GUÍA INDICADORES (KRI) RIESGO OPERACIONAL

Grupo de Trabajo
Responsables de Riesgos
de Aseguradoras

agers

Asociación Española
de Gerencia de
Riesgos y Seguros

INDICADORES DE RIESGO OPERACIONAL (KRI)

UNA GUIA PRÁCTICA

agers

ISBN: 978-84-09-43471-8
Depósito Legal: DEP637949514853421442
Copyright: M-21571-2022

Nota Legal - Copyright

Las conclusiones elaboradas en este texto son emitidas por el Grupo de Trabajo de Responsables de Riesgos de Aseguradoras, según su libre interpretación y tras las reuniones celebradas.

ÍNDICE

PRÓLOGO

¿Sabemos cuánto riesgo asumimos? ¿Tomamos las decisiones de forma consciente o nos conformamos con la intuición como mejor criterio?

¿Te gustaría tener una bola de cristal en la que confiar a la hora de tomar decisiones, pero crees que eso no existe ni se puede conseguir?

Cierto, no existe, pero aquí encontrarás una valiosa ayuda para que te construyas una. Esto no es magia sino ciencia: medir de forma objetiva nos permite disponer de información muy valiosa.

La gestión del riesgo es clave para mejorar la gestión de las compañías e incrementar las posibilidades de alcanzar sus objetivos. Implementando indicadores de riesgos podremos disponer de información muy valiosa. El análisis de los datos nos permitirá mirar al pasado, al presente, e incluso al futuro. Nos ayudará a identificar el origen de las desviaciones que precedieron a la materialización de un riesgo, comparar la situación actual con las óptimas con el objetivo de obtener los mejores resultados, e incluso proyectar las tendencias para predecir el futuro.

¿Pero qué medir y cómo?

Si en tu organización ya contáis con un sistema de indicadores de riesgos, encontrarás en este libro información útil para para contrastar que el modelo del que dispones está en línea con las propuestas en otras organizaciones o para identificar posibles mejoras. Pero si aún no dispones de unos indicadores de riesgos y quieres aventurarte a comenzar esta andadura, este libro seguro que te resultará muy útil en tus primeros pasos para comenzar con los riesgos operacionales. Vas a encontrar un montón de ejemplos de indicadores y recomendaciones para utilizarlos de la mejor manera o incluso diseñar tus propios indicadores. No se trata de usarlos todos, ni sobrecargar a la organización con mediciones, sino de seleccionar o proponer los más adecuados en cada caso. Es aquí donde el conocimiento profundo de la compañía se hace imprescindible y la visión de un experto aporta un gran valor.

Es de agradecer la generosidad de todos los participantes en la elaboración de este libro al compartir su experiencia, y el esfuerzo realizado por el grupo de trabajo de "responsables de riesgos de aseguradoras" para realizarlo sin centrarse exclusivamente en el sector asegurador, sino que lo enfocan desde una perspectiva más amplia para que sea útil en otras organizaciones. El resultado expone de forma práctica, llena de ejemplos y fácil de entender, una propuesta de indicadores sencillos y asequibles que resultarán de gran utilidad para gestionar el riesgo operacional, propósito más amplio para el que podrás encontrar también buenos consejos y recomendaciones en el libro "Manual de Riesgos Operacionales", elaborado en paralelo por el grupo de trabajo de "responsables de riesgos de grandes empresas" de AGERS.

Cástor Pérez Retamal
Jefe de Área de Gestión, Seguimiento y
Coordinación del Sistema de Gestión Integral de Riesgos en Adif.

MIEMBROS DEL GRUPO DE TRABAJO

Adeslas SegurCaixa	Ruth B. Rodriguez Torrellas
AXA	Lidia Sanz Carballo
CONSORCIO DE COMPENSACION DE SEGUROS	Eva Valentí Ramírez María Nuche Otero
El Corte Inglés seguros	José Andrés Mayo González
MMT SEGUROS	Sonia Vicente Alonso
Sanitas	Ignacio Reclusa Etayo Marta Olona Delgado
ZURICH	Ricardo Mariano González

OBJETO DEL DOCUMENTO

La comisión de expertos de Responsables de Riesgos en Aseguradoras, tras la elaboración de la guía "La Función de la Gestión de Riesgos en entidades aseguradoras", se marcó un nuevo objetivo consistente en profundizar en el análisis del riesgo operacional, no centrándose exclusivamente en el sector asegurador sino desde una perspectiva más amplia.

Este trabajo presenta una propuesta de indicadores cuantitativos que permiten a las empresas abordar el riesgo operacional para todos y cada uno de los aspectos que lo conforman.

Se pretende ofrecer una propuesta abierta, no excluyente, que sirva a las organizaciones como guía para abordar el riesgo operacional, medirlo con indicadores sencillos y asequibles, y tener una idea amplia del funcionamiento de los procesos que definen y abordan el riesgo operacional.

Se ha seleccionado como base una estructura o marco (ORIC)[1] que entendemos cubre cada uno de los aspectos integrados en la propia definición del riesgo operacional (procesos, personas, aplicaciones, sistemas y acontecimientos externos), de manera que nos permita ir proponiendo indicadores prácticos que pueden ser utilizados por las entidades en su día a día en la gestión de riesgos, aplicables a cualquier entidad.

1. ORIC (Operational Risk Insurance Consortium)

DEFINICIÓN DE RIESGO OPERACIONAL

Entre las definiciones existentes la comisión de trabajo, ha considerado apropiada la que considera el riesgo operacional como "el riesgo de pérdida resultante de una falta de adecuación o de un fallo de los procesos, el personal o los sistemas internos, o bien como consecuencia de acontecimientos externos".[2]

Para garantizar una cobertura íntegra y acorde a la definición elegida, a la hora de buscar una estructura o marco sobre el que proponer indicadores de riesgo operacional consideramos oportuno utilizar la estructura de análisis que propone ORIC, el Consorcio de Riesgo Operacional, creado en el año 2005 por la Association of British Insurers (ABI) junto con 16 entidades aseguradoras, para promover la recopilación de información de pérdidas derivadas de riesgos operacionales. [3]

El Consorcio se encuentra en constante crecimiento, tanto en UK como a nivel internacional, añadiendo nuevas entidades cada año. Es una organización sin ánimo de lucro que cuenta en la actualidad con 24 miembros. En esta estructura tiene cabida la incorporación de riesgos emergentes, y de actualidad, como son los riesgos de seguridad de la información y los riesgos tecnológicos, así como los riesgos de gobierno, medioambientales y sociales (ESG), que si bien podrían ser motivo de un trabajo específico adicional y cuyos indicadores vienen marcados principalmente por las exigencias de reporte normativo aplicables a cada entidad, así como por los compromisos estratégicos definidos en particular por cada organización.

Consideramos esta estructura marco con el fin de proponer un análisis íntegro del riesgo operacional, pero lo suficientemente fácil y estructurado en su interpretación, al presentar una propuesta de indicadores para cada uno de los bloques presentados en los gráficos siguientes, de manera que puedan servir a los gestores de riesgo para asegurar la gestión a través de

2. Definición del art. 14 Ley 20/2015 de ordenación, supervisión y solvencia de las entidades aseguradoras (LOSSEAR). Si bien no es solo aplicable a entidades de seguros, sino que tiene alcance para todo tipo de organizaciones. En el Manual de riesgos operacionales elaborado por la Comisión de Riesgos de AGERS, se considera una definición amplia: "Riesgo operacional es todo aquel que afecta a las operaciones desarrolladas por una organización y, por tanto, a los resultados obtenidos".
3. https://www.oricinternational.com/

indicadores de todos y cada uno de los bloques que definirían el riesgo operacional.

Esta estructura se basa principalmente en definir el análisis del riesgo operacional desde diferentes niveles:

- Primer nivel: 7 tipos de eventos y sus definiciones.
- Segundo nivel: desglosa por categorías los eventos del primer nivel.
- Tercer nivel: añade ejemplos de actividades de cada una de las categorías del segundo nivel.

El objetivo de este documento es proporcionar indicadores sencillos que den cobertura a todas y cada una de las actividades propuestas y que permitan no solo identificar los riesgos, sino disponer de indicadores cuantitativos que favorezcan la gestión y la toma de decisiones.

