servicenow

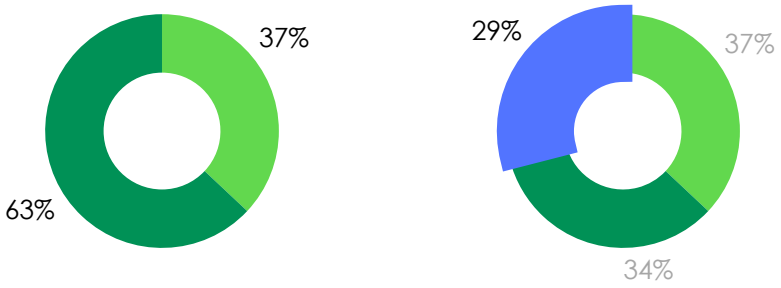
Digital Operational Resilience Act (DORA)

¿Estamos preparados?

Con el lanzamiento en Europa del Digital Operational Resilience Act (DORA), nos encontramos en un punto de inflexión en la gestión de riesgos en la banca. En una industria tan compleja y fuertemente regulada como ésta, es justo decir que se está volviendo extremadamente difícil cumplir con el creciente escrutinio normativo y los costes derivados de ese cumplimiento.

Complejidad acelerada en muchas ocasiones, por la falta de acceso o acceso sesgado a los datos, muchas veces en silos, procedimientos procesados no necesariamente actualizados o los controles manuales existentes.

En un estudio reciente realizado en colaboración con Thoughtlab, tanto la gestión de riesgos y como la resiliencia son prioridades para el 63% de los CEO del sector. El mismo estudio indica no obstante que sólo un 29% de estas organizaciones utilizan actualmente soluciones digitales para la gestión de riesgos transversal e integrada.



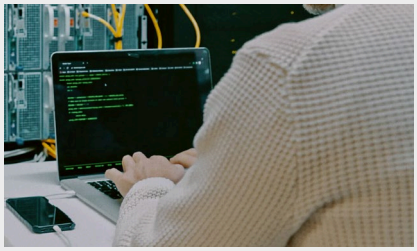
Encuestas realizadas por ServiceNow y ThoughtLab a 1.000 ejecutivos de nivel C de cinco sectores y 13 países de empresas de entre 350 millones de dólares y más de 5.000 millones de dólares de ingresos anuales.

Es por tanto un área significativa de aceleración y de mejora. Donde cada vez es más frecuente ver a los reguladores mundiales en busca de escenarios de incumplimiento. Esta es una de las razones principales por la que toda entidad financiera está empezando a poner foco en sus riesgos críticos, y en los retos que plantea la gestión transversal y unificada de los mismos:

- Silos organizativos y redefinición de funciones y responsabilidades. Hay una falta de seguimiento integrada así como de la trazabilidad extremo a extremo, dando lugar a una gestión inconsistente.
- Visión inconsistente en las líneas de defensa provocada por percepciones disjuntas de los datos: diferentes sistemas ofrecen diferente interpretación de los datos sobre el mismo elemento.
- Dispersión tecnológica debida a varias fuentes y sistemas de datos. Falta de integración de las fuentes de gestión de riesgos y de recopilación de dato, por lo que resulta costoso disponer de una verdad única para tomar las decisiones adecuadas a tiempo.

DORA es el catalizador para que las instituciones del sector:

- Tengan control, conocimiento y detalle de sus prácticas de resiliencia operativa de las TIC y de gestión de riesgos cibernéticos y de terceros que afectan a la resiliencia de sus funciones más críticas.
- Desarrollen nuevas capacidades operativas, como nuevos métodos más exhaustivos de prueba de escenarios.



DORA tiene como objetivo reforzar y armonizar a nivel europeo los principales requisitos de ciberseguridad para las empresas financieras.

29%

de las organizaciones utilizan soluciones digitales para la gestión de riesgos transversal e integrada

Fuente: Digital Operational Resilience Act (DORA)

Los grandes bancos suelen gestionar más de 1.500 requisitos normativos a lo largo de todas sus líneas de negocio. A menudo se centran en marcos de ámbito internacional y regional como Basilea III, SOX, CCARS y así como en aquellos asuntos que requieren atención (MRA). Dar prioridad a estas iniciativas es clave para integrar eficazmente datos, procesos y marcos normativos.

