probabilidad: probabilidad de que surja el riesgo.
- Impacto: impacto económico que tendría en la empresa en caso de que ocurra.

En función de estas variables conoceremos aquellos riesgos que debemos tener más en cuenta. Por lo general los principales riesgos suelen provenir de imitadores, piratería y sobre todo ciberataques. [7] Como muestra la siguiente encuesta realizada por ISACA, la mayoría de las empresas considera como muy probable el riesgo de un ataque cibernético. [8]



La misma encuesta también nos muestra la frecuencia con la que las empresas pierden activos protegidos por propiedad intelectual.



Por último, aunque podemos pensar que las empresas están protegidas por la ley, la realidad es que en muchos países no se lucha activamente contra estos infringimientos lo que supone un alto coste económico para la empresa.[7]

En el siguiente post os comentaré los controles que se pueden llevar a cabo para tratar los diferentes riesgos comentados previamente.

Referencias:

[1]https://www.ipeg.com/ip-risk-management-how-to-deal-with-it-part-1/

[2]https://lat.motorsport.com/f1/news/analisis-nace-un-nuevo-caso-de-spygate-en-la-f1/1594861/

[3]https://www.forbes.com/sites/connieguglielmo/2012/08/23/apple-samsung-patent-war-puts-future-of-innovation-at-risk/#6f5b250d6c76

[4]https://whatis.techtarget.com/definition/non-practicing-entity-NPE

[5]https://whatis.techtarget.com/definition/patent-troll

[6]https://www.abc.es/tecnologia/redes/abci-32-por-ciento-empresas-espanolas-admiten-haber-recibido-menos-ciberataque-ultimo-201705121805_noticia.html

[7]https://info.knowledgeleader.com/bid/164620/What-is-Intellectual-Property-Risk

[8]https://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf

Social media y networking desde una perspectiva corporativa – Controlando y auditando

¡Hola a tod@s!

Son varios ya los posts respecto al tema que nos compete, hemos arrojado algo de luz sobre diferentes aspectos: riesgos, relevancia… Hoy, vamos a ponerle la guinda al pastel. Vamos a abordar cómo se deben auditar y controlar la social media y las formas de hacer networking en nuestras organizaciones. Auditar y poner controles es lo que nos va a permitir evitar los riesgos, o, por lo menos minimizarlos. En este sentido, vamos a tratar de explicar los controles a implantar y el proceso para auditar correctamente y proteger nuestra empresa. Pongámonos a ello.

Lo mencionamos en el anterior post y en este lo volvemos a repetir, una buena gobernanza es clave en esto. Establecer unas políticas de uso adecuadas en cuanto a medios sociales y networking se refiere puede resultar muy beneficioso para la empresa y evitar riesgos. En cuanto a los medios sociales, hay que dirigir la política tanto a las cuentas oficiales como a las cuentas personales de los empleados. Al fin y al cabo debemos dar unas líneas generales en cuanto al uso de los medios:

- Normas y reglamentos a cumplir
- Roles y responsabilidades de cada uno
- Riesgos jurídicos y de seguridad que pueden existir

Un claro ejemplo de una política de este tipo es la de Nvidia, una empresa dedicada al desarrollo de hardware (UPGs principalmente) que hace pública su política.

Sobre cómo auditar, vamos a explicar las bases sin entrar en detalles. Existen muchos y diversos matices a la hora de cómo afrontar una auditoría sobre los medios sociales y el networking. Sin embargo, debemos tener en cuenta que una auditoría de medios sociales debe responder a varias preguntas clave:

- ¿Existe una estrategia para medios sociales apoyada por las políticas, procesos y estructuras adecuadas?
- ¿Está la estrategia social alineada con la estrategia corporativa?
- ¿Cuáles son los riesgos asociados a los medios sociales?¿Son mitigados?¿Logran los beneficios ser mayores que los costes?
- ¿Existen controles de identidad y acceso a la hora de manejar los medios sociales?
- …

No me quiero extender demasiado ya que en las referencias podéis encontrar con más exactitud todas las preguntas. Ahora bien, si que voy a exponer los aspectos a tener en cuenta por parte de un reporte de una auditoría sobre los medios sociales:

