DORA Y SEGURIDAD BANCARIA

Introducción

El auge de los ciberataques, las estafas electrónicas y demás clases de fraudes económicos de origen digital surgidos en la última década han hecho que muchos usuarios **comiencen a perder la confianza en las entidades financieras** de manera generalizada.

Los riesgos tecnológicos no tienen fronteras y el sector financiero ofrece sus servicios a escala ampliamente transfronteriza, dentro y fuera de la Unión Europea. A esto se suma el **incremento de la desaparición de activos e información, la incapacidad de defenderse y, sobre todo, la de recuperarse tras un ciberataque**. Es por ello por lo que, con el fin de que se pueda llegar a proteger tanto a las entidades financieras y sus intereses como a los usuarios y sus activos dentro de las mismas, se establece la **necesidad de crear una legislación unificada para el sector**.

Por

Mercedes Gómez

Gerente de
Ciberseguridad
en Grupo Oesía

Legislación DORA y su aplicación a la banca

La legislación DORA nace principalmente con la idea de formalizar una estrategia que sea capaz de **regular la resiliencia operativa digital de todas las empresas** involucradas en el sector de las finanzas, para que estas puedan asegurarse, resistir y responder ante cualquier tipo de ciberataque o amenaza relacionada con las Tecnologías de la Información y Comunicación (en adelante, TIC) y demás entornos digitales. Esta legislación busca también que las instituciones dispongan de la **capacidad de recuperar ante las pérdidas económicas y de datos** que puedan sufrir tras una amenaza cibernética.

En lo que respecta al sector bancario, se hace de vital interés que pueda utilizarse un Reglamento como la legislación DORA para **mejorar considerablemente todos los aspectos relacionados a la ciberseguridad**. Esto **devolverá la confianza de los usuarios** a la hora de utilizar los servicios digitales que ofrecen las entidades bancarias, además, servirá a las instituciones para **fortalecer y dar seguimiento** a todos los trámites y movimientos de activos entre las diversas entidades financieras, sin que se corran riesgos de pérdidas o malversaciones por parte de terceros.

Se sabe que el mundo moderno trabaja en su mayor parte desde la red, con **almacenamiento de datos y moneda digitalizada**; anteriormente, cada institución financiera había tenido que desarrollar por su cuenta sus propios protocolos o servicios de seguridad, los cuales, al haberse gestionado de manera individual, muchas veces llegaban a presentar fallos de seguridad que los delincuentes comenzaron a aprovechar cada vez más. La importancia que el Reglamento DORA impone sobre la seguridad de la banca en general es que determina una **serie de acciones a tomar en cuenta para mayor efectividad de los procesos** de ciberseguridad.

Principales Reglas de DORA para la banca

La legislación DORA establece una serie de acciones y protocolos que deben ser aplicados por instituciones financieras de la UE y sus proveedores de servicios TIC.

Gestión de riesgos vinculados a las TIC

Las TIC están más presentes que nunca en el sector bancario. Esto supone, que a medida que aparecen nuevos servicios financieros digitales y aumenta la cantidad de usuarios y clientes, también aumenten los riesgos en la utilización de estos servicios. Para poder controlar esto, el Reglamento DORA impulsa a las entidades financieras a que sean capaces de:

- Determinar los niveles de **tolerancia al riesgo** que pueda manejar la institución para establecer un límite a la cantidad de negocios de carácter digital que una institución puede ofrecer sin que exista riesgo frente a un ciberataque.
- Hacer **revisiones periódicas** sobre la estructura y planificación de los diversos esquemas de seguridad que sean de interés para la institución.
- Realizar un **seguimiento a los acuerdos establecidos** con los proveedores de servicios TIC para que exista una mayor trasparencia en el desarrollo de los acuerdos y una mejor comunicación entre los mismos.
- Recibir **notificaciones inmediatas** sobre cualquier eventualidad o incidente de seguridad que se presente. Con esto se busca que las instituciones estén totalmente preparadas para reaccionar de manera efectiva ante cualquier intento de violación de seguridad que pueda existir.

