EBA Consultation Paper on ICT Risk Assessment (SREP)

Documento Consultivo *EBA/CP/2016/14*

Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP)

Financial Risk Management

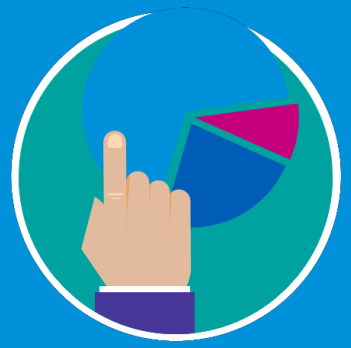
Octubre 2016

kpmg.es

Índice

KPMG

Introducción



Introducción
Contexto y objetivo del documento

A raíz de la coyuntura económica de los últimos años, marcada por una crisis financiera cuyo alcance se ha extendido a la gran mayoría de sectores económicos, y en el contexto de la búsqueda de unos estándares de supervisión nacionales y transnacionales homogéneos, se han producido una serie de innovaciones regulatorias impulsadas tanto por organismos supranacionales como por los reguladores locales de cada país.

La Autoridad Bancaria Europea ha emitido una consulta sobre su iniciativa de evaluación del riesgo de la tecnología de la información y comunicación (ICT por sus siglas en inglés) bajo el marco del SREP. Estas líneas de actuación están dirigidas a las autoridades competentes y tienen por objeto promover el desarrollo de procedimientos y metodologías comunes para la evaluación del riesgo ICT, las cuales complementarían a las directrices publicadas en el marco del SREP por la EBA. Las partes involucradas en la evaluación o que quieran participar pueden enviar sus comentarios hasta el 06 de enero de 2017.

En este contexto, el presente documento expone cómo identificar, evaluar y proceder con el riesgo de la tecnología de la información y comunicación, destacando los siguientes puntos:

- Se identifican los requerimientos regulatorios exigidos por la EBA
- Se analiza la manera en la que se ha de proceder bajo dichos requerimientos
- Se diseña un plan de acción para acometer las instrucciones del regulador

Introducción

Contexto y objetivo del documento

Desde un punto de vista estratégico, los recursos tecnológicos tienen un rol crucial en el sector bancario al ser la base sobre la que se soportan la inmensa mayoría de los procesos de las Entidades. En consecuencia, la innovación tecnológica puede suponer una ventaja competitiva, convirtiéndose en un aspecto fundamental para que una Entidad mantenga su competitividad en el sector financiero.

En este contexto de creciente importancia del riesgo de la tecnología de la información y comunicación se están generalizando algunas tendencias en el sector:

- Ataques tecnológicos, como ciberataques, y la vulnerabilidad de las Entidades frente al cibercrimen y el ciberterrorismo.
- Creciente propensión a la externalización a terceros de los servicios de IT, generalmente en forma de paquetes tecnológicos que puede derivar en potenciales limitaciones o incluso riesgo de concentración.

OBJETIVO

Considerando estas nuevas tendencias y a pesar de que la guía no es vinculante, ésta servirá para ampliar las expectativas supervisoras a considerar en el proceso de supervisión del SREP, y de forma más específica, en la metodología correspondiente al Riesgo Operacional.

La guía, se centra en la definición de unas metodologías de evaluación y considera tres ámbitos distintos:

- Definición del contexto y alcance del ejercicio de evaluación.

Gobierno y Estrategia

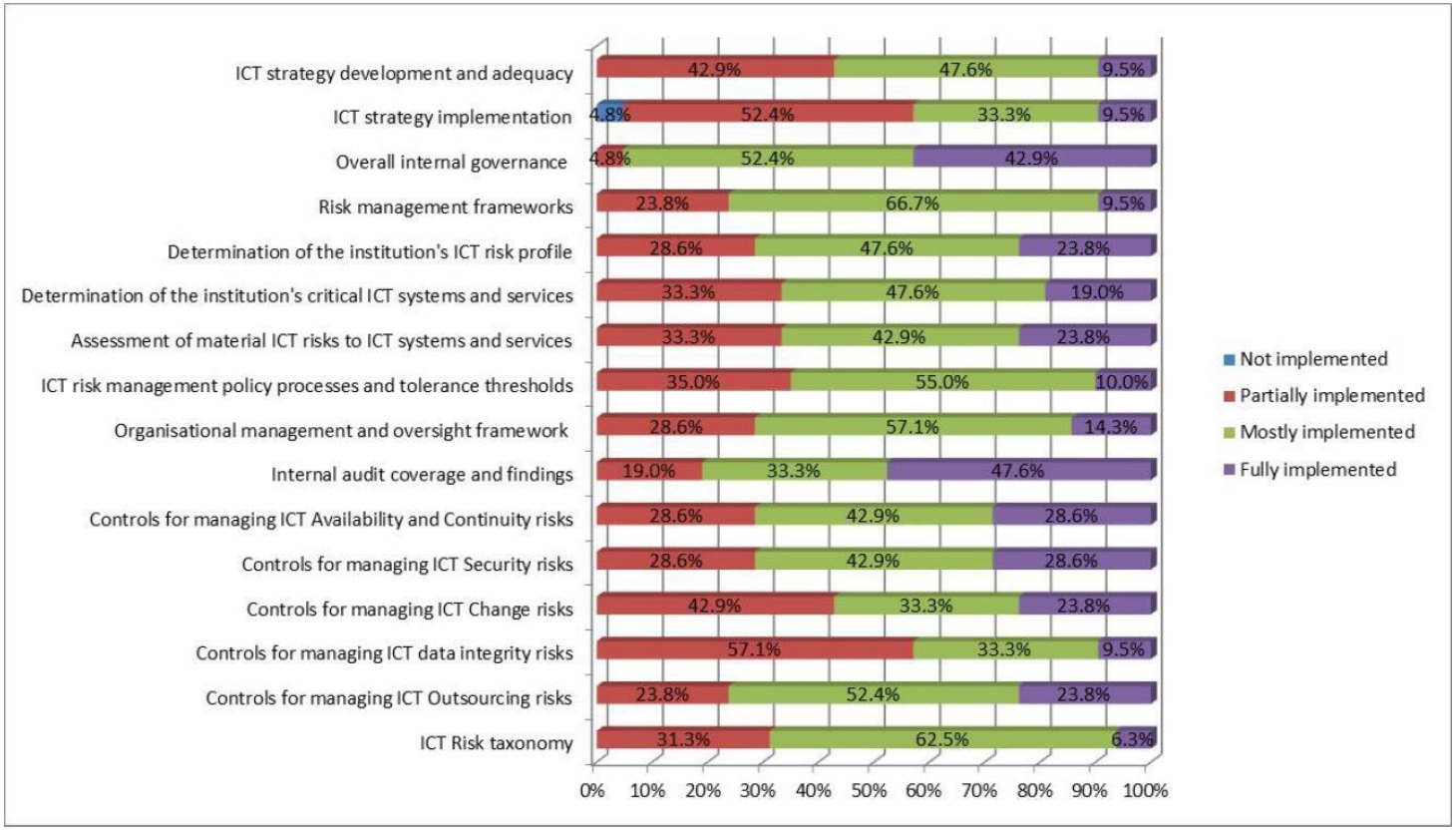
- Reconocimiento de la importancia del gobierno y control interno sobre el riesgo ICT.
- Evaluación en relación a la alineamiento con el modelo de negocio y la estrategia de la Entidad.

Evaluación del Riesgo

- Evaluación de la exposición asociada al riesgo ICT y la efectividad de los controles establecidos.
- Ampliación de las expectativas supervisoras ya existentes en el proceso SREP.

Introducción
Situación actual

La siguiente tabla muestra el nivel de implementación, en los Estados miembros en términos porcentuales, de las directrices publicadas. Ésta ofrece una visión general de los posibles nuevos esfuerzos que, tanto las autoridades competentes como las entidades, deben trabajar previamente a su entrada en vigor para lograr un mayor grado cumplimiento de las directrices propuestas.