La Ley de Resiliencia Operativa Digital (DORA) en la UE conforma un impacto regulatorio de gran relevancia. Para el mercado europeo de servicios financieros, DORA representa la iniciativa más importante para la resiliencia operativa y la ciberseguridad en los servicios financieros. Se trata de un marco acordado que exigirá a las entidades financieras, una visión más amplia y completa de la resiliencia. Y por primera vez en el sector, con responsabilidad en el nivel de alta dirección.

Esta regulación establece el marco de trabajo para que los supervisores (FSAs) examinen 5 pilares principales: Gestión de riesgos de las TIC, notificación de incidentes, pruebas de resistencia, gestión de riesgos de terceros e intercambio de conocimientos.

Desde la firma del acuerdo, las organizaciones de SL dispondrán de un plazo de 22 meses, que concluirá a finales del cuarto trimestre de 2024. Para entonces, las organizaciones supervisoras esperarán de las empresas del sector el cumplimiento pleno de los nuevos requisitos.

Dicho otro modo, esta expectativa representa una hoja de ruta en la que las organizaciones de servicios financieros (bancos, entidades de pago, empresas de inversión, criptomonedas...) necesitan establecer su estado actual, a partir del cual desarrollar su hoja de ruta y adecuar su gestión de la resiliencia operativa a los estándares descritos en el DORA.

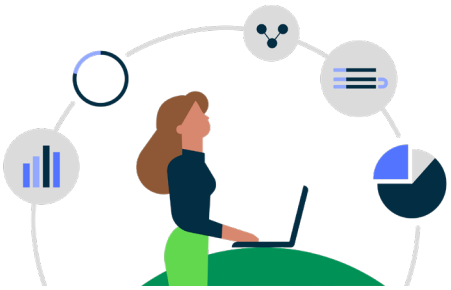
Resillencia Operativa Vs. DORA. La Resiliencia Operativa entendida en el contexto del marco regulatorio británico es una iniciativa que recoge un conjunto de principios y de resultados objetivo. En términos generales, podríamos inferir que la resiliencia operativa consiste en evitar que los incidentes operativos afecten a consumidores y sistemas financieros. DORA por su parte, abarca un contexto más amplio y expone además un conjunto de requisitos legislativos con mayor foco en la gestión del riesgo digital y de las TIC.

¿Qué significa DORA en términos prácticos?

La primera reflexión es que la conversación no ha hecho más que empezar. Si seguimos los cinco pilares recogidos en el marco normativo, podemos dar una mejor visión de lo que significa para una institución financiera. Igualmente, podremos analizar por dónde comenzar el análisis de carencias, paso necesario que nos permitirá establecer la hoja de ruta.

> “DORA representa la iniciativa más importante para la resiliencia operativa y la ciberseguridad en los servicios financieros.

> “Esta regulación establece el marco de trabajo para que los supervisores (FSAs) examinen 5 pilares principales.



1. Gestión del riesgo de las TIC

DORA traslada la propiedad y la responsabilidad a la dirección de las empresas. A partir de la entrada en vigor de la norma, asumirán un papel activo en la definición de la estrategia de resiliencia operativa digital. Las entidades de servicios financieros tendrán que:

- Establecer tolerancias de riesgo, KPI y métricas además de las interrupciones de las TIC.
- Identificar las funciones críticas (CIF) y trazar un mapa de sus activos y dependencias.
- Comprender las interdependencias entre activos, procesos y sistemas de TIC.
- Llevar a cabo análisis de impacto en negocio basados en escenarios de destrucción grave del negocio. Dicho de otro modo, diseñar escenarios de prueba más sofisticados complejos y completos, así como llevar acabo su ejecución.

