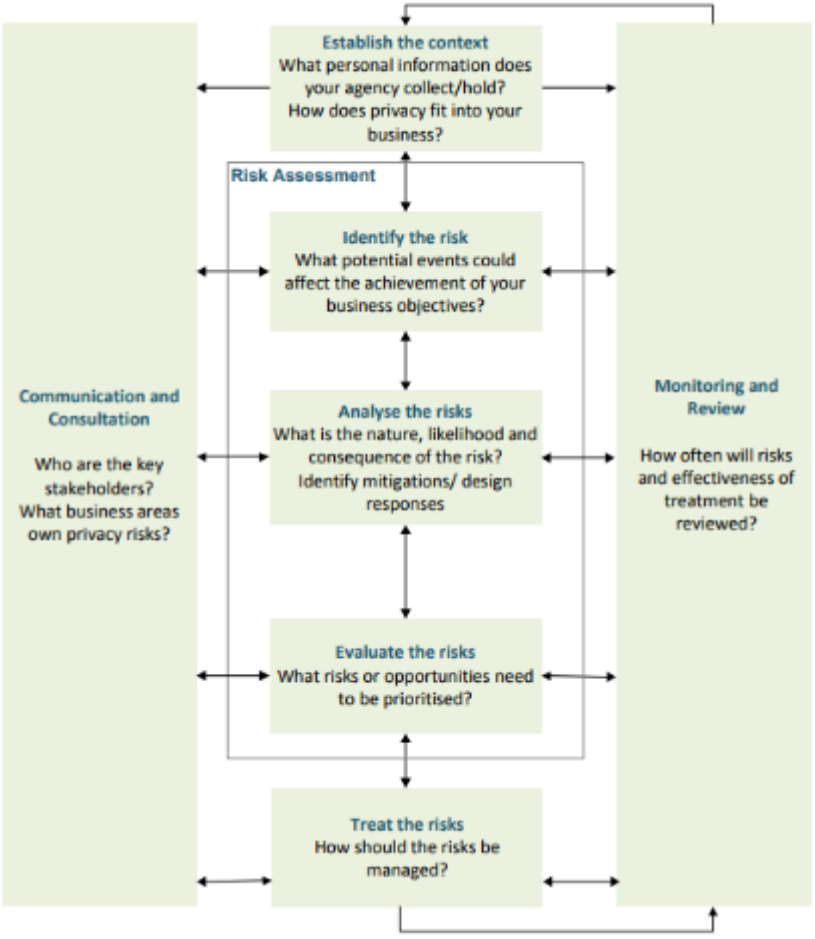
Privacidad desde una perspectiva internacional: controles y auditoría

En el post anterior hemos visto la gran diversidad de problemas y riesgos que deben afrontar las empresas. Con el propósito de prevenir que estos riesgos se hagan realidades necesario conocer, analizar y actuar para prevenir los riesgos que puedan poner en jaque mate a nuestra empresa.

Identificar y gestionar estos riesgos de privacidad es clave para gestionar información personal en cualquier entidad. Es necesario tener en consideración realizar una auditoria para realizar estas labores. Los auditores consideran riesgos clave y puntos métodos de control cuando realizan una auditoria. De esta forma una empresa se puede evaluar para ver cómo se enfrentan sus políticas de privacidad ante los requisitos legislativos.
La metodología que se sigue tiene un fuerte vínculo con los conceptos que se presentan en la ISO 31000:2009 *Risk Management – Principles and Guidelines*. El diagrama que se muestra a continuación está basado en el proceso de gestión de riesgos de privacidad de la ISO 3100:2009.



Como se puede observar en el diagrama [1] [2] este proceso cuenta con varias fases:

- ***Establecer el contexto:*** cada caso a auditar es completamente distinto,

ya que los problemas que una empresa pueda son derivados de su propio entorno, el cual está sujeto a muy diversas circunstancias. Además la definición de privacidad es muy subjetiva dependiendo el país, la cultura o la organización, por lo que entender el contexto bajo el cual se lleva a cabo el proceso de auditoría es vital para que sea exitoso. Además también es imperativo que la visión de todos los involucrados sea la misma.