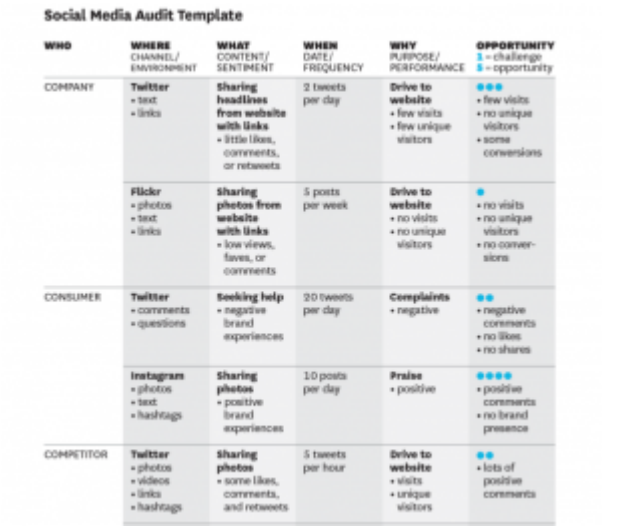
- Identificar los riesgos de los medios sociales que tienen un gran impacto en los objetivos clave de la organización
- Relacionar los riesgos con objetivos comerciales específicos
- Evitar observaciones genéricas sin valor comercial alguno
- Identificar posibles problemas de incumplimiento en el negocio
- Proporcionar una perspectiva de cara a futuro
- Hacer diagramas cuando sea posible

Teniendo esto en cuenta, debemos dirigir nuestra auditoría para que cumpla y conteste estos aspectos. Obviamente, todo esto debe siempre ir en concordancia con el proceso de pre-auditoría: entender y analizar el negocio, entender y analizar el entorno de los medios sociales, realizar una evaluación de los riesgos y planificar la auditoría.

Hay que recalcar que es aconsejable realizar auditorías sobre las redes sociales en concreto con cierta asiduidad debido a que son entornos muy cambiantes y exigen de una continua revisión. Auditar las redes sociales no implica hacer una audición completa, sino simplemente asegurar que cada una de las redes que tenemos funciona y responde acorde a lo que buscamos. Por ejemplo, podemos auditar nuestras redes sociales basándonos en el enfoque de las 5 Ws:

- Who: indica quien es el creador del contenido
- Where: hace referencia al canal
- What: representa el tipo de contenido
- When: nos dice con qué frecuencia se sucede
- Why: es el propósito del mensaje

Una vez hecho éste análisis, valoramos cada red con una puntuación del 1 al 5 representando el 1 que la opción es un problema y el 5 una oportunidad. Una tabla de ejemplo rellenada:



Social Media Audit Template

WHO	WHERE CHANNEL/ ENVIRONMENT	WHAT CONTENT/ SENTIMENT	WHEN DATE/ FREQUENCY	WHY PURPOSE/ PERFORMANCE	OPPORTUNITY 1 = challenge 5 = opportunity
COMPANY	**Twitter** • text • links	**Sharing headlines from website with links** • little likes, comments, or retweets	2 tweets per day	**Drive to website** • few visits • few unique visitors	●●● • few visits • no unique visitors • some conversions
	Flickr • photos • text • links	**Sharing photos from website with links** • low views, faves, or comments	5 posts per week	**Drive to website** • no visits • no unique visitors	● • no visits • no unique visitors • no conversions
CONSUMER	**Twitter** • comments • questions	**Seeking help** • negative brand experiences	20 tweets per day	**Complaints** • negative	●● • negative comments • no likes • no shares
	Instagram • photos • text • hashtags	**Sharing photos** • positive brand experiences	10 posts per day	**Praise** • positive	●●●● • positive comments • no brand presence
COMPETITOR	**Twitter** • photos • videos • links • hashtags	**Sharing photos** • some likes, comments, and retweets	5 tweets per hour	**Drive to website** • visits • unique visitors	●● • lots of positive comments

Con esto podemos llevar a cabo una micro-auditoría que nos va ayudar a darle continuidad y sensatez al uso de nuestras redes sociales. Es una forma sencilla y simple de asegurar que vamos en el buen camino.

Esto es todo, espero que os haya gustado esta humilde serie de posts, cualquier comentario, proposición o aportación será más que bienvenida.

¡Saludos!

[1] «Política de utilización de los medios sociales«, Nvidia, acceso el 30 de Noviembre, http://www.nvidia.es/object/social-media-guidelines-es.html

[2] «Auditing Social Media: A Governance and Risk Guide», Océano, acceso el 30 de Noviembre, https://oceano.biblioteca.deusto.es/primo-explore/fulldisplay?docid=TN_emerald_s10.1108%2F14684521211241459&context=PC&vid=deusto&lang=en_US&search_scope=default_scope&adaptor=primo_central_multiple_fe&tab=default_tab&query=any,contains,social%20media%20auditing&sortby=rank&offset=0

[3] «Conducting a Social Media Audit», Harvard Business Review, acceso el 30 de Noviembre, https://hbr.org/2015/11/conducting-a-social-media-audit

[4] «Creating Business Value through Governance & Auditing of Social Media Using COBIT 5», Isaca, acceso el 30 de Noviembre, https://m.isaca.org/Education/Conferences/Documents/COBIT/COBIT-NA-2016/8.pdf

---

¿Podemos controlar nuestras identidades digitales?

