Faro de Auditoría

Boletín Flash del Comité Latinoamericano de Auditoría Interna (CLAIN)

FELABAN

27 – DICIEMBRE 2018

En esta edición, seguimos profundizando en tendencias, a través de un Reporte de Investigación de la Fundación del IIA referido a la **Alineación de Auditoría Interna con la Estrategia Organizacional** y del Blog de Richard Chambers que nos invita a una **Revisión de las prioridades de auditoría interna para el año 2019**. También se hace referencia a la Guía Complementaria reciente del IIA Global sobre la **Auditoría a la gestión de riesgos de terceros**. Compartimos documento del IIA de España sobre las **Siete preguntas que un Consejero debe plantearse para la supervisión del reglamento general de protección de datos de Europa (RGPD).** Además, información sobre seminario efectuado en Chile de la Industria Financiera: **"Desafío de la Auditoría Interna en la Era Digital"**, donde FELABAN y el Comité CLAIN patrocinaron el evento y donde estuvo presente el Sr. Henry Bolaños, presidente de nuestro Comité. Finalmente, en su visita en noviembre a Chile, el Sr. Bolaños compartió con el Auditor General del Gobierno de Chile, Sr. Eugenio Rebolledo, reunión donde se interiorizó de los documentos técnicos que emite el Consejo de Auditoría General de Gobierno de Chile (CAIGG), siendo uno de los últimos, el **Modelo de Madurez/Capacidad para el Sistema de Prevención de Delitos LA/FT/DF en el Sector Público**, el que como modelo y evaluación de madurez de sus componentes puede ser homologado a la industria financiera.

Hernan Rebolledo Migliardi, CIA, CRMA y QA IIA, ISO 31000, 22301 y 27005
Coordinador Boletín FARO CLAIN-FELABAN.

I.- TENDENCIAS

1.- Reporte de Investigación de la Fundación del IIA, nos invita a analizar: "Alineación de las actividades y alcance de la auditoría interna a la Estrategia organizacional". Las preguntas son:

¿Cómo el entorno de negocios y la estrategia organizacional impacta a la Auditoría Interna?
El entorno empresarial actual está cambiando constantemente, y muchas organizaciones están cambiando su Estrategia para hacer frente a este entorno vibrante.

¿Cómo afecta el cambio a la función de auditoría interna?
¿En qué niveles impacta la estrategia de la organización el alcance y el rol de la auditoría interna?

Para comprender la alineación entre la estrategia y la función de auditoría interna, el proyecto de investigación fue dividido en dos fases.

En primer lugar, los jefes de auditoría (CAE) y el comité de auditoría, donde los miembros fueron entrevistados

En segundo lugar, se envió una encuesta a los auditores internos a través del AII. Red en América del Norte. Las personas entrevistadas o encuestadas operan en diversas industrias en Sectores financieros y no financieros.

El análisis combina las respuestas de la entrevista con los resultados de la encuesta. En consecuencia, los siguientes los resultados emergen:

- El entorno cambiante requiere que la función de auditoría interna tenga una planificación dinámica para poder adaptarse a la misma velocidad en que cambian los riesgos estratégicos.
- Los riesgos estratégicos se hacen cada vez más importantes. Sin embargo, la función de auditoría interna no los considera una prioridad máxima.
- El entorno empresarial se vuelve cada vez más digital y los riesgos de TI crecen en importancia.
- La digitalización está afectando los cambios en las habilidades requeridas de los auditores internos. Las habilidades de TI (particularmente las habilidades de análisis de datos) son consideradas cada vez más entre las más importantes.
- Las demandas de servicios de asesoría y consultoría han aumentado con el tiempo. Esto es una consecuencia del entorno empresarial cambiante y digitalizado.
- Los perfiles estratégicos específicos influyen en la externalización de las actividades de auditoría interna. Esto implica estrategias basadas en fusiones, adquisiciones, diversificación no relacionada e integración vertical. La subcontratación de las actividades de auditoría interna requiere un mayor nivel de coordinación entre los auditores internos debido a la combinación de personal interno y externo.
- Las organizaciones que atraviesan importantes cambios estructurales (debido a fusiones, adquisiciones, diversificación no relacionada e integración vertical) parecen externalizar más sus actividades de auditoría interna. Esto puede verse como una solución (temporal) para compensar las habilidades faltantes o un aumento significativo en la carga de trabajo de auditoría debido a estos cambios estructurales.
- El nivel de credibilidad de la función de auditoría interna otorgada por los auditados, la administración y la junta, afecta la comprensión de la estrategia por parte de los auditores internos.