Fuente: Tabla 2 *Current practices with respect to the content of the draft guidelines. Consultation paper EBA/CP/2016/14 "Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP)"*

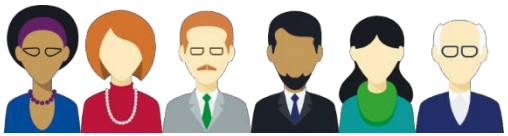
KPMG

Disposiciones generales

Gobierno y estrategia
Evaluación de riesgos ICT

En este apartado se pretende contextualizar y establecer el alcance de la evaluación:

Ámbito de aplicación	▪ Los requisitos establecidos en las Directrices deberían aplicarse a todas las instituciones. ▪ No se especifica si la evaluación de esta tipología de riesgo debe llevarse a cabo mediante inspecciones *on site* u *off site*, dejando al mejor criterio de las autoridades competentes el método más eficiente y efectivo para llevarlas a cabo en función de las características de cada sistema financiero nacional. ▪ Asimismo, estas Directrices no introducen ningún requerimiento adicional de *reporting* para las Entidades.
Proporcionalidad	▪ Las autoridades competentes deben aplicar estas directrices de manera proporcional al tamaño, la estructura y el entorno operativo de las instituciones, así como la naturaleza, escala y complejidad de sus actividades. ▪ Las autoridades competentes deben aplicar dichas Directrices en línea a la categorización de las instituciones, basándose en el nivel mínimo tal y como se especifica en las Directrices del SREP. ▪ Las autoridades competentes podrán confiar y tener en cuenta el trabajo ya realizado en el contexto de otras evaluaciones de riesgo. Además, deben seleccionar el método más adecuado de evaluación de auditoría y la metodología que mejor se adapte a la institución para informar de la evaluación a las autoridades.



Gobierno y estrategia
Evaluación de riesgos ICT

Disposiciones generales

En este apartado se pretende contextualizar y establecer el alcance de la evaluación:

Resultados de la evaluación	▪ La conclusión de la evaluación debe dar lugar al resumen de los resultados bajo el título de las Directrices del proceso SREP y la puntuación de dicha evaluación debe alinearse de acuerdo con las consideraciones expuestas en la tabla de las Directrices de dicho proceso. ✓ En la evaluación del modelo de negocio, las autoridades deben tener en cuenta que la institución puede tener falta de recursos o de capacidades para llevar a cabo los cambios estratégicos planificados. En tal caso, se debe informar de la continuidad en la evaluación del modelo de negocio. ✓ En la evaluación del modelo de gobierno y control interno de la Entidad, al evaluarse la consideración y conocimiento de esta tipología de riesgo por la Alta Dirección y el Consejo de Administración. ✓ Los resultados de la evaluación deben confluir en el resumen de los resultados de Riesgo Operacional y deben ser considerados como información para las evaluaciones posteriores. ▪ Si las autoridades competentes consideran que el riesgo ICT es material y deciden evaluar y puntuar este riesgo de forma individual como una subcategoría de Riesgo Operacional, deben utilizar la tabla de puntuación "*Consideraciones de supervisión para la asignación de una puntuación de riesgo ICT*". ▪ Para identificar si el riesgo ICT debe ser considerado como material, las autoridades competentes podrán utilizar la lista de fuentes definidas en el párrafo 120 de la Directrices el proceso SREP. ▪ En el caso de aplicar estas Directrices, las autoridades competentes deberán tener en cuenta la lista no exhaustiva de las subcategorías de riesgo ICT y los escenarios de riesgo que figuran en el anexo del documento.

KPMG

Gobierno y estrategia

Gobierno y estrategia

Evaluación del gobierno de las instituciones y estrategia en ICT

Las autoridades competentes evaluarán los siguientes requisitos:

- ✓ Si el gobierno de la Entidad y de control interno cubren debidamente los sistemas asociados a la tecnología de la información y comunicación y los riesgos relacionados a la misma.
- ✓ Si el Consejo de Administración gestiona de manera adecuada estos aspectos.

Dicha evaluación se centrará en las siguientes áreas, sólo debiendo informar sobre la gestión de riesgos y controles:

- ✓ Estrategia sobre la tecnología de la información y comunicación
- ✓ Gobierno interno
- ✓ Riesgo de las ICT en el marco de gestión de riesgos de la Entidad

Estrategia ICT

- Las autoridades competentes evaluarán si la estrategia de ICT está sujeta a una correcta supervisión del órgano de dirección de la Entidad y si la Entidad cuenta con una estrategia de ICT consistente con el modelo de negocio.
- Las autoridades competentes evaluarán si la Entidad cuenta con un marco adecuado para el desarrollo de su estrategia de ICT, teniendo en cuenta los siguientes factores:
  - ✓ Los responsables de la gestión e implementación de los sistemas son conocedores de la estrategia comercial.
  - ✓ La estrategia de ICT es viable, está documentada y está soportada por una planificación de hitos y recursos realista.
  - ✓ Actualización periódica de la estrategia de ICT con objeto de asegurar su alineamiento con el negocio.
  - ✓ Aprobación y supervisión por parte del Consejo de Administración de la estrategia de ICT y sus planes de implementación asociados.

Gobierno y estrategia

Evaluación del gobierno de las instituciones y estrategia en ICT

1

Estrategia ICT
(*cont)

- Si la estrategia ICT requiere de la implementación de cambios con consecuencias materiales para el modelo de la Entidad, las autoridades competentes deben evaluar si la Entidad cuenta con un marco de control que apoye la aplicación efectiva de dicha estrategia:
  - ✓ Los cambios están respaldados tanto por los procesos de gobierno como por los organismos pertinentes.
  - ✓ Se han definido y asignado los roles y responsabilidades para la ejecución de dichos cambios.
  - ✓ Los riesgos asociados a la implementación de la estrategia ICT se han identificado, evaluado y mitigado de manera efectiva.
  - ✓ Existe un proceso de revisión de la planificación que ofrece la flexibilidad para responder a posibles incertidumbres futuras.

2

Gobierno interno

- Las autoridades competentes deben evaluar si la Entidad cuenta con una estructura corporativa adecuada y transparente apropiada para el propósito del cambio. En este ámbito se evaluará si la Entidad posee:
  - ✓ Una estructura organizativa sólida y transparente que asegure que la información importante relacionada con las ICT se traslada de manera adecuada a nivel del Consejo de Administración.
  - ✓ El Consejo de Administración conoce y se ocupa de los riesgos asociados a las ICT.
- Las autoridades competentes deberían evaluar si los responsables de la gestión e implementación de los sistemas y servicios de ICT son conocedores de la estrategia comercial de la Entidad.

Gobierno y estrategia

Evaluación del gobierno de las instituciones y estrategia en ICT

3

Riesgo de las ICT en el marco de gestión de riesgos de la Entidad

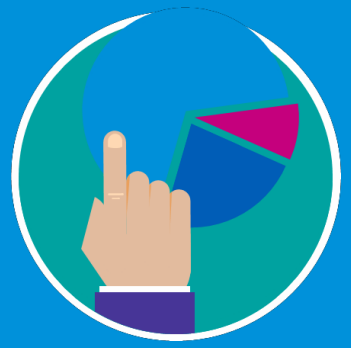
- Las autoridades competentes considerarán si las funciones de control y de auditoría interna son adecuados para garantizar un nivel suficiente de independencia entre las ICT y las propias funciones de control y auditoría, dado el tamaño y el perfil de riesgo de la Entidad. Determinarán si:
  - ✓ El apetito al riesgo y el ICAAP cubren los riesgos de las ICT, tanto los esperados como los no previsibles.
  - ✓ Los riesgos de ICT están dentro del alcance de la gestión de riesgos en toda la Entidad y del marco de control interno.