Fuente: AGERS

NIVEL 1	NIVEL 2	NIVEL 3
1) Fraude Interno		
Son actuaciones efectuadas con ánimo de dolo o lucro por parte del personal interno de la entidad, así como acciones no autorizadas por el uso incorrecto de los poderes o atribuciones otorgados al personal de la compañía.	1.1. Actividades no autorizadas	- Operaciones no reportadas (intencionadas)
		- Operaciones mal reportadas (intencionadas)
		- Tipo de operación no autorizada (con pérdidas monetarias)
	1.2. Robos y fraude	- Hurto / Extorsión / Malversación / Robo
		- Malversación de activos
		- Destrucción delictiva de activo
		- Falsificación (interno) y suplantación de identidad
		- Contrabando
		- Suplantación de identidad
		- Incumplimiento o evasión de las obligaciones fiscales
		- Soborno
		- Utilización de información privilegiada (tráfico, contratación, etc.)
2) Fraude externo		
Riesgo como consecuencia e la comisión de hechos de carácter delictivo por personal no interno de la compañía, clientes, proveedores...	2.1. Robo y fraude (externo)	- Robo
		- Fraude (agentes, mediadores, peritos, médicos, etc)
		- Falsificación (externo) y suplantación de identidad
	2.2. Seguridad de sistemas	- Daños de piratas informáticos
		- Robo de información (con pérdidas monetarias)
3) Prácticas laborales y seguridad en el trabajo		
Riesgo en la gestión de los Recursos Humanos, incluye los incumplimientos de la normativa laboral.	3.1. Relaciones de empleados	- Indemnizaciones a empleados, prestaciones y despido laboral.
		- Actividades laborales organizadas (huelgas sindicales).
		- Acoso moral.
		- Acoso sexual.
	3.2. Seguridad del entorno	- Responsabilidad civil (caídas, golpes, etc.)
		- Casos relacionados con la salud y seguridad de los trabajadores
		- Indemnizaciones a empleados
	3.3. Diversidad y discriminación	- Discriminación social, cultural, étnica, etc.

NIVEL 1	NIVEL 2	NIVEL 3
4) Prácticas con clientes, productos o negocios		
Riesgo por expectativas de clientes no satisfechas por malas prácticas o por deficiencias en la venta de servicios. Multas, sanciones o indemnizaciones por incorrectas prácticas comerciales.	4.1. Adecuación, información y confidencialidad	- Fallos o violaciones de directrices
		- Fallo en la información sobre la idoneidad del cliente
		- Revelación de información de consumidores
		- Violación de la intimidad
		- Pérdidas producidas por ventas demasiado agresivas
		- Abuso de información confidencial
	4.2. Prácticas de mercado o de negocio impropias	- Sentencia judicial antimonopolio
		- Prácticas de mercado incorrectas
		- Manipulación del mercado
		- Utilización de información privilegiada (tráfico, contratación, etc.)
		- Actividades no autorizadas en la entidad
		- Blanqueo de dinero
	4.3. Errores o defectos en los productos	- Defectos del producto
		- Fallos de valoración
	4.4. Selección, soporte y exposición de clientes	- Falta de investigación del cliente según los procedimientos internos
		- Exceso de riesgo con el cliente
	4.5. Actividades de consultoría	- Disputas relacionadas a actividades de asesoramiento
5) Daños a activos materiales		
Riesgo de acontecimientos externos, ya sean naturales, accidentales, como provocados que dañen los activos físicos o interrumpan las actividades de la empresa.	5.1. Desastre y eventos.	- Pérdidas por desastres naturales
		- Pérdidas humanas por causas externas (terrorismo, etc.)
6) Interrupción del negocio y fallos en el sistema		
Riesgo por deficiencias en el diseño e implantación de sistemas de información, deficiente funcionamiento de los sistemas de comunicación.	6.1. Sistemas	- Software
		- Hardware
		- Telecomunicaciones
		- Fallos de alimentación de sistemas

NIVEL 1	NIVEL 2	NIVEL 3
7) Ejecución, entrega y gestión de procesos.		
Riesgo debido a las deficiencias de los procesos de la compañía, tanto por el diseño como por la gestión de los mismos. Errores en la ejecución de procedimientos y operaciones.	7.1. Captura, ejecución y mantenimiento de transacciones	- Errores en la introducción de datos y mantenimiento
		- Incumplimiento de fechas límite y/u obligaciones
		- Disfunciones en modelos de valoración o sistemas
		- Error de contabilidad o error de atribución a una entidad
		- Mala ejecución de tareas
		- Incumplimiento o fallos de entrega
	7.2. Supervisión y reporte de información	- Incumplimiento de la obligación de informar
		- Importe externo inexacto
	7.3. Errores o pérdida de documentos	- Falta de cláusulas de exención de responsabilidad
		- Falta de documentos jurídicos o documentos jurídicos incompletos
	7.4. Gestión de cuentas de clientes	- Acceso sin autorización a información sensible
		- Documentación de clientes incorrecta
		- Pérdidas o daños del activo del cliente por negligencia
	7.5. Contrapartes de negocio	- Mala actuación de la contrapartida (no cliente)
		- Disputas varias de la contrapartida (no cliente)
	7.6. Proveedores y prestaciones de servicios.	- Subcontratación de servicios propios ("outsourcing")
		- Disputas de vendedores

Fuente: AGERS

ASPECTOS SIGNIFICATIVOS EN LA DEFINICIÓN CUANTITATIVA DEL RIESGO

En el ámbito de la Normativa Solvencia II, **el perfil de riesgo** de una entidad se entiende como la naturaleza, el volumen y la complejidad de los riesgos inherentes a la actividad de una empresa de seguros o de reaseguros. En un ámbito más amplio, se puede definir el perfil de riesgo de una organización como el vínculo entre los objetivos que desea alcanzar y los riesgos que está dispuesta a asumir en ese proceso, teniendo en cuenta su capacidad para gestionar dichos riesgos.

El **apetito de riesgo** de una entidad se define como la cantidad y tipología de riesgos que está dispuesta a asumir, los cuales influyen en la variabilidad de los resultados y en la consecución de los objetivos establecidos. Este apetito de riesgo contiene aspectos cuantitativos y cualitativos, por lo que debe estar totalmente vinculado a la estrategia de la entidad y a su perfil de riesgo.

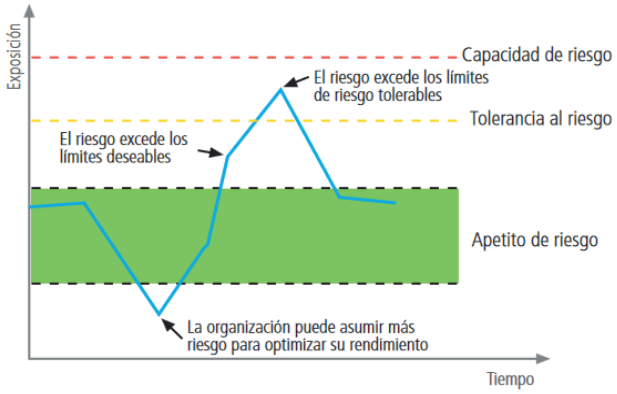
Los límites de apetito de riesgo ayudan a convertir las declaraciones de apetito de riesgo en métricas cuantitativas y/o cualitativas concretas y medibles, y los **intervalos de tolerancia** sirven para establecer el nivel de desviación aceptable sobre los límites.

Es recomendable definir igualmente la **capacidad de riesgo**, entendida como el riesgo máximo que la organización es capaz de soportar en la persecución de sus objetivos. Es el límite a partir del cual la compañía tendría problemas de solvencia y/o podría ver peligrar su continuidad.

CONCEPTO	¿A QUÉ HACE REFERENCIA?	EJEMPLO
Apetito	Nivel de riesgo que la empresa **quiere aceptar,** aquel con el que se siente cómoda.	La empresa A quiere pagar un precio máximo por la licencia de 20 millones de €. Comienza la subasta y ofrece 10 millones de €. Esta cifra está dentro de los límites de riesgo que desea asumir, considerado el objetivo que persigue y el beneficio esperado de la explotación de esa licencia.
Tolerancia	**Desviación** respecto al nivel en el que la empresa se siente cómoda. Sirve de **alerta** para evitar llegar al nivel que establece su capacidad.	La subasta continúa y tras varias pujas un competidor ofrece 24 millones de €. La empresa debe decidir si hacer una oferta superior, sobrepasando el nivel que deseaba pagar inicialmente (20 millones de €). Finalmente puja por 25 millones de € y asume un riesgo que estaría por encima del nivel que deseaba asumir.
Capacidad	Nivel máximo de riesgo que la empresa **puede soportar.**	La subasta continúa y otro competidor llega hasta 29 millones de €. La empresa A sabe que los recursos máximos con los que cuenta son 30 millones de €. Si puja asumirá el máximo riesgo que sus actuales recursos le permiten, quedándose al límite de sus recursos, por lo que decide no seguir pujando.

Fuente: Definición e implantación del apetito de riesgo. Instituto de Auditores Internos de España.

Si representáramos gráficamente estos conceptos para entenderlos mejor, tendríamos lo siguiente:



Fuente: Definición e implantación del apetito de riesgo. Instituto de Auditores Internos de España.

INDICADOR CLAVE DE RIESGO

1. DEFINICIÓN Y OBJETIVO DE LOS INDICADORES DE RIESGO

Los indicadores de riesgo clave (Key Risk Indicator, KRI) son una métrica para determinar cuándo se está superando el apetito de riesgo fijado por la organización. Mide la exposición al riesgo.

