Ley de Resiliencia Operativa Digital (DORA)
La Solvencia de la tecnología

Introducción

El próximo 17 de enero de 2025 será de aplicación la nueva normativa DORA (Digital Operations Resilience Act) proveniente de la Unión Europea, que no ha necesitado de trasposición local y lleva vigente desde hace dos años.

La nueva normativa afecta a un gran número de compañías en el sector financiero y asegurador, incluyendo sectores hasta ahora poco regulados como son las compañías proveedoras de servicios de Criptoactivos. En el caso del sector segurador se ven afectadas la mayoría las compañías salvo excepciones por tamaño en ingresos por primas, en el caso de la intermediación por facturación o número de empleados o en el caso de fondos de pensiones de empleo por número de partícipes

DORA hace referencia a la gestión del riesgo asociado a la tecnología y dado que hoy en día la tecnología soporta todos los procesos de negocio esta normativa afectará a la relación que existe entre negocio y tecnología en cada uno de los ámbitos de la entidad. En este artículo trataremos de desgranar como afecta DORA a las entidades, que puntos deberán revisar y propondremos una metodología para la adopción de esta normativa.

¿Como afecta DORA a las compañías?

A la pregunta de ¿Dónde afecta DORA a las compañías?, le respuesta es sencilla, en casi todo. Hoy en día no existe casi ningún proceso de negocio que no esté soportado por la tecnología y esto hace que sea muy difícil para los responsables de la implantación de esta nueva norma compartimentar y organizar el trabajo, por otro lado, dada la magnitud de la normativa se hace imposible abordar la implantación como un todo necesitando crear grupos de actividades a la hora asignar responsables, plazos y recursos.

Para ayudar en esta tarea y revisar como afecta DORA a las compañías en el Sector Asegurador vamos a revisar cinco grandes grupos de actividades: Gobernanza, Auditoría, Continuidad, Ciberseguridad y Proveedores.

Gobernanza interna de las TICs

Aunque el sector asegurador está acostumbrado a trabajar en la Gobernanza de la compañía, su negocio y los riesgos asociados el área de tecnología ha quedado al margen de estos modelos de gobierno produciendo que en algunos casos la tecnología haya quedado fuera de la gestión de los riesgos asociados y de los órganos de decisión de la entidad. DORA obliga a las entidades a realizar una gestión del riesgo asociado a las TICs y a incluir dentro de sus procedimientos y órganos de gestión el riesgo asociado al mero hecho de utilizar la tecnología para soportar los procesos de negocio.

Los Modelos de Gobierno de la tecnología van a ser necesarios para regular la relación con el negocio, el servicio que prestan y los acuerdos sobre niveles de servicio con los diferentes departamentos. Estos modelos deberán incluir modelos de relación entre los diferentes departamentos y el departamento de tecnología especificando quién se relaciona con quién y en que foros y como se van a medir y reportar los servicios entregados.

Una práctica habitual dentro de las compañías ha sido comunicar un problema o petición relacionada con la tecnología al primer empleado de este departamento que se cruzaba en nuestro camino sin documentación, evidencia de tal comunicación o análisis previo en el caso de que la petición tenga un impacto económico. Estás prácticas quedarán reguladas obligando a la gestión de incidencias con o sin herramientas específicas, pero siempre con el mantenimiento de registros y actualizaciones a los usuarios

Auditoría TIC

Las compañías pertenecientes al Sector Asegurador están acostumbradas a las auditorías tanto externas como internas sobre los diferentes elementos de su negocio, pero hasta la fecha no era obligatorio la creación de la función de Auditoría TIC. DORA hace necesaria esta función especificando que el resultado de las auditorias debe ser conocido y aprobado por la Dirección.

La norma hace especial referencia al marco de gestión de riesgos mencionando los procedimientos, estrategias, protocolos, procedimientos y herramientas para la gestión de este riesgo.

En cuanto a terceros que soportan procesos de negocio críticos o esenciales, DORA especifica la necesidad de incluir los derechos ilimitados de auditoría, acceso e inspección, así como la necesidad de auditar los servicios prestados periódicamente.

Continuidad del Negocio

Aunque muchas de las entidades aseguradoras ya tienen un Plan de Continuidad del Negocio, DORA hace referencia a la necesidad de que estos planes estén coordinados con los requerimientos del negocio, estén actualizados, incluyan a los proveedores de tecnología que soporten procesos críticos estén aprobados por todas las unidades de negocio afectadas, se prueben periódicamente y se adopten las medidas correctivas necesarias para adecuar estos planes a los cambios. Con la llegada de DORA se hace necesaria la aparición de un presupuesto destinado a Continuidad y su gestión y conocimiento de este por parte de la Dirección.

Esta gestión de los Planes de Continuidad también redundará en beneficio de la compañía. Siempre se ha dicho que la Continuidad cuesta dinero, si gestiona por debajo del servicio necesario se asumen riesgos que pueden afectar gravemente al negocio, si se gestiona por exceso se están empleando recursos para cubrir servicios ante eventos que el Negocio no necesita ni reclama. En consecuencia,

DORA pondrá las bases para que la gestión de estos servicios sea la óptima en cuanto a costes y cobertura.

Los Planes de Continuidad deberán estar coordinados con los planes de continuidad globales de la compañía, deberá incluir la creación de comités de crisis, gestionar la documentación sobre las actividades realizadas durante las crisis y mantener informada a la Dirección de los resultados de las pruebas, puntos de mejora y recomendaciones. También deben contener un plan de comunicación a las partes interesadas e incluir a los proveedores TIC que dan soporte a funciones críticas en estos planes.