Desafortunadamente, no podemos cuantificar la confiabilidad de un sistema, método o técnica, por mucho que existan distintas herramientas las cuales intentan darnos esa seguridad, nosotros lo único que podemos hacer es tratar de cuantificar el riesgo y equilibrarlo. Las empresas han estado analizando el riesgo durante años, y para ello se deben tener varios conocimientos sobre la misma, como por ejemplo, un resumen detallado del sistema, evaluaciones de la interacción requerida con los socios y su capacidad para realizar las tareas. Lo importante es cuantificar las pérdidas potenciales y sus probabilidades a un nivel de detalle que depende de la madurez de la infraestructura de identidad. Por lo que, con todo esto estamos hablando de

una auditoría exhaustiva que nos ayude a mitigar esos riesgos de los que hablábamos en las publicaciones anteriores. [1]

Tanto las personas como las organizaciones deben tomar el control de su gestión de identidad, de forma que mejoren su seguridad y privacidad. Para ello pueden llevar a cabo una serie de estrategias:

1. Una auditoría de identidad personal para comprender donde acaba su huella digital, si cualquiera puede acceder a ella o no, etc.
2. Utilizar herramientas para mejorar la privacidad.
3. Mantenerse informado como ciudadano digital sobre cómo proteger su privacidad digital.

La siguiente matriz iría relacionada con el primer punto:

Riesgos	**Controles**
Suplantación de identidad	– Conocer en detalle la forma en la que se ha dado la suplantación de identidad. – Determinar que la organización ha definido una fuente de identidad confiable, como la base de datos de recursos humanos.
Registro abusivo de nombre de dominio	– Verificar que la empresa cuenta con una estrategia en caso de ciber ocupación. **–** Determinar que posee los recursos legales apropiados para reprimir este acto. [3]
Ataques de denegación de servicio distribuido o ataque «DDoS»	– Determinar si se puede soportar ese tipo de ataque. – Verificar que la empresa cuenta con una estrategia en caso de que el ataque le afecte.
Fuga de información	– Determinar que el sistema de manejo de identidad verifica cada solicitud de una identificación nueva o modificada contra la fuente confiable. – Determinar que las plataformas siguen la política de manejo de identidad de la organización. – Verificar que las aplicaciones heredadas que no se adhieren a la política de manejo de la identidad hayan sido formalmente aprobadas por un ejecutivo de TI en un nivel superior apropiado. – Determinar si un marco de gestión de seguridad apropiado, como ISO / IEC 27002 o la serie NIST 800, se utilizará como referencia de buenas prácticas. [4]

Publicaciones por terceros de informaciones negativas	– Determinar por qué han ocurrido esas publicaciones. – Determinar si existe una estrategia alternativa que solucione esa información negativa.
Utilización no consentida de derechos de propiedad industrial	– Comprobar que la organización conoce los métodos legales y que puede aplicarlos para evitar esa utilización no consentida.

Me parece interesante comentaros, con respecto al segundo punto, algo que he estado leyendo: La Estrategia Nacional para Identidades de Confianza en el Ciberespacio (NSTIC). Se trata de una organización que describe una visión del futuro, un **Ecosistema de Identidad**, donde individuos, empresas y otras organizaciones (comunidades) disfrutan de mayor confianza y seguridad mientras realizan transacciones confidenciales en línea. Y os preguntareis, pero ¿de qué se trata? Pues bien, es un entorno en el cual las tecnologías, las políticas y los estándares están acordados de manera que respaldan todas las transacciones (desde las que van de valores anónimos hasta totalmente autenticados, de altos a bajos). Los componentes de este ecosistema de identidad son los siguientes:

- El **Marco del Ecosistema de Identidad (Identity Ecosystem Framework – IDEF)** es el conjunto general de estándares de interoperabilidad, modelos de riesgo, políticas de privacidad y responsabilidad, requisitos y mecanismos de responsabilidad que estructuran el ecosistema de identidad.
- El **Servicio de Listado de Autoevaluación de IDEF (Self-Assessment Listing Service – SALS)** está diseñado para generar confianza en línea. Se trata de una página web donde los proveedores de servicios de identidad en línea y las aplicaciones que autentican las credenciales pueden informar sobre su estado mediante una autoevaluación con un conjunto de estándares comunes.
- El **Grupo Directivo del Ecosistema de Identidad (Identity Ecosystem Steering Group – IDESG)** administra el desarrollo de políticas, estándares y procesos de acreditación para el IDEF de acuerdo con los Principios Rectores en la Estrategia. El IDESG también asegura que las autoridades de acreditación validen la adherencia de los participantes a los requisitos del IDEF.
- Los **marcos de confianza** son desarrollados por una comunidad cuyos miembros tienen metas y perspectivas similares, como los Pilotos NSTIC. Un marco de confianza define los derechos y las responsabilidades de los participantes de esa comunidad, especifica las políticas y estándares específicos de la comunidad y define los procesos y procedimientos específicos de la comunidad que brindan seguridad. Un marco de confianza

debe abordar el nivel de riesgo asociado con los tipos de transacción de sus participantes. Para ser parte del Ecosistema de Identidad, todos los marcos de confianza deben cumplir con los estándares de referencia establecidos por el IDEF.