Resumen de resultados

- Los resultados de las evaluaciones deberán reflejarse bajo el Título 5 de las Directrices del SREP y deben formar parte de la puntuación respectiva de acuerdo con las consideraciones expuestas en la Tabla 3 de dichas Directrices:
  - ✓ Si las autoridades competentes llegan a la conclusión de que el marco de gobierno de la Entidad es insuficiente para desarrollar e implementar su estrategia de ICT, se deberá informar a la supervisión de la gestión interna de la Entidad en el Título 5 de las Directrices EBA SREP en el punto 87 (a).
  - ✓ Si las autoridades competentes llegan a la conclusión de que habría un desajuste importante entre la estrategia de ICT y la estrategia de negocio, se debería informar a la supervisión del modelo de negocio del Título 4 del PRES GL.
  - ✓ Si las autoridades competentes llegan a la conclusión de que la Entidad puede no tener suficientes recursos y falta de capacidad para llevar a cabo y apoyar importantes cambios estratégicos planificados, se debería informar a la supervisión del modelo de negocio del Título 4 de las Directrices del SREP bajo el punto 70 (b).

KPMG

Evaluación del riesgo



Evaluación del riesgo

Aspectos generales

En el proceso de evaluación del riesgo de la tecnología de información y comunicación se pueden distinguir dos fases importantes a llevar a cabo:

Evaluación del los procedimientos de identificación, gestión y mitigación del riesgo	▪ Las autoridades competentes deben evaluar si la Entidad ha identificado correctamente, evaluado y mitigado los riesgos tecnológicos. Este proceso debe ser parte del marco de gestión del riesgo operacional. ▪ Se entiende como riesgo tecnológico la pérdida potencial por daños, interrupción, alteración o fallos derivados del uso o dependencia en el *hardware*, *software*, sistemas, aplicaciones, redes y cualquier otro canal de distribución de información que una Entidad dispone para prestar sus servicios.

Evaluación de resultados	▪ Para la ejecución de las prioridades de evaluación de estos riesgos tecnológicos, las autoridades responsables deben valorar: ✓ Riesgo ICT y controles sobre procesos internos de auto-evaluación (ejemplo ICAAP). ✓ Riesgo ICT relativo a gestión de la información reportados al Consejo de Administración y a la Alta Dirección. ✓ Resultados ICT extraídos de auditorías internas/externas, reportados al Comité de Auditoría de la Entidad.

Evaluación del riesgo

Identificación de riesgos relevantes

Las autoridades competentes deben identificar los riesgos ICT relevantes a los que la Entidad esté o pueda estar expuesta, siguiendo los pasos detallados a continuación:

1

Revisión del perfil riesgo

- Las autoridades competentes deberán revisar:
  - ✓ El impacto potencial de una parada de los sistemas ICT en el sistema financiero.
  - ✓ Si la Entidad está llevando cambios en sus sistemas ICT y en su función.
  - ✓ Si la Entidad sitúa sus centros más importantes de operaciones / ICT de datos en lugares expuestos a contingencias externas a la propia Entidad.
  - ✓ Si la Entidad está sujeta a riesgos de seguridad y a riesgos de continuidad debido a las dependencias de internet, que puede hacer que sea un objetivo más probable para ataques cibernéticos.
  - ✓ Si la Entidad ha externalizado los servicios ICT dentro o fuera del Grupo que puedan exponerlo a riesgos materiales de externalización.
  - ✓ Si la Entidad está implementando medidas de reducción de costes ICT necesarios, recursos y conocimientos de TI.

2

Revisión de la documentación

- Las autoridades competentes deberán revisar la documentación de cada Entidad para determinar qué sistemas y servicios de ICT son fundamentales:
  - ✓ Cumpliendo con un adecuado funcionamiento, disponibilidad, continuidad y la seguridad de las actividades esenciales de la Entidad.

Evaluación del riesgo

Identificación de riesgos

3

Revisión de sistemas y servicios

- Las autoridades competentes deberán revisar la metodología y los procesos aplicados por la Entidad para identificar los sistemas y servicios ICT que son críticos. Para determinarlo, hay que cumplir, al menos, alguno de los siguientes aspectos:
  - ✓ Apoyar las operaciones de negocio y canales de distribución de la Entidad (cajeros automáticos, internet, banca móvil).
  - ✓ Apoyar los procesos de gobierno esenciales y funciones corporativas, incluyendo la gestión de riesgos.
  - ✓ Cumplir los requisitos legales o reglamentos especiales (si los hay) que imponen mayor disponibilidad, capacidad de recuperación, confidencialidad o requisitos de seguridad.
  - ✓ Procesar o almacenar datos confidenciales o sensibles a los que el acceso no autorizado podría afectar significativamente en la reputación de la Entidad, en sus resultados financieros o la solidez y continuidad de su negocio.

4

Evaluación del impacto potencial

- Cuando la autoridad evalúe el impacto potencial de los riesgos ICT en los sistemas y servicios críticos de una Entidad, deben de tener en cuenta:
  - ✓ El impacto financiero, incluyendo la pérdida de fondos o activos, compensación de clientes potenciales, costes legales, daños contractuales y la pérdida de ingresos.
  - ✓ El potencial para la interrupción del negocio, considerando la criticidad de los servicios financieros, número de clientes y / o sucursales y empleados afectados.
  - ✓ El potencial impacto reputacional de la Entidad basada en la criticidad del servicio de banca o de la actividad operativa afectados.
  - ✓ El impacto de la regulación, incluyendo el potencial posible afectado por el regulador, multas o incluso la variación de permisos.
  - ✓ El impacto estratégico en la Entidad, por ejemplo, si los planes estratégicos de productos o de negocios se ven comprometidos o son sustraídos.

Evaluación del riesgo

Controles para mitigar los riesgos ICT

Para los riesgos materiales identificados de ICT, las autoridades competentes deberán revisar los siguientes aspectos:

Política de gestión, controles y umbrales de tolerancia

✓ Se comprobará si la Entidad cuenta con políticas adecuadas de gestión de riesgos, con procesos y umbrales de tolerancia definidos para los riesgos relevantes ICT identificados. Estos pueden ser una parte del marco de gestión del riesgo operacional o un documento separado.

- Todos los agentes implicados deben ser informados.
- La política aplicable cubre todos las elementos significativos.
- La Entidad ha implementado procesos para la identificación y monitorización de los mismos.
- La Entidad cuenta con una gestión de riesgos ICT para proporcionar información relevante para el negocio.

✓ Se debe evaluar cómo los roles y responsabilidades de gestión de riesgos se integran en la organización interna para gestionar y supervisar los riesgos ICT identificados. Las instituciones deben cumplir entre otras:

Gestión organizativa y marco de supervisión

- Responsabilidades y funciones claras para la identificación, evaluación, seguimiento, mitigación, *reporting* y supervisión del material del riesgo ICT.
- Incluir roles y responsabilidades para la recopilación y agregación de información de riesgos y reporte al Consejo de Administración.
- Un adecuado seguimiento y respuesta al Consejo de Administración.
- Las excepciones y políticas de las normas de ICT aplicables estén registradas y documentadas.

Evaluación del riesgo

Controles para mitigar los riesgos ICT

Cobertura de auditoría interna

✓ Considerar si la función de Auditoría Interna es eficaz con respecto a la auditoría del control de riesgos ICT, comprobando los siguientes aspectos:

- Calidad, profundidad, frecuencia y proporcionalidad en cuanto al tamaño y perfil del riesgo.
- Si el plan de auditoría incluye la revisión de los riesgos identificados.
- Notificación de los resultados obtenidos y reporte a la Alta Dirección.

Controles para la identificación de los riesgos ICT relevantes

✓ Evaluar si la Entidad cuenta con controles específicos para abordar e identificar los riesgos ICT relevantes (*):

- Riesgos ICT de disponibilidad y continuidad.
- Riesgos ICT de seguridad.
- Riesgos ICT de cambio.
- Riesgos ICT en la integridad de los datos.
- Riesgos ICT de externalización.