Factores clave a tener en cuenta en la gestión de riesgos

Identificación

Es importante que las instituciones financieras estén en capacidad de identificar de manera adecuada, cuáles son sus funciones empresariales que se relacionan con las TIC y cuáles son los activos vinculados a dichas funciones.

Prevención

Las instituciones deben organizar una planificación que incite a prever y resolver, por medio de estrategias y procesos de seguridad, todos los posibles fallos e incidentes que puedan ocurrir con respecto a la disponibilidad de los sistemas, o a la protección de datos.

Detección

La legislación DORA establece que las instituciones deben contar con estrategias y mecanismos que puedan detectar de manera efectiva cualquier actividad sospechosa vinculada con las TIC.

Respuesta

Las entidades bancarias y financieras en general deben tener una capacidad de respuesta efectiva ante cualquier conflicto o incidente de seguridad que se presente. La respuesta debe ser inmediata, buscando que se logre una recuperación óptima de los procesos afectados. Para ello, se establece que se pongan en marcha distintos planes destinados a lograr este cometido, por ejemplo, un plan para estimar los daños y las pérdidas sufridas o un plan de recuperación de los activos en casos de catástrofe

Informe de incidentes

Se hace vital que las instituciones y entidades financieras sean capaces de generar de manera rápida y precisa notificaciones con respecto a cualquier ataque o incidente cibernético que hayan presentado. El Reglamento Dora establece en este sentido:

01. Plantillas

Generación de una serie de plantillas digitales que permitan la emisión de informes de incidentes, daños y conflictos en algún punto del sistema

02. Canales

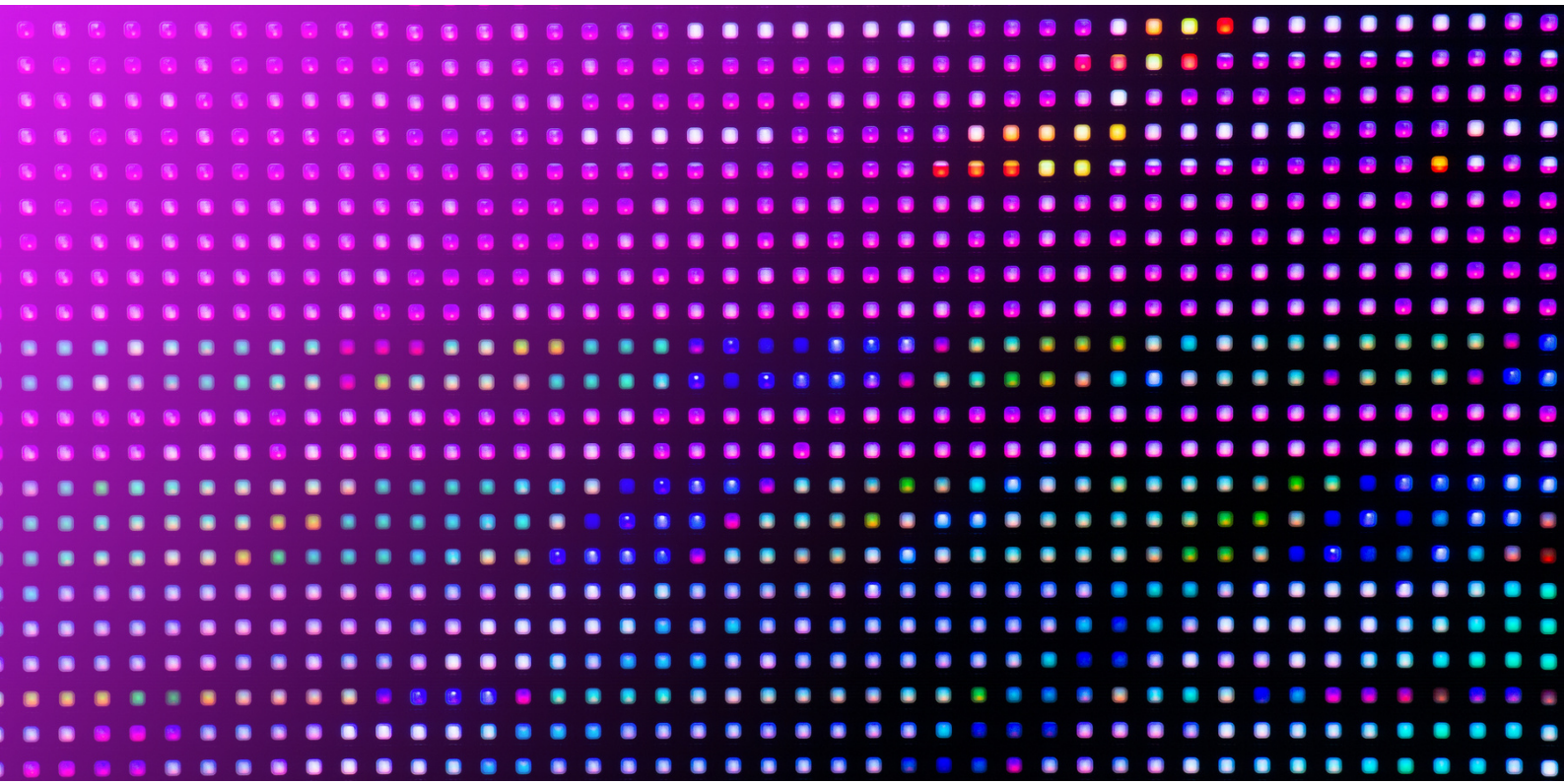
Crear canales de comunicación directa entre las entidades financieras y las autoridades competentes para el intercambio rápido de acciones y respuestas de amenazas cibernéticas, indicadores de compromiso, tácticas, técnicas, etc.

