Edición Invierno 2017

KPMG

La Gaceta

Instituto de Comités de Auditoría
Temas relevantes para los directores y alta gerencia

La nueva mentalidad en la seguridad cibernética: El foco del Directorio.

En esta edición, presentamos los siguientes tópicos:

- La nueva mentalidad en la seguridad cibernética.
- Estar preparado para las nuevas normas NIIF – 2017.

¿En las reuniones de Directorio, los riesgos cibernéticos y las discusiones sobre seguridad tienen el mismo ritmo que los negocios? Mejor aún, ¿tiene la junta directiva la seguridad de que las operaciones, la tecnología y la gestión de riesgos están comunicándose sobre expectativas y prioridades cibernéticas?

En el Webcast del Comité de Auditoría de KPMG US / NACD más reciente, el Copresidente Global de Cyber Seguridad de KPMG, Greg Bell, detalló que los componentes de un marco cibernético maduro pueden ayudar a los directores corporativos a evaluar las capacidades cibernéticas de sus empresas.

"La cibernética está mucho más relacionada a la estrategia de negocios de su empresa y planes de innovación que a la arquitectura tecnológica", dijo Bell. "Cuando las empresas hablan de riesgos cibernéticos, ese debe ser el foco".

"Estamos haciendo negocios de manera diferente. Es muy raro que todas las funciones empresariales de una empresa existan dentro de sus propias paredes", dijo Bell. "Las cadenas de suministro, los socios de negocios y las relaciones de outsourcing están manejando los datos críticos de la empresa, incluidos los datos de los clientes. ¿Cómo protegemos esta información y nos aseguramos que estamos prestando la debida atención? "

Por ejemplo, Bell relató reuniones separadas, celebradas a horas de distancia, en las cuales los ejecutivos de la misma empresa detallaron sus respectivos enfoques sobre el uso de intermediarios y agentes de terceros para adquirir nuevos clientes. El ejecutivo de tecnología se estaba preparando para revisar los sistemas de la compañía para defenderse contra los hackers cibernéticos de información de los clientes a través de la infraestructura tecnológica de terceros. Mientras tanto, el ejecutivo de negocios ya había establecido planes para eliminar totalmente a terceros.

"El negocio se movía a un ritmo tan rápido que la capacidad cibernética no podía ponerse al día", dijo Bell. "Ese es el riesgo que enfrentamos hoy en día". De hecho, de los principales riesgos cibernéticos identificados en una reciente encuesta del Comité de Auditoría (2017 Global Audit Committee Pulse Survey), los sistemas de tecnología fueron sólo uno de los cuatro principales desafíos. Los otros tres se centraron en los negocios:

la vulnerabilidad de la cadena de suministro, el riesgo de las personas y la conciencia organizacional.

El marco de la madurez cibernética

Los actuales marcos de seguridad cibernética se enfocan muy poco en la gobernabilidad y el papel de la junta directiva, dijo Bell. La ampliación del alcance del marco existente de seguridad cibernética de la empresa al consejo puede definir y aclarar cómo el consejo se involucra con la administración en asuntos cibernéticos.

"El elemento más importante es el liderazgo y la gobernabilidad", dijo Bell. "¿Cómo está alineada la organización tecnológica con el negocio? La gerencia realmente necesita asegurarse de que pueden explicar eso a la junta. "

Bell analizó las líneas de investigación en seis áreas de supervisión de la junta, así como los indicadores clave de desempeño (KPIs) relacionados que pueden servir como un tablero para ayudar a la junta a evaluar el entorno cibernético.

