Riesgo de Terceros: hacia una gestión preventiva y estratégica en línea con la continuidad de negocio

Club de Gestión de Riesgos de la República Dominicana

III Jornada Anual de Riesgos

1. Retos en la gestión del Riesgo de Terceros

2. Framework de gestión

3. Claves de evolución para una gestión más estratégica y anticipativa

4. Conclusiones

Management Solutions
Making things happen

Las nuevas condiciones regulatorias y en el contexto de gestión de las externalizaciones actúan como impulsores de cambio, generando un entorno que obliga a las empresas a evolucionar sus frameworks de riesgo de terceros

Complejidad y dinamismo del entorno regulatorio

La **proliferación de regulaciones exige un esfuerzo constante de actualización y adaptación para garantizar el cumplimiento normativo**, tanto a nivel local como internacional.

Desafíos en las nuevas relaciones con proveedores

Aparición de riesgos emergentes	Relaciones más complejas
Ciberseguridad y datos	Cadena de suministro extendida
Sistemas de IA	Multiproveedor en un mismo servicio
Sostenibilidad y ESG	Concentración del riesgo
Geopolítica	Interdependencia tecnológica

Eventos de riesgo materializados

Ciberseguridad y datos	• Robo o filtración de información. • Ataques a través de sistemas del proveedor.	**Continuidad de negocio**	• Interrupciones por quiebra, huelga o fallas críticas del proveedor.
Fraude y conducta indebida	• Facturación falsa o inflada. • Corrupción, sobornos o suplantación de identidad.	**Reputación y sostenibilidad**	• Escándalos medioambientales o sociales. • Prácticas poco éticas o discriminatorias.
Cumplimiento regulatorio y legal	• Incumplimiento de normas (datos, laborales, ambientales). • Falta de licencias o certificaciones.	**Operaciones y logística**	• Pérdida, robo o mal manejo de productos. • Retrasos o incumplimientos en entregas/servicios.

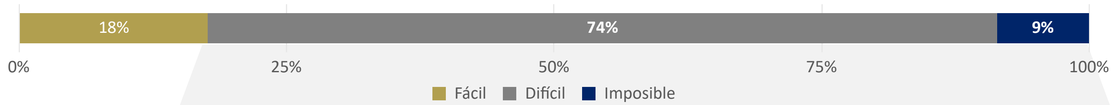
Desde el punto de vista de continuidad, la gestión de riesgo de terceros por su impacto en procesos críticos y por la dificultad a menudo de activar procesos de reversión / sustitución del proveedor

DESGLOSE DE CONTRATOS ACTIVOS, CRÍTICOS Y EXTRA-GRUPO (EN %)

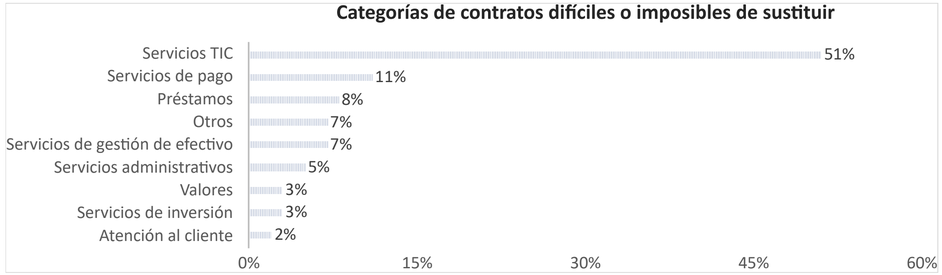
De todos los contratos de externalización, más de un 44% se consideran críticos.

En muchos casos, sustituir esos contratos tiene una complejidad especial, siendo crítico asegurar el alineamiento de SLAs con los tiempso de recuperación (RTO)

Sustituibilidad de los contratos según lo indicado por los bancos



Categorías de contratos difíciles o imposibles de sustituir



FUENTE: Elaboración propia a partir del registro de acuerdos de externalización en instituciones significativas publicado por el ECB

Management Solutions
Making things happen

Retos en la gestión de riesgo de terceros. Madurez en su gestión

A pesar de los avances realizados por la industria, la gestión del riesgo de terceros mantiene todavía retos relevantes como componente central de la continuidad de negocio