- Las **autoridades de acreditación** evalúan y validan a los proveedores de identidad, proveedores de atributos, partes confiables y medios de identidad, asegurando que todos se adhieran a un marco de confianza acordado. Las autoridades de acreditación pueden emitir marcas de confianza a los participantes que validan.
- Los **esquemas de marca de confianza** son la combinación de criterios que se miden para determinar el cumplimiento del proveedor de servicios con el IDEF. El IDEF proporciona un conjunto básico de estándares y políticas que se aplican a todos los marcos de confianza participantes. Esta línea de base es más permisiva en los niveles más bajos de seguridad, para garantizar que no sirva como una barrera indebida a la entrada, y más detallada en niveles más altos de seguridad, para garantizar que los requisitos estén alineados con el riesgo de cualquier transacción dada. [2]

Por último, con respecto al tercer y último punto de estas posibles estrategias a seguir, os invito a que accedáis al Instituto Nacional de Ciberseguridad de España, y os leáis la guía de aproximación para el empresario sobre Ciberseguridad en la identidad digital y la reputación online. En ella encontramos, entre otras cosas, nuestro derecho (marco legal) y unas recomendaciones para la gestión de la identidad digital y la reputación online. Además, también me ha parecido interesante una página web del Gobierno de Australia (https://esafety.gov.au/) la cual se compromete a ayudar a los jóvenes a tener experiencias positivas y seguras en línea.

Por lo tanto, en algunas empresas más grandes se dispondrá de un Social Media Manager, el cual será el responsable de la identidad digital, sin embargo, en otras más pequeñas y con menos presupuesto, quizás se encargue el Community Manager. Lo que está claro es que el adecuado manejo de los riesgos, la gobernabilidad, etc. evita en gran medida esos problemas referentes a la seguridad de la identidad digital, lo cual, según empresas como Deloitte, produce mucho valor para la misma.

Referencias

[1] Phillip J. Windley (2005). <<Digital Identity: Unmasking Identity Management Architecture (IMA)>>. Acceso el 16 de noviembre de 2017, https://books.google.es/books?id=o8mHSbDHgPsC.

[2] IDESG. <<Overview>>. Acceso el 15 de noviembre de 2017, https://www.idesg.org/The-ID-Ecosystem/Overview

[3] JUS. <<Disputa de nombres de dominio>>. Acceso el 16 de noviembre de 2017, https://jus.com.br/artigos/3977/disputa-de-nombres-de-dominio

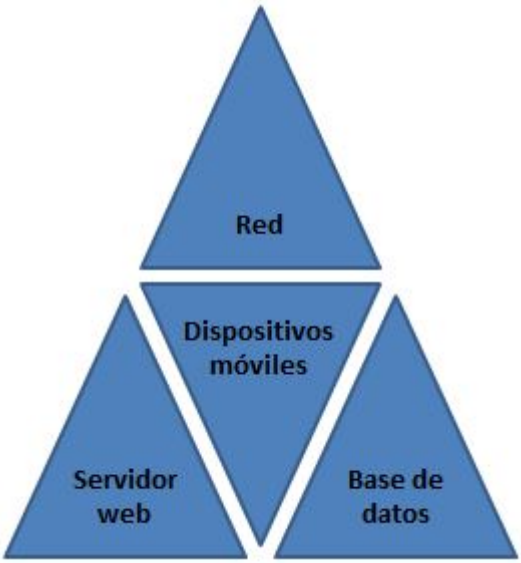
[4] ISACA. <<Identity Management Audit/Assurance Program>>. Acceso el 15 de noviembre de 2017, https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Identity-Management-Audit-Assurance-Program.aspx

---

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.

Errar es de humanos

Si bien es cierto que esta frase tiene todo el sentido del mundo, creo que queda incompleta sin la coletilla de “y rectificar de sabios”. Lo cierto es que esto siempre lo he creído así, no siempre se puede salir victorioso, y, por tanto, debemos amoldarnos y ser flexibles frente a lo que puede ocurrirnos, rectificar en definitiva. Mi madre siempre me tiene dicho que “cuando dios cierra una puerta, abre una ventana”, aunque esto, desde pequeño, yo siempre lo he puesto en duda (¿Cómo voy a salir por la ventana si vivimos en un quinto piso?). En cualquier caso, un error, problema o acontecimiento inesperado puede convertirse en una oportunidad. Lo importante es estar preparado para correr el **riesgo** y **controlarlo** en la medida de lo posible, para ver si se hace más o menos probable. Como se ha dicho, cualquiera se puede equivocar y yo el primero. Este es mi último post y me gustaría redondear todo lo que hemos visto estos meses atrás, para poner la guinda a “nuestra relación” dentro del mundo del Outsourcing TI.