Supervisión del Directorio	Líneas de indagación	¿Cómo gana comodidad el Directorio? (Ejemplo de KPI)
Liderazgo y gobernabilidad	Comprensión de la estructura de gobierno y reunirse con el equipo de liderazgo Revisión de la producción de la evaluación de la capacidad Revisar y aprobar la estrategia y las solicitudes de financiación Participar en la educación general del consejo Solicitar actualizaciones periódicas del programa	Gastos de seguridad como porcentaje del presupuesto general de TI Revisión del rendimiento de la capacidad madurez Certificaciones en las posiciones de liderazgo clave Número de sesiones de educación del consejo (frecuencia)
Factores humanos	Establecer el tono para la cultura Revisar patrones / tendencias de asuntos sobre el personal Entender los protocolos de entrenamiento y conciencia	Porcentaje de empleados / contratistas que asisten a la capacitación Tendencias relacionadas con cyberseguridad denunciante o informadas a la hotline
Gestión de la información	Comprender el enfoque de gestión de riesgos y su vinculación con el riesgo empresarial Revisar y aprobar el riesgo tolerable Entender el programa de proveedores externos Revisar y cuestionar las métricas del programa	Resultados de la evaluación de riesgos / vinculación con el programa ERM Métricas y mediciones del riesgo tolerable Número de proveedores externos de alto riesgo y revisión del estado de los mismos Revisión de las métricas de salida
Continuidad del negocio y gestión de crisis	Comprender la capacidad de respuesta actual Revisar el estado de madurez del plan general Reunirse con el personal de comunicaciones Participar en los ejercicios de simulación	Número de procesos críticos con planes en marcha Número de simulacros (frecuencia) y resultados
Operaciones y tecnología	Comprender la madurez actual de la estructura de control Seleccionar controles marcos y revisar la relevancia Revisar las métricas de tendencia de incidentes relevantes Reunirse con CIO o equivalente para entender la integración de la informática con las tendencias de información tecnológica.	Porcentaje de activos de "corona / joya" incluidos en el monitoreo de cobertura Clasificación de riesgo de vulnerabilidades de seguridad (considerando el valor de los activos) Mediciones de tendencias de incidentes cibernéticos
Aspectos legales y cumplimiento	Evaluación comparativa de políticas de seguridad cibernética con organizaciones similares	Evaluación comparativa de políticas de seguridad cibernética con organizaciones similares

Edición Invierno 2017

La Gaceta

Instituto de Comités de Auditoría

Temas relevantes para los directores y alta gerencia

Perspectivas para los Directores

Los directores deben permanecer vigilantes, pero es más importante mantenerse enfocados. Este es un área que puede demandar mucha energía y tiempo. Si bien está claro que el riesgo cibernético es un hecho al hacer negocios hoy en día, va a seguir evolucionando y planteando nuevos desafíos.

El Directorio debe considerar lo siguiente en sus discusiones con la gerencia:

Aprender a vivir con el riesgo cibernético.

Entender que es un desafío y una oportunidad para toda la empresa.

- La cibernética es un asunto de negocios que afecta a la empresa en su estrategia, operaciones, cadena de suministro, regulación, reputación y más.
- Comunicaciones y reportes regulares al Directorio son críticos, idealmente con un panel de control y KPIs robustos. Establecer un ritmo, conocer a la gente, ser mejor educados.
- Se trata de la cultura y la actitud de la administración superior. ¿Están el CEO y sus ejecutivos haciéndose escuchar sobre la importancia de la buena higiene cibernética?

Manténgase al corriente de las prácticas de la industria y conéctese con la aplicación de la ley.

¿Cómo se adapta el directorio a las tendencias del sector y a las mejores prácticas? ¿Está la empresa aplicando la ley de manera proactiva para entender las tendencias en el riesgo cibernético y la respuesta?

Tener un plan de preparación y respuesta de incidentes.

Se producirán incumplimientos. ¿Tiene la compañía un plan de contingencia claro que ha sido revisado y testeado? ¿Quién dirige el equipo de respuesta a incidentes cibernéticos? ¿Qué pasa con los planes de continuidad de negocios?

Estar preparado para las nuevas normas NIIF – 2017

En este trimestre no ha habido nuevas actualizaciones adicionales a aquellas que fueron cubiertas en nuestras Gacetas anteriores.

Mirando hacia el futuro, la NIIF 9 Instrumentos financieros y la NIIF 15 Ingresos de contratos con clientes, que serán de aplicación efectiva en 2018, tendrán un impacto significativo.

La NIIF 16 es de aplicación efectiva en 2019, no obstante su aplicación anticipada está permitida para aquellas entidades que apliquen la NIIF 15.

Dado que además de modificar el tratamiento contable, requerirá de una revisión de los procesos utilizados para producir la información financiera requerida. Esta es la oportunidad para prepararse para la implementación de estos grandes cambios.

