Instituto Mexicano de
Contadores Públicos

Comisión de Prevención de lavado de dinero y FT

La auditoría interna: Pieza clave para la defensa ante el incremento de ciber amenazas.

Por: Daniel Alberto Ortiz de Montellano Velázquez, CAMS,CFCS

Integrante de la Comisión de PLD/FT y Anticorrupción del IMCP

Texto Original (En inglés): Deloitte. (15 de Agosto de 2016). As Cyberthreats Mount, Internal Audit Can Help Play Defense. Recuperado el 18 de Agosto de 2016, de Risk Management | Deloitte: http://mobile.deloitte.wsj.com/riskandcompliance/2016/08/15/as-cyberthreats-mount-internal-audit-can-help-play-defense-2/

La auditoría interna ha sido una pieza fundamental dentro de las organizaciones desde que las diversas regulaciones, a raíz de la crisis financiera 2008 – 2010, sentaron un marco de supervisión continua y de la evaluación del ambiente de control; Sin embargo, hoy en día, las organizaciones no solo se enfrentan a riesgos financieros, sino también a ciber amenazas que, conforme pasa el tiempo, incrementan su complejidad y su forma de realización.

Considerando a la expansión tecnológica, al aumento en el crecimiento de los datos, a los cambios en los modelos de negocios y los ataques motivados, la amenaza de los ciberataques se encuentra evolucionando constantemente. Diversas estadísticas sugieren que el cibercrimen podría costar a los negocios en 2019 más de 2 billones de dólares, casi 4 veces más que lo pronosticado para 2015.

En respuesta a la creciente amenaza, diversos comités de auditoría y juntas directivas, han puesto su expectativa en que las áreas de auditoría interna, realicen una medición independiente y objetiva de las habilidades con las que cuenta la organización para gestionar los riesgos asociados.

Un primer paso en esta creciente expectativa, es que la auditoría interna realice una medición de los riesgos cibernéticos y presente los hallazgos en un informe para el comité de auditoría y la junta directiva. Lo anterior, podría proveer el soporte necesario para un plan multi anual de auditoría interna basado en riesgos, que permita gestionar los ciber riesgos.

“Las fuerzas que conducen el crecimiento del negocio y su eficiencia también son caminos abiertos para los ciber ataques.” Comentó Michael Juergens, Director de Advisory en Deloitte & Touch LLP.

“Internet, las nubes, los móviles y las tecnologías sociales son plataformas inherentemente orientadas para compartir. Al mismo tiempo, el mantener las fuerzas de trabajo a través de outsourcing está cambiando el control interno, “ añade Michael.

Muchas organizaciones eran midiendo las maneras cibernéticas con múltiples líneas de defensa. Por ejemplo, las unidades de negocio y el departamento de tecnología o sistemas, en muchas organizaciones, integran la administración del ciber riesgo en una toma de decisiones y operaciones diaria, que comprende la primera línea de defensa de la organización.

Para la segunda línea de defensa, son los directores de administración del riesgo tecnológico y de información los que desarrollan protocolos de gobierno corporativo y vigilancia. El monitoreo de operaciones y la toma de acciones necesarias, generalmente las realiza el Director de Seguridad de la Información (CISCO, *Chief Information Security Officer).*

“Cada vez más, muchas empresas están reconociendo la imperiosa necesidad de una tercer linea de defensa cibernética – la revisión independiente de las medidas de seguridad y rendimiento la debe de efectuar él área de auditoría interna.- “ comenta Sandy Pundmann, socia director de Advisory en Deloitte & Touche LLP. “ La auditoría inercia debe de desempeñar un papel integral en la evaluación y en la identificación de oportunidades para fortalecer la seguridad de las empresas. Asimismo, el asesorar a los interesados sobre las tendencias y las prácticas líderes en ciber delitos, es una de las crecientes expectativas de los responsables de esta área” añade Sandy.

Al mismo tiempo, la auditoría interna tiene el deber d e informar al comité de unitaria y a la junta directiva, que los controles de los que son responsables estén funcionando correctamente – una preocupación importante para los directivos es que pueden enfrentar sanciones legales y financieras. Dado que las iniciativas cibernéticas de muchas organizaciones aún están en desarrollo, algunos departamentos de autoría han decidido diferir la auditoría de estos procesos hasta que estén concluidos. Esto podría funcionar para las revisiones de bajo nivel, sin embargo, para la medición de los ciber delitos, no es una solución viable.

Marco de gestión de riesgos cibernéticos

Muchas funciones de auditoría interna han desarrollado y probado procedimientos para evaluar los componentes con los que una organización cuneta para hacer frente a las ciber amenazas. Estas autorizas específicas, tales como el ataque y pe tracción de procedimientos, son valiosas, pero no garantizan del todo que la organización pueda hacer frente a los riesgos cibernéticos. Para proporcionar una visión completa de la capacidad de una organización de ser segura, vigilante y resistente a los riesgos cibernéticos, la auditoría interna debe d e considerar la adopción de un amplio enfoque programático para garantizar los ciber ataques y no realizar solo auditorías específicas ya que le podría dar una falsa sensación de seguridad a la organización.