(*) En el Anexo se detallan cada uno de estos riesgos

KPMG

Marco de Riesgos ICT

Marco riesgos ICT
Características a cumplir

Las autoridades competentes deben evaluar si la institución cuenta con un marco adecuado para identificar, comprender, medir y mitigar la disponibilidad y continuidad de los riesgos ICT. Los principales aspectos son:

Procesos y Sistemas	Identifica los procesos críticos de ICT y los sistemas ICT de apoyo que deben formar parte de la capacidad de recuperación de negocio y planes de continuidad.
Capacidad Recuperación	Dispone de la capacidad de recuperación de negocio, las políticas de control de entorno continuidad y normas y controles operativos.
Plan Continuidad	Tiene disponibles *tests* ICT y planes de continuidad, que permitan evaluarse frente un conjunto de escenarios realistas que incluyen ciberataques, entre otras situaciones.
Roles	Tiene definido de una manera clara los roles y responsabilidades.
Seguridad	Dispone de una política de seguridad ICT que toma en consideración y se adhiere a las normas de seguridad de las ICT y a los principios de seguridad reconocida internacionalmente
Gestión Incidentes	Dispone de un proceso de gestión de incidentes de seguridad documentado y el reporte a los superiores.
Sensibilización	Dispone de campañas o iniciativas de sensibilización e información para informar a todos los niveles de la institución sobre el uso seguro y la protección de los sistemas ICT de la institución.
Seguridad Física	Dispone de medidas de seguridad física para evitar el acceso físico no autorizado a los sistemas de ICT críticos y sensibles.
Medidas Riesgo de Cambio	Dispone de medidas/sistemas para identificar, comprender, medir y mitigar el riesgo de cambio de las ICT a la naturaleza, escala y complejidad de las actividades de la institución.

Marco riesgos ICT

Características a cumplir

- Procesos y Sistemas
- Capacidad
- Plan Continuidad
- Seguridad
- Gestión Incidentes
- Sensibilización
- Seguridad Física
- Medidas Riesgo de Cambio

Procesos y Sistemas

Identifica los procesos críticos de ICT y los sistemas ICT de apoyo que deben formar parte de la capacidad de recuperación de negocio y planes de continuidad.

Para la evaluación de este aspecto del marco, las autoridades deben asegurar que los procesos y sistemas ICT cumplen al menos una de estas condiciones:

- ✓ Apoyan las operaciones de negocio y canales de distribución (por ejemplo, cajeros).
- ✓ Apoyan los procesos de gobierno esenciales y funciones corporativas.
- ✓ Aseguran que entran dentro de los requisitos legales o reglamentos especiales.
- ✓ Procesan o almacenan datos confidenciales o sensibles, asegurando el acceso no autorizado.
- ✓ Proporcionan funcionalidades elementales que son vitales para el funcionamiento adecuado de los servicios de la Entidad.

Capacidad

Dispone de la capacidad de recuperación de negocio, de las políticas de control del entorno de continuidad y normas y controles operativos. Debiendo las autoridades valorar:

- ✓ Distancia suficiente entre la producción de ICT y los sistemas de recuperación para evitar que ambos sean impactados por el mismo incidente o desastre.
- ✓ *Backup* y recuperación de los procedimientos del sistema ICT para el *software* y los datos críticos, que aseguran que estas copias de seguridad se almacenan en un lugar seguro.
- ✓ Si dispone de soluciones de monitorización para la detección temprana de los incidentes sobre la disponibilidad de ICT o de continuidad.
- ✓ Soluciones para proteger las actividades esenciales de Internet o servicios (por ejemplo, servicios de banca electrónica), cuando sea necesario.

Marco riesgos ICT

Características a cumplir

- Procesos y Sistemas
- Capacidad Recuperación
- Plan Continuidad
- Roles
- Seguridad
- Gestión Incidentes
- Sensibilización
- Seguridad Física
- Medidas Riesgo de Cambio

Plan Continuidad

Tiene disponibles test ICT y planes de continuidad, que permitan validarse frente a un conjunto de escenarios realistas que incluyen ataques cibernéticos, entre otras situaciones. Los mismos se caracterizan por:

- ✓ Planificarse, ser formalizados y documentados, y que los resultados de los mismos sean utilizados para fortalecer la eficacia de las soluciones de disponibilidad y continuidad de ICT.
- ✓ Incluir a los *stakeholders* y sus funciones dentro de los mismos.
- ✓ La importancia de la involucración de la Alta Dirección (por ejemplo, como parte de los equipos de gestión de crisis), siendo relevante el traslado a la Alta Dirección de los resultados de los dichos test.

Roles

Tiene definido de una manera clara los roles y responsabilidades. Las autoridades deben evaluar si la Entidad considera los siguientes aspectos:

- ✓ Tiene las funciones y responsabilidades claras para la identificación, evaluación, seguimiento, mitigación y supervisión del riesgo material involucrado en ICT.
- ✓ Las actividades de gestión de riesgos se realizan con los recursos humanos y técnicos suficientes y cualitativamente adecuados.
- ✓ Dispone de un seguimiento adecuado y una respuesta al Consejo de Administración y Alta Dirección relativa a las funciones de control independiente respecto al riesgo ICT.
- ✓ Las excepciones de las normas y políticas de ICT aplicables son registradas y están sujetas a un análisis documentado y a la presentación de informes, actividades que realiza la función de control independiente, basándose en un enfoque asociado a los riesgos relacionados.

Marco riesgos ICT

Características a cumplir

- Procesos y Sistemas
- Capacidad Recuperación
- Plan Continuidad
- Roles
- Seguridad
- Gestión Incidentes
- Sensibilización
- Seguridad Física
- Medidas Riesgo de Cambio

Seguridad

Disponibilidad por parte de la Entidad de una política de seguridad ICT que tome en consideración y se adhiera a las normas de seguridad de las ICT (por ejemplo, ISO 27001 e ISO 27015) y los principios de seguridad reconocidos internacionalmente (por ejemplo, el "principio de privilegio mínimo", es decir, limitar el acceso al nivel mínimo, permitiendo el funcionamiento normal de los derechos de acceso.

Gestión Incidentes

Disponibilidad por parte de la Entidad de un proceso de gestión de incidentes de seguridad documentado e involucración en el mismo de los órganos de dirección, lo que proporciona una orientación sobre los diferentes roles y responsabilidades de la gestión de incidentes y de su escalamiento hacia el órgano superior, los miembros del comité de crisis y la cadena de mando en caso de emergencias de seguridad.

Por otra parte, también se debe evaluar el registro de actividades administrativas con el propósito de permitir un control eficaz y la detección y respuesta a las actividades no autorizadas de manera oportuna.

Sensibilización

Disponibilidad de campañas o iniciativas de sensibilización e información para trasladar a todos los niveles de la Entidad el uso seguro y la protección de los sistemas ICT frente a los riesgos que se deben tener en cuenta.

Se debe prestar especial atención a las amenazas informáticas existentes y sus evoluciones (por ejemplo, virus informáticos, los posibles abusos o ataques internos o externos, los ciberataques, etc.).

Marco riesgos ICT

Características a cumplir

Procesos y Sistemas

Capacidad Recuperación

Plan Continuidad

Gestión Incidentes

Sensibilización

Seguridad Física

Medidas Riesgo de Cambio

Seguridad Física

Disponibilidad de medidas de seguridad física para evitar el acceso físico no autorizado a los sistemas ICT. Asimismo, deberá disponer también de medidas para la protección frente a ataques de internet u otras amenazas. Las autoridades deben evaluar si el marco considera lo siguiente:

- ✓ Un proceso y soluciones para mantener un inventario completo y actualizado y una visión general de todos los puntos de conexión a la red orientadas hacia el exterior.
- ✓ Capacidad para manejar y controlar las medidas de seguridad (por ejemplo, cortafuegos, servidores proxy, antivirus, etc.) para proteger el tráfico de red.
- ✓ Procesos y soluciones para asegurar sitios web y aplicaciones que pueden ser punto de entrada a sistemas ICT internos.
- ✓ Pruebas periódicas de penetración de seguridad para evaluar la eficacia de la política cibernética actual y sus medidas de seguridad asociadas. Estas pruebas deben ser realizadas por personal y/o expertos externos con los conocimientos técnicos adecuados.