Como comentamos anteriormente, el outsourcing es una práctica conocida en el mundo empresarial, tanto para el área TI como para otras tareas de la empresa. Quizás cuando hablamos de Outsourcing Ti se nos vienen a la cabeza cantidad de nombres de empresas de primera fila, generalmente multinacionales, las cuales tienen una extensa plantilla de trabajadores distribuidos por el mundo y que realizan este tipo de prácticas, como el offshoring. Es probable que no os haya ocurrido, pero este fue mi caso, la verdad, por eso hablé de externalizaciones a la India. Sin embargo, con un

poco más de *research* llegué a la conclusión de que mi proveedor de internet es una de las empresas a nivel local que sigue esta práctica: Euskaltel. "Euskaltel, cada vez menos Euskaltel" [1], "La externalización de Euskaltel, una epidemia entre las grandes empresas" [2] o "ELA presenta una demanda contra la externalización de Euskaltel" [3] son algunos de los titulares de prensa que podemos leer al respecto. Su relación también se desarrolla en muchos casos en empresas locales (como por ejemplo, Ibermática) o estatales, pero también hay algún proveedor de servicios chino (ZTE). A veces te pasa lo que me pasó a mí, que los árboles no te dejan ver el bosque, y que ves ejemplos al otro lado del charco cuando los tienes a la distancia del cable Ethernet.

Dicho esto, ¿Qué es lo que le depara el futuro al outsourcing TI? ¿Empresas como Euskaltel seguirán externalizando sus servicios? ¡Quién lo sabe con certeza! Aunque hay algunos expertos que se atreven a aventurarse a predecir lo que será "trending topic" durante este año y el siguiente, como por ejemplo Stephanie Overby en CIO [4]. La seguridad informática de las empresas, el cloud computing (las empresas pasarán a tener todos sus datos en la nube), la creación de VMO (Vendor Management Office), debida a la tendencia de trabajar con proveedores de servicios distintos para cada tarea externalizada, la expansión de los servicios externalizados, el crecimiento del enfoque ágil para las empresas de outsourcing o la automatización de algunos procesos TI (RPA lo llaman, Robotic Process Automation) son algunas de las tendencias que tienen y tendrán importancia durante 2017 según comenta Stephanie. Con lo cual, las empresas dedicadas a proveer servicios pueden estar tranquilas, tienen "tema" para rato. Dentro de estas tendencias también se habla del crecimiento del Big Data o el IoT como futuras tareas/áreas en ser externalizadas [5]. Esto último como el Cloud Computing son prácticas crecientes en ser externalizadas, en este caso desde el punto de vista de un grande como EY [6].

A la hora de hablar de casos de éxito o fracaso, se pueden encontrar noticias, opiniones y artículos de todo tipo. Por un lado se pueden ver ejemplos como el de General Motors en el 2012 que volvió a integrar en la empresa gran parte de las tareas TI que tenía fuera de ella, en concreto en EDS, compañía que fue de su propiedad [7] (una compañía absorbida por completo por HP durante ese periodo). ¿Por qué volvió al trabajo *In-house*? Otro ejemplo es el fracaso de Fujitsu en Inglaterra, en el cual se retrasó en proveer el servicio que había firmado con el gobierno británico. Sin embargo, también hay luces, como la que se comenta en la fuente, en relación con la compañía ATOS, que proveía servicio durante los Juegos Olímpicos de Londres. El funcionamiento fue excepcional y con un presupuesto ajustado. ¡*Chapo!*

En efecto, todo cuento tiene un final, pero lo que importa es recordar bien la moraleja. Durante los artículos anteriores hemos analizado a fondo el tema del Outsourcing, por decirlo de alguna manera, desde una perspectiva de la auditoría y la gestión. Hemos hablado del origen, de noticias relacionadas, del riesgo y de controles, lo que nos ha permitido conocer en mayor profundidad el tema y, dicho sea de paso, aprender conceptos que, personalmente yo al menos, desconocía. Lo que también espero es que hayáis llegado a una conclusión similar a la mía: auditar es una práctica esencial,

no sólo para detectar el fraude, sino para comprobar que estamos yendo en la dirección correcta. Mi tema es el outsourcing TI, pero esto es aplicable a cualquier otro tema. Para finalizar, cabe destacar que el outsourcing TI es un tema esencial a tratar en una empresa y que requiere un análisis exhaustivo para que tenga éxito. No es llegar y besar el santo, todo requiere un tiempo de preparación, como la preparación de este último artículo, la cual me permite rectificar y, quizás, algún día, convertirme en sabio.