Retos de gestión de terceros

Falta de claridad en la definición de roles y responsabilidades

Muchas **debilidades en el modelo operativo y en la implantación de un framework integral** de gestión del riesgo de terceros emanan de falta de claridad en los roles definidos

Escaso desarrollo de los procesos de monitoring

Debilidad en la identificación de proveedores sobre los que desarrollar una **vigilancia especial** por su impacto y dependencia y la gestión de alertas

Inexistencia de un marco adaptado de apetito al riesgo

La **falta de definición de indicadores clave de riesgo** (KRIs) y su **integración** en el **marco global** de apetito al riesgo hace que la entidad **carezca de herramientas** para medir y monitorizar riesgos de forma consistente con sus niveles de **tolerancia** y sus **metas/objetivos estratégicos.**

Debilidades en los sistemas de gestión de continuidad de negocio de los proveedores

Mayor revisión de los SGCN en los proveedores, su suficiencia y adaptación al servicio contratado, las evidencias de los ejercicios de recuperación y cumplimiento de SLAs según la necesidad

Falta de un enfoque estratégico (risk-based) en homologaciones

La **ausencia** de **un sistema de clasificación** de **proveedores** según sus **riesgos** y **capacidades** técnicas **dificulta** el **alineamiento** de sus servicios con los **objetivos** y **estándares** de gestión de riesgos de la entidad

Necesidad de mejorar la mitigación y resiliencia integrada

Necesidad de plantear escenarios más complejos y reales, integrando a proveedores en ejercicios de continuidad de procesos y recuperación de activos tecnológicos
Identificación y cuantificación de NO conformidades

Cobertura no completa de los dominios de riesgos

Los **marcos actuales de gestión** del riesgo a menudo **no incorporan** los **dominios** derivados de las nuevas normativas o **cambios en el entorno,** lo que dificulta la identificación y mitigación de riesgos **relacionados con el outsourcing** y la gestión de proveedores críticos.

Baja productividad por falta de automatización

El **manejo** de **datos no estructurados**, la **ausencia** de accesos **optimizados** a la **información interna** y la falta de **automatización** en tareas repetitivas ralentizan los procesos, **aumentando** los **errores** y **dificultando el cumplimiento normativo.**

1. Retos en la gestión del Riesgo de Terceros

2. Framework de gestión

3. Claves de evolución para una gestión más estratégica y anticipativa

4. Conclusiones

Management Solutions
Making things happen

Los frameworks de gestión del riesgo de terceros debe integrar todas las tipologías de riesgo relevante (transversalidad)

Ejemplos de tipos de riesgos

1. Estratégico

Incorrecta decisión en la **elección** del proveedor / servicio a externalizar **o** en su **gestión**

- Pérdida de control
- Administración deficiente de la externalización

2. Reputacional

Daños a la imagen que los clientes poseen de la entidad

- Pérdida de calidad / cese del servicio
- Divulgación de información confidencial
- Incumplimiento de ANS
- ★ Riesgos asociados a los aspectos ESG

3. Dependencia del Proveedor

Conocimiento para la prestación del servicio **exclusivo del proveedor**

- Cese del servicio
- Concentración de proveedores
- Fuga de información
- ★ Difícil internalización del know-how

4. Regulatorio / Laboral

Incumplimiento de normativa / requerimientos del regulador

- Prestamismo laboral
- Multas / costes de litigios

5. Fraudes

Fraudes cometidos **por el proveedor** a la entidad

- Robo de información sensible
- Falsificación de datos
- Apropiación indebida

6. Operacional / Tecnológico

Pérdidas provocadas **por errores**, **procedimientos inadecuados**, fallos en los **sistemas** o **causas externas**

- Seguridad, Continuidad de negocio, gestión del cambio, integridad,…
- Errores humanos

7. Seguridad de datos

Vulnerabilidades en la **protección** de **datos**

- Exposición de datos (p.e. sensibles)
- ★ Vulnerabilidades en la infraestructura digital (p.e. **AI Risk,**)
- Cumplimiento con regulaciones de protección de datos (p.e. DORA)

8. ESG

Desafíos de **sostenibilidad** y **responsabilidad social**

- ★ Impacto ambiental y gestión de recursos (cadena de contratación)
- ★ Prácticas laborales y derechos humanos
- ★ Transparencia en la gobernanza

