Riesgos

A pesar del gran potencial que tiene el Big Data y su relevancia en la industria actual, es clave saber identificar y poder hacer frente a los riesgos que conlleva este análisis masivo de los datos. Uno de los papeles más importantes que tienen que cumplir las organizaciones consiste en comprender la importancia del Big Data, reconociendo así los puntos en los que más valor se puede conseguir gracias a su aplicación.

A medida que las organizaciones aumentan el número de soluciones basadas en Big Data para conseguir un valor y una ventaja competitiva, es importante que el auditor de la Seguridad de la Información sea capaz de entender los riesgos que esto conlleva y asegure que estos se están gestionando de manera correcta. El uso de la analítica avanzada puede ser vital para la detección de riesgos, a la vez que ayuda a señalar posibles sesgos en el pensamiento de la gestión, ineficiencias en el mercado y desarrollos emergentes. En resumen, los datos brindan una nueva ventana al mundo, pero los análisis adecuados son los que ayudan a comprender lo que significan para la organización [1]. A continuación, se muestran algunos de los principales riesgos que hay que mantener a raya [2].

Estrategia IT y recursos: Es importante entender la estrategia general de la empresa y como el Big Data debe ser utilizado o aplicado para apoyar esa estrategia. Muchas organizaciones no están preparadas para capitalizar las oportunidades que el Big Data puede ofrecer, especialmente en lo que a talento de los trabajadores se refiere, ya que es una tecnología todavía en alza que cuenta con una falta de expertos en su ámbito.
Los auditores de la seguridad de la información deberían evaluar estrategias tecnológicas y la gestión de recursos con el fin de asegurar que las iniciativas tecnológicas y están alineadas con la estrategia de la empresa y que esta cuenta con recursos suficientes y bien cualificados.

Desarrollo e implementación: Para este apartado listaremos una serie de riesgos que pueden experimentar los proyectos de tecnología de Big Data.

- Desafíos con el alcance, la calidad, el costo y el tiempo de comercialización.
    - Los auditores de SI deben determinar si las soluciones de Big Data se adquieren y desarrollan de manera controlada utilizando procesos apropiados de gestión de proyectos y desarrollo de sistemas.
- Las iniciativas de Big Data a menudo utilizan metodologías de desarrollo ágiles iterativas como Scrum. Sin embargo, es probable que los auditores de SI estén familiarizados con los procesos de desarrollo de sistemas en cascada tradicionales, enfatizados más en la documentación completa y detallada.
    - Los auditores de SI pueden tener el desafío de obtener la seguridad de que se realizaron las pruebas adecuadas para determinar que la solución de Big Data funciona según lo previsto.
- La veracidad de los datos, conocida a menudo como la cuarta V.
    - Para lograr este objetivo, los auditores de SI deben evaluar la estrategia de aseguramiento de la calidad de Big Data de la organización o incluso determinar si se ha implementado un programa efectivo de gobernanza de datos.

Privacidad y seguridad de los datos: una de las grandes preocupaciones asociada al manejo de tanta cantidad de información es garantizar que se cumple con los requisitos de privacidad y seguridad. Los datos pueden ponerse en peligro por una serie de razones, incluidos los controles de seguridad inadecuados, amenazas tanto internas como externas o configuraciones del sistema débiles.
A la hora de manejar datos confidenciales existen requisitos

normativos de la industria que recogen como se protegen, comparten y depuran esos datos. Se debe prestar especial atención a datos financieros, de salud e información de identificación personal. Los auditores de SI deben revisar las regulaciones para la protección de datos y la privacidad, y evaluar los controles de seguridad en detalle.
Como dato curioso y práctico que demuestra lo que sucede cuando las cosas no se hacen como se deberían, está la fuga de datos que sufrió una empresa de análisis de datos en 2017 que incluía información, 1,1 terabytes, sobre los votantes estadounidenses.

Tecnologías *open source* y *cloud:* muchas organizaciones pueden optar por utilizar plataformas de código abierto o entornos de computación en la nube de terceros, como podrían ser Apache Hadoop o Amazon Web Services (AWS). Este tipo de tecnologías presentan riesgos únicos que deben ser considerador por los auditores.
Otro riesgo asociado a las soluciones de código abierto es el relacionado con las licencias. Dependiendo del tipo de licencia que se utilice, existe el riesgo de infracción de la propiedad intelectual o la exposición del código propio de la organización.
Los auditores SI deben evaluar por una parte que los proveedores de tecnología en la nube tienen controles de seguridad adecuados, que la supervisión con los proveedores externos es suficiente, y, por otro lado, evaluar los controles que se encargan de gestionar y mitigar las vulnerabilidades del código abierto, a la vez que monitorean el cumplimiento de las licencias mencionadas.

A pesar de que cada vez estos riesgos estén más controlados y las medidas que se toman para mantenerlos a raya mejoren continuamente, las soluciones de Big Data también crecen a un ritmo desmesurado. Para hacer frente a ese crecimiento y esta evolución del Big Data hacia los datos no estructurados y el software de código abierto, los auditores SI deberán ampliar

su conocimiento y desarrollar nuevas habilidades. Y, por último, volviendo a la analítica avanzada que hemos comentado en el comienzo del post, la utilización de esta ayudará también a reducir los riesgos en financiación, talento, tiempo y tecnologías mal asignadas.

Referencias

[1] «The Real Deal With Big Data», Deloitte. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/regulatory/us-director-advisory-real-deal-with-big-data-013015.pdf

[2] «Auditing Big Data in the Enterprise», ISACA. https://www.isaca.org/resources/isaca-journal/issues/2018/volume-2/auditing-big-data-in-the-enterprise