Al Día con Deloitte

Tendencias en riesgos en sector financiero

- Plan de auditoría basado en riesgos.
- Entendiendo la matriz de riesgo de legitimación de capitales.

Deloitte.

Contenido

Al Día con **Deloitte**

Información y análisis para los responsables de la toma de decisiones.

Enero 2019

Al Día con Deloitte

Un Plan de auditoría basado en riesgos

Mauricio Solano
Socio
Risk Advisory Deloitte
msolano@deloitte.com

La Auditoría Interna es fundamental para asegurar que las organizaciones gestionan el negocio bajo un ambiente de control y según su apetito de riesgo.

Los auditores han tenido que transformar la tradicional forma de hacer auditoría y esto representa retos y oportunidades. El valor que puede dar la auditoría dependerá de cuanto los equipos de auditores incorporen las mejores prácticas y contribuyan a la generación de valor.

Algunas de las principales características de los planes de auditoría basados en riesgos son:

1

Priorización de los riesgos relevantes:

Desarrolla las diferentes revisiones según lo que la organización tiene identificado como riesgos relevantes. Todo riesgo relevante debe tener una política, estrategia, límites y estructura clara de cómo la organización lo administra. Es ahí donde el equipo de auditoría debe concentrar sus horas, revisiones y entendimiento con las áreas de negocio o monitoreo de la entidad, pues en la medida que los riesgos más importantes tengan un mayor control, es más probable que la entidad se encuentra entre límites aceptados.

2

Enfocado en procesos:

El mapeo de los procesos críticos de la organización es fundamental previo a la gestión del riesgo operativo. Es en los procesos críticos, sea desde el punto de vista de continuidad o de impacto, en los que la auditoría debe focalizar sus revisiones, posibles errores o bien, posibles mejoras en el proceso. Ya la auditoría preocupada por ir al detalle de las transacciones y generalmente vinculada a temas estrictamente financieros no es la que predomina.

3

Se especializa en el negocio:

Planes de auditoría efectivos entienden el funcionamiento de las líneas de negocio y evalúan la integridad de los riesgos comprendiendo la especificidad y alcance de cada uno, donde la regulación es cada vez más extensa y detallada. Dejó de ser efectivo el enfoque estándar de auditoría que aplicaba las mismas pruebas en cualquier industria, lo cual requiere preparación. Por eso, los planes de capacitación de los auditores ahora deben estar diseñados para fortalecer el análisis cuantitativo y de datos, la evaluación de metodologías y modelos de gestión.

4

Es integral:

Los planes de auditoría deben evaluar la gestión de cada riesgo o bien de cada proceso crítico desde tres perspectivas: gobierno, para asegurar que la estructura de roles y responsabilidades funciona; riesgo, para comprender si los tomadores de decisiones siguen la estrategia del riesgo de la organización, y control, para asegurar que las medidas preventivas o mitigadores forman parte de la cultura de todos los colaboradores.

5

Genera valor:

El auditor moderno comprende que en sus revisiones el objetivo final no es encontrar observaciones o darse por satisfecho en cuanto a si las actividades de los procesos están de acuerdo a los procedimientos. El auditor también debe preocuparse por entender el negocio para poder generar recomendaciones y valor, de alternativas con las que podría mejorarse la gestión de la organización. Conservando su independencia, puede dar recomendaciones o sugerencias de acuerdo a su experiencia.

La auditoría interna continúa evolucionando de acuerdo a las tendencias en los diferentes sectores. El enfoque de supervisión basado en riesgos llegó para quedarse y el aseguramiento de evaluaciones formales, integrales y continuas son parte clave para que las organizaciones persigan sus objetivos en ambientes de control.

¿Qué debe seguir en la supervisión basada en riesgos?

El sistema financiero dominicano comenzó un proceso de transformación de su marco regulatorio para incorporar las mejores prácticas internacionales con el fin de que los intermediarios financieros gestionen el negocio de acuerdo a un enfoque basado en riesgos.

Pedro Aguilar
Gerente
Risk Advisory Deloitte
paguilar@deloitte.com

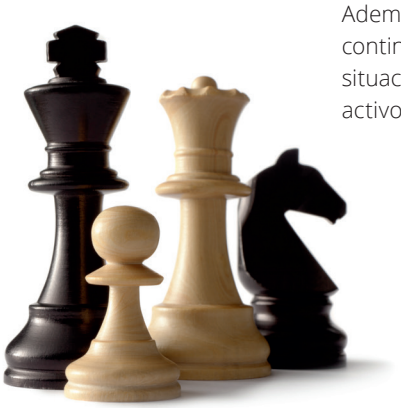
El reglamento de gestión de riesgos y el establecimiento de la matriz de riesgo de legitimación de capitales son dos ejemplos de la transformación que impulsa la Superintendencia de Bancos y que trazan una ruta correcta hacia la adopción de las mejores prácticas.