Medidas Riesgo de Cambio

Dispone de medidas / sistemas para identificar, comprender, medir y mitigar el riesgo de cambio de las ICT a la naturaleza, escala y complejidad de las actividades de la Entidad y el perfil de riesgo de las ICT.

Las mismas medidas deben cubrir los riesgos asociados al desarrollo, prueba y aprobación de cambios en los sistemas ICT, incluyendo el desarrollo o el cambio de *software*, antes de que se migren al entorno de producción, garantizando una adecuada gestión del ciclo de vida de las ICT; y la preservación de la integridad de los datos almacenados y procesados por los sistemas ICT.

KPMG

Servicios KPMG

Servicios KPMG

El riesgo tecnológico en el papel de ser uno de los mayores riesgos a los que se enfrenta la industria bancaria, KPMG ha mantenido conversaciones con todos *los stakeholders* implicados así como los supervisores para discutir la importancia cada vez mayor y la creciente complejidad de los riesgos de TI.

Entre las cuestiones clave, hay dos prioridades clave emergentes que requieren atención inmediata con el fin de aportar claridad:

- Taxonomía de riesgos tecnológicos: la ausencia de un lenguaje común para definir los riesgos tecnológicos y;
- Armonización: actualmente no existe por parte del Regulador una visión holística en relación a los requerimientos de los riesgos tecnológicos: marco, políticas, controles, evaluación, eventuales *add-ons* de capital, etc.

En este contexto KPMG ofrece una serie de iniciativas orientadas a cumplir con los nuevos requerimientos del SREP establecidos en estas Directrices:

KPMG

Evaluación de impacto

Evaluación de impacto

Según el artículo 16(2) de la *EBA Regulation (Regulation* (EU) No 1093/2010 del Parlamento Europeo) cualquier manual desarrollado por la EBA debe estar acompañado por una evaluación de impacto complementaria ofreciendo una visión conjunta del problema identificado, las opciones evaluadas para solucionarlo y su potencial impacto en lo que a costes y beneficios se refiere.

Impact Assesment

1) *Identificación del problema*
2) *Objetivos de la política*
3) *Escenario base*
4) *Evaluación de las opciones considerades y llevades a cabo*
5) *Análisis coste - beneficio*

- ✓ La evaluación de impacto preparada por la EBA es un cuestionario cualitativo que pretende reunir información básica referente a las prácticas actuales llevadas a cabo por los Estados Miembros y los costes y beneficios esperados en relación con la evaluación de los riesgos ICT.
- ✓ El cuestionario está dirigido a las autoridades nacionales competentes.

Evaluación de impacto

A continuación de muestra el detalle de los aspectos más relevantes a los que hace referencia el anexo.

1 Identificación del problema	▪ El riesgo ICT es un componente intrínseco del funcionamiento operacional y de la implementación y desarrollo del modelo de negocio de cada institución financiera. Es decir, hay un impacto en el modelo de negocio de la Entidad, la gobernanza y el capital derivado del riesgo tecnológico. ▪ Es por ello, los riesgos que pueden ser originados por los riesgos ICT deben ser gestionados por la Entidad.
2 Objetivos de la política	▪ El principal objetivo es especificar un conjunto de reglas que complementen las Directrices del marco SREP a aplicar por las autoridades competentes, utilizando el principio de proporcionalidad, en su evaluación del riesgo. ▪ Precisamente, las Directrices tienen por objeto informar a los supervisores de cómo deben evaluar y supervisar este riesgo y crear prácticas coherentes y un marco común a través de las distintas jurisdicciones.
3 Escenario base	▪ En el anexo publicado por la EBA se presenta una tabla resumen que muestra el nivel de cumplimiento de las Entidades y las autoridades competentes respecto a las Directrices del manual. Se presenta una visión general de los esfuerzos en los que debe focalizarse cada autoridad competente y sirve de base para la estimación de costes y beneficios que se expondrá más adelante. ▪ También se muestra en otra tabla el nivel de implementación, en términos porcentuales, indicado por los estados miembros. Como resultado, todas las categorías expuestas en el documento están cubiertas total o parcialmente excepto 2 (En el anexo de este documento se pueden consultar estos resultados)

Evaluación de impacto

A continuación de muestra el detalle de los aspectos más relevantes a los que hace referencia el anexo. (cont.)

Evaluación de las acciones consideradas y llevadas a cabo

- A continuación se presenta la evaluación de cuatro políticas y se especifican las razones por las que se llevaron a cabo:

  ✓ Desarrollo de las Directrices de evaluación del riesgo ICT a partir de las ya existentes por parte de la EBA o desarrollo de una metodología aparte: se consideró completar las Directrices ya existentes de la EBA porque no sólo complementaba la sección de riesgo operacional sino también la del modelo de negocio.

  ✓ Inclusión o exclusión de una provisión específica al riesgo tecnológico: sin la inclusión de tales provisiones la EBA no sería capaz de medir la cantidad de recursos tecnológicos por parte de las Entidades ni serían capaces de identificar la idoneidad del modelo de negocio de la Entidad respecto a los recursos tecnológicos de los que dispone.

  ✓ Inclusión o exclusión de controles de riesgo tecnológico material: se facilitó una lista de controles específicos de modo que los supervisores pudieran entender exactamente qué factores mitigantes pueden controlar los riesgos identificados.

  ✓ Inclusión o exclusión de una taxonomía de riesgos no exhaustiva: dado que la supervisión de riesgos tecnológicos es un concepto relativamente nuevo para la mayoría de los supervisores se propuso la creación de una terminología común para lograr consistencia en el modo de evaluación de este riesgo.

Evaluación de impacto

A continuación de muestra el detalle de los aspectos más relevantes a los que hace referencia el anexo. (cont.)

Análisis Coste Beneficio

- Entre las principales causas de incrementos potenciales de costes para las Entidades se señalaron las siguientes:
  - ✓ Formalización de los principales procesos de las Entidades en función de un entorno estratégico.
  - ✓ Esfuerzos adicionales.
  - ✓ Formación de empleados y necesidades adicionales para cumplir con el marco normativo.

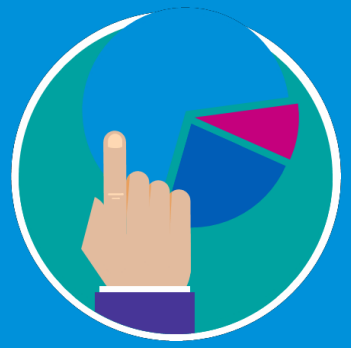
- Entre las principales causas de incrementos potenciales de costes para las autoridades competentes se señalaron las siguientes:
  - ✓ Formación del personal actual de IT y contratación de personal adicional.
  - ✓ Introducción de un nuevo marco supervisor o formalización del actual.
  - ✓ Preparación o actualización de manuales de cara al cumplimiento de las nuevas Directrices en las Entidades.

- Entre los principales beneficios se señalaron:
  - ✓ Aumento de la conciencia de riesgos asociados al riesgo ICT tanto en Entidades y autoridades competentes.
  - ✓ Aumento de la calidad y la integridad de los datos.
  - ✓ Mejora de la supervisión de los sistemas críticos.
  - ✓ Estandarización de las categorías de riesgo ICT.
  - ✓ Estandarización de la taxonomía de riesgos que implique un lenguaje homogéneo y un entendimiento común.

Los resultados señalaron que se espera que los costes de la aplicación del presente manual sean superiores para las autoridades competentes que para las instituciones.

KPMG

¿Por qué KPMG?



¿Por qué KPMG?