Estos indicadores o parámetros deben definirse en base al apetito de riesgo y nos permitirán anticipar posibles cambios en la exposición del riesgo, realizar un seguimiento de este, y en su caso, proceder a la aplicación de planes de acción correctivos.

Los indicadores clave informan a la organización sobre la efectividad de las acciones y controles incluyendo los niveles de riesgo y cumplimiento. Permiten conocer si la organización cumple sus objetivos de negocio de acuerdo con el objetivo de apetito de riesgo fijado, y acorde a las tolerancias definidas y sirven como criterio para la toma de decisiones.

Deben entenderse como alertas que se activan cuando se sobrepasan (por exceso o por defecto) los niveles de riesgo fijados. En caso de activarse, dependiendo del ámbito en el que estén definidos, las acciones a emprender variarán:

- Las áreas operativas alertan de que se está produciendo el riesgo lo que indicaría que los controles no tienen la efectividad adecuada y deben ser revisados.
- A nivel de órganos de dirección, alineados con el apetito de riesgo, sirven para poner en marcha las acciones de gestión definidas en el marco de apetito de riesgo para cuando se sobrepasen los niveles de tolerancia marcados.

Para que un indicador de riesgo sea plenamente funcional debe estar integrado en un sistema de control de riesgos que incluya una política escrita y actualizada de Gestión de riesgos, donde se describan los indicadores asignados a cada riesgo clave, su ámbito de aplicación dentro de la compañía, sus umbrales de tolerancia, la periodicidad de los controles y

las acciones a emprender en caso de vulnerar esos umbrales y, otra política de apetito de riesgo, donde se definan los valores de referencia de los indicadores de apetito de riesgo y los intervalos de apetito, tolerancia y capacidad establecidos así como las acciones de gestión a emprender en caso de vulnerarse.

Por último, no se debe confundir los KRI con los indicadores clave de desempeño (Key Performance Indicators, KPI), los cuales se usan para medir el desempeño de un departamento o una empresa con respecto a la consecución del resultado esperado.

2. CARACTERÍSTICAS DE UN INDICADOR DE RIESGO

Las características que debe tener un indicador de riesgo están recogidas en el acrónimo "SMART": específicos, medibles, alcanzables, relevantes y revisados en un tiempo/plazo fijado.

- **Específicos (S)**

Que un indicador sea específico significa que debe tener un objetivo concreto y bien definido. Un indicador definido de manera específica debería poder dar respuesta a las siguientes preguntas: ¿Quién está involucrado en su generación?
Para ello es necesario identificar claramente al área responsable de su consecución. ¿A qué riesgo concreto corresponde? ¿cuáles son los límites de riesgo definido?, y ¿los intervalos de tolerancia?

- **Medibles (M)**

Cuando algo es medible se pueden establecer criterios concretos para cuantificar y evaluar el progreso con el fin de hacer las modificaciones necesarias. Por tanto, los indicadores deben ser cuantificables de manera que indiquen claramente si el límite fijado se ha sobrepasado o no. El ser medible debe indicar claramente si el límite fijado se ha sobrepasado o no.

Debe referirse a unidades concretas (por ejemplo, número de días, empleados, porcentajes, valores monetarios, duraciones de tiempo, etc).

Los indicadores deben tener valores que sean precisos y no propensos a una subjetividad excesiva (por ejemplo, los valores cardinales son más precisos que los ordinales).

Es conveniente que los datos a los que se refieren se basen en fuentes primarias, es decir, datos directos de la fuente original y no sujetos a interpretaciones por un tercero. Deberían ser fáciles de recopilar y monitorizar. Por ejemplo, los indicadores que se describen por texto tienden a ser subjetivos y son más fáciles de malinterpretarse que los numéricos.

- **Alcanzables (A)**

Un indicador alcanzable es razonable y conseguible. La organización debe revisar que no se establezcan valores imposibles de alcanzar en los límites de riesgo (lo que podría indicar que siempre se está por debajo del límite y no hay que emprender ninguna acción correctora), pero tampoco limites no mejorables, que no supongan una motivación para las áreas.

Un indicador alcanzable debe ser realista. Al establecerlo, debe ser posible identificar oportunidades o recursos que tal vez no se habían considerado inicialmente. Esto implica que hay que tener en cuenta para su definición tanto las posibilidades como las limitaciones ya sea de recursos humanos como de tipo económico.

Un indicador alcanzable responde a preguntas que se responden con los planes de acción fijados entre la Alta Dirección y las áreas gestoras de los riesgos: ¿Cómo se puede alcanzar la meta?

- **Relevantes (R)**

Un objetivo relevante es aquel que está alineado con otras metas y que, por tanto, tiene sentido en el conjunto del proyecto. Los indicadores elegidos han de ser relevantes, estar alineados con el plan estratégico anual.

Un indicador relevante debe ayudarnos a contestar a estas preguntas: ¿el indicador elegido ayuda a cuantificar o medir el riesgo? y ¿ayuda a que la organización pueda controlar y o gestionar la exposición y sus consecuencias?

- **Temporal: con límite de tiempo (T)**

Es importante establecer la medición del indicador dentro de un marco de tiempo, fijando una fecha límite, ya que esto ayuda a concentrar todos los esfuerzos en alcanzar la meta. Los indicadores son anuales, por regla general, pero se monitorizan en periodos trimestrales. Si hubiese incumplimientos a nivel trimestral, se toman medidas de manera preventiva, para que a nivel anual no se incumpla el límite, y se pueda tener una reacción durante el ejercicio, sin sobresaltos si solo se monitoriza una vez al año.

Otras características esenciales que proponemos que han de tener los indicadores de riesgo que se elijan son las siguientes:

- *Simplicidad*, siendo capaces de diagnosticar una actividad o proceso en concreto de forma sencilla y comprensible.

- *Veri icabilidad*, siendo capaces de identificar el cálculo trazado y verificado para obtener el dato.

- *Robustez*, no susceptible de manipulación (no solo en los datos, sino en conductas que puedan desvirtuarlo y hacer que las anomalías pasen inadvertidas. Evitar “trabajar para el indicador”.

- *Revisión y cuestionamiento continuo*, ya que han de debatirse, han de consensuarse y hay que analizar el resultado, preferiblemente en el seno de un comité, tanto a la hora de definirse, como a la hora de monitorizar el resultado, de manera que no haya malas interpretaciones, sino consenso en el resultado de las mediciones, en cuanto a la cuantía de desviación. Deben revisarse de manera continua, pues incluso alguno puede dejar de tener valor, o ya no responder a la realidad de la gestión de los riesgos. NNo existe una respuesta adecuada que defina la correcta frecuencia de los informes sobre los indicadores de riesgo,

pues dependerá de la naturaleza de los riesgos, indicadores y de los flujos de reporte e información en cada organización. La presentación de resultados de dichos indicadores debe estar vinculada a la oportunidad de la toma de decisiones y se requerirá la formulación de acciones e informes de diferente frecuencia para adaptarse a audiencias específicas. Si bien, nuestra propuesta es que al menos sea trimestral.

- *Uniformidad y consistencia durante el ejercicio anual*, por lo que se mantienen y comparan los datos periódicamente. Los indicadores han de ser prospectivos, comparables a lo largo del tiempo. Auditables.

En la guía de "La Función de la Gestión de Riesgos en las entidades aseguradoras" se hacía hincapié en que la función gestión de riesgos en su labor de asesoramiento y apoyo a las líneas de gestión desempeñaba un rol clave en la definición de una metodología de riesgo adecuada y útil que aportara valor a la organización en la toma de decisiones. Será pues esencial, que la función gestión de riesgos en su asesoramiento en la identificación y establecimiento de los indicadores de riesgo a utilizar por la organización tenga en cuenta estos atributos mencionados anteriormente, y pueda debatir y consensuar con el resto de las áreas y funciones involucradas en el sistema de gestión de riesgos.

3. CALIBRACIÓN: UN PASO ADELANTE EN LA GESTIÓN POR INDICADORES

No solo es necesario identificar el indicador a usar para medir el riesgo, sino ser capaz de equilibrarlo para calcular el impacto de su incumplimiento en balance/cuenta de pérdidas y ganancias.

