Faro de Auditoría

Boletín Flash del Comité Latinoamericano de Auditoría Interna (CLAIN)

FELABAN

No.13 –Octubre 2016

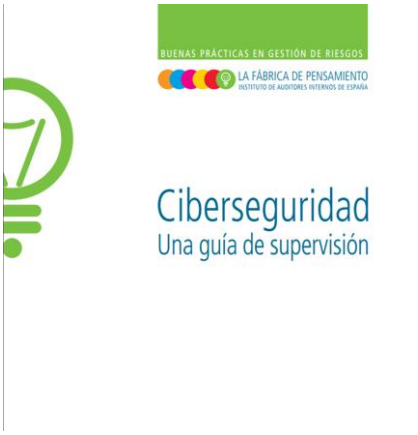
Ciberseguridad: una guía de supervisión

La edición No.12 de nuestro Faro de Auditoría terminó con la excelente noticia de la publicación de la Guía Práctica "Evaluando el Riesgo de Ciberseguridad". Dicha GTAC no solo nos habla sobre la identificación de los principales riesgos asociados a la ciberseguridad, sino principalmente al rol y responsabilidad de cada una de las 3 líneas de defensa, en su gobierno y gestión.

En esta ocasión, la Escuela del Pensamiento del Instituto de Auditores de España también nos sorprende con la publicación de su Guía de Supervisión de Ciberseguridad.

Los ciberdelitos le cuestan a España unos 14,000 millones de euros al año; por ello la ciberseguridad se ha convertido en uno de los principales bastiones de control en las entidades.

Esta guía nos introduce 20 controles críticos de seguridad que todas las organizaciones deben implementar y el rol de auditoría interna en la revisión de cada uno; también nos da un interesante panorama sobre los distintos enforques o marcos de gobierno para la gestión del riesgo de seguridad; finalmente lista una serie de certificaciones profesionales sobre ciberseguridad.



https://auditoresinternos.es/uploads/media_items/guia-supervision-ciberseguridad-fabrica-pensamiento-iai.original.pdf

El fantasma en la máquina: administrando el riesgo tecnológico

La "tecnología" es un sinónimo de la banca. Desde los algoritmos utilizados en las estrategias de trading de la cartera propia a las aplicaciones móviles que los clientes utilizan al depositar cheques y pagar cuentas, la tecnología soporta y mejora cada movimiento que hacen los bancos y sus clientes.

McKinsey recomienda que la mitigación de los riesgos de tecnología requiere de un esfuerzo coordinado que va más allá de respuestas centradas sólo en los equipos de TI. Bancos líderes están creando equipos especializados dentro del grupo de la administración integral de riesgos para gestionar el riesgo tecnológico, en todas sus manifestaciones, a través de las organizaciones.

Para ello sugiere 6 principios que dichos equipos deben utilizar para estar bien interconectados e integrados con el resto del banco.

http://www.mckinsey.com/business-functions/risk/our-insights/the-ghost-in-the-machine-managing-technology-risk?cid=other-eml-alt-mip-mck-oth-1610

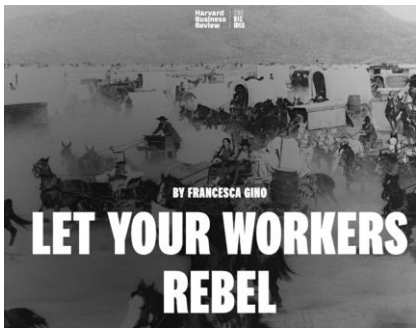
Smart Device : pago inteligente 2.0

Este interesante artículo de Deloitte University Press nos resume sus puntos de vista respecto al impacto que está teniendo en la economía de los Estados Unidos y del resto del globo, el incremento exponencial del uso de teléfonos móviles para realizar transacciones financieras, principalmente pagos, en tiendas. Es tal el impacto, que se está redefiniendo el ecosistema de dichos pagos (mPay-at-POS).
También nos muestra un pantallazo interesante sobre los retos de una más rápida aplicación de los pagos móviles y sus tendencias; la rapidez de la transaccionalidad -por ejemplo 18 países han implementado alguna versión de pago en tiempo real y 12 lo están explorando-; cómo las soluciones de pagos móviles requerirán de colaboración más que de competencia entre "*constelaciones*"; y finalmente la recomendación de 4 estrategias para facilitar esta colaboración: a) buscar la colaboración; b) flexibilizar los lazos que atan; c) encontrar maneras de reducir los costos de transferencia; d) ganar al contribuir en un valor conjunto, no por la asfixia de sus socios.

http://dupress.deloitte.com/dup-us-en/industry/telecommunications/faster-payments-system-mpayments.html?id=us:2em:3na:dup3418:awa:fsi:102016

Deje a sus colaboradores rebelarse

En esta oportunidad hemos seleccionado un tema totalmente distinto al de la auditoría y gestión de riesgos; pero que indirectamente nos atañe pues como auditores necesitamos avivar nuestra creatividad.
Mantener a los colaboradores comprometidos es un problema. Para solucionarlo, anímelos a romper las reglas y a ser ellos mismos. En este artículo de Francesca Gino publicado en Harvard Business Review, se nos muestra quién lo hace bien y cómo podemos hacerlo .
Hay que decirle ¡NO al conformismo! y promover una "incorformidad constructiva". Consejos:
1. Dele la oportunidad a sus colaboradores de ser ellos mismos
2. Aliéntelos a sacar a relucir sus propias fortalezas
3. Cuestione el *status quo*
4. Cree experiencias retadoras
5. Fomente perspectivas más amplias
6. Anime opiniones divergentes



https://hbr.org/cover-story/2016/10/let-your-workers-rebel?referral=03692&cm_mmc=email-_-newsletter-_-thebigidea-_-20161024&utm_source=thebigidea&utm_medium=email&utm_campaign=promo_20161024&spMailingID=15724878&spUserID=ODEzNDA3NDIzNzAS1&spJobID=881851174&spReportId=ODgxODUxMTc0S0

COSO: Guía de la Gestión del Riesgo de Fraude

Desde la publicación de la versión 2013 del Marco de Control Interno COSO, donde se introducen los 17 principios básicos, la evaluación del Octavo Principio "la organización considera el potencial de fraude al evaluar los riesgos para el cumplimiento de objetivos" tal vez ha sido el reto principal.
Relevar y documentar cómo se evalúa el fraude tanto a nivel entidad como a nivel de procesos y unidades de negocio ha sido una tarea implementada de muy diversas formas y hasta antes de la publicación de este documento, no se podía aseverar la existencia de una "mejor práctica". La nueva guía, con un costo reducido para los miembros de IIA, ayuda a responder esta necesidad.

http://www.coso.org/documents/COSO-Fraud-Risk-Management-Guide-Executive-Summary.pdf