Para mayores detalles, link a: https://na.theiia.org/iiarf/Pages/Latest-Research-and-Products.aspx

2.- El Blog de Richard Chambers, del 19 de noviembre de 2018, nos invita a: **"Una mirada temprana a las prioridades de auditoría interna para 2019".** En forma resumida señala: Dos informes recientemente publicados, uno de Gartner Inc. y otro de la Confederación Europea de Institutos de

Auditoría Interna (ECIIA), identifican a un enemigo familiar como el **principal riesgo para 2019: la ciberseguridad.** A lo largo de los años, este desafío para las organizaciones ha escalado constantemente la jerarquía de riesgos en los informes anuales. También nos ha abierto los ojos a otras categorías de riesgo, ya que nuestra comprensión del ciberespacio se vuelve más sofisticada y nuestros enfoques para su gestión maduran.

De hecho, el enfoque en la seguridad cibernética nos ha ayudado a comprender que la tecnología y los datos están inexorablemente entrelazados, y ha aumentado nuestra conciencia del riesgo relacionado con el gobierno y la privacidad de los datos. Nos ha llevado a ser más conscientes de los riesgos relacionados con las relaciones con terceros, el gobierno de TI y la cultura.

Por ejemplo, cuatro de los cinco riesgos principales en el **informe de Gartner** pueden derivarse de nuestro enfoque en la ciberseguridad: **la preparación de la ciberseguridad, la privacidad de los datos, la gobernanza de los datos y el riesgo de terceros.**

Risk in Focus 2019, el informe desarrollado y producido por ECIIA, **agrupa la ciberseguridad, el gobierno de TI y los riesgos de terceros en una categoría.** Otra categoría en el informe ECIIA **es la protección de datos y las estrategias en un mundo posterior a GDPR (**Reglamento General de Protección de Datos).

Los datos y la tecnología también son fundamentales para las discusiones sobre **riesgos en digitalización, automatización e inteligencia artificial**. Estas discusiones demuestran claramente el desafío de equilibrar el riesgo y la oportunidad. Como señala el informe ECIIA*: "Los beneficios de costo y eficiencia de la automatización y otros procesos digitales pueden ser transformadores, si se aprovechan a su máximo potencial. Pero las organizaciones también deben considerar el riesgo asociado con dicha transformación".*

Al preparar sus **planes de auditoría interna para el año 2019, debe asegurarse de haber considerado todos los riesgos que enfrenta su organización y discutirlos con sus comités de auditoría y la administración ejecutiva.** La lista no es de ninguna manera completa ni necesariamente aplicable a todas las organizaciones.

https://iaonline.theiia.org/blogs/chambers/2018/Pages/An-Early-Look-at-Internal-Audit-Priorities-for-2019.aspx

II.-GUIAS COMPLEMENTARIAS

El Instituto de Auditores Internos IIA Global, en octubre del año 2018, emitió la GUIA:

Auditoría a la gestión de riesgos de terceros

Las organizaciones aprovechan y confían en proveedores externos, así como en proveedores de servicios secundarios o de "terceros" para llevar a cabo actividades comerciales.

Estas relaciones continúan expandiéndose y evolucionando, lo que presenta numerosos riesgos que la organización debe evaluar y gestionar de forma adecuada y continua para lograr los resultados de negocio deseados. En las industrias reguladas, los tribunales de justicia y la opinión pública, una organización no puede escapar a la culpa, incluidas las repercusiones potencialmente graves en términos de reputación o sanciones económicas, si un proveedor tercero no cumple con lo contratado o sufre su propio evento desafortunado o prácticas poco éticas.