★ Nuevas tendencias de riesgo

El framework debe integrar la gestión e2e del ciclo de vida del proveedor 1) Decisión y planificación, 2) Homologación, 3) Negociación y Contratación, 4) Seguimiento del servicio y 5) Terminación, diferenciada según nivel criticidad y nivel de riesgo

Estrategia y gobierno

- Estrategia de Externalización
- Framework de apetito al riesgo
- Estructura de Comités y protocolos de escalado
- Normativa interna

Ciclo de vida

DECISIÓN Y PLANIFICACIÓN

- Planteamiento de la necesidad y decisión de contratación externa
- Evaluación de criticidad y riesgo
- Plan de mitigación según riesgo potencial

Asegurar que la entidad conoce y gestiona riesgos

HOMOLOGACIÓN

- Estratificación de proveedores
- Análisis info del proveedor
- Valoración de la idoneidad del proveedor.

Asegurar que los proveedores cumplen las condiciones

NEGOCIACIÓN Y CONTRATO

- Acordar SLAs según nivel mínimo de servicio requerido para que el negocio funcione según defininciones del apetito
- Clausulado específico según riesgo potencial

Asegurar la correcta formalización de acuerdos

SEGUIMIENTO

- Test de continuidad (revisión de evidencias de pruebas idel proveedor)
- Mantenimiento de reuniones de seguimiento.
- Seguimiento de incidencias y planes de mitigación acordados

Asegurar el cumplimiento del contrato y los SLAs

TERMINACIÓN

- Causas de terminación del contrato
- Ejecución de estrategia de salida (toma de control, transferencia de conocimiento, destrucción de información, etc.)

Asegurar el funcionamiento tras la terminación

Modelo de soporte

- Sistema de VRM (gestión e2e del riesgo)
- Integración con módulos de compras / contratos
- Reporting / Analítica
- Sistemas de Alertas

Asimismo, requiere de la coordinación de múltiples áreas (bajo modelos de 3 líneas de defensa) para el aseguramiento efectivo del riesgo con Terceros

Control a través del establecimiento de las 3LoD

Primera línea de defensa
Seguimiento en primera instancia

- **Gestor del servicio:** owner del servicio y relación con el proveedor
- **Responsables de procesos** de negocio (BIA/PCN)
- Responsables de activos tecnlógicos
- **Compras:** owner del proceso (homologación del proveedor, gestión de
- **Función especialista:** owner de los dominios de riesgo

Segunda línea de defensa
Riesgos / Continuidad de negocio

- **Función independiente de challenge,** que asegura control y seguimiento sobre la subcontratación y gestión de riesgos por las primeras líneas.

Tercera línea de defensa
Auditoría interna

- **Funciones de verificación** realizadas recurrentemente.

Aspectos relevantes

Función centralizada que coordina y supervisa la implantación del marco de Vendor Risk Management.

Se potencia el rol de la tercera línea con Audit independientes de los acuerdos de externalización, incluyendo aspectos de gobierno organizativos y de gestión y control de riesgos.

La homologación de ciertos servicios requiere de la participación de las funciones especializadas (p.e. tecnología) para establecer metodologías y criterios de valoración y asegurar su correcta evaluación.

Participación adicional de otras áreas:
Asesoría legal: revisión de clausulados específicos (incorporando elementos adicionales según los riesgos identificados).
Cumplimiento: fija requerimientos en el proceso de contratación y control del servicio (p.e. en materia de privacidad de dato).

1. Retos en la gestión del Riesgo de Terceros
2. Framework de gestión
3. Claves de evolución para una gestión más estratégica y anticipativa
4. Conclusiones

Management Solutions
Making things happen

Management Solutions
Making things happen

Claves de evolución para una gestión más estratégica y anticipativa. ¿Dónde están poniendo foco las entidades?

En el contexto actual, las entidades están poniendo especial foco en algunas claves para una gestión más estratégica y anticipativa en línea con la continuidad de negocio

Tendencias

Análisis del Mapa de Proveedores

- Analizar el **mapa de proveedores** y realizar actuaciones hacia **relaciones más estratégicas** (sin olvidar los riesgos de concentración) facilita la gestión del riesgo de terceros y la colaboración en pruebas / simulacros conjuntos.

