



Faro de Auditoría

Boletín Flash del Comité Latinoamericano de Auditoría Interna (CLAIN)

FELABAN

No. 5 –Febrero 2016

2016: Claves en Seguridad de la Información

Basados en información de origen heterogéneo, informes de análisis públicos, opinión de expertos, colaboradores y previsiones propias de SIMETRICA para 2016, se elaboró un informe en relación a la seguridad en los activos de información, local y globalmente. En síntesis indican, que la seguridad de la información en 2016 se verá gravemente afectada por múltiples factores. Entre ellos se puede mencionar la abundancia información disponible (calidad y cantidad), susceptible de ser vulnerada; la proliferación de dispositivos (Tipo y cantidad) y la interacción de estos conceptos respecto de los perímetros de seguridad de las organizaciones. Debemos considerar hoy que las superficies de ataque se han multiplicado en los últimos años haciendo más viable cualquier innovación en temas de malware y/o estrategias sociales. Se espera que en 2016 crezcan los incidentes de seguridad detectados a nivel global y en las organizaciones en más de un 30 % con respecto a 2015.

El futuro de la gestión de riesgos en la banca

McKinsey ha publicado un reseña sumamente interesante del trabajo realizado por Phillip Harle, Andras Havas y otros autores sobre el futuro de la administración o gestión de riesgos en la banca mirando hacia el año 2025. Los autores mencionan que si bien esta función se ha incrementado sustantivamente durante los últimos 10 años básicamente por presión regulatoria luego de la crisis financiera, se ve en el horizonte un cambio incluso mayor en la próxima década. Ello en virtud de 6 tendencias estructurales que transformarán la gestión de riesgos: i) mayor regulación, ii) mayores expectativas de los clientes, iii) tecnología y análisis de data avanzado, iv) mejores decisiones de riesgo al eliminarse sesgos estadísticos, y vi) la necesaria reducción de costos.

Para responder a este reto, los autores sugieren 5 iniciativas básicas que los bancos deberían empezar a trabajar:

1. Digitalizar los procesos *core*
2. Experimentar con análisis estadístico o *analytics* de avanzada
3. Mejorar el reporte de los riesgos
4. Colaborar en la optimización del balance
5. Construir la mezcla óptima de infraestructura para procesar información y el talento que la administre.

Muy recomendable



UNA VISION PARTICULAR PARA EL AÑO 2016 SOBRE LA SEGURIDAD EN LOS ACTIVOS DE INFORMACION

2016: Claves en Seguridad de la Información

para América del Sur y su Aproximación

Global Hoy:



<http://www.simetrica.biz/wpacvlv2016210116.html>

McKinsey & Company

Phillip Harle,
Andras Havas,
and Howard Bernstein

The future of bank risk management

Risk February 2016

Banks have made dramatic changes to risk management in the past decade—and the pace of change shows no signs of slowing. Here are five initiatives to help them stay ahead.

Risk management in banking has been transformed over the past decade, largely in response to regulations that emerged from the global financial crisis. But we believe it could be set to undergo even more sweeping change in the next decade. Indeed, while risk-operational processes such as credit administration today account for some 50 percent of the function's staff, and analytics just 15 percent, by 2025 those figures could be around 25 percent and 40 percent respectively.

The trends shaping the risk function come from all directions. While we cannot draw a blueprint of what a bank's risk function will look like in 2025—we can predict all the disruptions that might lie ahead—we can paint a picture of some important changes that are relatively certain. We see financial and nonfinancial regulation continuing to broaden and deepen as public sentiment becomes ever less tolerant of any appearance of preventable errors and inappropriate practices, or of bank failures. Simultaneously, customers' expectations will rise in line with changing technology. In the battle for customer relationships, banks will need to offer real-time responses to customer requests to open an account or take out a loan, for example, which means the risk function will need to find ways to assess risks automatically, without human intervention. Risk functions will also have to cope with additional, emerging risks—from cyberattacks to contagion in global markets and losses made due to the increasing use of models to make decisions (losses that are not uncommon but seldom reported).