Debido a que las organizaciones y sus clientes pueden sufrir consecuencias adversas como resultado de las acciones (o la inacción) de sus proveedores externos, los reguladores y las organizaciones que generan estándares para algunas industrias (por ejemplo, servicios financieros), han establecido reglas, regulaciones y orientación con respecto a la gestión de proveedores terceros.

Estas reglas pueden exigir modelos sofisticados de gestión de riesgos de terceros, pero los principios utilizados para construir estos requisitos son adaptables a otras industrias que pueden no tener puntos de referencia o parámetros definidos para guiarlos en el desarrollo y la ejecución de la gestión de riesgos de terceros.

Esta guía presenta a los auditores internos el concepto de un marco de gestión de riesgos de terceros como un elemento de un marco de gestión de riesgos empresarial más amplio. También considera que las organizaciones pueden tener distintas formas y tamaños, con diferente disponibilidad de recursos, herramientas y técnicas.

Con ese fin, esta guía apoya a los auditores internos para que aprendan los objetivos del proceso de selección y administración de proveedores externos de la organización. También proporciona consideraciones prácticas para desarrollar una auditoría de los marcos de gestión de riesgos de terceros de la organización.

Aprender los elementos de los procesos de gestión de riesgos de terceros de una organización puede permitir que la función de auditoría interna identifique las áreas donde la organización puede obtener un valor adicional de sus relaciones con terceros al tiempo que ayuda a la organización a protegerse de una exposición innecesaria al riesgo.

La guía aborda preguntas como:

- ¿Tiene la organización un inventario completo de sus proveedores externos?
- ¿El programa de gestión de riesgos de terceros de la organización se alinea con su apetito de riesgo?
- ¿Tiene la organización una lista de los tipos de riesgos (reputación, estrategia, cumplimiento, recursos financieros, recursos humanos, TI, etc.) que pueden plantear los terceros?
- ¿Cómo identifica, define y administra la organización los riesgos de terceros?
- ¿Cuáles son los criterios de evaluación apropiados para los riesgos de terceros (por ejemplo, escalas de impacto y probabilidad)?
- ¿Cómo mide la organización el impacto que los terceros individuales pueden tener en su estrategia de continuidad del negocio?
- ¿Qué tan abajo en la cadena de suministro deben considerarse los terceros? ¿Deben supervisarse los proveedores de servicios secundarios o de terceros?
- ¿Qué métricas deben revisarse para garantizar que un proveedor externo se desempeña dentro de la tolerancia al riesgo de la organización?
- ¿La organización podrá recurrir para recuperar los daños de un tercero si surgen problemas?
- ¿Los contratos con terceros incluyen el derecho a que la actividad de auditoría interna de la organización contratante u otras funciones de control realicen auditorías si existe la necesidad o el deseo de hacerlo?
- ¿El tercero está manejando datos que requieren un nivel específico de control? ¿Cómo valida la organización que el tercero sigue todas las leyes, regulaciones y requisitos técnicos relevantes para la seguridad de los datos?
- ¿Cómo coordina la auditoría interna con la segunda línea de defensa de la organización (por ejemplo, legal, cumplimiento, adquisiciones) que puede estar realizando actividades de administración de riesgos con respecto a terceros?
- ¿Cómo garantiza la organización el comportamiento ético de los terceros?

https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Auditing-Third-Party-Risk-Management-Practice-Guide.aspx

III.- IIA ESPAÑA

El Instituto de Auditores Internos de España, nos comparte el documento **EDICION CONSEJEROS: SUPERVISIÓN DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS: SIETE PREGUNTAS QUE UN CONSEJERO DEBE PLANTEARSE:**

Como es sabido, a partir del 25 de mayo de 2018 es obligatorio implantar el Reglamento General de Protección de Datos (RGPD) para todas las organizaciones establecidas o con relaciones comerciales con la Unión Europea. Las exigencias de cumplimiento, y las penalizaciones en caso contrario (que podrían

llegar a alcanzar hasta 20 millones de euros o el 4 % de la facturación anual), pueden tener consecuencias económicas, legales y reputacionales muy importantes.