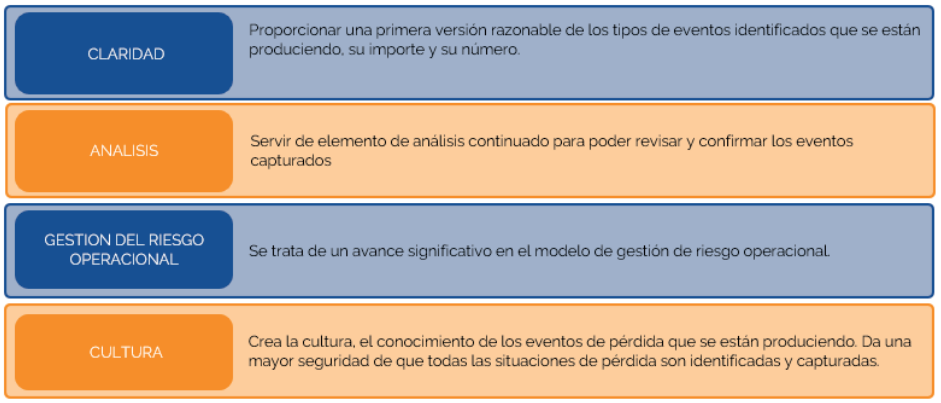
Un buen ejemplo de incorporar la gestión y control de estos indicadores en la toma de decisiones es que afecten a la política de remuneración.

KRI´s, KPI´s y la Base de Datos de Eventos de Pérdida

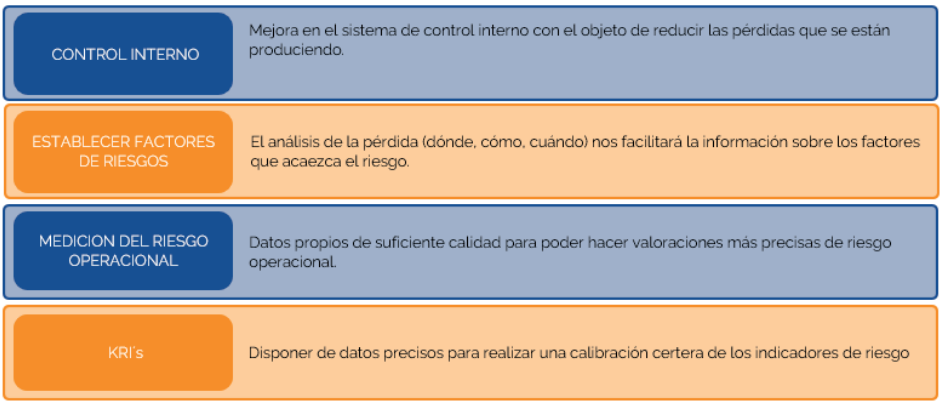
Para el establecimiento de un indicador de riesgo (Key Risk Indicator KRI) y para su posterior calibración y establecimiento de umbrales, la compañía debería tener previamente implementados indicadores de desempeño (Key Performance Indicator KPI) y disponer de información de eventos de pérdida, que nos permitirán cuantificar el riesgo.

Indicador clave de riesgo (KRI, Key Risk indicator)	Indicador clave de desempeño (KPI, Key Performance indicator)
• Métrica para determinar/alertar cuándo se está superando el apetito de riesgo	• Métrica para determinar el desempeño de un departamento/organización con respecto a la consecución del resultado esperado
• Definición en base al apetito de riesgo	• Definición en base a los datos del desempeño histórico de los departamentos/organizaciones

El proceso de captura de eventos de pérdida permite lo siguiente:



A medida que se acumula información histórica con el suficiente contraste de integridad y calidad, la captura de eventos permitirá adicionalmente lo siguiente:



El seguimiento de los eventos de pérdida no deja de ser una **medida reactiva** a un riesgo que ya se ha producido, pero este conocimiento nos facilita el análisis y nos aporta información sobre cuáles son los factores de riesgo que hacen que el riesgo se produzca y si se dispone de ello es clave para el establecimiento de indicadores de riesgo (KRI) como **medida proactiva.**

Estas herramientas facilitarán el establecimiento de los indicadores de riesgo y la definición de los umbrales de tolerancia, ya que ayudarán a que estos estén basados en datos reales de ocurrencia de los eventos a los que está expuesta la compañía.

Como criterio general, un indicador de desempeño, o en su caso, el seguimiento de la evolución de un determinado evento de pérdida como, por ejemplo, el “pago de prestaciones”, nos permiten monitorizar en qué medida está acaeciendo el evento de riesgo concreto y nos debería facilitar el diseño de un indicador de riesgo que nos ayude a establecer una métrica que ayude a medir que factores de riesgo son una alerta de la ocurrencia del riesgo. El indicador de riesgo (KRI) a diferencia del indicador de rendimiento (KPI) proporciona una señal temprana y oportuna de una exposición al riesgo.

El análisis de la base de datos de eventos de pérdida y de cada uno de los eventos, así como de la causa raíz que genera los eventos debe tener un vínculo con el indicador de riesgo que se establezca, cuanta más información real tengamos más acertada será la elección de ese factor de riesgo y del indicador asociado.

EJEMPLOS DE INDICADORES CLAVE DE RIESGO BAJO ESTRUCTURA ORIC

Como explicamos anteriormente, tomando como estructura marco la propuesta por el Consorcio ORIC, presentada en el punto 2 de este documento y una vez analizados los atributos que proponen las buenas prácticas y que han de tener los indicadores de riesgo, en este apartado nos centraremos en concretar indicadores sencillos y específicos para cada una de las actividades propuestas en el marco.

1. FRAUDE INTERNO

Riesgo de actuaciones efectuadas con ánimo de dolo o lucro por parte del personal interno de la organización, así como acciones no autorizadas por el uso incorrecto de los poderes o atribuciones otorgados al personal de la compañía.

RIESGO	INDICADOR
1.1. Actividades no autorizadas - Operaciones no reportadas (intencionadas) - Operaciones mal reportadas (intencionadas) - Tipo de operación no autorizada (con pérdidas monetarias)	Autorizaciones o Pagos aprobados por encima del límite establecido o por personal no autorizado
	nº pagos introducidos/validados y pagados por el mismo usuario
	Nº de cancelaciones de registros, por ejemplo nº facturas borradas del sistema o de apuntes contables
1.2. Robos y fraude - Hurto / Extorsión / Malversación / Robo - Malversación de activos - Destrucción delictiva de activo - Falsificación (interno) y suplantación de identidad - Contrabando - Suplantación de identidad - Incumplimiento o evasión de las obligaciones fiscales - Soborno - Utilización de información privilegiado(tráfico, contratación, etc.)	Número de casos de fraude detectados, Número de reclamaciones de clientes, número casos registrados en el canal de denuncias
	Robo de datos de clientes / brechas de privacidad intencionadas

2. FRAUDE EXTERNO

Riesgo como consecuencia de la comisión de hechos de carácter delictivo por personal no interno de la compañía, clientes, proveedores...

En este apartado sí nos parece interesante descender y particularizar al ejemplo práctico aplicable a entidades aseguradoras, dada el gran número de colaboradores de distinta naturaleza con los que se trabaja en el sector y sus particularidades. Los indicadores en otras organizaciones podrán particularizarse a la naturaleza de cualquier proveedor y sus procesos y servicios ofrecidos a las organizaciones.

RIESGO		INDICADOR
Valoración inadecuada de los daños declarados en el siniestro por parte de los peritos tasadores en expedientes de siniestros	Valoración inadecuada de los daños declarados en el siniestro por parte de los peritos tasadores en expedientes de siniestros	Valoraciones rechazadas / total de valoraciones
Valoración inadecuada por parte de un perito de otra entidad aseguradora de los daños declarados en el siniestro de una solicitud de reembolso	Valoración inadecuada por parte de un perito de otra entidad aseguradora de los daños declarados en el siniestro de una solicitud de reembolso	Valoraciones rechazadas / total de solicitudes de reembolso
Valoración inadecuada de los daños declarados en el siniestro por parte de los peritos médicos en expedientes de siniestros	Valoración inadecuada de los daños declarados en el siniestro por parte de los peritos médicos en expedientes de siniestros	Valoraciones rechazadas / total de valoraciones
Valoración inadecuada de los Gastos Asistenciales	Riesgo de abonar gastos asistenciales fuera de Convenio desproporcionados	Nº de rechazos / total de solicitudes de revisión
Riesgo de pago de mismos daños en diferentes siniestros	Riesgo de pago de mismos daños en diferentes siniestros	Control por rechazos por número de antecedentes / total de solicitudes por ramo
Falta de rotación de peritos tasadores	Falta de rotación de peritos tasadores en mismas zonas	Comparativa peritos asignados a zonas en diferentes períodos
Riesgo de abono de daños por encima de los importes medios	Connivencia con talleres de zona para elevar precios	Control de los importes medios de reparaciones de vehículos por zonas y por tipos de daños
	Connivencia con clínicas fuera de Convenio para elevar precios	Control de los importes medios de gastos asistenciales (rehabilitación por ej.) por zonas y tipo de prestación sanitaria
Riesgo de conflicto de intereses	Perjudicado sea colaborador de la entidad	Nº alertas activadas por este tipo / total de solicitudes
Riesgo de pago de daños previos en póliza distinto tomador	Cambio de titular de la póliza para evitar alertas y poder declarar daños previos al siniestro	Nº alertas actividas por este tipo / total de solicitudes
Riesgo de fraude por parte del cliente al proporcionar datos incompletos o incorrectos necesarios para la valoración del riesgo.	Datos aportados son incorrectos con el objeto de obtener un enriquecimiento injusto	Nº solicitudes rechazadas por datos incorrectos / total de solicitudes
Riesgo de fraude en el ramo del seguro de automóviles	Coincidencia de matrícula interviniente en más de 4 siniestros en el mismo año	Coincidencia de matrícula interviniente en más de 4 siniestros en el mismo año
	Coincidencia de matrícula con expediente anterior donde el vehículo hubiera sido declarado siniestro total	Coincidencia de matrícula con expediente anterior donde el vehículo hubiera sido declarado siniestro total
	Coincidencia de datos en partícipes diferentes (por ejemplo IBAN, teléfonos, direcciones...)	Coincidencia de datos en partícipes diferentes (por ejemplo IBAN, teléfonos, direcciones...)
	Alertas por siniestros cercanos a la contratación (por ejemplo 10 días desde fecha contratación)	Alertas por siniestros cercanos a la contratación (por ejemplo 10 días desde fecha contratación)
Riesgo de fraude en el ramo de seguro diversos	Coincidencia de datos en partícipes diferentes (por ejemplo IBAN, teléfonos, direcciones...)	Coincidencia de datos en partícipes diferentes (por ejemplo IBAN, teléfonos, direcciones...)
	Coincidencia de póliza interviniente en más de 4 siniestros en el mismo año	Coincidencia de póliza interviniente en más de 4 siniestros en el mismo año