A nivel internacional, ya terminó el periodo de implementación de Basilea III y comenzaron medidas transitorias que se extenderán hasta el 2027. Los principales retos que la regulación dominicana y por lo tanto los intermediarios financieros deben tomar en pro de asegurar la estabilidad y seguridad en los mercados son:

1 Gestión del riesgo de liquidez:

Actualmente la medición estándar que tienen las entidades continúa a través de ratios financieros, que son métricas cada vez menos utilizadas dentro de una gestión integral del riesgo de liquidez. Es momento de avanzar a las mejores prácticas establecidas en Basilea III. Como punto de partida, el marco regulatorio debe establecer en sus roles y responsabilidades que las entidades definan su estrategia de liquidez y sus principales políticas.

Esto incorpora la necesidad de establecer un marco de Gobierno que pasa a considerar tipos de liquidez (diaria, operativa, estructural), más el conocido índice de cobertura de liquide (ICL), que considera el nivel de calidad de los activos para enfrentar problemas en el flujo de caja en el corto plazo.
Además, se consolidan los modelos de pruebas de estrés, simulacros de crisis y los planes de contingencia de liquidez, para formalizar el marco a través del cual las entidades actuarían ante situaciones adversas. Todo esto contribuye a entidades más seguras y más eficientes en la gestión de sus activos.



2 Marco de riesgo operativo:

Actualmente las entidades no consideran requerimiento de capital en el índice de solvencia por riesgo operativo. Debe avanzarse al menos con el enfoque estándar promovido por Basilea II desde el 2004 y continuar la gestión del riesgo operativo a través de las metodologías de mapeo de proceso críticos y registro de incidentes. A través de esto último, algunas entidades podrían comenzar a comparar los requerimientos de capital de sus modelos internos con los establecidos en el enfoque estándar. Es necesario que las entidades asuman capital por sus riesgos operativos pues es una exposición inherente al negocio.

3 Riesgo de crédito y la pérdida esperada:

La regulación debe promover los incentivos para que las entidades desarrollen los modelos de pérdida esperada de sus carteras de crédito, no solo como parte de la estandarización hacia las Normas Internacionales de información financiera, sino como una mejor forma de reflejar los resultados esperados en los estados financieros. De igual forma, los modelos de pérdida esperada deberían a contribuir a reflejar los factores cíclicos de la economía dominicana, de forma que le permita al regulador establecer medidas macro prudenciales para que el sistema sea más seguro y esté más preparado ante posibles crisis.

4 Valor razonable y riesgos de mercado:

La gestión de riesgos de mercado debe ser integral y considerar la optimización de la liquidez y de las partidas del balance general. Con el instructivo que promueve el uso del valor razonable, recientemente publicado, se entiende que el primer paso previo a cualquier cálculo es categorizar las inversiones según los objetivos de negocio, para posteriormente valorarlas y finalmente reflejarlo en los estados financieros.

Con esto, el paso a seguir es robustecer las herramientas de medición para medir la sensibilidad de la entidad ante cambios en los factores de riesgo de mercado, sean las tasas de interés, los precios o el tipo de cambio y considerar el impacto en los indicadores de negocio y de riesgo.

Similar a la gestión de la liquidez, la gestión de pruebas de estrés y planes de contingencia es esencial para los riesgos de mercado, donde puede tomarse como base para el planeamiento y las simulaciones el ejercicio de adecuación de capital que exige el reglamento de riesgos.

5 Riesgo estratégico y gobierno corporativo:

El gobierno corporativo moderno no solo debe contar con una estructura formal, establecida y documentada. Debe incorporar la estrategia como parte fundamental para evaluar el funcionamiento de la estructura de gobierno. Ya la regulación ha avanzado en el establecimiento de perfiles de riesgo como descriptores en un momento del tiempo del nivel de riesgo. Pero, estos indicadores pueden ser sólo de monitoreo o propios de la gestión del área de riesgos sin necesidad de estar vinculados a los objetivos estratégicos. Por ello, aparece el concepto de Declaración de Apetito de Riesgo (DAR) como la revelación del apetito de riesgo organizacional, lo cual se compone por definir el apetito y el riesgo de los diferentes objetivos estratégicos. En la DAR, las Juntas Directivas se aseguran que las valoraciones cuantitativas o cualitativas clave de la entidad, se miden y monitorean, permitiendo tomar acciones en caso de ser necesario y asegurando entendimiento entre el riesgo y el negocio.

El sistema financiero dominicano ha dado pasos importantes para consolidarse con mejores prácticas y buscando la eficiencia y la estabilidad. El reto es acelerar el paso a nivel normativo para profundizar la cultura de riesgos y que todo el proceso permita madurar a las entidades para que la gestión del riesgo se convierta de un simple cumplimiento normativo a un activo productivo dentro de la entidad.