El Reglamento no solo es de aplicación a las organizaciones ubicadas en la Unión Europea, sino también a otras que, encontrándose fuera de ella, ofrezcan productos o servicios, o monitoricen el comportamiento de ciudadanos de la Unión Europea.

Las comunicaciones de datos transfronterizas podrán llevarse a cabo siempre que las normas de protección de datos de los países de destino sean similares a la norma RGPD.

Los Consejos de Administración tienen un papel fundamental en sus organizaciones para supervisar que el cumplimiento del nuevo Reglamento tiene un enfoque de privacidad basado en riesgos y proporciona una seguridad razonable que se han destinado los recursos necesarios para proteger los derechos y libertades de las personas físicas.

Este documento aborda 7 cuestiones clave que un consejero debe tener en cuenta para garantizar que su organización alcanza la conformidad con el nuevo Reglamento.

1.- ¿La entidad es consciente de que la conformidad con el nuevo reglamento va más allá de la adaptación de los controles actuales de ciberseguridad?

2.- ¿La organización tiene diseñado e implantado un Modelo de Gobierno de la Privacidad?

3.- ¿Se ha asignado un Delegado de Protección de Datos (Data Protection Officer - DPO) que reporte directamente al consejo u otros miembros de la alta dirección?

4.- ¿La entidad realiza Evaluaciones de Impacto de Privacidad (Privacy Impact Assessment - PIA) para los procesos de tratamiento de datos?

5.- ¿Se ha establecido un procedimiento de actuación en caso de fugas de información?

6.- ¿Ha implantado la organización un programa de concienciación sobre la protección de datos dirigido a empleados?

7.- ¿Se ha definido formalmente un modelo de relación entre el DPO (Data Protection Officer - DPO), y el área de Auditoría Interna?

https://auditoresinternos.es/uploads/media_items/rgpd-7-preguntas-consejeros.original.pdf

IV.- IIA CHILE

El Sr. Henry Bolados, Presidente del Comité Latinoamericano de Auditoría Interna y Evaluación de Riesgos de la Federación Latinoamericana de Bancos, FELABAN recibe Galvano de Reconocimiento por ser patrocinador de seminario de la Industria Financiera: **"Desafío de la Auditoría Interna en la Era Digital"**, de mano del Presidente del IAI Chile don Eladio Piña.

En el seminario se debatió y relevó la necesidad de fortalecer la auditoría interna financiera frente a las fuerzas disruptivas actuales, donde lo digital toma un rol central.

En el seminario se desarrollaron presentaciones de Directores de Empresas, de líderes del mundo de la transformación digital, experiencias de Bancos sobre innovación (Bancocolombia) auditoría ágil (Itau Unibanco) y de ciberseguridad, entre lo más relevante.

https://iaichile.org/eventos/seminario-sector-financiero-desafio-de-la-auditoria-interna-en-la-era-digital/

V.- Consejo Auditoría Interna General de Gobierno - CAIGG CHILE

El Sr. Henry Bolados, presidente del Comité Latinoamericano de Auditoría Interna y Evaluación de Riesgos de la Federación Latinoamericana de Bancos, FELABAN se reunió con el Auditor General de Gobierno de Chile, Sr. Eugenio Rebolledo y su equipo de Estudios (Sr., Ricardo Correa y Sra. Camila Rojas).

En la reunión, el Auditor General efectuó reseña de los documentos técnicos que han emitido para apoyar a la red de auditores internos de servicios/empresas públicas y presentó en detalle el **Modelo de Madurez/Capacidad para el Sistema de Prevención de Delitos LA/FT/DF en el Sector Público.**

http://www.auditoriainternadegobierno.gob.cl/wp-content/upLoads/2018/10/DOCUMENTO-TECNICO-N-107-MODELO-DE-MADUREZ.pdf
http://www.auditoriainternadegobierno.gob.cl/publicacion/otros-documentos-relacionados/