COL·LEGI D'ACTUARIS DE CATALUNYA

CONFERENCIA

Barcelona, 13 de febrero de 2025

DORA:
LA SOLVENCIA DE LA TECNOLOGÍA

Jesús Ansón, Responsable
AREA XXI Technologies.

Ley de Resiliencia Operativa Digital (DORA)

La Solvencia de la tecnología

AREA XXI

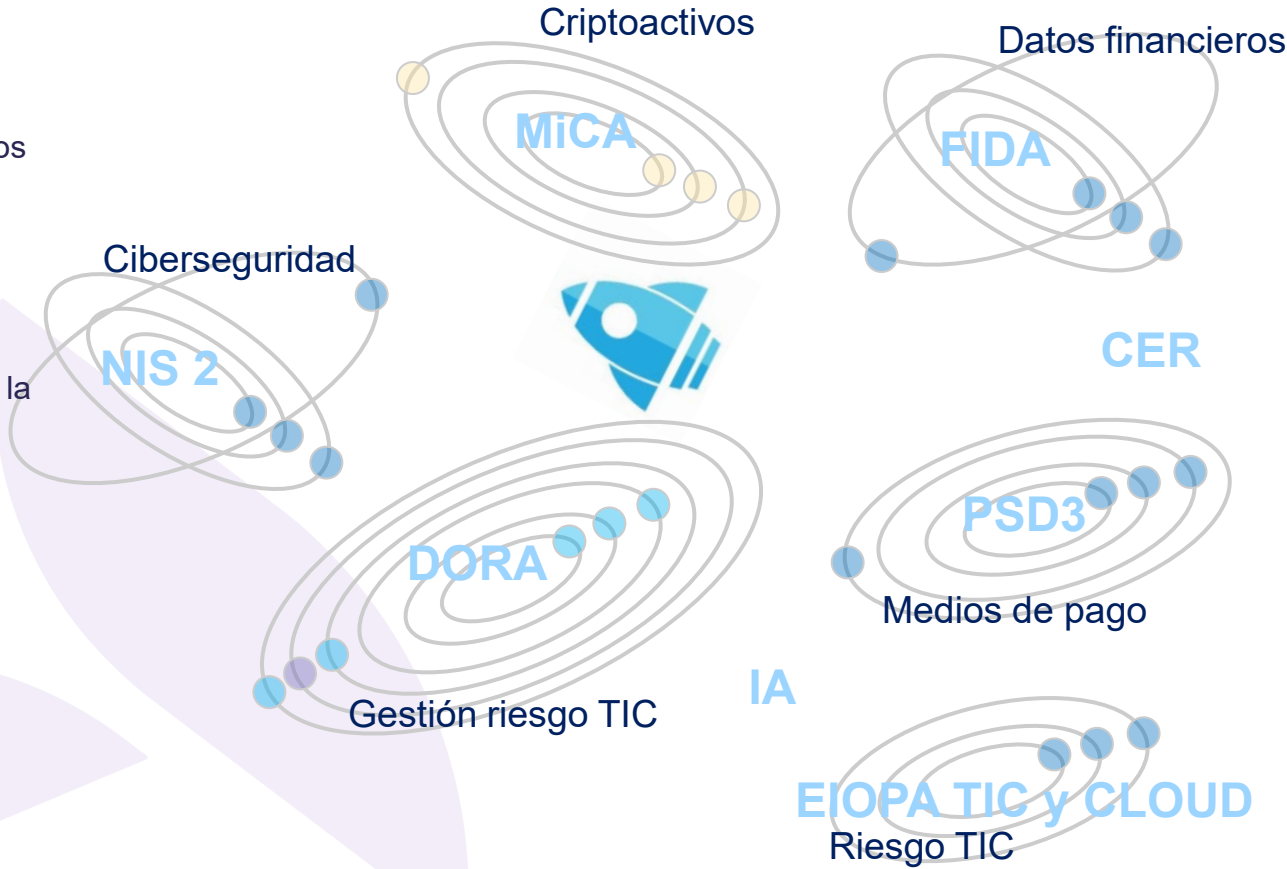
Antecedentes

- La preocupación de los reguladores en materia de gobierno de las tecnologías es creciente dado el gran número de incidentes que se producen cada año
- Desde que la AESPJ puede emitir recomendaciones para el sector segurador ha detectado la necesidad de desarrollar una orientación específica sobre la gobernanza y seguridad de las tecnologías de la información y las comunicaciones (TICs)
- No se ha conseguido reflejar la importancia de la TICs con un marco regulador fragmentado y amplia variedad de actuaciones en cuanto a supervisión
- La complejidad de las TICs va en aumento así como la frecuencia de los incidentes asociados