Los servicios de KPMG proveen asesoramiento para garantizar el cumplimiento normativo de los nuevos requerimientos regulatorios. Adaptarse anticipadamente a las nuevas exigencias permite a la Organización obtener numerosos beneficios como se ilustra a continuación:

'Maximizar el valor de la Organización'

'Generar un marco de apetito al riesgo consecuente con el perfil de riesgo definido'

'Alinear políticas y procedimientos en relación a los requerimientos regulatorios'

'Adaptación del Negocio a la nueva situación Regulatoria'

¿Por qué KPMG?

Aspectos clave	Qué te ofrece KPMG
Conocimiento de los nuevos requerimientos regulatorios contenidos en la Circular así como en la CRD y CRR respectivamente.	**Amplia experiencia en regulación bancaria: Basilea, CRD IV, Liquidez, RDA, MIFID, EMIR, Dodd Frank, SREP, MUS, etc.**
Análisis de la información de la Entidad y mapeo con los requerimientos del proyecto de Circular.	**Metodología de trabajo basada en la realización del Diagnóstico de la Situación Actual** (AS-IS) y contraste frente al Modelo Objetivo**(TO-BE) incluido en el proyecto de Circular.**
Definición de los nuevos reportes regulatorios en la Entidad contenidos en el proyecto de la Circular a partir del análisis de los requerimientos.	**Amplia experiencia en la definición funcional y técnica para cumplir con los diversos requerimientos de reporting.**
Implantación de un proceso estable y consistente para el cálculo de los colchones de capital.	**Amplio conocimiento en relación al cálculo de capital contrastado por su implicación en la mayor parte de Entidades en los ejercicios de Optimización RWA y AQR.**
Mejora del gobierno interno cumpliendo con todas las nuevas exigencias regulatorias (organización, funciones, marcos y políticas, comités, etc)	**Coordinación y planificación óptima para cumplir con las fechas comprometidas con las Autoridades Regulatorias para cumplir con los nuevos requerimientos regulatorios.**
Nuevas especificaciones para el tratamiento y seguimiento de los riesgos: crédito, mercado, liquidez y estructural, titulizaciones, etc.	**Experiencia contrastada con especialistas por cada uno de los riesgos tanto a nivel nacional como internacional.**
Tratamiento de los conglomerados financieros.	**Experiencia en proyectos transversales en conglomerados financieros nacionales e internacionales.**

Próximos pasos

'AS IS –TO BE'

Implantación en la organización de todas las exigencias regulatorias

¿Por qué KPMG?

1. El equipo de Financial Risk Management de KPMG dispone de amplia experiencia internacional en el asesoramiento a Entidades Financieras en la implementación de requerimientos normativos y regulatorios tanto de ámbito local como internacional (Basilea, EBA, Banco de España)

2. KPMG ha colaborado con las principales Instituciones Financieras en relación a las exigencias regulatorias de adaptación a la normativa de solvencia. También ha participado en multitud de proyectos relativos a COREP, FINREP, Reporting de Liquidez, RDA, IRP, MIFID, EMIR, Dodd Frank, nuevo proceso de supervisión SREP, etc.

3. Conocemos tanto a nivel funcional como técnico una buena parte de las herramientas empleadas en la generación de reporting en las entidades. Hemos implantado además Datamarts y herramientas de reporting de riesgos en multitud de entidades nacionales e internacionales.

4. El equipo de Financial Risk Management de KPMG dispone de amplia experiencia internacional en el asesoramiento a Entidades Financieras en el ámbito de la gestión de los riesgos asociados a la actividad bancaria. Somos un equipo multidisciplinar, que combina perfiles con amplios conocimientos de negocio en relación con la gestión de riesgos y el capital, con profesionales con experiencia en tecnología y sistemas de información

5. KPMG garantiza la calidad de sus servicios, el cumplimiento de los plazos, así como el máximo aprovechamiento de sus recursos para cubrir las mejores expectativas de sus Clientes.

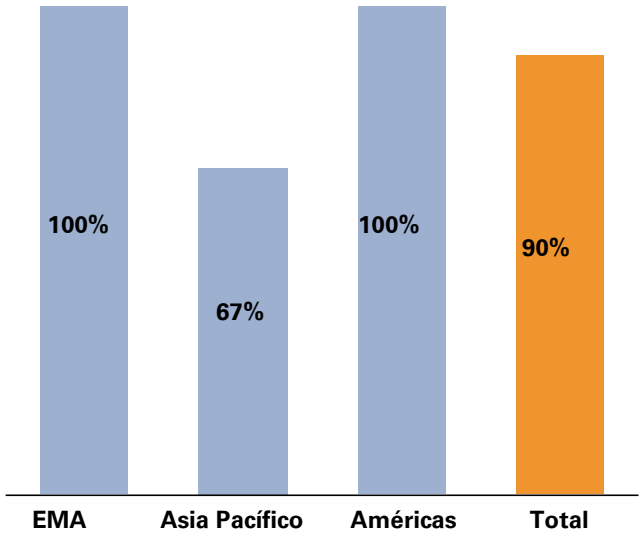
¿Por qué KPMG?

Líderes a nivel mundial en la prestación de servicios a la industria financiera …

KPMG Financial Advisory Services…

- ✓ …**asesora al 60% de los 500 mayores bancos del mundo**, liderando el segmento de los 20 bancos más grandes.
- ✓ …**audita el 30% de los 20 mayores bancos** por capitalización bursátil y el 35% por activos gestionados.
- ✓ …posee un **equipo especializado** con más de **800 socios** y **7000 profesionales** con **dedicación exclusiva** al **sector financiero**.
- ✓ …es **líder en el asesoramiento a Gobiemos y Autoridades Económicas** de las **principales economías europeas** (Reino Unido, Alemania, Irlanda, Holanda, España, Chipre) en los procesos de reestructuración en sus respectivos sistemas financieros, así como en el cumplimiento de los protocolos necesarios para acudir a los programas de estabilización y ayuda diseñados por la Comisión Europea.

Clientes de KPMG entre las 20 mayores Entidades Financieras



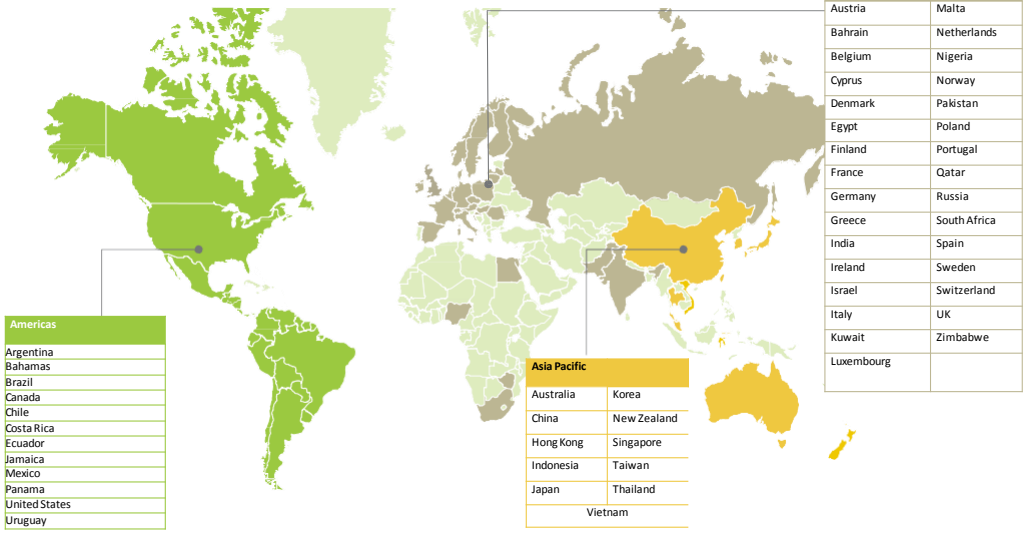
¿Por qué KPMG?