Referencias:

[1] ”Euskaltel, cada vez menos Euskaltel”, Eldiario.es, acceso el 12 de Noviembre del 2016, http://www.eldiario.es/norte/euskadi/Euskaltel-vez-euskal_0_326518251.html%20-%20

[2] “La externalización de Euskaltel, una epidemia entre las grandes empresas”, El Correo, acceso el 12 de Noviembre del 2016, http://www.elcorreo.com/vizcaya/20131216/economia/externalizacion-servicios-euskaltel-epidemia-201312152102.html

[3] “ELA presenta una demanda contra la externalización de Euskaltel”, Eitb, acceso el 12 de Noviembre del 2016, http://deloitte.wsj.com/cio/2012/07/10/it-outsourcing-4-serious-risks-and-ways-to-mitigate-them/

[4] ”10 outsourcing trends to watch in 2016”, CIO, acceso el 12 de Noviembre del 2016, http://www.cio.com/article/3018638/outsourcing/10-outsourcing-trends-to-watch-in-2016.html

[5] “Top 5 IT Outsourcing Trends for 2016”, Kosbit, acceso el 12 de Noviembre del 2016, http://www.kosbit.net/top-5-it-outsourcing-trends-for-2016/

[6] “Major outsourcing trends and risk factors”, EY, acceso el 12 de Noviembre del 2016, http://www.ey.com/gl/en/services/advisory/major-outsourcing-trends-and-risk-factors

[7] “TOP 10 IT outsourcing stories of 2012”, ComputerWeekly, acceso el 12 de Noviembre del 2016, http://www.computerweekly.com/news/2240174665/Top-ten-IT-outsourcing-stories-of-2012

Auditar es Controlar

En artículos anteriores he hablado de diferentes aspectos del outsourcing TI, como su historia, evidencias sobre su práctica, ventajas y desventajas de su aplicación, riesgos asociados… El único punto a tratar que no he comentado es el control de dichos riesgos. Todo riesgo es considerado como una incertidumbre, algo que puede ocurrir durante el funcionamiento normal o las acciones de la empresa y que tiene impacto (generalmente negativo) en los resultados. Cuando hablo de acciones, esto es perfectamente aplicable a la acción de externalizar la tecnología de la empresa, que es el tema que nos incumbe. Para que este proceso sea lo más satisfactorio posible, es necesario establecer una serie de medidas para comprobar cuál es el nivel del riesgo (o la probabilidad de que dicho riesgo ocurra) en cada caso y que permitan obtener una mayor certeza (diría **seguridad**, los humanos somos inseguros por naturaleza) de la fiabilidad de la empresa.

Siguiendo el artículo anterior, en el que establecí 4 riesgos importantes [1] (riesgo operacional y transaccional, riesgos de la confidencialidad de la información, riesgo de la continuidad del negocio y riesgo de conformidad), podemos hacer el trabajo de un auditor y establecer la siguiente matriz de riesgos y controles. Los riesgos asociados pueden ser controlados o mitigados en cada caso. El control es posible gracias a una serie de evidencias que confirman el buen hacer de la empresa que está dando el servicio que se ha externalizado.

Riesgo	Control / Mitigación
Riesgo operacional y transaccional	• Conocer en detalle el flujo de las operaciones y transacciones. • Conociendo el flujo, analizar y descubrir donde una transacción puede fallar y determinar qué rol tiene la empresa que provee el servicio en dicho fallo. • A futuro, establecer posibles acciones a tomar en respuesta al fallo (contractuales, …).
Riesgo de confidencialidad de la información	• Determinar los datos transmitidos a la empresa. • Comprobar y garantizar la seguridad y los controles de protección de datos de la empresa (in situ). • Pedir el SSAE16/SOC (o SAS 70), que evalúa los controles y la seguridad de la empresa (según un auditor externo). • Aumentar la frecuencia de visitas a la empresa en función de la importancia de los datos.

Riesgo de la continuidad del negocio	• Simular una crisis y preguntar a la empresa para determinar cómo reaccionan a dicha situación y en cuanto tiempo. • Preguntar los efectos de dicha crisis en la empresa contratada y establecer a la empresa la importancia de los procesos externalizados para la empresa que la contrata (pérdidas de dinero, confianza, clientes…). • Disponer de una estrategia en caso de fallo del proveedor, es decir, un plan de contingencia. • Comprobar y evitar demasiados "lazos" de externalización con una misma empresa.
Riesgo de conformidad	• Comprobación de que la empresa dispone de los medios necesarios para realizar la función crítica en el tiempo establecido.