Planes de contingencia efectivos

Todo plan de contingencia debe estar formalmente aprobado por la Junta Directiva, debe estar sujeto a simulacros de prueba y constante mejora.

Pedro Aguilar
Gerente
Risk Advisory Deloitte
paguilar@deloitte.com

Tanto la Superintendencia de Bancos como la Superintendencia de Valores establecen en sus correspondientes reglamentos de riesgos que los intermediarios deben contar con planes de contingencia formales y conocidos por los colaboradores. El principal objetivo de estos, es garantizar que las entidades puedan mantenerse seguras y estables ante situaciones anormales o inesperadas, donde lo recomendable es que todo riesgo considerado como relevante tenga medidas contingentes.

Todo plan de contingencia debe estar formalmente aprobado por la Junta Directiva, debe estar sujeto a simulacros de prueba y constante mejora, pues gran parte de las posibles contingencias dependerán de situaciones de mercado dinámicas y difíciles de prever.

A continuación, se detalla una estructura efectiva con la que puede contar un plan:

Equipo de gestión de crisis:

Las entidades deben definir los integrantes, con sus respectivos roles y responsabilidades. Hay entidades que establecen el mismo equipo para los diferentes tipos de riesgos, lo cual puede ser deseable si la entidad apenas inicia con este tipo de herramientas. El elemento clave es que el dueño del proceso en cuestión tenga un rol principal, por ejemplo, en el caso de una contingencia de liquidez, correspondería al Tesorero o encargado del área financiera. Los equipos de crisis tienden a tener entre sus miembros a miembros de la Alta Gerencia, unidad de riesgo y encargados del manejo de relaciones públicas de la entidad.

Señales de alerta:

La entidad debe establecer indicadores con niveles a partir de los cuales se generan alertas que podrían implicar la necesidad de aplicar el plan contingente. Estos indicadores pueden ser cuantitativos o cualitativos. Deben ser constantemente monitoreados e informados, principalmente a quienes integran el equipo de crisis. En el set de indicadores, es normal que varíen entre sectores y entidades, pues cada entidad presenta distintos niveles de vulnerabilidad y capacidad de respuesta. Por ejemplo, en un banco con un alto volumen de activos líquidos, el margen para soportar salidas de efectivo es mayor que uno con similar volumen, pero mayor concentración, mientras que en el caso de los puestos de bolsa, aquellos con mayor margen de garantías adicionales para las operaciones de recompra, tendrán más capacidad de soportar posible desmejora en el valor de los activos que otros puestos de bolsa que solo cubren estas operaciones con los niveles regulatorios.

Identificación de fuentes de contingencia:

De forma previa y de constante actualización, la entidad debe establecer las distintas fuentes que podría utilizar en caso de contingencia. Es importante que estas diferencien si responden a una contingencia interna o a una sistémica. Por ejemplo, ante un escenario de crisis de liquidez, una sociedad de fondos de inversión o un banco, difícilmente puedan utilizar una línea de crédito para cubrir sus faltantes de liquidez, pero esta sí sería una fuente viable si la crisis es interna. También se recomienda predeterminar los tipos y niveles de activos que podrían ser utilizados.

Estrategias de gestión de activos y pasivos:

También variarán dependiendo del tipo de riesgo sobre el cual se trate la contingencia. En el caso de riesgos de mercado, una entidad puede disponer desde cambios de moneda en el patrimonio que podría implicar cambios en el activo, pasivo o ambas hasta contar con derivados financieros como las opciones. En el caso de situaciones de liquidez, las primeras medidas podrían ser generar liquidez a través de recompras, o bien, líneas de crédito.
El factor clave es que las estrategias estén claras en el orden que deben considerarse dependiendo de la contingencia.

Protocolos de comunicación:

Son clave para sobrellevar los escenarios de crisis, tanto en el proceso de comunicación de la misma, durante la gestión y al momento donde los indicadores vuelven a sus niveles normales.

En esta etapa, el apoyo de las áreas que lideran la comunicación corporativa es clave, para identificar el tipo de comunicación que debe realizarse según cada grupo de interés, donde los colaboradores deben estar claros no solo de los protocolos sino también de los roles. Por ejemplo, en los puestos de bolsa es posible que ciertos clientes de volumen administrado significativo o bien contrapartes, requieran una comunicación más directa de puestos clave dentro de la entidad sobre la situación que ocurre, mientras que la base de clientes minoristas podrían recibir comunicados más estándar a través de internet. Esto forma parte también de la gestión del riesgo reputacional.