Edición Invierno 2017

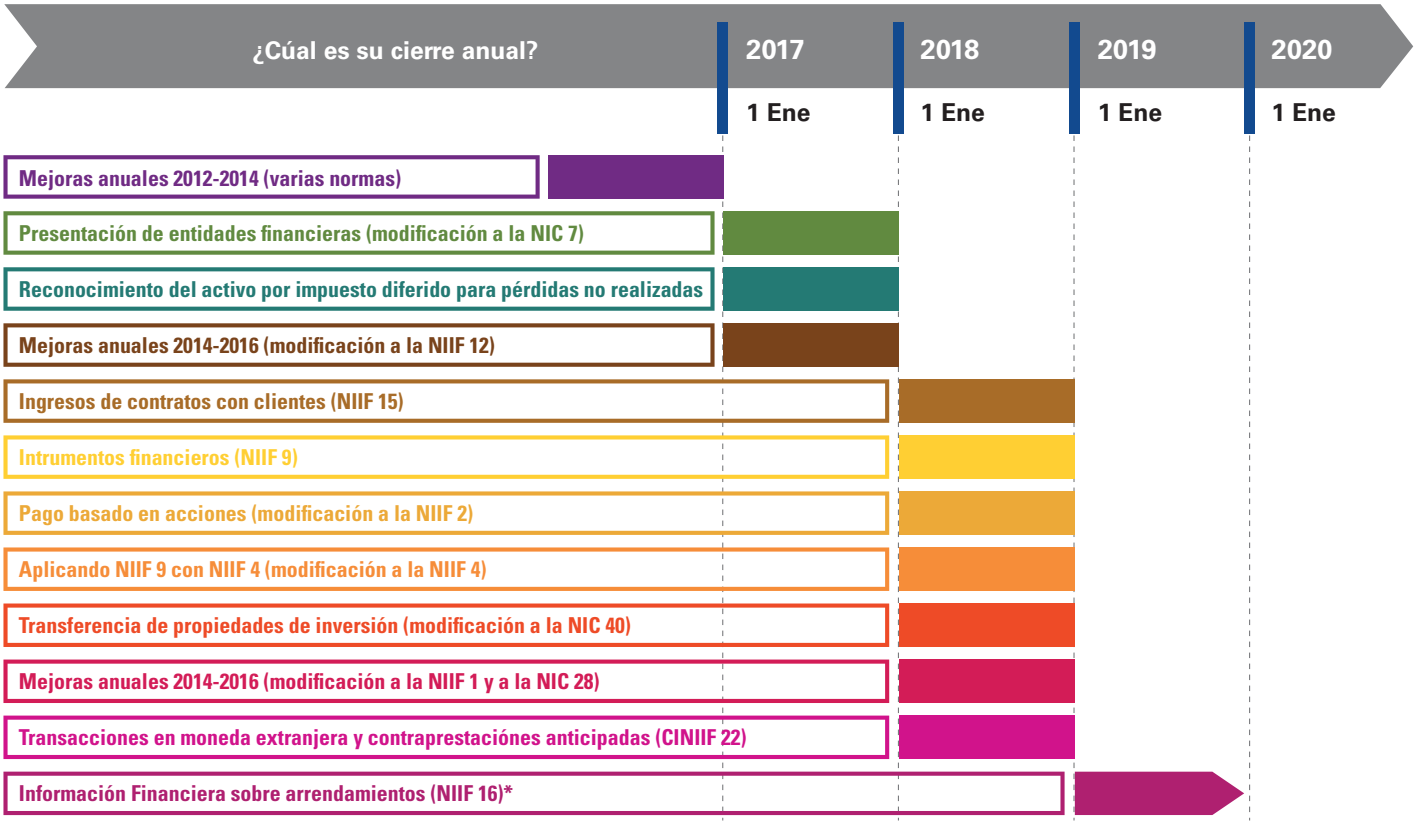
KPMG

La Gaceta

Instituto de Comités de Auditoría

Temas relevantes para los directores y alta gerencia

¿Qué normas son obligatorias para mi cierre anual?



Cómo leer el gráfico

Identifique su inicio de su ejercicio financiero en la línea de tiempo. Cada una de las barras contiene una norma e indica si ya es de aplicación efectiva o no y si es factible su aplicación en forma anticipada.

