Faro de Auditoría

Boletín Flash del Comité Latinoamericano de Auditoría Interna (CLAIN)

FELABAN

No.17 –Febrero 2017

Riesgo Digital: transformando la gestión de riesgos para los 2020s

En este interesantísimo artículo de McKinsey, podremos observar el concepto del *riesgo digital* en los bancos desde otra óptica. Se lo define como un concepto que abarca todos los habilitadores digitales que mejoren la eficiencia y eficacia de la gestión de riesgos, particularmente mediante automatización de flujos, reconocimiento de caracteres ópticos, analítica avanzada -incluyendo inteligencia artificial y aprendizaje automático-, nuevas fuentes de información así como la aplicación de robótica a procesos e interfases.

En la actualidad, la mayoría de nuestros bancos están pasando por un proceso de transformación digital, observándose mejoras significativas en la experiencia al cliente, ingresos y menores costos.

Se sostiene en este documento, además con información de fuente propia, que en esta transformación digital, la función de riesgos no puede ser la excepción.

Para ello se requiere un cambio tridimensional en: i) procesos, ii) data y iii) organización.

McKinsey recomienda la aplicación a 3 procesos críticos de la administración de riesgos, donde la digitalización será más efectiva para esfuerzos en el corto plazo: i) riesgo crediticio, 2) análsiis de estrés, y 3) riesgo operativo y de cumplimiento.

http://www.mckinsey.com/business-functions/risk/our-insights/digital-risk-transforming-risk-management-for-the-2020s?cid=other-eml-alt-mip-mck-oth-1702

Panorama 2017 de la Administración de Inversiones

Como en anteriores ediciones del Faro de Auditoría, tratamos de introducir algún tema que si bien no está en el centro del negocio bancario en muchas de nuestras instituciones, sigue siendo una temática relevante a seguir de cerca.

En esta oportunidad, Deloitte nos presenta un resumen de los impactos que podría tener la industria de inversiones en los Estados Unidos el 2017, que sin duda tendrán efectos colaterales en nuestras economías.

Estos impactos provendrán de tendencias significativas como los cambios en el comportamiento de los compradores a medida de la generación milenaria se convierta en una fuerza determinante en el mercado de inversionistas, mayor regulación por parte de la Comisión de Valores (SEC) y los efectos transformacionales que el blockchain, la robótica y otras tecnologías emergentes tendrán sobre la industria.

https://www2.deloitte.com/us/en/pages/financial-services/articles/investment-management-industry-outlook.html

Riesgos No Financieros hoy : alineando el riesgo y el negocio

Durante los últimos meses, nuestra región ha sido conmovida por noticias nefastas de actos de corrupción que involucran gobiernos, empresas y sistemas judiciales. Es la práctica anticorrupción parte de nuestra gestión de riesgos? Debemos auditar los modelos o marcos que existen en nuestras instituciones para detectar y detener los riesgos llamados “no financieros”.

Hemos elegido este artículo debido a siempre es bueno refrescar conceptos y modelos, sobre todo cuando el día a día no nos da mucho tiempo para meditar y cuando está en riesgo no sólo sanciones y multas a las empresas, la alta gerencia y el directorio sino primordialmente cuando se pone en juego la reputación de la empresa y sus colaboradores. McKinsey nos recuerda cómo transitar por este camino de los riesgos no financieros a la luz de la actualidad:

i) uniformizar el lenguaje; ii)mapear los riesgos ; iii)entender los controle; iv) reporte adecuado; y, v) hacer del proceso extensivo a toda la compañía y mantenerlo.

http://www.mckinsey.com/business-functions/risk/our-insights/nonfinancial-risk-today-getting-risk-and-the-business-aligned?cid=other-eml-alt-mip-mck-oth-1702

En el camino de la preparación del SOC 2

Hay una tendencia hacia la sustitución de las aplicaciones de TI hechas internamente, sistemas y procesos relacionados con servicios de terceros. Sin embargo, la confidencialidad de la información al cliente, los secretos comerciales y los datos de los empleados hacia partes externas han hecho que las organizaciones deban demostrar que los datos y los sistemas están bien controlados y disponibles, independientemente de dónde éstos residan.

Aunque la responsabilidad de gestionar el riesgo de TI residirá siempre dentro de la organización, la carga de asegurar que los controles apropiados para los procesos y sistemas tercerizados sean correctos está siendo dirigida hacia al proveedor del servicio. De este enfoque en el entorno de la organización de servicios ha surgido una serie de cuestionarios de seguridad y control y de auditorías a proveedores. Para muchos especialistas, el informe de Control de Organización de Servicios (SOC 2), emitido por un auditor de servicios, se ha convertido en el estándar de elección.

En este artículo que se obtiene bajo registro sin costo en Protiviti, se explica a mayor detalle el contenido del SOC 2, incluyendo los 5 principios de servicios de confianza (TSP por sus siglas en inglés)

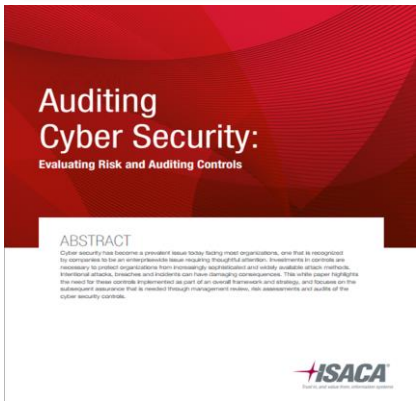
https://www.knowledgeleader.com/KnowledgeLeader/Content.nsf/Web+Content/ARTOntheRoadtoSOC2Readiness!OpenDocument

Auditando ciber seguridad

Este documento de registro libre es elaborado por ISACA.

Hoy, todas las empresas están proecupadas por violaciones o robos de sus bases de datos, pédida de confianza del consumidor y severas multas producto de los riesgos de ciberseguidad. Como respuesta, se están inviertiendo grandes cantidades de dinero en barreras de protección. ¿Cuál es el mejor lugar para invertir el dólar adicional?¿ El monto invertido es el correcto? ¿La infraestructura actual es suficiente? Para responder estas preguntas ISACA recomienda: a) evaluar los riesgos actuales y emergentes de la orgzanización y b) auditar los controles de seguridad existentes y por implementarse.

En esta guía se desarrollan ambos aspectos.



https://www.isaca.org/Pages/DocumentDownloadRegistration.aspx?file=http%3a%2f%2fwww.isaca.org%2fKnowledge-Center%2fResearch%2fDocuments%2