La elaboración de los planes de contingencia y su uso efectivo depende en gran parte del involucramiento que las áreas de negocio tengan en el proceso, pues son las que conocen a profundidad el comportamiento de los indicadores y gestionan las posibles estrategias a seguir. Como complemento, las áreas de riesgo aparecen como soporte, que facilita la calibración de los indicadores, sensibilización de posibles escenarios y evaluación de los factores de riesgo.

Finalmente, los ejercicios de simulación de posibles crisis, permiten a la organización calibrar sus planes de contingencia y mejorar su capacidad de respuesta operativa y de negocio. Son ejercicios de gran aprendizaje, que también deben ser de conocimiento de la Junta Directiva, para de ser necesario, tomar acciones preventivas en las brechas y oportunidades de mejora encontradas

Matriz de riesgo de legitimación de capitales

Claudio Rodríguez
Socio
Risk Advisory Deloitte
clarodriguez@deloitte.com

La matriz de riesgo es una herramienta que comúnmente solicitan los reguladores para que las entidades establezcan un proceso continuo de gestión del riesgo de legitimación de capitales. La herramienta considera 4 factores de riesgo: clientes, canales, productos y servicios y ubicación geográfica.

El objetivo es evaluar la exposición al riesgo de legitimación de capitales para implementar estrategias y reducirlos en caso de que sus niveles no estén de acuerdo a lo que la entidad considera como normales.

Aunque la matriz de riesgo se construye en base a los mismos 4 factores, es clave distinguir que el análisis cambia según la naturaleza del sector. Por ejemplo, un puesto de bolsa que es intensivo en banca de inversión o productos estructurados y tiene una base de clientes muy antigua tendrá riesgos más relevantes en productos y servicios que en clientes, mientras que en un banco que tiene muchas sucursales en el país, el principal factor de riesgo puede venir del factor geográfico, pero si la entidad promueve más los sistemas electrónicos para realizar las transacciones, el riesgo puede venir más de los canales.

La matriz de riesgos refleja el perfil de riesgo de la entidad, es decir la evaluación, en un momento en el tiempo, de la exposición al riesgo. Esta evaluación es dinámica en el tiempo, pero permita a la entidad crear un monitoreo constante de forma que pueda pueden establecer de acuerdo a su estructura de Gobierno, Riesgo y Control los planes de acción para que el riesgo esté de acuerdo al apetito de riesgo escogido. No debe confundirse la matriz de riesgo de legitimación de capitales con las conocidas matrices de calor que miden probabilidad e impacto y que responden más al proceso de gestión de eventos de riesgo operativo.

Hay tres etapas clave para la construcción de una matriz de legitimación de capitales.

1 Identificación de los riesgos

Es fundamental comprender las líneas de negocio relevantes y la estrategia de la entidad para enfocarse en los procesos críticos. Hay dos perspectivas de identificación que se complementan:

a. El riesgo inherente a un factor que se puede considerar por criterio experto o evidencia empírica. Por ejemplo, evaluar una sucursal como más riesgosa que otra es un factor esperado, que da una condición de mayor riesgo, sin que esté contrarrestado por los datos. Si de los clientes totales se tiene un alto porcentaje en la sucursal de alto riesgo, ese nivel refleja la exposición institucional.

b. El riesgo efectivo, que depende de por cuales de los 4 factores hay más posibles eventos. Por ejemplo, la entidad puede demostrar con los datos transaccionales que la sucursal que aparentemente es de alto riesgo, es la que menos desvíos del perfil trasnacional de los clientes y menos alerta genera. Esta valoración debe considerarse en la identificación del riesgo.

2 Evaluación de la exposición

Después de identificar los riesgos se tiene información de dos posibles situaciones que permitirán definir el perfil de riesgo de la entidad.

a. Los niveles de riesgo dados responden al negocio y a la estrategia, por lo que la entidad dispondrá de sus elementos de Gobierno, Riesgo y Control para gestionarlos en los niveles aceptados. Esto es independientemente del nivel de riesgo.

b. Los niveles de riesgo muestran niveles más allá de los considerados como normales según el apetito. Debe diferenciarse si el nivel no aceptado, responde a la realidad del negocio o a al comportamiento de las variables. Si responde a lo primero, quizá la entidad deba cambiar su estrategia y si es a lo segundo, se activan de nuevo los elementos de Gobierno, Riesgo y Control, ya no tanto a modo preventivo, sino para trazar planes de acción que lleven los indicadores a los niveles de apetito.

Por ejemplo, una entidad puede tener el 20% de las transacciones en sucursales ubicadas en alto riesgo. Si ese nivel no es tolerado, entonces había que redefinir los planes de expansión en otras zonas. Pero, si ese nivel es tolerado, la entidad posiblemente deba reforzar los procesos de control para que los asesores de esas sucursales conozcan bien como realizar las debidas diligencias. En ambos casos, se busque que la estrategia de negocio esté acorde a la estrategia de riesgos.