Por ejemplo, si sus estados financieros inician el 1 de enero de 2017, entonces las normas desde presentación de entidades financieras hasta mejoras anuales 2014-2016 (modificación a la NIIF 12) son de aplicación obligatoria por primera vez. El resto de las normas no son de apicación obligatoria en los estados financieros con fecha de cierre 31de diciembre de 2017.

* La aplicación anticipada de la NIIF 16 Información Financiera sobre arrendamientos está permitida solo para Compañías que también aplican la NIIF 15 Ingresos de contratos con clientes.

Referencia

Norma aún no efectiva, pero disponible para adopción anticipada.

Norma efectiva para aplicar por primera vez.

Edición Invierno 2017

La Gaceta

Instituto de Comités de Auditoría

Temas relevantes para los directores y alta gerencia

Nuevas normas efectivas

Nuevas normas efectivas que deben ser consideradas para estados financieros a partir del 1 de enero de 2017.

Efectivas para año de cierre	Norma
1 de enero de 2017	Iniciativa de revelaciones (Modificaciones a la NIC 7).
	Reconocimiento del activo por impuesto diferido de ganancias no realizadas (Modificaciones a la NIC 12).
	Mejoras anuales a las NIIF - ciclo 2014-2016 - (modificaciones a la NIIF 12).

Normas aún no efectivas, pero disponibles para su aplicación anticipada

Las normas detalladas a continuación aún no son obligatorias para ninguna entidad, pero estan diponibles para se aplicadas en forma anticipada. Incluso si usted no está adoptando anticipadamente, el impacto de exposición de la NIC 8 debe proporcionarse, tanto los inversores como los reguladores esperan progresivamente mas información cualitativa y cuantitativa sobre el impacto de las nuevas normas del alcalde como su enfoque de fecha efectiva.

Efectivas para año de cierre	Norma
1 de enero de 2018	NIIF 15 Ingresos de contratos con clientes.
	NIIF 9 Instrumentos financieros.
	Pago basado en acciones (modificación a la NIIF 2).
	Aplicando NIIF 9 Instrumentos financieros con NIIF 4 contratos de seguros (Modificaciones a la NIIF 4).
	Transferencia de propiedades de inversión (modificación a la NIC 40).
	Mejoras anuales a las NIIF - ciclo 2014-2016 - (modificación a la NIIF 1 y a la NIC 28).
	CINIIF Transacciones en moneda extranjera y contraprestaciónes anticipadas.
31 de diciembre de 2019	NIIF 16 Información financiera sobre arrendamientos.

Dónde consultar

Para mayor información acerca de la vigencia de las nuevas normas, no dude en consultarnos en **ica@kpmg.com.ar**

Acerca de los Institutos del Comité de Auditoría de KPMG

Patrocinado por más de 30 firmas miembro en todo el mundo, los Institutos del Comité de Auditoría de KPMG (ACI por sus siglas en inglés) brindan a los miembros de los comités de auditoría y a los directores conocimientos prácticos, recursos y oportunidades de intercambio entre pares con foco en el fortalecimiento de la supervisión de la emisión de información financiera y de la calidad de la auditoría, así como la variedad de desafíos que enfrentan los Directorios de las empresas de hoy – desde la problemática de la gestión del riesgo y de las nuevas tecnologías hasta las cuestiones relacionadas con la estrategia y el cumplimiento.

Para conocer más sobre los programas del ACI, póngase en contacto con nosotros en: ica@kpmg.com.ar

Contáctenos

Para más información, por favor visítenos online en **www.kpmg.com/AR/ICA**, envíenos un email a ica@kpmg.com.ar o contacte a:

Néstor García
Socio Líder de Auditoría
T: +54 11 4316 5870
E: nrgarcia@kpmg.com.ar

Guillermo Calciati
Socio
T: +54 11 4316 5802
E: grcalciati@kpmg.com.ar

Viviana Picco
Socia
T: +54 11 4316 5729
E: vpicco@kpmg.com.ar

kpmg.com.ar

@KPMGArgentina
KPMG Argentina
KPMG Argentina
KPMG AR Talentos

Diseñado por el equipo de Servicios Creativos - Marketing y Comunicaciones - Argentina.