… contando con más de 2.600 profesionales especializados en Financial Risk Management distribuidos en 54 países…

KPMG Financial Risk Management…

- ✓ … tiene áreas específicas de FRM en **54 países**,
- ✓ …en los que cuenta con más de **2.600 profesionales especializados** en este ámbito.
- ✓ …el área de FRM **en España** se creó en 2005 y **cuenta en la actualidad con más de 260 profesionales**.

Países en los que KPMG tiene un área especializada de FRM



Americas
Argentina
Bahamas
Brazil
Canada
Chile
Costa Rica
Ecuador
Jamaica
Mexico
Panama
United States
Uruguay

Asia Pacific	
Australia	Korea
China	New Zealand
Hong Kong	Singapore
Indonesia	Taiwan
Japan	Thailand
Vietnam	

EMA	
Austria	Malta
Bahrain	Netherlands
Belgium	Nigeria
Cyprus	Norway
Denmark	Pakistan
Egypt	Poland
Finland	Portugal
France	Qatar
Germany	Russia
Greece	South Africa
India	Spain
Ireland	Sweden
Israel	Switzerland
Italy	UK
Kuwait	Zimbabwe
Luxembourg	

Nº de recursos especializados en FRM

(*) El total EMA que se muestra no contabiliza los recursos de España.

¿Por qué KPMG?

… y con los medios organizativos, tecnológicos y humanos para poner en valor todo nuestro conocimiento a nivel mundial.

Panel de expertos internacional KPMG

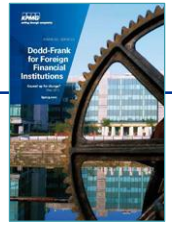
- **Panel de expertos con amplia experiencia** en la implantación de nueva normativa en múltiples entidades financieras compuesto por personal de KPMG
- Reuniones y actualizaciones regulares con el objetivo de discutir las *best practices* en el mercado provocado por demandas regulatorias, avances técnicos, existencia en el mercado de actualizaciones normativas, etc.

Actualización *best practices* del mercado

- Identificación de principales novedades y requerimientos normativos
- Preparación de workshops, evaluación e impacto de la nueva normativa, soluciones técnicas que den soporte a los requerimientos normativos, etc.
- Consultas on- call

KPMG Centro de Excelencia Regulatorio

- KPMG cuenta con un Centro de Excelencia Regulatorio a nivel europeo que apoya a toda KPMG en diferentes proyectos de índole normativa (con sedes en Londres, Frankfurt y Bruselas)
- Esta compuesta por expertos en el Sector Financiero ubicados en los diferentes países que participan en los diferentes foros y grupos de trabajo.
- Nuestro CoE emite continuamente alertas y publicaciones sobre materias relevantes, trabaja con nuestros clientes apoyando los proyectos directa e indirectamente y forman parte de los paneles técnicos de nuestros clientes

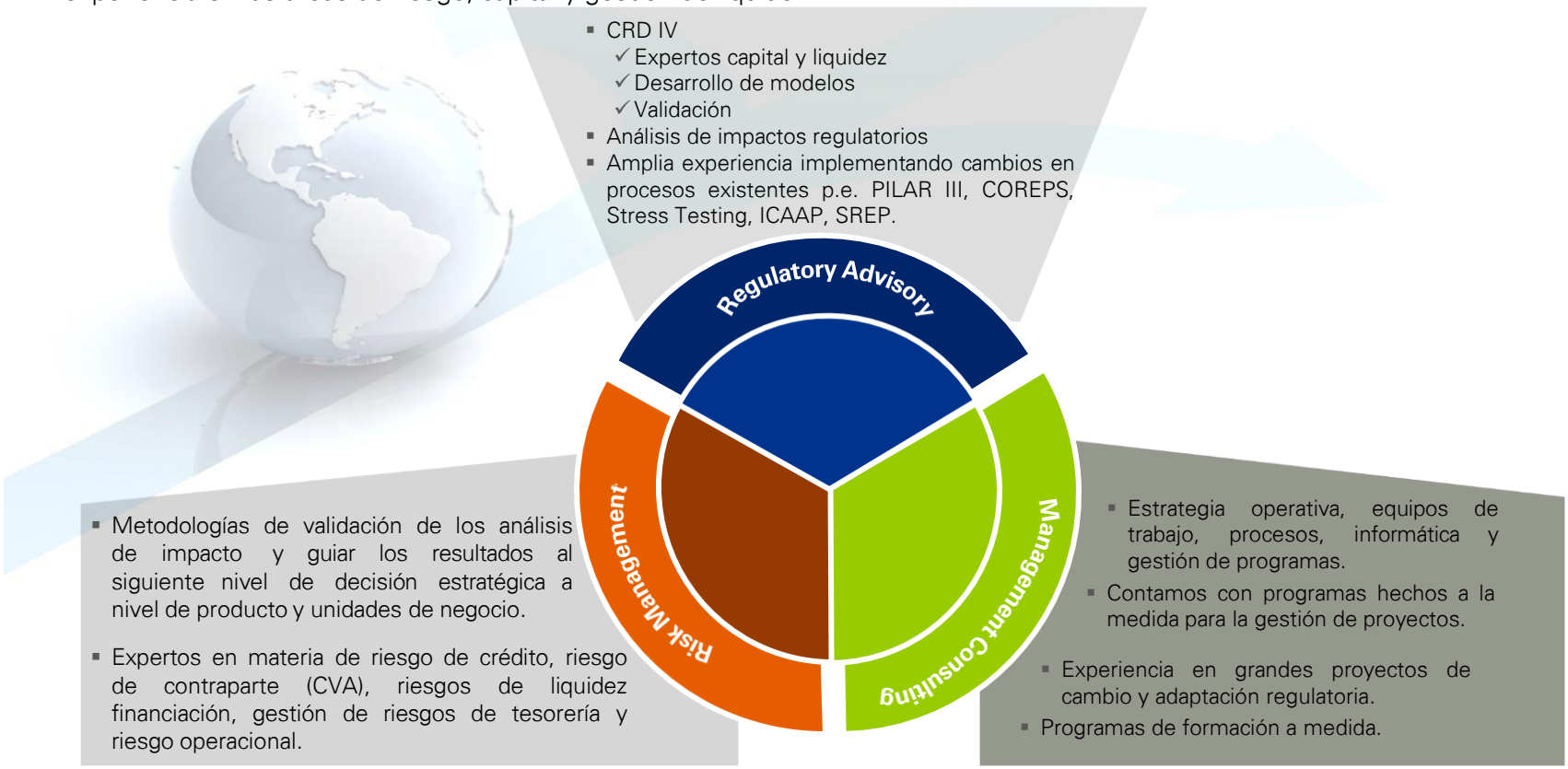


Thought leadership

- Publicaciones de primer nivel
- Papeles de discusión en foros relevantes
- Avances relevantes en el mercado
- Proyectos de éxito en el sector financiero y otros
- Aparición de nuevas tecnologías y contraste de funcionalidades

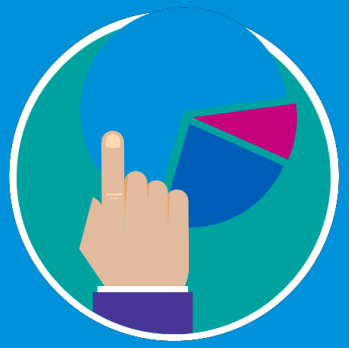
¿Por qué KPMG?

- KPMG dispone y domina las disciplinas y competencias adecuadas para dar soporte a una gestión exitosa de la trasposición y adaptación a la normativa internacional.
- Si las necesidades o inquietudes proviene de la comprensión de la propia norma, la necesidad de evaluar su impacto en el negocio, desarrollar una estrategia o implementar un cambio organizacional; nuestras capacidades de asesoramiento, gestión de riesgos y consultoría de gestión aseguran que podemos ofrecer el mejor servicio, sin importar cuales sean los aspectos a cubrir. Al formar parte de una red internacional, KPMG cuenta con algunos de los expertos con mayor experiencia en las áreas de riesgo, capital y gestión de liquidez.