Desarrollo del marco de apetito al riesgo

- Desarrollar un **macro de apetito al riesgo incluyendo métricas / KRIs de riesgo de terceros**, facilita alinear el nivel de riesgo y actuaciones con la estrategia de la entidad.

Clasificación y gestión basada en riesgo

- Desarrollar metodologías para **evaluar el riesgo inherente / riesgo residual** (por dominio de riesgo y global) para dirigir mejor los controles.
- **Gestión diferencia risk-based**: la profundidad de homologación,cláulas mitigantes en el contrato, intensidad en el seguimiento etc debe ser coherente con el nivel de riesgo/ criticidad.

Impulsar el seguimiento continuo

- Identificar **proveedores a los que prestar una vigilancia especial y proveedores únicos (Single Point of Failure) con especial impacto en la continuidad de negocio.**
- Integrar una **visión 360 del proveedor con alertas internas y alertas externas** para impusar un seguimiento más proactivo.

Planificar protocolos de actuación

- Definir **estrategias de salida** desde la fase de planificación.
- Revisión del testing del proveedor de su PCN y valicaión de SLAs vs RTOs e identificar no conformidades
- Participación de **ejercicios conjuntos de continuidad** de procesos y recuperación de servicios TIC
- **Protocolos de respuesta a incidentes** para minimizar la disrupción

Mejoras en herramientas y datos

- **Potenciar la calidad de información del inventario de servicios / proveedores** (integrando información de riesgos/ contratos / proveedores) y su uso en **analítica / reporting**
- **Mejoras en los workflows de gestión para una visión integrada**
- **Impulso de IA** el acceso y análisis de datos críticos de los proveedores

Framework, políticas y metodologías | **Procesos de gestión y control** | **Herramientas y datos**

Los modelos de análisis y clasificación del mapa de proveedores, permiten identificar proveedores estratégicos y alcanzar una gestión más global y robusta de los procesos de gestión del riesgo de terceros con ellos

1. Evaluar nivel de concentración

Permite segmentar proveedores (críticos, relevantes, etc.), evaluar nivel de concentración e impulsar en su caso estrategias de diversificación (proveedores "*challengers*" homologados) o redundancia

2. Planificación la homologación

Listado de proveedores prehomologados por tipología de servicio para facilitar los tiempos en la contratación

3. Mejoras en el proceso y la coordinación con el proveedor

Permite una reducción en el coste de la gestión de terceros (ie. centralizar la homologación, compartir información entre empresas del Grupo etc.)

4. Facilita el seguimiento

Permite aplicar evaluaciones 360 de los proveedores (rendimiento / riesgo) y coordinar actuaciones según su resultado

5. Involucración en planes de mitigación

Facilita un mayor foco del proveedor en la corrección de los aspectos identificados en los procesos de revisión

6. Facilita la coordinación con el proveedor en auditorías/ tests

Mayor participación en simulacros, pruebas de resiliencia conjunta bajo escenarios coordinados

Actualizar el marco de apetito al riesgo es clave para gestionar los riesgos emergentes y garantizar que la organización esté alineada con los objetivos estratégicos, cumpla con las normativas regulatorias y mantenga la continuidad operativa frente a nuevos desafíos

Implicaciones de la actualización del marco de apetito al riesgo

Identificación de riesgos clave

- **Además de los riesgos tradicionales**, como los financieros y operacionales, es necesario incorporar **riesgos emergentes que impactan significativamente en la relación con los proveedores** (ie. inteligencia artificial) .
- Es fundamental que el **marco de apetito al riesgo se ajuste para incluir estos factores nuevos, garantizando que la Entidad pueda responder de manera efectiva a cualquier desafío emergente.**

Establecimiento de umbrales de tolerancia

Es necesario **definir umbrales de tolerancia al riesgo que sean específicos, claros y medibles,** y que reflejen el nivel de riesgo aceptable en cada categoría. Estos umbrales deben considerar lo siguiente:

- **Métricas y KRIs**. Identificar métricas globales sobre el **despliegue del framework de terceros** (ie. % proveedores no homologados en servicios críticos, % SPoF en procesos críticos) como por **dominios de riesgos**
- **Límites de tolerancia.** Establecer umbrales alineados con la tolerancia al riesgo de la entidad

Alineación del apetito al riesgo con la estrategia

- El apetito al riesgo debe estar **alineado con los objetivos estratégicos** de la Entidad (ie. digitalización, outsourcing, potenciar la eficiencia vía corporativización u offshoring etc.)
- Es crucial que las decisiones sobre el apetito al riesgo reflejen la dirección estratégica de la organización.