- **Identificar los riesgos:** los riesgos de privacidad, como ya hemos visto están relacionados con la gestión de información personal, y pueden tener consecuencias tanto para los propietarios de esos datos como para las empresas que lo tratan. Por ellos, es necesario identificarlos mediante el uso de diferentes herramientas. Existen áreas que tienen un alto nivel de riesgo en este ámbito por lo que en ellas podemos identificar algunos. Estas áreas son, las redes sociales, Big Data, dispositivos mçoviles y el modelo operativo. Además en este proceso también se pueden identificar oportunidades para mejorar o fortalecer la gestión de información personal.
- **Analizar los riesgos:** este proceso cuenta con dos fases, por un lado asignar calificaciones basadas en el riesgo que suponen, el impacto que pueden tener, y por otro lado la evaluación de los controles implementados. La calificación se puede obtener se puede obtener en base a una matriz que tenga en cuenta el impacto y la probabilidad.

Probabilidad	Consecuencia/Impacto				
	1 – Inapreciable	2 – Menor	3- Moderado	4 – Alto	5 – Severo
5 – Seguro	Riesgo Moderado	Riesgo Significativo	Riesgo Significativo	Riesgo Extremo	Riesgo Extremo
4 – Probable	Riesgo Moderado	Riesgo Significativo	Riesgo Significativo	Riesgo Extremo	Riesgo Extremo
3 – Posible	Riesgo Moderado	Riesgo Moderado	Riesgo Significativo	Riesgo Significativo	Riesgo Extremo
2 – Improbable	Riesgo Bajo	Riesgo Moderado	Riesgo Significativo	Riesgo Significativo	Riesgo Extremo
1 – Raro	Riesgo Bajo	Riesgo Bajo	Riesgo Moderado	Riesgo Moderado	Riesgo Significativo

Una vez realizada la matriz para la calificación de los riesgos es necesario evaluar los controles existentes para conocer el nivel de mitigación existente. Algunos ejemplo de controles de privacidad de una organización son las políticas de privacidad, los controles de privacidad de la base de datos y la criptografía.

- **Evaluar los riesgos:** en este paso se calcula el riesgo residual. Este riesgo residual es el resultado del nivel de riesgo tras valorar el riesgo y los controles existentes para mitigarlo. En base a esto se puede priorizar aquello que más daño pueda causar a la empresa auditada y desarrollar un plan de auditoria.
- **Tratar los riesgos:** el auditor, basándose en su criterio, debe determinar una respuesta apropiada a un riesgo o a una oportunidad. Muchas agencias de auditoria de TI tienen sus propios criterios y frameworks de tratamiento de riesgos por lo que los auditores puede apoyarse en estas guías predefinidas. Algunas respuestas básicas incluyen, dejar de realizar una tarea que pueda causar que el riesgo

ocurra, modificar los controles existentes en cierto aspecto para reducir la probabilidad de que ocurran o para minimizar su impacto. También es preciso destacar que es necesario considerar la relación entre el coste y el beneficio al tratar un riesgo.

- **Monitorización:** es importante monitorizar y realizar revisiones continuamente de los riesgos de privacidad y del tratamiento de los datos. Hay una alta probabilidad de que estos riesgos cambien a lo largo del tiempo y tal vez sea necesario reconsiderar su relevancia y si siguen presentes o han sido solucionados. Además es óptimo que cualquier toma de decisiones esté basada en información lo más actualizada posible.
- **Comunicación y consultoria:** se deben proveer reportes a las personas involucradas en la auditoría en cada fase de la misma. Y es necesario notificar todos los puntos importantes que surjan en el proceso.

En conclusión, la noción y el entendimiento de la privacidad va a continuar creciendo día a día, y con ello se espera que aparezcan nuevos requisitos regulatorios para las prácticas que manipulen datos personales, y como ya hemos visto a los largo de esta serie de artículos, el debate está servido, ya que existen opiniones excesivamente dispares.

Por lo que en este escenario tan volátil, los auditores deben de ser capaces de establecer y seguir metodologías de auditoría de privacidad para evitar que las organizaciones para las que trabajan se vean involucradas con riesgos innecesarios. Además como hemos explicado existen una serie de pasos para poder minimizar estos riesgos hasta un nivel aceptable, aunque en un mundo tan cambiante los auditores deben ser conscientes de las nuevas tendencias tecnológicas que surgen con el paso de los años. Debido a todos estos motivos, es una gran idea añadir el plan de auditoria de privacidad al plan de auditoría anual.

Referencias:

[1] <<Privacy Audit—Methodology and Related Considerations>>, ISACA, acceso 29 de noviembre del 2017, **https://www.isaca.org/Journal/archives/2014/Volume-1/Pages/Privacy-Audit-Methodology-and-Related-Considerations.aspx?utm_referrer=**

[2] <<Privacy risk and opportunity identification>>, ICT, acceso el 29 de noviembre de 2017, **https://www.ict.govt.nz/assets/GCPO/Privacy-risk-and-opportunity-identification.pdf**