3 Monitoreo y control

Los 4 factores de riesgo y los indicadores utilizados para medirlos están en constante cambio, sea porque responden al comportamiento transaccional del negocio, o bien, porque la estrategia cambia y hay necesidad de incorporar o restar riesgos. Con los factores de riesgo gestionados por la administración, es más fácil darle seguimiento a la tendencia de los perfiles de riesgo y los planes de acción establecidos para realizar correcciones.

Además, ahora esta matriz de riesgo se deerá actualizar periódicamente, ponerse en conocimiento de los órganos de gobierno y ser parte integral de los procesos de planificación estratégica.

La matriz de riesgo de legitimación de capitales descansa en el marco de análisis de la gestión de riesgo moderno, permitiendo a la entidad evaluar el riesgo de su negocio, su capacidad de tolerarlo, gestionarlo y vincularlo con los planes de la administración.

Recomendaciones para el valor razonable

> *La Superintendencia de Bancos publicó el instructivo sobre el uso de valor razonable para el registro contable de los instrumentos financieros que rige a partir de enero de 2020.*

Pedro Aguilar
Gerente
Risk Advisory Deloitte
paguilar@deloitte.com

El principal objetivo del instructivo sobre el uso de valor razonable para el registro contable de los instrumentos financieros, publicado por la Superintendencia de Bancos, es que las entidades valoren los instrumentos financieros de acuerdo al precio que tendría un instrumento bajo condiciones normales transado en el mercado, es decir, lo más cercano posible a precios de mercado.

A continuación, algunas recomendaciones para contar con un proceso exitoso en la implementación de las técnicas de valor razonable en la entidad.

De Gobierno:

1. Definir la estrategia de inversiones:
Las áreas de negocio deben establecer como parte de su planificación financiera cuales inversiones adquiere para negociar, cuales para la venta y cuales para el vencimiento. Para establecer estos criterios debe tenerse claro que el principal objetivo del portafolio de un banco es asegurar liquidez, mientras que otros son aprovechar oportunidades de corto plazo o bien generar una mayor rentabilidad. Esta definición es importante pues así será el reconocimiento contable de los cambios en la valoración sobre los resultados o sobre la solvencia.

2. Establecer políticas:
Que incluyan el apetito de riesgo sobre la composición del portafolio de inversiones, sobre los modelos y procedimientos de valoración. También deben considerarse la necesidad de valoraciones continuas al desempeño de los modelos y el tratamiento a diferencias surgidas del proceso de valoración y los registros contables.

3. Definir unidad que medirá el valor razonable:
Esta debe ser independiente de la administración y debe contar con las calificaciones técnicas para proponer, ejecutar y calcular el valor razonable de los instrumentos.

4. Definir unidad de valoración:
Tanto el modelo de valoración como cualquier cambio sustancial que se le realice, debe ser validado previo a su uso por una unidad independiente y debidamente calificada dentro de la entidad.

5. Criterios de valoración y uso de modelos:
El valor razonable debe determinarse diariamente y en la medida de lo posible a precios de mercado. Cuando esto no sea posible, deben tomarse técnicas de valoración que deben cumplir con estas características:
a) Reconocimiento técnico: deberán considerar las peculiaridades del instrumento, características de los mercados del país y los distintos tipos de riesgo asociados al instrumento.

b) Datos observables: deberán maximizar el uso de datos observables y limitar el uso de datos no observables.

c) Factores claves a considerar: estimación y posibles variaciones en el monto y tiempo de los flujos de efectivo futuros; valor del dinero en el tiempo, en base a las tasas de interés libres de riesgo; prima de riesgo por la incertidumbre que genere el modelo y la limitada liquidez; otros factores, como el riesgo de incumplimiento.

d) Mejora continua: contar con modelos alternativos o cambios a los modelos sólo en casos de nuevos mercados, nueva información, información que deje de estar disponible, mejora de los modelos, cambios en las condiciones de mercado.