Al momento de evaluar las ciber políticas, él área de auditoría interna se puede beneficiar de entender las habilidades a través de un gran número de dominios, el cómo se abordan y las lanas que puedan existir dentro de la organización. Hay varios factores que son dignos de mención como profesionales de auditoría interna al realizar la medición de riesgos cibernéticos,

- ***Es vital involucrar a la gente con la experiencia y habilidades necesarias.*** Él área de auditoría interna tiene el “know how” para efectuar las mediciones. De cualquier manera, entender si el departamento de TI o el CISCO están haciendo de manera efectiva su trabajo para modelar los riesgos, puede requerir especialistas en la materia que realicen pregunta

efectivas para ayudar a evaluar la fuerza de los modelos. Un auditor de tecnología orientado en el mundo cibernético puede ser un recurso indispensable.

- ***Es importante evaluar el marco de políticas cibernéticas en su totalidad y no sólo escoger pequeñas muestras.*** Esta evaluación involucra un entendimiento múltiple de los componentes del plan, incluyendo el estado actual de las políticas comparado con las características del marco de gestión; si la organización está avanzando con respecto a implementar un plan de contingencia cibernética y las mínimas prácticas esperadas dentro de la industria.

- ***La evaluación inicial debe de ser general.*** La primera mención no debe de ser exhaustiva ni tampoco debe de requerir pruebas complejas. Al contrario, debe de estar orientada a los riesgos y a la preparación de la organización para enfrentar los ciberataques,

Análisis de la Madurez

Algunas organizaciones prefieren utilizar un enfoque de análisis de la madurez, en lugar de una estrategia de gestión de riesgos. " Un análisis de madurez puede brindar valor adicional a la administración y a los directivos al proveer una rápida regencia visual que proporciona indicaciones claras sobre las áreas que pueden explorar más a fondo" comenta Juerguens.

Las contó etapas de la madurez son – inicial, gestiona le, definida, previsible y optimizable – que reflejan el progreso que una organización ha hecho en mantener sus habilidades de seguridad para ayudar a mitigar las ciber amenazas y alanzar su nivel de madurez deseado.

"En la práctica, el consejo directivo puede acordar el nivel de madurez deseando, tomando como base el resultado del trabajo de re mediación, momento en el que la auditoría interna pondría a prueba el marco de gestión y confirmaría con el consejo qué nivel se ha alcanzado." Comenta Ms. Pundmann.

Adicionalmente, una revisión independiente con base en métricas podría soportar la evaluación de madurez, destacando en detalle, los riesgos cibernéticos que rodean a las personas, procesos y a la tecnología. Para que el análisis sea festivo, los hallazgos de en de estar documentaos y se deben de emitir recomendaciones para las brechas identificadas.

En algunos casos, la evaluación de riesgos cibernéticos puede también generar una lista de brechas y proveer a la organización un programa de remediación a corto y largo plazo.

Construyendo las bases para una evaluación continúa

La evaluación de riesgos cibernéticos sustenta tanto el análisis de madurez proporcionando al comité de auditoría y al consejo y el desarrollo de un plan multi anual de auditoría interna basado en riesgos para la ciber seguridad. Éste plan puede ser desarrollado a través de los resultados de la evaluación, con algunas auditorías ocurriendo con mayor frecuencia que otras, basadas en la urgencia y en las demás actividades de la organización.

Es importante recordar que la función de auditoría interna enfocada en la ciber seguridad no está escrita en piedra. Se pueden hacer ajustes conforme nuevos riesgos aparezcan, cambios en la intensidad y la importancia de las amenazas existentes y otras cuestiones de la organización.

“La auditoría interna tiene un papel fundamental en ayudar a las organizaciones en la batalla en curso de la gestión de las ciber amenazas, proveyendo una evaluación independiente de los controles actuales y necesarios y ayudando a que el comité de auditoría y la dirección puedan medir los diversos riesgos en un mundo manejado por la tecnología. “ dijo Juergens.

¿Qué podemos aprender?

En un mundo en donde estamos expuestos día con día a las ciber amenazas, las organizaciones necesitan robustecer sus ambientes de control para mitigar sus riesgos. Muchas veces los ataques y grandes filtraciones se hacen a través de un colaborador y no precisamente a la organización, es decir, aunque el colaborador parezca no tener importancia para los hackers, éstos saben que a través de él pueden llegar a la organización y de esta manera, todos debemos de estar protegidos.

Ya sea con una evaluación de madurez o bien unas gestión de riesgos cibernéticos, las entidades deben de considerar implementar un equipo de auditoría interna para poder estar monitoreando constantemente el nivel de seguridad del ambiente de control. La época en que esta función quedaba fuera de las entidades quedó atrás.

Debemos de comprender que vivimos en una era en donde los delitos financieros también han evolucionado y que éstos día con día se cometen a través de medios electrónicos. Casos reales nos sobran para comprender la magnitud del problema y para que emprendamos acciones... Como dice el dicho, más vale prevenir que lamentar.