Planes de acción ante desviaciones

El cumplimiento del marco de apetito debe monitorizarse a máximo nivel (Consejo / Comisión de Riesgos) e implicar actuaciones:

- **Análisis del portfolio de proveedores**
- **Activación de planes de mitigación/ salida en proveedores**
- **Revisión de la política de externalización**
- **Medidas de gobierno** (ie. impacto en objetivos)

La gestión diferenciada basada en riesgo implica establecer protocolos de control ajustados a la criticidad del servicio y al nivel de riesgo que supone

Visión servicio

Evaluación de la relevancia del servicio y riesgo inherente

Relevancia
Relevancia baja

Riesgos inherentes por dominio y global
- Riesgo continuidad
- Riesgo seguridad
- Riesgo operacional…

Crítico
Alto
Medio
Bajo
Sin riesgo

Impacta en:

- Criterios de homologación
- Estrategias de salida

Visión proveedor

Análisis técnico del proveedor

Se evalúa la idoneidad del proveedor para la gestión de los riesgos identificados

Evaluación del proveedor empresa
((i. solvencia, reputación, cumplimiento etc.)

Ambos proveedores puntaje suficiente > 70%

+

Evaluación de capacidades técnicas
(según dominios aplicables)

Visión de riesgo residual

Visión servicio + proveedor

Decisión final con respecto a capacidades técnicas del proveedor

- Riesgo residual asumible
- Planes de mitigación c/ proveedor
- Clausulas contractuales

Impacto en contratación

Seguimiento servicio + proveedor

Monitroring reforzado

Testing

Vigencia de la certificación

Para fortalecer el modelo de monitorización es clave identificar a los proveedores más críticos y activar un seguimiento más proactivo que asegure una visión 360 del riesgo

Palancas para reforzar el modelo de monitoring

Gestión de Alta Dependencia/ Single-Point-of-Failure (SPoF)

Identificar proveedores que requieren de una **vigilancia especial**, con:
1) **alta dependencia** al soportar procesos críticos del negocio con alto impacto en caso de disrupción
2) Sin **alternativa inmediata**

Gestión de alertas

Internas

- Resultados del BCP testing,
- Incumplimiento de planes de mitigación
- Reducción en calidad percibida

Externas

- R. Cyber: Bajadas de rating de ciberseguridad, noticias negativas, vulnerabilidades detectadas etc
- R. Compliance: screening listas negras
- R. Reputacional: alerta noticias, litigios, etc
- R. Financiero: alertas de solvencia (pérdidascaídas en ventas etc.)

- **Realizar una monitorización reforzada**
- **Identificar mitigantes**

- **Ajuste de nivel de riesgo**
- **Solicitud de info**
- **Nuevo plan de mitigación con proveedor**
- **Adopción de medidas contractuales / hold de negociaciones**

Para fortalecer el modelo de monitorización es clave identificar a los proveedores más críticos y activar un seguimiento más proactivo que asegure una visión 360 del riesgo

Planificar protocolos de actuación

PLANES DE SALIDA	Diseñar un plan para la gestión adecuada de la salida de un proveedor, minimizando riesgos para evitar perturbaciones indebidas e impactos adversos	• Identificación de proveedores alternativos/ estrategia de reversión • Establecer obligaciones contractuales • Criterios de activación (triggers) • Gestión de datos compartidos
BCP TESTING	Asegurar que los escenarios de interrupción, pruebas y resultados están alineadas con los requerimientos de RTO / RPO de la entidad Revisar SLAs vs requerimientos de RTO	• Matriz de criticidad de escenarios (probabilidad / impacto) • Evidencias de realización y resultado • Acciones mitigantes
PRUEBAS DE RESILIENCIA CONJUNTAS	Gestión coordinada con el proveedor de escenarios de crisis o interrupción para comprobar si los planes de continuidad son compatibles, realistas y efectivos	• Integrar pruebas tecnológicas y operativas • Definir objetivos y planificación conjunta (diseño, ejecución y evaluación de resultados) • Comunicación estructurada (ie. war room digital) y protocolos de escalado
PROTOCOLOS DE RESPUESTA A INCIDENTES	Desarrollo de planes de respuesta documentados incluyendo a los proveedores en los protocolos, en los simulacros y responsabilidades (RACI conjunto)	• Medición: establecer KRIs y monitorio continuo • Clausulas contractuales (tiempos máx de comunicación, compartir evidencias etc.)