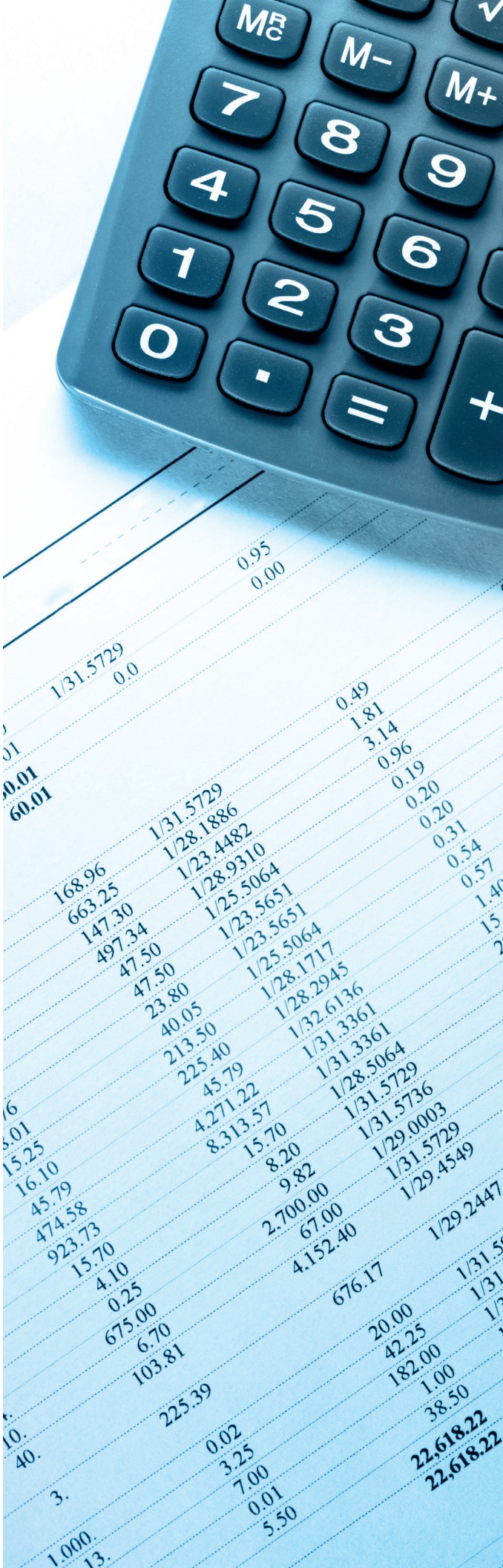
e) Suficiente y ampliamente documentados: incluyendo la razón para su elección.

f) Evaluación periódica: del modelo y examen de su validez. Además, los cambios o rectificaciones deben ser notificados previamente a la Superintendencia de Bancos.

6. Automatización de los modelos:
La adecuación a los lineamientos establecidos por el Instructivo conllevaría el desarrollo de una herramienta de cálculo que permita valorar correctamente las distintas posiciones en instrumentos financieros (activos, pasivos y derivados), como así también estimar a partir de datos del mercado los parámetros necesarios para tales valoraciones. Esto disminuye el riesgo operativo, agiliza el reporte contable y permite calibrar con mejores modelos las valoraciones.

Estas recomendaciones permiten prevenir los principales riesgos asociados al uso del valor razonable, tales como: problemas de objetividad al definir estrategias y modelos de valoración, errores en la especificación de modelos, estructura administrativa que no garantiza la independencia en la valoración o evaluación de los modelos y la omisión de relacionar todos los procesos de estrategia y valoración con el impacto en indicadores de negocio y de riesgo clave dentro de la entidad.

Las exposiciones dentro y fuera del balance deberían reflejar lo más cercano posible el valor de mercado, lo cual es un principio de formación de precios que facilita la toma de decisiones e interioriza dentro del balance de la entidad los riesgos asumidos por la Administración.



Gestión del ciber riesgo y los retos para su aplicación

Andrés Casas
Socio
Risk Advisory Deloitte
ancasas@deloitte.com

República Dominicana demuestra ser un país de vanguardia con la publicación de la resolución JM 181101-02 en materia de seguridad cibernética y de la información. Ya hemos visto como el crimen organizado viene cambiando su modo de operar y ha encontrado en los sistemas financieros una fuente de ingreso rápida e interesante para ellos, donde Latinoamérica es un mercado atractivo que desean explotar como observamos con los incidentes de seguridad sufridos en México y Chile.

Lo más importante de la regulación dominicana está en los beneficios de su aplicación. Por un lado, tenemos al ciudadano quien llega a estar más protegido por las acciones de protección y respuesta ante situaciones que afecten la seguridad de sus datos. Por otro lado, las organizaciones logran una mejora en la gestión de sus riesgos, protegiéndose ante posibles situaciones que le generen pérdidas monetarias.

Cuando iniciamos la lectura de la resolución, podemos identificar que algunos de sus apartados son técnicos y requieren de un especialista para comprender su objetivo y como lograrlo. Sin embargo, en Deloitte hemos definido un enfoque pasado en buenas prácticas, orientado a guiar a los directivos de las organizaciones en su esfuerzo de apoyar la gestión del ciber riesgo y lograr una mejor comunicación interna cuando se aplica un mismo entendimiento. El modelo fue llamado Deloitte Cyber Security Framework y cubre los siguientes componentes:

Gobierno

Establece la estructura requerida para brindar soporte a todo modelo de gestión del ciber riesgo, enfocando en definir una estrategia, articular dicha estrategia por medio de estructuras de gobierno con roles y responsabilidades, generando una cultura organizacional consiente de la importancia de la ciber seguridad y su rol en ella.