file:///C:/Users/s06676/Downloads/Future%20of%20bank%20risk%20management.pdf

Cambios en las Normas del IIA

El IIA Global ha iniciado una consulta a los miembros de la comunidad de auditores, para realizar cambios a las Normas. Dentro de la revisión de las propuestas encontramos 3 que valen la pena resaltar:

- La incorporación de los principios fundamentales al MIPP y sobre todo que se otorgó importancia superlativa a alinear el trabajo de auditoría con las estrategias, objetivos y riesgos de la organización, con énfasis en nuevas tendencias y temas emergentes.
- Cambio en Norma 2100 – Naturaleza del trabajo: “La actividad de auditoría interna debe evaluar y contribuir a la mejora de los procesos de gobierno, gestión de riesgos y control, utilizando un enfoque sistemático, y disciplinado y basado en riesgos. *La credibilidad y valor de auditoría interna se refuerzan cuando los auditores son proactivos y sus evaluaciones ofrecen nuevos análisis y consideran impactos futuros.*”
- Nueva Norma 1112: ante distintas realidades regulatorias y de complejidad de las operaciones, se hace explícito que dentro de las labores de DEA pueda, con las salvaguardas del caso, realizar actividades de gestión integral de riesgos (ERM por sus siglas en inglés) y de cumplimiento. La consulta pública termina el 30 de abril de 2016.

Una Guía Ejecutiva del Internet de las Cosas (“IoT”)

Para cambiar un poco el tono del Faro y pensar un momento fuera del trabajo cotidiano, traemos un interesante documento sobre el Internet de las Cosas. Según Wikipedia https://es.wikipedia.org/wiki/Internet_de_las_cosas el Internet de las cosas (en inglés Internet of things, abreviado IoT) es un concepto que se refiere a la interconexión digital de objetos cotidianos con internet.

En este artículo de la Revista Trimestral de McKinsey señala que si bien el crecimiento del IoT traerá mucho ruido “positivo” en los medios propagandísticos debido a la mejora en la calidad de vida de las personas que tengan acceso, el potencial para nuevos negocios es mucho mayor.

Ello traerá diversas implicancias para los líderes empresariales, identificándose 3 grupos de oportunidades:

- la expansión global de los negocios B2B,
- nuevas palancas para la excelencia operativa, y
- grandes posibilidades para modelos de negocio innovadores.

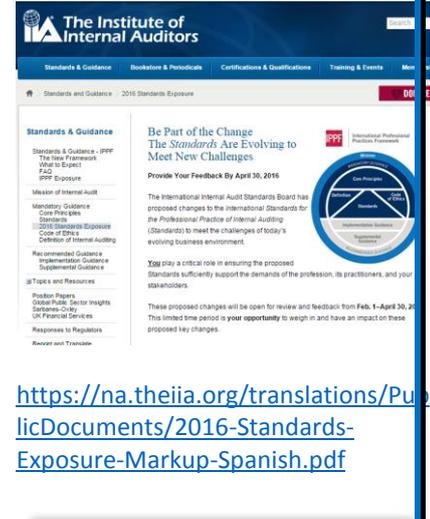
Está funcionando correctamente nuestro programa PCI DSS?

Los bancos de la región trabajamos con tarjetas de crédito y débito de distintas marcas y emisores, y cada país tiene un diferente nivel de penetración, exigencias de servicio al cliente y seguridad.

Sin embargo, nuestro común denominador es el cumplimiento de los programas PCI DSS.

ISACA ofrece todo un programa completo de auditoría y aseguramiento, pero también, previo registro simple, ha publicado un cuestionario muy sencillo que permite a través de 20 preguntas, llevarnos una idea general sobre nuestro nivel de cumplimiento con la norma.

Además cada una de las preguntas están interrelacionadas con los procesos COBIT 5 relacionados, lo que facilita enormemente su comprensión y uso.