1 Recovery Time Objetive / Recovery Point Objetive

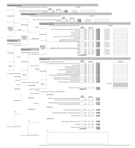
Para que la gestión y control de riesgos sea eficaz, se necesita disponer de una herramienta con visión “end-to-end” que permita almacenar, suministrar y gestionar la información de Proveedores y llevar a cabo evaluaciones completas y automatizadas de riesgo

Herramientas de soporte

Herramienta soporte de gestión “end-to-end” y con capacidad de trazabilidad del proceso

- Repositorio documental centralizado (visión gestor/proveedor)
- Soporte completo al proceso de evaluación (modelado de procesos de supervisión de riesgos y testeo, y validación de controles establecidos).
- Informes periódicos (KPIs y KRIs) que faciliten el seguimiento, la toma/escalado de decisiones y la anticipación de posibles contingencias.
- Cuadros de mando con visión 360º.

Herramienta valoración relevancia y riesgo



Cuestionarios de certificación (financiero / calidad / riesgo)

Cuadro de mando (KPIs, KRIs)

Aspectos relevantes

- ✓Foco en herramientas que permiten la **doble visión Gestor - Proveedor** permitiendo al segundo el acceso directo para revisión de los informes de control y calidad sobre su servicio
- ✓La **calidad del dato y su completitud** tanto sobre el propio servicio externalizado como sobre los Proveedores debe ser revisada de forma periódica para asegurar la correcta actualización de cambios en la criticidad, situación del Proveedor, etc.
- ✓El éxito de un **modelo de Proveedores** no radica en exclusiva en la capacidad del software instalado que lo implementa sino en la **conjunción práctica** los distintos elementos
- ✓El mercado de soluciones de VRM está en **constante evolución** debido al incremento de la actividad reguladora, así como a una mayor apreciación del riesgo de terceros

1. Retos en la gestión del Riesgo de Terceros
2. Framework de gestión
3. Claves de evolución para una gestión más estratégica y anticipativa
4. Conclusiones

Management Solutions
Making things happen

Conclusiones. Transformación de la gestión de riesgos de proveedores

De una gestión pasiva y reactiva a un enfoque estratégico, integrado y proactivo en la gestión de proveedores críticos

	De…		*a…*
	De una gestión pasiva ante situaciones de vendor locking	…	a una **visión estratégica** del mapa de proveedores y definir planes de salida en proveedores críticos
	De una gestión no segmentada	…	a **identificar proveedores críticos y con alta dependencia** sobre los que focalizar un seguimiento reforzado
	De controles no integrados	…	a un **marco único** que combine continuidad de negocio, ciberseguridad, cumplimiento etc. y **aliniado con el apetito al riesgo** que aprueba la Alta Dirección
	De focalizar esfuerzos en homologaciones puntuales	…	a un seguimiento continuo con **alertas internas y externas** en todo el ciclo de relación con el proveedor
	De planes de continuidad genéricos	…	a **pruebas conjuntas de resiliencia** con escenarios comunes y protocolos más realistas
	EN DEFINITIVA		
	De modelos reactivos que dan respuesta a incidentes	…	a frameworks con **perfiles del nivel de riesgo**, con un **seguimiento continuo y anticipación en las actuaciones**

Management Solutions
Making things happen

Un equipo internacional

Equipo multidisciplinar

Buenas prácticas
Know-how

Experiencia demostrada

Máximo compromiso

Carlos Suarez Fernandez
Socio de Management Solutions
Carlos.Suarez.Fernandez@msspain.com