Ciberseguridad y comunicación de incidentes a los reguladores

El Centro Criptológico Nacional, sólo en España, gestionó durante 2023, 49.685 incidentes suponiendo un aumento del 380% con respecto al año anterior, durante el año en curso de media se detecta un ataque cada 32 segundos y la gravedad de los ataques también está creciendo. Con este entorno es normal que los reguladores se preocupen por los eventos que puedan sufrir las entidades que pongan en riesgos los datos de sus clientes o el servicio que prestan a estos.

DORA exige que se mida el riesgo de ciber ataques, se mitiguen esos riesgos y se realicen pruebas periódicas de la seguridad perimetral con test de penetración que deben ser llevados a cabo, al menos en ocasiones marcadas por proveedores externos de reconocido prestigio. También exige que se asegure contractualmente la buena gestión de los resultados y la inclusión en estas pruebas de los proveedores TIC que den soporte a proceso críticos de negocio.

DORA también demanda que la información sobre los ciberataques sea comunicada a los reguladores, a los foros que será necesario crear en los diferentes sectores y en algunos casos a los clientes, con lo que se hace necesario crear una política de comunicación de estos.

Gestión de proveedores

Aunque es el último punto de nuestra lista, es posiblemente uno de los más importantes para DORA y que más afectas a las entidades dado que organiza el modelo de relación con los proveedores TIC. DORA exige la existencia de una política de externalización de servicios TIC que debe estar aprobada por la Dirección, donde se especifiquen la necesidad de evaluar los riesgos asociados a un proveedor antes de la contratación y los riesgos asociados a la externalización del servicio.

Se establece también la necesidad de informar a los reguladores de la externalización de servicios TIC que den soporte a procesos críticos para la entidad y de asegurarse que los proveedores cumplen con los estándares de seguridad de la información. También se deberán evaluar la concentración de contratos en proveedores y su riesgo asociado, la solvencia de los proveedores, el riesgo asociado a la cadena de subcontratación y el riesgo asociado a la localización de los proveedores

A nivel contractual DORA establece la necesidad de incluir cláusulas de salida del contrato y planes de devolución del servicio con el fin de evitar que el servicio al cliente final se vea afectado, herramientas para medir los niveles del servicio entregado, la obligatoriedad de prestar soporte ante incidentes que afecten al servicio, derechos en caso de terminación ,los planes de continuidad del servicio prestado,

la obligatoriedad de participar en los test de ciberseguridad y garantizar el acceso de los reguladores a los datos.

Como abordar un proyecto de implantación DORA

DORA afecta a la mayoría las áreas de la tecnología de forma transversal dado que el principal objetivo de la norma es gestionar y controlar el riesgo inherente al uso de la tecnología y por tanto en mayor o menor medida se verán afectados aquellos departamentos del negocio de la entidad que utilicen la tecnología para soportar sus procesos. Es decir, hoy en día casi todos los departamentos.

Para poder abordar un proyecto de implantación de esta norma con garantías de éxito se hace necesaria la utilización de una metodología que tenga en cuenta la extensión de la normativa y la gran variedad de afectaciones que pueden surgir dentro la operativa normal del negocio.

La norma se compone de 64 artículos de los cuales las compañías afectadas deben atender especialmente a 24 de ellos. Para hacer accesible esta normativa y su aplicación, en AREA XXI hemos creado una metodología dividiendo la normativa en y 5 grandes grupos de revisión y 11 áreas de trabajo que coinciden con funciones identificables dentro de las organizaciones de tal forma que sea más sencilla la organización del trabajo. Nuestra metodología se basa en las siguientes fases:

- Gap analysis
- Recomendaciones
- Documentación

Gap Analysis

Siguiendo esta metodología de la normativa se extraen 150 puntos de revisión para cumplir con DORA. Se realiza una revisión conjunta con los departamentos de tecnología y en algunos casos con los responsables de los departamentos de negocio afectados.

Los resultados de la revisión de estos 150 puntos es lo que denominamos el “Gap Analysis” y da una idea a la Dirección de la compañía de cómo se encuentra la entidad frente a la normativa, Por lo que estamos viendo en nuestros clientes la media de cumplimiento se encuentra entre el 25% y el 40%. Datos que indican el esfuerzo a realizar durante los próximos meses en las entidades Aseguradoras y Financieras.

Recomendaciones

De los resultados obtenidos en la fase de “Gap Analysis” se desprenden una serie de recomendaciones encaminadas a crear o modificar procedimientos, políticas, protocolos y herramientas para que se adapten a DORA.

Generalmente y por la experiencia en nuestros clientes, surgen entre 80 y 100 acciones referentes a procedimientos, herramientas, políticas y documentación que serán agrupadas en proyectos asignadas a las 11 áreas de trabajo mencionadas anteriormente.

Documentación

Una de las exigencias de DORA es la documentación de los riesgos e impactos, procesos, políticas y protocolos asociados a la tecnología, para ello se revisan o se crean entre 20 y 25 documentos que deben reflejar las directrices que marca DORA y que deberán ser mantenidos periódicamente. Entre otros documentos se deberán generar y mantener análisis de impacto, planes de continuidad, políticas de gestión del riesgo TIC, políticas de externalización, procedimientos de alerta temprana, etc.

Conclusión

DORA es una normativa que va a revolucionar la manera en que se relaciona el negocio y la tecnología en las compañías financieras y aseguradoras. Su principal objetivo es la gestión del riesgo asociado a la tecnología y su implantación conlleva la implicación, no sólo del departamento de tecnología, si no de otras áreas del negocio y dada la magnitud del proyecto se hace necesaria la aplicación de una metodología específica. Durante los próximos meses las compañías afectadas tendrán elaborar y ejecutar proyectos de actualización e implantación y actualizar sus procedimientos para mantener en el tiempo los resultados de estos proyectos.