KPMG

Anexo



Categorización de riesgos ICT
Taxonomía de Riesgos

A continuación se detallan los cinco grandes ámbitos de categorización de riesgos ICT:

1 Riesgos ICT de disponibilidad y continuidad	
Gestión de una capacidad inadecuada	▪ La falta de recursos (por ejemplo, *hardware, software*, personal, proveedores de servicios) puede dar lugar a una incapacidad para escalar el servicio; y de esta manera satisfacer las necesidades del negocio, interrupciones del sistema, la degradación del servicio y/o errores operacionales.
Fallos de los sistemas ICT	▪ Pérdida de disponibilidad debido a fallos de *hardware*. ▪ Pérdida de disponibilidad debido a fallos de *software* y "*bugs*".
Continuidad inadecuada de ICT y planificación de recuperación de desastres	▪ Fallo en la planificación de disponibilidad de ICT y/o soluciones de continuidad y/o recuperación de desastres (por ejemplo de recuperación de información del centro de datos) cuando se activa en respuesta a una contingencia.
2 Riesgos ICT de seguridad	
Seguridad inadecuada de los elementos ICT	▪ Mal uso o robo de los bienes ICT a través del acceso físico, que cause daños, pérdida de activos o de datos o para hacer posibles otras amenazas.
	▪ El daño deliberado o accidental de los activos ICT físicos causados por el terrorismo, accidentes o manipulaciones desafortunadas/erróneas por parte del personal de la institución y/o terceros (proveedores, técnicos).
	▪ Protección física insuficiente frente a los desastres naturales que resulta en la destrucción parcial o total de los sistemas/centros de datos.

Categorización de riesgos ICT
Taxonomía de Riesgos

A continuación se detallan los cinco grandes ámbitos de categorización de riesgos ICT:

2

Riesgos ICT de seguridad *(cont)*	
Inadecuado nivel de seguridad ICT interno	▪ Obtener acceso no autorizado a los sistemas críticos ICT dentro de la Entidad para diferentes propósitos (fraude, robo de datos) por una variedad de técnicas (por ejemplo, abusar de privilegios, el robo de identidad, despliegue de software malicioso).
	▪ Manipulaciones no autorizadas ICT debido a los procedimientos y prácticas de gestión de acceso inadecuado.
	▪ Amenazas de seguridad debido a la falta de conciencia de la seguridad mediante el cual los empleados no entienden, cometen alguna negligencia o no se adhieren a las políticas y procedimientos de seguridad ICT.
	▪ El almacenamiento no autorizado o la transferencia de información confidencial fuera de la Entidad.
Ciberataques	▪ Ataques con diferentes propósitos, que dan lugar a una sobrecarga de los sistemas y la red.
	▪ Los ataques realizados a partir de las redes de Internet para diferentes propósitos (fraude, espionaje, terrorismo cibernético) usando una variedad de técnicas (por ejemplo, la ingeniería social, despliegue de software malicioso), resultando decisivo en la toma del control de los sistemas de ICT internos.
	▪ Ejecución de operaciones de pago o de valores fraudulentas por *hackers* a través de la ruptura o la neutralización de la seguridad de los servicios de banca electrónica y de pago.
	▪ Ataques a las conexiones de comunicación y conversaciones de todo tipo o sistemas ICT con el objetivo de recopilar información y/o cometer fraudes.

Categorización de riesgos ICT
Taxonomía de Riesgos

A continuación se detallan los cinco grandes ámbitos de categorización de riesgos ICT:

3	Riesgos ICT de Cambio
Controles inadecuados sobre los cambios en sistemas ICT y sus desarrollos	▪ Incidencias causadas por errores no detectados o vulnerabilidades como resultado del cambio (por ejemplo, efectos imprevistos de un cambio o un cambio mal administrado debido a la falta de pruebas o prácticas inadecuadas)
Arquitectura inadecuada de los sistemas ICT	▪ Una escasa gestión en el desarrollo, construcción y mantenimiento de la arquitectura de los sistemas ICT (*software*, *hardware*, datos) puede conducir con el tiempo a sistemas ICT rígidos, que ya no estén alineados con las necesidades del negocio y no que no pueden dar cobertura a las necesidades reales de gestión de riesgos.
Ciclo de vida inadecuado	▪ Fallo en el control del inventario de los activos ICT o incoherencias con lo recogido en el control de revisiones. Esto puede provocar una insuficiencia en los sistemas y por consiguiente lo convierte en más vulnerable. La obsolescencia en los sistemas puede conllevar un mal servicio al negocio y a la propia necesidad de gestión del riesgo.

4	Riesgos ICT de integridad de los datos
Procesamiento y manejo de datos	▪ Debido al proceso de carga de datos en el sistema, los datos podrían estar dañados o corruptos (debido a diversas causas como por ejemplo ejecución errónea o transferencia incompleta de datos).
Diseño de controles de validación de datos en sistemas ICT	▪ Errores relativos a la falta o ineficacia de controles de entrada de datos automatizados y de aceptación, transferencia de datos, procesamiento y controles de salida de los sistemas ICT (controles de validez de entrada de datos, reconciliaciones).

Categorización de riesgos ICT

Taxonomía de Riesgos

A continuación se detallan los cinco grandes ámbitos de categorización de riesgos ICT:

4	Riesgos ICT de integridad de los datos
Cambios en los datos de sistemas ICT	▪ Errores en los datos introducidos debido a la falta de controles sobre la exactitud y la naturaleza en los sistemas ICT en Producción.
Diseño y/o gestión de la arquitectura de datos, flujos, modelos y diccionarios de datos	▪ Errores de identificación al no haber una fuente específica de datos que pueden dar lugar a varias versiones de los mismos en los sistemas de ICT, que no son compatibles debido a aplicarse de manera diferente en modelos de datos o definiciones de datos.

5	Riesgos de externalización
Capacidad de recuperación inadecuada	▪ Indisponibilidad de servicios críticos externalizados ICT, servicios de telecomunicaciones y servicios públicos. Además dentro de esta categorización se incluye la pérdida o corrupción de datos críticos / sensibles encomendadas al proveedor de servicios.
Inadecuada externalización del Governance	▪ Degradación del servicio o fallos debidos a procesos de control ineficientes del proveedor de los servicios externalizados. También se incluye una gobernabilidad ineficaz en cuanto a la externalización, la misma puede resultar en una falta de habilidades y capacidades para identificar plenamente, evaluar, mitigar y controlar los riesgos de ICT apropiados y puede limitar la capacidad operativa de las entidades.
Falta de seguridad de terceros o de otra entidad del Grupo	▪ La piratería de los sistemas ICT externalizados a proveedores puede tener un impacto directo en los servicios externalizados o datos críticos/confidenciales almacenados en el mismo. El personal de dicho proveedor puede obtener acceso no autorizado a los datos críticos/confidenciales almacenados.

Gonzalo Ruiz-Garma Gorostiza
Head partner Financial Risk Management
gruiz@kpmg.es

Alberto Esteban Henche
Partner Financial Risk Management
albertoesteban@kpmg.es

Alfonso Figal Morate
Partner Financial Risk Management
afigal@kpmg.es

Alfredo Garaizabal Ariza
Partner Financial Risk Management
agaraizabal@kpmg.es

Inmaculada González Bayón
Partner Financial Risk Management
inmaculadagonzalez@kpmg.es

Javier Olaso Bescos
Partner Financial Risk Management
jolaso@kpmg.es

Jordi Oliver Hernández-Nieto
Partner Financial Risk Management
jordioliver@kpmg.es

Francisco Pérez Bermejo
Partner Financial Risk Management
franciscoperez@kpmg.es

David Timon Zapata
Partner Financial Risk Management
dtimon@kpmg.es

Carlos Zayas Pinedo
Partner Financial Risk Management
czayas@kpmg.es

kpmg.es