3. PRÁCTICAS LABORALES Y SEGURIDAD EN EL TRABAJO

Riesgo de pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, de higiene o seguridad en el empleo, del pago de reclamaciones por daños a las personas, o de eventos de diversidad o discriminación.

RIESGO		INDICADOR
3.1. Relaciones de empleados	Incumplimiento de la legislación y regulación laboral pertinente	Número de despidos improcedentes y litigios laborales Número de sanciones administrativas
	Gestión de recursos humanos	Ratio de rotación de personas superior a un % prestablecido, número de posiciones abiertas y el periodo medio de contratación
	La falta de competencias y/o capacidades de los empleados afecta negativamente a los clientes y a la propia Entidad.	Número de horas de formación por persona anualmente
3.2. Seguridad del entorno	Daños evitables por la Entidad por la falta de protección de la salud y seguridad de sus empleados, residentes, pacientes, clientes, visitantes y otras personas directamente afectadas por las actividades de la Entidad.	Número de accidentes laborales ocurridos, número de lesiones graves o fallecimientos Ratio número de bajas laborales divididas en problemas físicos y psicológicos por el total de empleados
	Incumplimiento de la legislación en materia de salud y seguridad que dé lugar a acciones legales.	Porcentaje mensual de accidentes laborales respecto al nº de empleados en plantilla
3.3. Diversidad y discriminación	Trato desfavorable o negativo a los empleados	Puntuación inferior al <x% de las preguntas sobre Ambiente de trabajo en la encuesta anual a los trabajadores.
	Discriminación sexual	Ratio de hombres/mujeres en puestos de responsabilidad

4. PRÁCTICAS CON CLIENTES, PRODUCTOS O NEGOCIOS

Riesgo por pérdidas derivadas del incumplimiento involuntario o negligente de una obligación profesional frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto.

Riesgo por expectativas de clientes no satisfechas por malas prácticas o por deficiencias en la venta de servicios. Multas, sanciones o indemnizaciones por incorrectas prácticas comerciales.

RIESGO	INDICADOR
4.1. Adecuación, información y confidencialidad - Fallos o violaciones de directrices --> solicitud del seguro - Fallo en la información sobre la idoneidad del cliente --> conocimiento del riesgo, adecuación clientes vs producto - Revelación de información de consumidores --> privacidad, confidencialidad - Violación de la intimidad --> seguridade de la información - Pérdidas producidas por ventas demasiado agresivas --> IDD - Abuso de información confidencial	- Seguimiento de actividad en redes sociales o medios de comunicación: nº de "dislikes" referentes a proceso de venta del seguro (adecuación solicitud a propuesta del seguro, etc) - Nº de issues de auditoría interna y verificaciones de control interno - Nivel de satisfacción (clientes, mediadores): encuestas, NPS relacionadas con la información del producto - Nº de incidentes (por derechos de privacidad, - Nº de quejas (por derechos de privacidad, mala venta de producto, coberturas no adecuadas o suficientemente conocidas, - Nº de sanciones de AEPD - Nº de demandas judiciales por coberturas no inlcuidas, por información o conducta de mercado (pero no por mala praxis)
4.2. Prácticas de mercado o de negocio impropias - Sentencia judicial antimonopolio - Prácticas de mercado incorrectas - Manipulación del mercado - Utilización de información privilegiada (tráfico, contratación, etc - Actividades no autorizadas en la entidad - Blanqueo de dinero	- Seguimiento de actividad en redes sociales: nº de "dislikes" referentes a facilidad de acceso a información, trato justo al cliente, etc. - Nº de quejas ante el supervisor con resultado desfavorable para la compañía (por denegación de coberturas, etc). - Nº de inspecciones relacionadas con condicionados o prácticas de cobertura de mercado
4.3. Errores o defectos en los productos - Defectos del producto - Fallos de valoración ---> IDD / POG consumidores objetivos para los que se configura el producto	- Estudios de notoriedad marca y bachmark mercado: evolución con respecto al estudio anterior y benchmark de pares. '- Seguimiento de actividad en redes sociales: nº de "dislikes" referentes a producto, coberturas, precio - Nivel de satisfacción (clientes, mediadores): encuestas, NPS relacionadas con satisfacción del producto (coberturas incluidas, etc)
4.4. Selección, soporte y exposición de clientes - Falta de investigación del cliente según los procedimientos internos - Exceso de riesgo con el cliente	- Nº de sanciones por inadecaución de producto a cliente
4.5. Actividades de consultoría - Disputas relacionadas a actividades de asesoramiento --> venta inadecuada, IDD	- Nº de quejas (mala venta de producto, coberturas no adecuadas o suficientemente conocidas

5. DAÑOS A ACTIVOS MATERIALES

Riesgos de acontecimientos externos, ya sean naturales, accidentales, como provocados que dañen a los activos físicos o interrumpan actividades de la empresa.

5.1. Desastre y eventos. Pérdidas por desastres naturales Pérdidas humanas por causas externas	Número de cortes de suministro eléctrico
	Número de eventos de daños por agua registrados
	Número de personas lesionadas/fallecidas por el evento
	Numero de intentos de acceso a sedes no autorizados identificados
	Número de robos en activos (robos infraestructuras)
	Número de robos/pérdidas de documentación
	Número de personas lesionadas/fallecidas por el evento
	INDICADOR Coste de pérdidas provocadas (directas o cubiertas por la póliza de seguros a las que se transfiere el riesgo);
	Coste medio de los daños físicos generados por el evento en los activos de la compañía
	INDICADOR Coste de oportunidad de ingresos por inactividad a consecuencia del daño a los bienes
	Coste económico de pérdida de ingresos por la inactividad producida debido al evento que daña el activo

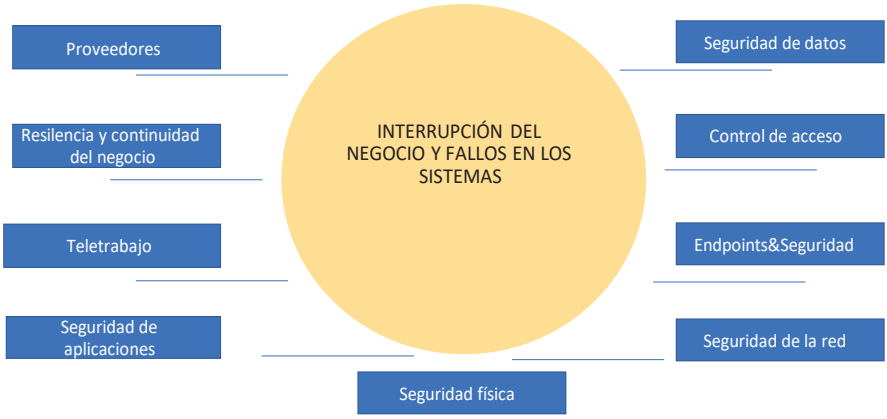
6. INTERRUPCIÓN DEL NEGOCIO Y FALLOS EN LOS SISTEMAS

Riesgo por deficiencias en el diseño e implantación de sistemas de información, deficiente funcionamiento de los sistemas de comunicación.