- Los reguladores están preocupados ya que los modelos negocio tanto tradicionales como innovadores están en el uso de las TICs, poniendo en riesgo los objetivos estratégicos, corporativos, operativos y de reputación de la empresa
- EIOPA ha emitido una serie de Directrices de obligado cumplimiento desde 31 de Julio de 2021
- La UE ha emitido recomendaciones y Directrices sobre gobernanza y Resiliencia, de obligado cumplimiento en Enero de 2025
- El sector Financiero y Asegurador será el primer sector en adoptar estas medidas

Universo normativo TIC

- La tecnología ya soporta prácticamente la totalidad de los procesos de negocio
- Se hace necesario controlar el riesgo inherente al uso de la tecnología
- Existe dispersión en cuanto a la normativa
- En los próximos años se espera una avalancha normativa sobre temas relacionados con la tecnología



DORA (Digital Operations Resiliance Act)

- Se define RESILIENCIA como la capacidad de sobreponerse a eventos adversos
- Dada la cantidad de regulaciones locales y globales existentes se hacía necesaria la armonización de normas
- La Comisión Europea ha elaborado un borrador que de reglamento que establece un marco normativo único para la gestión de riesgos TIC
- La normativa es vinculante y obligatoria para todos los estados miembros no necesitando transposición local
- La EBA, ESMA , EIOPA y AES crearán un marco único de gestión y supervisión a nivel europeo
- El objetivo es
  - reforzar la exigencia de los supervisores sobre riesgos digitales
  - Establecer pruebas de los sistemas TICs
  - Facultar a los supervisores para la supervisión de los riesgos derivados de la dependencia de las TICs
  - Unificar y mejorar la gestión de riesgos TICs

Afecta a todos los actores del sector financiero y asegurador con excepciones por tamaño y cartera gestionada

DORA (Digital Operations Resiliance Act)

El BOE ha publicado el Real Decreto 410/2024, de 23 de abril, por el que se desarrolla la estructura orgánica básica del **Ministerio de Economía, Comercio y Empresa**. En su artículo 8, aborda la **estructura y funciones de la DGSFP**, tanto en su labor regulatoria; supervisora del mercado asegurador, reasegurador y de pensiones, y de atención a las reclamaciones de los asegurados.

En cuanto a estructura, se añade una **nueva División de Supervisión Tecnológica y de Innovación Digital**, que asumirá las funciones de coordinación de las relaciones con las instituciones de la Unión Europea y con los supervisores de otros Estados y con organismos internacionales y el análisis de la documentación que deben remitir las entidades para facilitar el control de su actividad en materia tecnológica y de innovación digital.

Situación actual

- Nivel de adaptación de las compañías
  - Adaptación global 50% al 75%
  - Totalmente adecuada 1,2%
  - Entre el 75% y el 100% el 21,4%
- Confianza frente a la adaptación para Enero de 2025
  - Confían en ser capaces 41,7%
  - No van a ser capaces 23,8%
- Principales dificultades
  - Plazo limitado 97,5%
  - Falta de personal cualificado 62,5%
  - Falta de formación o especialización 42,5%
- Mayores desafíos
  - Gestión de riesgos de terceros 76,5%
  - Gestión de riesgos TIC 60,5%
  - Testeo Resiliencia Operativa 58%

Fuente de los Datos ICEA

Impacto

¿Dónde impacta?

- Gobernanza interna de las TIC
- Auditorias TIC
- Continuidad y estrategia de resiliencia digital
- Cyberseguridad y comunicación de incidentes a los reguladores
- Gestión de proveedores, modelos de Gobierno, Gestión de SLAs, contratos

¿Qué se va a revisar?

- Sistemas, protocolos y herramientas
- Respuesta y recuperación de incidentes
- Políticas de seguridad
- Aprendizaje y evolución
- Comunicación de incidentes
- Adopción de nuevos estándares
- Pruebas de resiliencia operativa
- Gestión del riesgo de terceros
- Acuerdos de intercambio de información

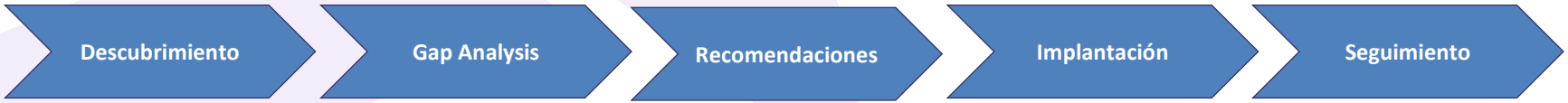
Metodología

El proyecto se divide en 11 bloques atendiendo a las mejores prácticas y la obligatoriedad de cumplimiento según DORA