<https://na.theiia.org/translations/PublicDocuments/2016-Standards-Exposure-Markup-Spanish.pdf>

Insights & Publications

Latest thinking Industries Functions Regions Themes

An executive's guide to the Internet of Things

The rate of adoption is accelerating. Here are six things you need to know.

August 2015 | by Jacques Dupuis, Michael Chiu, and James Marlowe

As the Internet of Things (IoT) has gained popular attention in the five years since we first published on the topic, it has also beguiled executives. When physical assets equipped with sensors give an information system the ability to capture, communicate, and process data—and even, in a sense, to collaborate—they create game-changing opportunities: production efficiency, distribution, and innovation all stand to benefit immensely. While the consumer's adoption of fitness bands and connected household appliances might generate some useful buzz, the potential for business impact is much greater. Research from the McKinsey Global Institute suggests that the operational efficiencies and greater market reach IoT affords will create substantial value in many industries. (For more, see the video “What’s the one piece of advice for a business leader interested in the Internet of Things?” And to see how experts believe the Internet of Things will evolve, see “The Internet of Things: Five critical questions.”)

There are many implications for senior leaders across this horizon of change. In what follows, we identify three sets of opportunities: expanding pools of value in global markets, new levers of operational excellence, and possibilities for innovative business models. In parallel, executives will need to deal with three sets of challenges: organizational misalignment, technological interoperability and analytics hurdles, and heightened cybersecurity risks.

Opportunities beckon... IoT's impact is already extending beyond its early, most visible applications. A much greater potential remains to be tapped.

<http://www.mckinsey.com/insights/business-technology/an-executive-s-guide-to-the-internet-of-things?cid=other-emi-alt-mkq-mck-oth-1602>

Is Your PCI DSS Compliance Program Working Correctly?

Use this Governance Checklist to ensure your enterprise employs the right strategy. The Internal Control questionnaire (ICQ) assesses program maturity through the completion of a Self-Assessment Questionnaire (SAQ). The task of the assessment is the performance and monitoring of the program. The ICQ is designed to help you assess the maturity of your PCI DSS compliance program and to identify areas for improvement.

Internal Control Questionnaire	Yes	No	N/A	Comments	COBIT 5 Reference
1. The organization must demonstrate that it has established and implemented a comprehensive PCI DSS compliance program that meets the requirements of the PCI DSS standard.					COBIT 5.02.01
2. The organization must demonstrate that it has established and implemented a comprehensive PCI DSS compliance program that meets the requirements of the PCI DSS standard.					COBIT 5.02.01
3. The organization must demonstrate that it has established and implemented a comprehensive PCI DSS compliance program that meets the requirements of the PCI DSS standard.					COBIT 5.02.01
4. The organization must demonstrate that it has established and implemented a comprehensive PCI DSS compliance program that meets the requirements of the PCI DSS standard.					COBIT 5.02.01
5. The organization must demonstrate that it has established and implemented a comprehensive PCI DSS compliance program that meets the requirements of the PCI DSS standard.					COBIT 5.02.01
6. The organization must demonstrate that it has established and implemented a comprehensive PCI DSS compliance program that meets the requirements of the PCI DSS standard.					COBIT 5.02.01
7. The organization must demonstrate that it has established and implemented a comprehensive PCI DSS compliance program that meets the requirements of the PCI DSS standard.					COBIT 5.02.01
8. The organization must demonstrate that it has established and implemented a comprehensive PCI DSS compliance program that meets the requirements of the PCI DSS standard.					COBIT 5.02.01
9. The organization must demonstrate that it has established and implemented a comprehensive PCI DSS compliance program that meets the requirements of the PCI DSS standard.					COBIT 5.02.01
10. The organization must demonstrate that it has established and implemented a comprehensive PCI DSS compliance program that meets the requirements of the PCI DSS standard.					COBIT 5.02.01

http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/pci-dss.aspx?cid=edmi_1201113&Appeal=EDMi&sp_rid=OTA4NDUyODY3MDI&sp_mid=12680188