NIVEL 1	NIVEL 2	NIVEL 3
6) Interrupción del negocio y fallos en el sistema		
Riesgo por deficiencias en el diseño e implantación de sistemas de información, deficiente funcionamiento de los sistemas de comunicación.	6.1. Sistemas	- Software - Hardware - Telecomunicaciones - Fallos de alimentación de sistemas

En este apartado, hemos considerado que era necesario profundizar en la propuesta del marco ORIC y basarnos en los distintos subriesgos que pueden integrar un adecuado sistema de seguridad y en los que se podría producir fallos en los mismos que generasen una interrupción del negocio.

Para ello nos hemos basado en la propuesta de subriesgos del marco INCIBE (Instituto Nacional de Ciberseguridad de España dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial), para proponer indicadores que aborden la integridad de los riesgos de seguridad por interrupción del negocio y fallos en los sistemas.



Fuente: AGERS

RIESGO	INDICADOR
Proveedores: Riesgo por deficiencias en el diseño e implantación y control de sistemas con los proveedores, y en el funcionamiento de los sistemas de información e intercambio con los proveedores	% de proveedores que no han pasado por una revisión de criticidad
	% de proveedores críticos cuyos datos no se capturan en un inventario
	% de los acuerdos críticos de externalización que no han sido sometidos a la diligencia debida
	% de acuerdos críticos de externalización sin evaluaciones de riesgos y control
	% de acuerdos críticos de externalización sin un contrato firmado en vigor o/y sin contrato firmado en vigor; o sin propietario acordado o asignado una correcta gestión de obligaciones
	% de acuerdos críticos de externalización en los que no hemos completado una evaluación de viabilidad financiera
	% de acuerdos críticos de externalización sin continuidad comprobada del negocio
	% de acuerdos críticos de subcontratación sin planes de terminación/salida aprobados

RIESGO	INDICADOR
Resilencia y continuidad de negocio: Riesgo por deficiencias en el diseño e implantación de un plan de contingencias y continuidad de negocio	% de análisis de impacto en el negocio (BIA) que no se han completado y revisado en su totalidad en los últimos 12 meses
	% de planes de continuidad de negocio no completamente completados y revisados en los últimos 12 meses
	% de procesos críticos de negocio sin planes de contingencia manual
	% de procesos críticos de negocio que no han sido sometidos a una prueba exitosa para la pérdida de acceso a la tecnología
	% de procesos críticos que no se han sometido a una prueba satisfactoria para la pérdida de acceso a las ubicaciones
	% de procesos críticos de negocio que no han sido sometidos a una prueba exitosa para la indisponibilidad de los empleados
	% de procesos críticos del negocio que no han sido sometidos a una prueba exitosa para la pérdida de servicios subcontratados
	% de aplicaciones críticas sin capacidad probada de recuperación ante desastres
	% de cambios fallidos de TI en la producción
	% de fallas críticas de backup de aplicaciones
	% de equipos de gestión de crisis e incidentes que no se han ejercitado en los últimos 12 meses

RIESGO	INDICADOR
Riesgo por deficiencias en el diseño e implantación de sistemas de control de acceso	% Sistemas que no cuentan con autenticación segura
	% cuentas clave (con privilegios) en las que no se ha implantado un multi factor de autenticación
	% cuentas en las que no se ha revaluado (de manera periódica) los privilegios.
	% usuarios con acceso de “cliente abierto”
	%usuarios que son baja en la entidad y que no se han dado de baja en los accesos o sistemas/dispositivos
	% dispositivos de usuarios sin las herramientas de seguridad necesarias (antivirus; control de accesos, etc. según se haya definido por la entidad un nivel mínimo de seguridad obligatorio)

RIESGO	INDICADOR
Riesgo por deficiencias en el diseño e implantación de un sistema de control de acceso a activos físicos (seguridad física)	% de activos de infraestructura de IT no identificados en el Inventario
	% de puntos finales/dispositivos de usuario final no registrados en el inventario de activos
	%de infraestructuras que no son activos revalidados por los propietarios en los últimos 12 meses
	%activos críticos con características específicas de acceso físico

RIESGO	INDICADOR
Riesgo por deficiencias en el diseño e implantación de un sistema de teletrabajo	% dispositivos revisados para garantizar las medidas de seguridad y continuidad de operaciones (recuperación/pérdida de datos) del total destinados a teletrabajo
	% dispositivos con vulnerabilidades críticas no parcheadas dentro de los plazos requeridos

RIESGO	INDICADOR
Riesgo por deficiencias en el diseño e implantación de un sistema seguridad de la red	•% de sistemas que permiten el acceso desde redes que no son de confianza para empleados y contratistas sin multi factor authentication (MFA)
	•% de sitios web conocidos con conexión a Internet con vulnerabilidades cuando se analizan
	•% de usuarios que sucumben al phishing en exceso del número esperado basado en la clasificación de susceptibilidad
	•%dispositivos de red con vulnerabilidades críticas no parcheadas dentro de los plazos requeridos

RIESGO	INDICADOR
Riesgo por deficiencias en el diseño e implantación de un sistema seguridad de los datos	•% de solicitudes que contienen datos confidenciales que no pueden aplicar el privilegio mínimo
	•% de objetos de datos clasificados como confidenciales/altamente confidenciales sin análisis
	•%objetos de datos no clasificados en materia de protección de datos
	•%objetos de datos sin definición de medidas de prevención de pérdida de datos
	•% objetos de datos revisados que cumplen con las medidas de privacidad y protección de datos
	•Nº brechas de seguridad informadas a la Agencia de Protección datos en el periodo
	•Nº vulnerabilidades de datos detectadas sobre total de objetos de datos revisados
	•%brechas de seguridad/ataques identificados

RIESGO	INDICADOR
Riesgo por deficiencias en el diseño e implantación de un sistema seguridad de las aplicaciones (software, hardware, usuario final, endpoints)	•% de aplicaciones (software) con vulnerabilidades críticas no parcheadas dentro de los plazos establecidos
	•% de servidores (hardware) con vulnerabilidades críticas no parcheadas dentro de los plazos establecidos
	•% de dispositivos de usuario final con vulnerabilidades críticas no parcheadas dentro de los plazos establecidos
	•%de dispositivos de usuario final/hardware al final de su vida útil sin medidas de apoyo mínimo a la seguridad
	•%dispositivos de usuario final/sistemas sin medidas mínimas de seguridad

NOTA: estos son ejemplos de algunos indicadores que pueden definirse. En el ejemplo práctico del punto 6, se ha incluso descendido a un nivel de detalle mayor en indicadores de seguridad y privacidad según las características y naturaleza de los riesgos de la compañía elegida para el ejemplo práctico.

7. EJECUCIÓN DE PROCESOS

7) Ejecución, entrega y gestión de procesos.		
Riesgo debido a las deficiencias de los procesos de la compañía, tanto por el diseño como por la gestión de los mismos. Errores en la ejecución de procedimientos y operaciones.	**7.1. Captura, ejecución y mantenimiento de transacciones**	- Errores en la introducción de datos y mantenimiento
		- Incumplimiento de fechas límite y/u obligaciones
		- Disfunciones en modelos de valoración o sistemas
		- Error de contabilidad o error de atribución a una entidad
		- Mala ejecución de tareas
		- Incumplimiento o fallos de entrega
	7.2. Supervisión y reporte de información	- Incumplimiento de la obligación de informar
		- Importe externo inexacto
	7.3. Errores o pérdida de documentos	- Falta de cláusulas de exención de responsabilidad
		- Falta de documentos jurídicos o documentos jurídicos incompletos
	7.4. Gestión de cuentas de clientes	- Acceso sin autorización a información sensible
		- Documentación de clientes incorrecta
		- Pérdidas o daños del activo del cliente por negligencia
	7.5. Contrapartes de negocio	- Mala actuación de la contrapartida (no cliente)
		- Disputas varias de la contrapartida (no cliente)
	7.6. Proveedores y prestaciones de servicios.	- Subcontratación de servicios propios ("outsourcing")
		- Disputas de vendedores

El objetivo era abordar el bloque ORIC 7, "Procesos", de la misma manera que habíamos analizado y propuesto indicadores para cada uno de los bloques 1 a 6 anteriores ("Estructura ORIC").

Tras el debate y el análisis, el grupo de trabajo llegó a la siguiente conclusión:

En líneas generales, en la mayoría de los grupos a los que hace mención ORIC, son procesos "controlados" por otras unidades de control según la naturaleza de los procesos, así, por ejemplo, control interno de los procesos, las de continuidad y contingencias, los departamentos financieros que generan o revisan la información financiera (informes) o por unidades de riesgos específicas, etc. Estas unidades tienen establecidos un apetito de riesgo o unos límites de control que deben supervisar.

Cuando estos niveles de incidencias o gestión de riesgo se superan es cuando informan a la unidad/función de gestión de riesgos dada la importancia, pues pueden existir causas significativas para estos incumplimientos.