5

Pilares principales

2. Notificación de incidentes de TIC

DORA exigirá a las instituciones de servicios financieros que optimicen los procesos obligatorios de notificación instantánea de la UE. Esto implicará la creación, clasificación, notificación y comunicación de incidentes, además de poner a prueba la capacidad de las empresas para recopilar, analizar y difundir información sobre incidentes de TIC y amenazas a los servicios. Un área de crecimiento muy relevante, ya que es un espacio en el que pocas organizaciones tienen capacidad para evaluar el impacto cuantitativo de sus incidentes. Por último, como parte de los requisitos de notificación de incidentes, se pedirá a las organizaciones que elaboren un informe conjunto en el que se evalúe la viabilidad de centralizar la notificación de incidentes a través de un Hub único en la UE para este tipo de comunicaciones TIC. Este modelo de reporte de incidentes TIC, se espera que ayude a redefinir y aliviar la carga que supone el cumplimiento de múltiples requisitos de notificación instantánea en los servicios financieros.

3. Pruebas

DORA exige a todas las empresas del ámbito de aplicación que la operación, resiliencia y pruebas cubran tres puntos clave:

- Demostrar que llevan a cabo un conjunto adecuado de pruebas de seguridad y resiliencia en sus sistemas y aplicaciones informáticas críticas con carácter anual.
- Abordar cualquier vulnerabilidad identificada en las pruebas.
- Las empresas que superen un determinado umbral de importancia y madurez deberán realizar pruebas avanzadas cada 3 años.

4. TIC Gestión de riesgos de terceros

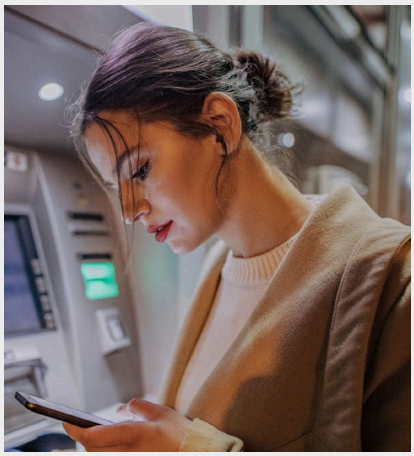
DORA, al igual que ocurre con las ESA (Entidades de Supervisión Europeas), contiene varios términos contractuales que las empresas deben incluir en los contratos de externalización de TIC. Como parte de la estrategia, cada entidad tendrá que llevar a cabo una concentración y evaluación de riesgos de todos los contratos de externalización que apoyan la entrega de CIF.

5. Intercambio de información e inteligencia.

Primer marco de supervisión CTPP para terceros. Aquellos terceros considerados críticos serán objeto de un amplio análisis de supervisión que proporcionará a la FSA la capacidad de sancionar en caso de incumplimiento. Los terceros tendrán que demostrar que pueden mejorar la resiliencia para apoyar los sistemas financieros.

Con ServiceNow, los bancos pueden orquestar y supervisar de forma inteligente la tecnología y los riesgos de seguridad. Esto permitirá a nuestros servicios financieros adaptarse más rápidamente en un enfoque por etapas para adoptar y abrazar los cambios necesarios que vienen con DORA. Ayudamos a los bancos a innovar con la única solución GRC integrada que supervisa de forma continua los riesgos y controles de personas, procesos y sistemas. La visibilidad continua en las tres líneas de defensa del banco, de arriba a abajo, proporciona a los equipos de riesgos de TI y seguridad y a los altos directivos información en tiempo real sobre controles, vulnerabilidades, planes, riesgos, indicadores clave de rendimiento y análisis.

La clave es la capacidad de automatizar todos los aspectos de la gestión del riesgo y el cumplimiento normativo, desde la primera línea hasta la tercera y en todos los departamentos y sistemas, y mantener a nuestros clientes europeos por delante de los cambios normativos.



servicenow

Bibliografía

Escrito por: Noelia Romanillos, Head of Financial Services GTM- UK & EMEA SOUTH ServiceNow.

Más de 20 años de experiencia en Experiencia de Cliente y Servicios Financieros. Experto en análisis estratégico de negocios, relaciones de experiencia del cliente y transformación empresarial impulsada por ServiceNow, ayudando a los clientes de servicios financieros a transformarse, crear excelentes experiencias de clientes y empleados para lograr los resultados comerciales correctos. He trabajado y participado en las instituciones financieras más grandes y complejas de Europa, así como en marcas globales que buscan transformar sus operaciones comerciales.