Tabla 1: Matriz riesgos/controles

Después de analizar esta matriz, tenemos los riesgos, los controles a esos riesgos y creo que me dejó algo…. ¡ah sí! falta la importantísima figura del "árbitro", es decir, el auditor. Como en cualquier otro área, a la hora de comprobar que los servicios TI son adecuados, cumplen con la ley y demás temas de vital importancia, el auditor juega su papel para comprobar que lo dicho o escrito está en consonancia con lo hecho. Cabe destacar, que como apunta el documento de GTAG para el outsourcing TI [2], este proceso tiene un ciclo de vida, desde la decisión de externalizar, pasando por la implementación y revisión, para posteriormente realizar una renegociación de lo acordado para las futuras colaboraciones. Sin embargo, debido a lo extenso del documento, supongamos que nos encontramos en la posición de evaluar los servicios externalizados, con lo que seguiríamos la siguiente tabla:

Stages	Objectives	Key Activities	Manager Roles *	Risks	Auditor Involvement
E: Monitoring and Reporting	Oversee and control the outsourced operation.	■ Manage relationship. ■ Assess results and performance. ■ Design ongoing reporting and process improvement model.	Process owner,* retained team, project sponsor, finance, HR, risk, and other experts.	■ Relationship and deliverables devolve with customer damage and loss of assets and ROI. ■ Process is not sustained and is not optimized as planned.	■ Determine how provider performance and compliance to the contract will be assessed and routinely reviewed by management. ■ Ask what metrics and other key performance indicators are used. ■ Ask how concerns and areas for improvement are communicated and leveraged to improve current and future operations/ contracts.

Tabla 2: Puntos clave a la hora de auditar las operaciones externalizadas

En este caso, como se apunta en la tabla, el auditor deberá determinar si el proveedor ha tenido un rendimiento adecuado y ha cumplido con el contrato.

Deberá pedir también las métricas utilizadas para medir el rendimiento, así como las áreas de mejora a tener en cuenta, las acciones a tomar en esas áreas para mejorar futuras acciones y operaciones. Aunque esto puede considerarse muy genérico, puede plasmarse de una manera más exacta mediante el plan descrito en un documento de ISACA [3]. Siguiendo un enfoque guiado por el riesgo, el auditor debe seguir 4 pasos importantes: realizar una evaluación del nivel del riesgo obtenido, realizar un trabajo de campo (si es offshore en el país, sino mediante reuniones), realizar un reporte sobre lo obtenido y continuar con las operaciones externalizadas, amoldándolas a las conclusiones obtenidas. El paso uno es el más importante y donde el auditor realiza gran parte del trabajo. En dicho paso, su función es entrevistarse con los stakeholders de la compañía, así como el proveedor del servicio, determinar los objetivos, riesgos y controles y comprobar si el proveedor dispone de algún tipo de informe (SOC1, ISO 2700X o similar). A partir de lo obtenido, deberá ajustar el alcance de la auditoría en función de los controles, desarrollar una matriz de riesgos y controles (similar a la que se ha visto en este artículo), así como un programa de auditoría. Finalmente, quizás sea necesario disponer del conocimiento de expertos, como abogados, para tomar decisiones, como por ejemplo en el tema de leyes y regulaciones.

Resumiendo, el trabajo de establecer controles para evitar, mitigar o gestionar riesgos es una tarea importante en cualquier acción de cualquier tipo, con especial importancia en el outsourcing TI. Al fin y al cabo, estás delegando funciones que podrían realizarse dentro de la empresa fuera de la empresa, con personas que no tienen ninguna unión con tu empresa (fuera del contrato) y que tienen métodos de funcionamiento o estrategias distintas a las que tu tenias y tienes. De similar manera, muchas veces se piensa que no se debe externalizar algo porque es demasiado arriesgado o, dicho de otra manera, puede tener mucho riesgo asociado. Pero la solución es clara: para obtener unos beneficios determinados hay que arriesgarse, disponiendo de una serie de controles que nos ofrezcan un mínimo de seguridad. Esa seguridad que nos puede transmitir un auditor cuando nos dice que los controles son correctos y que todo marcha como la seda. Aunque es cierto que el futuro es imprevisible y no se puede estar preparado para todo…

Referencias:

[1] ”4 IT Outsourcing Risks and How to Mitigate Them”, The Wall Street Journal (Deloitte), acceso el 31 de Octubre del 2016, http://deloitte.wsj.com/cio/2012/07/10/it-outsourcing-4-serious-risks-and-ways-to-mitigate-them/

[2] “Information Technology Outsourcing”, GTAG Global Technology Audit Guide, acceso el 31 de Octubre del 2016, https://chapters.theiia.org/montreal/ChapterDocuments/GTAG%207%20-%20Information%20technology%20outsourcing_2nd%20ed.pdf