La Función de Riesgos aparece más en estos casos como "Coordinadora", y no tanto como unidad encargada de la gestión y del control específico de esos procesos, aunque sí alerta a los Comités de riesgos a los que reporta, si se producen alertas en los incumplimientos o se considera que puede ser un mayor problema los incumplimientos transmitidos por las demás unidades de control.

EJEMPLO PRÁCTICO DE LA CREACIÓN E IMPLEMENTACIÓN DE UN INDICADOR DE RIESGO (KRI)

A continuación, se incluye un ejemplo sobre determinados indicadores de riesgo relacionados con la privacidad y seguridad de la información, así como su relación con el apetito de riesgo, la política y el proceso asociado a la gestión y protección de los datos.

La compañía considera entre los riesgos que pueden suponer una mayor amenaza para la consecución de su estrategia y sus objetivos, el riesgo asociado a la privacidad de los datos y a la seguridad de la información, por lo que realiza un especial seguimiento y monitorización de este.

El riesgo de privacidad y de seguridad de la información se incluye en el mapa de riesgos de la compañía, y es uno de los riesgos que supone un impacto potencial más alto para la entidad. Como parte de la gestión pormenorizada del mismo, se incluye en un informe trimestral, que se presenta en el Comité de Riesgos, así como en el informe ORSA que se presenta al supervisor.

Asimismo, la compañía dispone de una política relacionada con la seguridad de la información y con la privacidad de los datos en la que se desarrollan los principios necesarios que hay que cumplir para el tratamiento correcto de la información y en donde se establecen los límites de riesgo que definen el nivel acordado de exposición, más allá del cual se requiere la aceptación del riesgo o una mitigación adicional, y los controles mínimos que deben implementarse para asegurar que se cumplan los requerimientos de la política.

Asimismo, en la política se incluye el concepto de “materialidad” que se define por las dimensiones de impacto y probabilidad dentro de un determinado límite (apetito de riesgo)

Ejemplo de algunos riesgos y límites y controles mínimos relacionados con privacidad y seguridad de la información:

Los siguientes límites de riesgo aseguran que los riegos derivados de privacidad se minimizan teniendo en cuenta que la entidad no tiene apetito sobre incidentes de datos personales que resulten en un impacto material para los clientes, los empleados o los resultados.

Los límites de riesgo representan los niveles de exposición por encima de los cuales, si se superasen, debe ser comunicado a través de la estructura de gobierno adecuada, con el fin de garantizar que dichos incumplimientos se elevan al Consejo. La Dirección del negocio debe gestionar todos los riesgos e incidentes incluso cuando se encuentren por debajo de los límites de riesgo establecidos.

A modo de ejemplo, podríamos establecer un nivel de límites y acciones, en función de los umbrales de alerta y las medidas correctivas:

Rojo. El valor de este indicador es demasiado alto/bajo, lo que sugiere que la organización puede estar expuesta a un riesgo significativo. Se requiere una acción inmediata por parte de la dirección para gestionar los riesgos en cuestión.
Naranja. El valor de este indicador es más alto/bajo de lo normal, lo que sugiere que la organización puede estar expuesta a un nivel elevado y potencialmente significativo de riesgo. Se requiere la atención de la dirección para determinar si es necesario tomar medidas.
Verde. El valor del indicador está dentro de los parámetros normales, lo que sugiere que la organización no está expuesta a un riesgo significativo. No se requiere ninguna acción: el indicador y sus riesgos asociados están en condiciones adecuadas.

El esquema de colores en base a la materialidad establecida, y su consenso y aprobación, permitirá consensuar y eliminar interpretaciones subjetivas, y además fortalecerá un mismo lenguaje a nivel de gestión de riesgos, tanto en los gestores, como en las unidades de control y supervisión, así como en la Alta Dirección y el Consejo de Administración.

Frecuencia

La entidad establece que la frecuencia mínima a establecer en la monitorización de los resultados de los indicadores de riesgo será trimestral, al considerar que esta periodicidad permitirá a la entidad desarrollar medidas correctoras en caso de incumplimiento de manera ágil, y siempre bajo control.

Riesgo y Límite asociado	1. Tratamiento de datos sin base legítima: se incluye la falta de consentimiento explícito cuando sea necesario.	
Límites de Apetito de Riesgo: Una brecha en el apetito de riesgo ocurre cuando…	Control	Evidencia del control
La entidad no establece bases legales adecuadas para el tratamiento de datos que resulta en daños materiales a los clientes, personas y/o resultados	• Gobernanza: Foros de gobernanza para supervisar el riesgo de privacidad. • Avisos de privacidad: Existen procesos para garantizar que el uso de cualquier información personal tiene una base legal	• Actas de las reuniones. • Documentación del foro. • Acciones identificadas en el foro. • Copia de los procedimientos y controles. • Materiales de gobernanza.

Riesgo y Límite asociado	2. Datos inexactos. Mala calidad de los datos: No mantener los datos exactos y actualizados.	
Límites de Apetito de Riesgo: Una brecha en el apetito de riesgo ocurre cuando…	Control	Evidencia del control
Por ejemplo, la entidad cobra a los clientes una prima incorrecta; la entidad no puede contactar a un paciente con los resultados de su informe médico; la entidad envía un informe médico a la persona equivocada, etc.	• Evaluación de riesgos: Los riesgos se registran, se supervisan y se escalan adecuadamente • Supervisión y control de la calidad de los datos personales para controlar su exactitud, integridad, coherencia y fiabilidad.	• Copia de los procedimientos de control y gestión • Evaluaciones de riesgos • Entradas en el registro de riesgos • Supervisión de las pruebas de control.

Riesgo y Límite asociado	3. Conservación: Falta de eliminación o anonimización de los datos cuando ya no son necesarios (motivos legales u operativos)	
Límites de Apetito de Riesgo: Una brecha en el apetito de riesgo ocurre cuando…	Control	Evidencia del control
Por ejemplo, la entidad no elimina los datos inexactos que posteriormente se revelan y causan un perjuicio los clientes.	• Supervisión y control de la conservación de los datos personales. • Procesos y controles que garantizan el cumplimiento de la política, la gestión y revisión de los riesgos. • Los requisitos de conservación de datos de privacidad están claramente articulados y su cumplimiento se controla adecuadamente, incluyendo la supervisión de los procesos, sistemas y reglas establecidos para aplicar los requisitos de conservación de los datos personales.	• Copia de los procedimientos de control y gestión • Materiales de gobernanza • Materiales de comunicación • Informes de las pruebas de los procesos y controles con medidas correctoras cuando sean pertinentes • Calendario de conservación • Supervisión de las pruebas de control.

Riesgo y Límite asociado	4. Derechos de los interesados: Falta de respuesta a las solicitudes de derechos de los interesados.	
Límites de Apetito de Riesgo: Una brecha en el apetito de riesgo ocurre cuando…	Control	Evidencia del control
Por ejemplo, la entidad no responde a las solicitudes de derecho de acceso de los pacientes, lo que resulta en quejas al regulador y la entidad es investigada por ello; la Entidad responde a las solicitudes sin seguir procesos internos lo que resulta en la revelación no autorizada de información de terceros o legalmente privilegiada; la entidad borra por error datos resultando en la indisponibilidad permanente de los mismos.	• Riesgo de terceros: Existen procesos para identificar integrar y supervisar los requisitos de privacidad de los datos para terceros, principalmente de aquellos que procesan datos personales en nombre de la compañía y mantener la supervisión continua de los mismos. • Tramitación rápida de las solicitudes de derechos individuales: Existe un proceso adecuado para garantizar que todas las solicitudes de derechos individuales y las reclamaciones de personas que no están satisfechas con la forma en la que se gestionan sus datos personales se registran y se siguen hasta su resolución de manera oportuna y acorde a las leyes.	• Copia de los procedimientos de control y gestión • Evaluaciones de riesgos de terceros • Materiales de comunicación • El proceso se define, se comunica, se aprueba y se revisa en plazos definidos • Registro de solicitudes y reclamaciones • Copias de las respuestas a los denunciantes y al regulador

Riesgo y Límite asociado	5. Tratamiento inseguro: Falta de seguridad en el tratamiento de los datos e incapacidad de prevenir, ya sea accidental o ilícitamente, la: destrucción o pérdida de datos, la alteración de datos, y/o la divulgación o el acceso no autorizado a los datos.	
Límites de Apetito de Riesgo: Una brecha en el apetito de riesgo ocurre cuando…	Control	Evidencia del control
Por ejemplo, la entidad pierde los registros médicos y no puede restaurarlos; o los registros de salud de los clientes son hackeados y revelados en internet causando un perjuicio a los clientes.	• Formación y sensibilización: La formación y concienciación sobre la privacidad se lleva a cabo a través de una formación obligatoria y adecuada para aumentar la concienciación sobre la privacidad y los requisitos normativos. • Seguridad y control de la seguridad de la información: Existe una supervisión adecuada del riesgo de la seguridad de la información en relación con la privacidad • Se documenta y se eleva cualquier impacto en el perfil de riesgo	• Análisis de las necesidades de formación • Material de formación • Seguimiento de los registros de asistencia • Informes trimestrales de evaluación del apetito de riesgo