Asegurar

Se enfoca en la protección de la información que soporta los procesos claves del negocio, implementando procesos y controles que responden a la realidad y circunstancias del mismo.

Vigilar

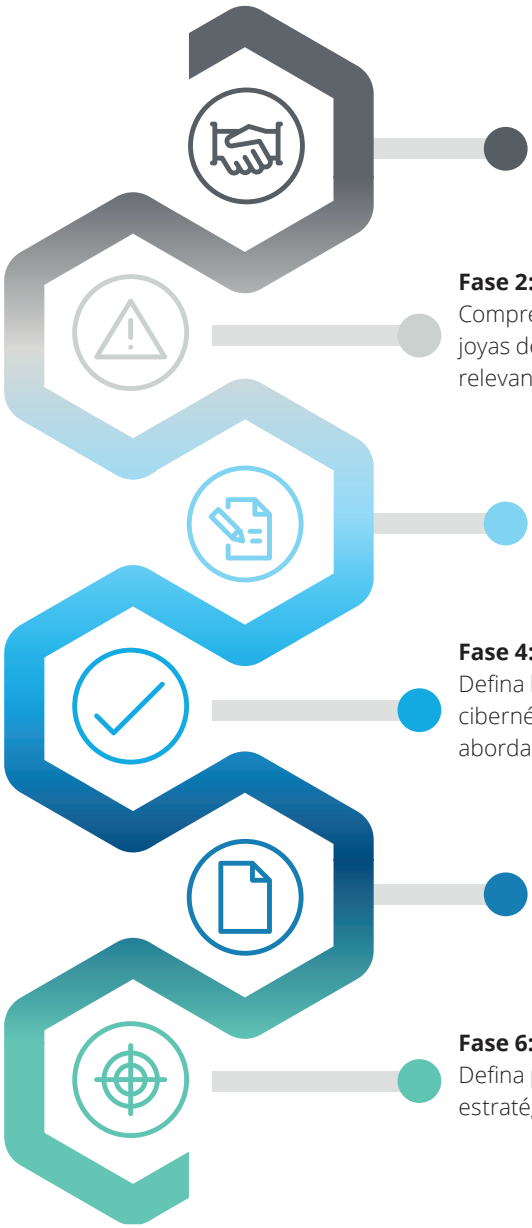
Reconoce la necesidad de establecer una cultura proactiva de estar atentos a las amenazas a fin de desarrollar una capacidad de detectar patrones de comportamiento que puedan indicar o predecir un ataque a la información crítica.

Responder

Significa tener la capacidad de controlar rápidamente un ataque y movilizar los recursos necesarios para manejar el impacto, incluyendo costos directos y disrupción del negocio, así como también daños a la reputación y marca.

Habiendo explicado las grandes áreas que llega a cubrir la resolución, nos queda la siguiente incógnita: ¿Por dónde debo iniciar?

Para responder a esa pregunta, realizamos un planteamiento de metodología de implementación que le permita identificar el nivel adecuado de controles a implementar basado en su negocio y perfil de riesgo.



Fase 1: Perfil del Negocio
Comprender el modelo de negocio, la misión y la estrategia para identificar las joyas de la corona organizativas.

Fase 2: Análisis de Amenazas
Comprenda las amenazas a las que están más expuestas las joyas de la corona para identificar capacidades cibernéticas relevantes.

Fase 3: Evaluación Estado Actual
Comprenda la madurez actual del estado de las capacidades cibernéticas para proporcionar una línea de base para mejoras futuras.

Fase 4: Estado Futuro & Recomendaciones
Defina la madurez del estado objetivo para las capacidades cibernéticas e identifique recomendaciones prácticas para abordar la brecha.

Fase 5: Reporte
Genere informes y paneles que visualizan las amenazas, la madurez actual / objetivo de las capacidades y la madurez cibernética en general.

Fase 6: Hoja de Ruta
Defina proyectos para abordar las brechas y crear planes de trabajo estratégicos para mejorar la madurez y la resistencia cibernética.