[3] Adnan Dakhwe, “Risk & Control Considerations for Outsourced IT Operations”, ISACA, Core Competencies – C32, San Francisco, acceso el 31 de Octubre del 2016,

http://www.sfisaca.org/images/FC13Presentations/C32_Presentation.pdf

[4] ”Outsourced IT Environments Audit/Assurance Program”, ISACA, acceso el 31 de Octubre del 2016, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Outsourced-IT-Environments-Audit-Assurance-Program.aspx

---

¿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):

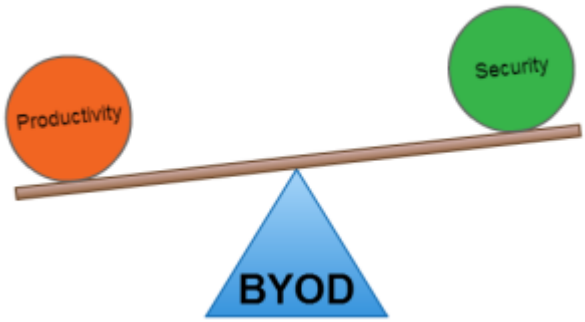
Según **un documento de ISACA** existen varias posibles decisiones estratégicas, cada una con sus respectivas ventajas y desventajas. A continuación, enumero algunas de las decisiones estratégicas que ISACA propone:

- 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.

Bueno, bonito y barato ¿es esto posible?

Generalmente en las organizaciones se habla de reducción de costes, mejora de servicio, y además se le debe agregar ¡recursos limitados! tal vez esto sueñe a locura, pero se puede lograr. Una opción a considerar es Lean, que aunque inicialmente estaba dirigida a la industria manufacturera (lean manufacturing), nos puede aportar mucho en TI.

Pero ahora se preguntarán: ¿Qué es lean manufacturing? Pues la filosofía **lean manufacturing** es una herramienta que ayuda a reducir las actividades que no agregan valor de los procesos para agilizarlos. Para lograr esto se basa en algunos principios, como el valor (lo que el cliente está dispuesto a pagar), la cadena de valor (modelar y registrar todas las acciones específicas requeridas para eliminar las actividades que no añaden valor), el flujo (eliminación de las interrupciones para lograr que el flujo de la cadena no tenga interrupciones), el dinamismo (capacidad de innovar los productos y los procesos a través de los conceptos que brinda la utilización por parte de los clientes) y la perfección (habilidad para lograr que las cosas se hagan bien desde el primer momento hasta la aplicación del esfuerzo de mejora continua).

Me imagino lo que estarán pensando: ¿y esto qué tiene que ver con las TI? Pues yo me preguntaba lo mismo, hasta que encontré que una fuente de lograr ventaja competitiva es la combinación de la tecnología de información con el Lean manufacturing; sí, la tan ansiada ventaja competitiva, que muchos buscas, pero que pocos alcanzan.

Con esta combinación, conocida como **Lean TI**, se busca eliminar desperdicios y

retrasos, reducir errores informáticos y aumentar la velocidad con la que la tecnología de información agrega valor al negocio, a los clientes y a los accionistas. Y pues, ya no se nos debe hacer extraño el término alineamiento estratégico, pues a Lean TI tampoco, ya que esta herramienta debe estar alineada con la visión del negocio y de esta manera poder tomar decisiones a largo plazo.

Algunos de los beneficios que pueden obtener son:

- Reducir de costos: Identificar procesos innec/esarios, rediseñarlos, buscar la eficiencia y por lo tanto disminuir el uso de los recursos.
- Incrementar el valor: Identificar las cadenas de valor que incluyen a la TI y seguir el mismo proceso que en los costos. Esto involucra a los gerentes de TI ya que participan proactivamente en las iniciativas para crear valor.
- Reducir tiempos de espera (retrasos y cuellos de botella): Diseñar los procesos de tal manera que ayuden a reducir estos retrasos lo máximo posible, para lo cual se debe considerar a la cultura organizacional y los perfiles del personal para que el cambio organizacional no sea tan drástico.
- Reducción de errores: Esto forma parte de lograr eficiencia en los procesos y reducir la espera.
- Eliminación de barreras: Eliminación de barreras entre el departamento de sistemas y el resto de los departamentos de la organización.

Entonces ¿te animas a probarlo? Pues yo sí.

Algunos dirán ¿y esto que tiene que ver con la auditoría o con la gestión de riesgos? La siguiente semana tocaré el tema “Six Sigma”. Luego de eso entenderán, pero les voy adelantando algo:

Lean + Six Sigma = Lean Six Sigma!!! … enfocado a las TI

Así que no se lo pierdan, nos vemos en el siguiente post….