Riesgo y Límite asociado	06. Reporte de brechas de privacidad: No reportar las brechas de privacidad a los reguladores o clientes y/o personas dentro de los plazos requeridos.	
Límites de Apetito de Riesgo: Una brecha en el apetito de riesgo ocurre cuando…	Control	Evidencia del control
Por ejemplo, los procesos internos de reporte son demasiado lentos para llegar al equipo de privacidad, lo que resulta en demoras en el reporte de brechas al regulador después de "conocer" el incidente, y resulta en una reparación tardía para los interesados y/o multas del regulador; o un tercero reporta una brecha de privacidad directamente a los clientes sin ponerse previamente en contacto con la entidad.	• Gestión de incidentes: Existe un proceso para la investigación, evaluación y gestión coherente y eficaz de los incidentes relacionados con la privacidad. • Análisis de la causa / raíz y resumen de las lecciones aprendidas para determinar qué control. • Registro de los incidentes materiales para seguir las acciones resultantes de las investigaciones de los incidentes. Las acciones deben asignarse a un propietario y completarse de manera oportuna.	• Registro de incidentes • Informes de investigación y de las causas principales • Planes de acción actualizados

Indicadores clave (KRIs)

La monitorización de los riesgos se realiza, entre otros aspectos, mediante el seguimiento de incidentes registrados por el negocio, las revisiones periódicas de riesgos específicos, la presentación en los Comités pertinentes de los principales proyectos relacionados con privacidad y seguridad de la información, y mediante las campañas anuales de revisión de riesgos y controles realizadas, de forma coordinada, por los equipos de Privacidad, Seguridad de la Información y Riesgos.

Asimismo, la Compañía tiene identificados unos KRIs que le alertan sobre un incremento de exposición al riesgo y su comparación con el nivel establecido de apetito de riesgo.

A continuación, se muestran algunos ejemplos de KRIs relacionados con la privacidad y seguridad de la información.

- Número y porcentaje de proveedores de alto riesgo (que poseen datos de clientes o empleados / o tienen acceso a los sistemas o redes) que se han sometido a una revisión de seguridad por parte de terceros en los últimos 12 meses.
- Porcentaje de personal que ha completado con éxito la formación genérica obligatoria de concienciación sobre la seguridad en el periodo requerido.
- Número de incidentes de seguridad de la información y privacidad de prioridad uno (P1).
- Número de reclamaciones de clientes acerca del acceso, rectificación o cancelación de su información que deriva en una inspección que indica que se están incumpliendo la normativa de protección de datos.
- Número de incidentes de seguridad de la información (de los cuales las violaciones de los datos personales son un subconjunto) notificados a un regulador y porcentaje notificado dentro de los plazos reglamentarios prescritos (por ejemplo, 72 horas para los reguladores de la privacidad).
- Número de riesgos de privacidad fuera del apetito de riesgo.

- Porcentaje de la huella tecnológica que ha sido evaluada en materia de seguridad en los últimos 12 meses.
- Porcentaje de aplicaciones e infraestructuras críticas que han sido sometidas a pruebas de penetración/escaneo en los últimos 12 meses.
- Número y porcentaje de parches que no se han aplicado en un plazo de 30 días a las vulnerabilidades calificadas como críticas y altas
- Número y porcentaje de usuarios de sistemas que contienen datos de nivel 2 y 3 cuya identidad y derechos han sido recertificados en un plazo de 12 meses.
- Número y porcentaje del entorno tecnológico no cubierto por la supervisión de la seguridad.

Monitorización de informes y responsables del seguimiento

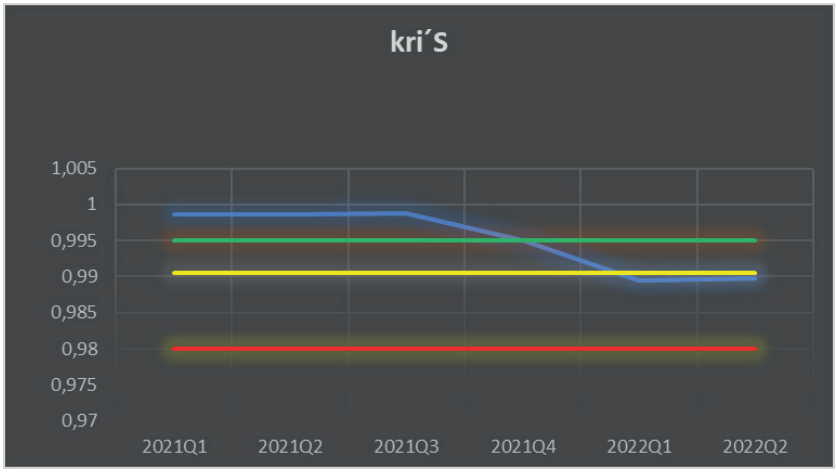
La entidad asegurará que las políticas, procesos y controles sean implementados y mantenidos para prevenir un incidente de datos personales que resulte en un impacto material para los clientes, personas o resultados de la entidad.

La primera línea de defensa es responsable de implementar las políticas y los límites de apetito de riesgo, y de garantizar la oportuna supervisión de la posición de riesgo de la compañía frente a los límites definidos. Con el apoyo y verificación de la 2ª, se garantiza una comprensión integral del perfil de riesgo de la Compañía.

Trimestralmente se remite al Comité de Riesgos un informe sobre el cumplimiento del apetito de riesgo para su aprobación.

Mostramos y proponemos algunos ejemplos de informes gráficos y fichas resumen que podrían elaborarse para cada indicador definido y que reflejan todos los conceptos analizados a lo largo de este documento.

KRIS´S						
Metrica	INDICADOR	APETITO	TOLERANCIA	CAPACIDAD	VALOR Q1	Nivel de Riesgo
A	% Disponibilidad del servicio	99,5%	99,1%	98,0%	99,8%	
B	Nivel de satisfacción (clientes, mediadores): encuestas, NPS	80%	70%	60%	78%	



Disponibilidad del servicio

DEFINICIÓN	OBJETIVO
Porcentaje de tiempo medio en que las aplicaciones que aplican o afectan a los procesos criticos estan disponibles en el mes de referencia.	Mide la disponibiñidad del servicio. Da una visión mensual del estado de los principales sistemas/aplicaciones que afectan a negocio y anticipa problemas de disponibilidad que podrian suponer un problema mayor de continuidad del negocio.

FORMA DE CÁLCULO	PERIODICIDAD
Se calcula descontando al tiempo total el tiempo de caídas de sistemas, o periodos con tiempos de respuesta superiores a los límites establecidos. Valor agregado medio del año,	Mensual
	RESPONSABLE
	Dir. Tecnología de la Información

MAGNITUDES UTILIZADAS	
Fuente del dato	Informe de Servicio de Tecnologia
Periodicidad	Mensual
Responsable	Departamento de Infraestructura

CALIBRACIÓN 2021			JUSTIFICACIÓN
APETITO	TOLERANCIA	CAPACIDAD	
99,50%	99,05%	98,00%	

GRACIAS A NUESTROS COLABORADORES

Platinum

COLIN VEGA FLETES ABOGADOS

MAPFRE

HERBERT SMITH FREEHILLS

ventiv

Golden

AIG

Allianz

AON

AXA XL Insurance

Berkshire Hathaway Specialty Insurance

CHUBB

grupo addvalora

DAC BEACHCROFT

CLYDE&CO

GENERALI Global Corporate & Commercial

MARCH R.S.

Marsh

sedgwick

QBE

Munich RE

Swiss Re Corporate Solutions

wtw

ZURICH

Silver

FBA sociados

HDI

HIGHDOME

INTERNATIONAL SOS

HASA

Liberty Specialty Markets

RSA

Esta guía expone de forma práctica, llena de ejemplos fáciles de entender, una propuesta de indicadores sencillos y asequibles que resultarán de gran utilidad para gestionar el riesgo operacional, propósito más amplio para el que podrás encontrar también buenos consejos y recomendaciones en el libro "Manual de Riesgos Operacionales", elaborado en paralelo por el grupo de trabajo de "responsables de Riesgos de Grandes Empresas" de AGERS.

Si en tu organización ya contáis con un sistema de indicadores de riesgos, encontrarás en este libro información útil para contrastar que el modelo del que dispones está en línea con las propuestas en otras organizaciones o para identificar posibles mejoras. Pero si aún no dispones de unos indicadores de riesgos y quieres aventurarte a comenzar esta andadura, este libro seguro que te resultará muy útil en tus primeros pasos para comenzar con los riesgos operacionales.