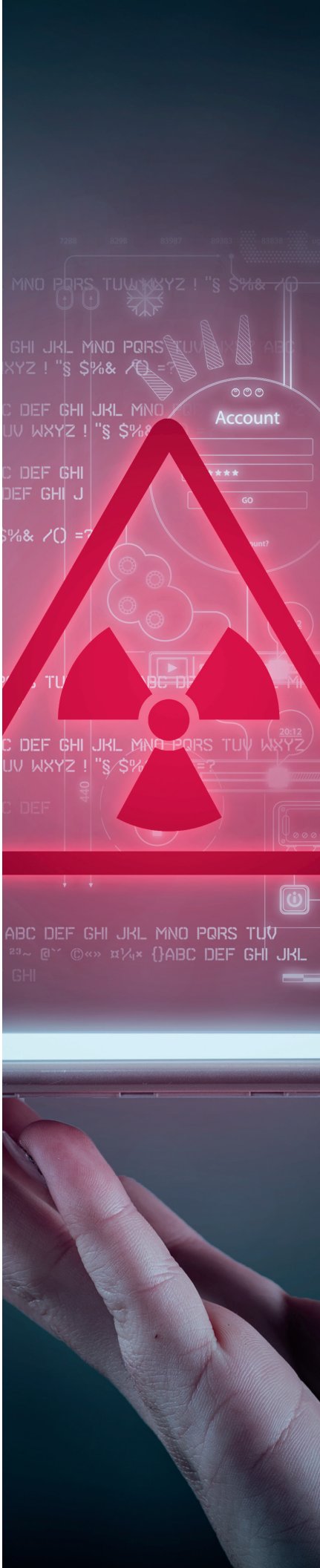
Hay que tener en cuenta que el desarrollo de un modelo de gestión de ciberseguridad es como la gestión de un programa, donde se agrupan diferentes proyectos que poseen un mismo objetivo, en nuestro caso implementar un sistema de gestión de ciberseguridad. A medida que avance irá descubriendo que cada área representa un reto en la gestión de controles, verá que existen varias opciones en la implementación de los mismos, algunas de ellas ofrecen automatización e inteligencia, llegando a tener un precio más elevado que otras manuales. En este caso es recomendable que evalúe su nivel de exposición a la amenaza que atenta contra su seguridad, para poder decidir si tiene sentido el costo beneficio de la medida a implementar. Por otra parte, verá que ese balance es necesario para lograr tener un tamaño de estructura organizacional acorde con perfil de Organización, si no selecciona bien los controles podría estar sub-dimensionando o sobre-dimensionando la cantidad de recursos que requiere para atender las tareas de ciberseguridad.

Patrones y retos en los fraudes tecnológicos

Deloitte en su *Encuesta sobre Ciber Riesgos & Seguridad de la Información en las Entidades Financieras de Latinoamérica*, ha identificado 5 patrones de comportamiento en los fraudes tecnológicos que proponen retos que deben ser considerados durante el desarrollo de las fases 2 y 3 de la metodología de implementación:

	Patrones de comportamiento	Retos
1	Los vectores de ataque han cambiado de **tecnología a personas.**	Modelamiento de riesgos de los actores. Monitoreo probabilístico de usuarios objetivo.
2	Los patrones de ataque están comenzando a parecerse cada vez más a comportamientos normales. Esto es porque han aumentado los casos de amenazas que permanecen **ocultas a la vista**. Algunas de estas amenazas se adaptan y tienen la capacidad de entrar en un modo inactive, haciéndose difícil su detección.	Aprendizaje. Modelo de riesgos adaptable. Inteligencia lateral y de evasión. Analíticas para riesgos.
3	Los criminales, los actores estatales e incluso los Hactivistas están construyendo una mejor inteligencia y capacidad, y tienen una red más amplia de recursos que las organizaciones (**brecha ampliada de capacidad**).	Mejor inteligencia. Inteligencia ampliada. Mayor inteligencia.
4	Crecimiento del compromiso de la seguridad de la cadena de suministro y de los socios de negocio (**entrada lateral**).	Inteligencia de negocio. Perfilamiento de amenazas adaptable. Tecnología inteligente.
5	Las amenazas avanzadas desafían las estrategias tradicionales **basadas en firma**.	Aprendizaje. Perfilamiento de amenazas adaptable.

Si bien hemos visto la importancia de la resolución, cómo lograr un entendimiento de alto nivel sobre las áreas que propone, una metodología de implementación y consideraciones en el diseño del programa de implementación de cara a los patrones de ataque, no debemos olvidar que para que todo lo anterior tenga éxito lo más importante es el equipo humano que forme para atender la resolución, la cultura organizacional que impregne de entusiasmo y escepticismo ante situaciones que tengan el potencial de afectar la Organización.



Contáctenos

Contacte a nuestros expertos en:
Auditoría y Aseguramiento,
Impuestos y Legal,
Asesoría Financiera,
Consultoría en Riesgos,
Consultoría (**Capital Humano**,
Estrategia y Operaciones y **Tecnología**)

Edificio Deloitte
Calle Rafael Augusto Sánchez No. 65
Ensanche Piantini
Tel.: (809) 563 5151
Fax: (809) 563 8585
www.deloitte.com/do

Deloitte.