03. Recolección

Establecer un sistema centralizado de la Unión Europea para la recolección de datos. Las entidades bancarias deben enviar los informes de incidentes y desde allí serán manejados y analizados.

Pruebas de resiliencia operativa digital

El fundamento de la legislación DORA recae en formalizar y diseñar estrategias preventivas que logren minimizar los intentos de fraude o alteración de la ciberseguridad, manteniendo la capacidad de resiliencia operativa digital de las entidades financieras. Para ello, instará a las entidades a ejecutar **pruebas periódicas para comprobar el funcionamiento de los sistemas de seguridad** de cada una ellas. Estas pruebas serán capaces de determinar si existe alguna debilidad en los sistemas de defensa y buscar qué aspectos deben corregirse o mejorarse.



Qué debe tener en cuenta cada institución

La creación de mecanismos para ejecutar pruebas precisas y determinantes. Estos mecanismos serán adaptables al tamaño de la institución. En los bancos se pondrán a prueba según sea la cantidad de productos digitales que se ofrezcan.

Los cambios constantes en el nivel de riesgo de las TIC. Esto es debido a las constantes actualizaciones y mejoras que suelen presentar las tecnologías de la comunicación.

Contar con una serie de políticas bien definidas para mejorar la clasificación y la resolución de los problemas.

La aplicación de **la legislación DORA en la banca pondrá más obstáculos a los delincuentes digitales** y expandirá el camino hacia el crecimiento y desarrollo de nuevas y más confiables tecnologías que puedan aplicarse para el beneficio y comodidad de los usuarios"

Cómo puede Grupo Oesía ayudarle con su adaptación a DORA

OSV es la solución que cumple con las exigencias de DORA

Nuestra solución OSV para DORA cuenta con todas las especificaciones necesarias para ayudar a las entidades a cumplir con el marco normativo de actuación:

- Gestión de riesgos
- Notificación de incidentes
- Pruebas de resiliencia operativa digital
- Intercambio de inteligencia
- Riesgos de tercero en materia TIC

Prevención y auditoría

- Asesoramiento en el desarrollo de políticas y procedimientos de seguridad de la información.
- Impartición de las formaciones que las entidades están obligadas a proporcionar a su personal y a sus directivos.
- Realización de análisis de riesgos sobre los sistemas de las entidades financieras.
- Realización de auditorías de resiliencia digital.

Más información en: grupooesia.com/areas/ciberseguridad