1. Análisis y comprobación
2. Aprendizaje, evolución y formación
3. BCP, DRP, respaldo, protección y pruebas
4. Ciberseguridad y pruebas
5. Comunicación a reguladores y foros
6. Contratos con proveedores
7. Gestión de incidentes
8. Gestión del riesgo
9. Modelo de gobierno
10. Operación TIC - Sistemas
11. Pruebas y protección de los sistemas

Fase 1 : Gap analysis

Fase 2 : Implantación



Metodología

Fases del proyecto: Fase 1- Gap Analysis

	Descubrimiento	Gap Analysis	Recomendaciones

ACCIONES	• Reuniones con negocio
	• Workshops
	• Generación de documentos
	• Validación de los requerimientos
	• Gestión de cambios a los requerimientos
		• Estudio de los datos obtenidos en ,
		  • Infraestructura
		  • Aplicaciones
		  • Proveedores IT
		• Comparación frente a mejores practicas
		• GAP ANALISYS frente normativa
		• Elaboración de la matriz de cumplimiento
			• Elaboración de documento con conclusiones
			• Elaboración de documento con recomendaciones y prioridades

ENTREGABLES	• Documentación Workshops • Actas de reuniones • Documento de estado TICs • Metodología para gestión de cambios al documento	• Informe de cumplimiento por artículo • Informe de cumplimiento por área	• Informe de recomendaciones • Informe de procesos, políticas y documentos a generar • Plan con acciones priorizadas

Metodología

Fases del proyecto : Fase 2- Implantación

	Implantación	Seguimiento
ACCIONES	• Seguimiento de los proyectos acordados durante la Fase 1 • Reuniones de seguimiento • Generación de documentación • Generación de políticas y procedimientos	• Seguimiento del modelo de gobierno • Implantación de los comités • Gestión de cambios al contrato/ servicio • Reuniones de seguimiento y reporting • Soporte frente a posibles auditorías

ENTREGABLES	• Documentación proyecto
	• PMO
	• Propuestas de mejora
	• Informes de avances
	• Soporte
	• Generación de documentos requeridos por DORA
	• Adaptación de procesos y políticas
	• BIA
	• BCP
	• Mod, Gobierno
		• Propuestas de innovación
		• Implantación de cambios según peticiones de negocio
		• Seguimiento proveedor a 3 niveles:
		  • Estratégico
		  • Táctico
		  • Operacional
		• Soporte frente a posibles auditorías

Metodología de implantación

Ejemplo práctico

Ley de Resiliencia Operativa Digital (DORA)

Proveedores y Gobernanza

AREA XXI

Proveedores y Gobernanza

- La gestión del riesgo tecnológico asociado a la externalización de servicios que den soporte a procesos críticos dentro de las entidades financieras y aseguradoras es uno de los puntos donde DORA pone foco.
- Tradicionalmente, fuera del mundo anglosajón, las relaciones contractuales con los proveedores no han especificado controles para el riesgo que se asume, Ahora DORA obliga a la inclusión de estos controles
- EIOPA CLOUD ya hacía referencia a algunos puntos sobre la externalización de servicios, DORA amplia esta normativa

- Las entidades aseguradoras están acostumbradas a la implantación del Gobierno Corporativo, hasta la fecha los departamentos de tecnología raramente participaban en estos modelos de gobierno
- DORA obliga a las entidades a incluir la tecnología dentro del modelo de Gobierno Corporativo.

Proveedores

Puntos a comprobar en un contrato de externalización de tecnología

1. Especificar estándares de seguridad de la información
2. Cláusulas de terminación
3. Planes de salida y derechos de terminación
4. Especificar derecho y obligaciones
5. Detalle de los servicios a externalizar
6. Subcontratación
7. Localización de los servicios
8. Disposiciones sobre integridad y confidencialidad de los datos
9. Accesibilidad a los datos y devolución
10. Niveles de Servicio
11. Obligación de prestación de servicio en caso de incidente
12. Colaboración con las autoridades
13. Participación en los planes de sensibilización sobre Resiliencia
14. Información sobre incidentes
15. Derechos de inspección y auditoría
16. Participación en los pentest

Gobierno

Puntos a comprobar en un modelo de Gobierno TIC

1. Órgano de Gobierno TIC documentado
2. Función de gestor servicios TIC externalizado
3. Función de gestor de riesgos en tecnología
4. Mecanismos de aprobación de tolerancia al riesgo
5. Mecanismos de supervisión de los planes de continuidad incluidos sus presupuestos
6. Mecanismos de supervisión de las auditorías TIC
7. Mecanismos de supervisión del riesgo asociado a proveedores TIC

Ruegos y preguntas

COL·LEGI
D'ACTUARIS
DE CATALUNYA

actuaris@actuaris.org
www.actuaris.org