DORA (Resiliencia Operativa)

Implicaciones en la gobernanza

ETHALO
Ethics & Algorithms

Reflexiones sobre Gobierno Corporativo

Imágenes realizadas por el autor con IA (Firefly)

Avenida Isabel de Farnesio (1512), local J
28660 Boadilla del Monte
www.ethalo.es

Serie Reflexiones sobre Gobierno Corporativo
Primera edición: abril 2024

Cita del presente documento:
Patxi Barceló. DORA (Resiliencia Operativa): Implicaciones en la gobernanza. Ethalo Advisory – Serie Reflexiones sobre gobierno corporativo. Abril 2024.

Reglamento de Resiliencia Operativa Digital (DORA)

Implicaciones en la gobernanza

Introducción

El reglamento de resiliencia operativa digital (DORA[1]), aplicable a partir del 17 de enero de 2025, da continuidad al objetivo de la Unión Europea de **reforzar los procesos de gobernanza y la responsabilidad del Consejo en el ámbito de la digitalización** de las empresas.

Si bien la estrategia y la gestión de riesgos son dos funciones indelegables del Consejo, su aterrizaje en los riesgos digitales no estaba desarrollado. La directiva de ciberseguridad (NIS 2) y el reglamento de resiliencia operativa (DORA) vienen a rellenar este hueco, junto con otras normas complementarias.

Aunque este reglamento afecta al sector financiero, debe considerarse este en sentido amplio e incluye también a terceros proveedores, lo que hace que su ámbito de aplicación sea extenso[2]. Las entidades financieras llevan ya un tiempo trabajando en la efectiva implantación, aunque algunas cuestiones de detalle están pendientes de la aprobación final de las directrices técnicas de desarrollo.

No obstante, **DORA pone especial énfasis en la responsabilidad del órgano de dirección** en su definición y supervisión, por lo que es necesario dedicar un breve espacio a la reflexión sobre el alcance de este reglamento en la gobernanza y sus implicaciones como **referencia de buenas prácticas para el resto de las empresas**.

¿Qué es la resiliencia operativa?

Se define la resiliencia operativa como la capacidad de una entidad financiera para construir, asegurar y revisar su integridad y fiabilidad operativas asegurando, directa o indirectamente mediante el uso de servicios prestados por proveedores terceros de servicios de TIC, toda la gama de capacidades relacionadas con las TIC necesarias para preservar la seguridad de las redes y los sistemas de información que utiliza una entidad financiera y que sustentan la prestación continuada de servicios financieros y su calidad, incluso en caso de perturbaciones.

Por tanto, los elementos centrales de atención son:

- La **continuidad** del servicio, incluso en caso de perturbaciones.
- En todo lo relacionado con la capacidad de los **sistemas de redes y de información** de resistir, con un nivel determinado de fiabilidad, cualquier hecho que pueda comprometer la **disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o de los servicios ofrecidos** por tales sistemas de redes y de información o accesibles a través de ellos[3].

[1] Texto completo accesible en diferentes idiomas disponible en EUR-LEX https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32022R2554

[2] El artículo 4 del Real decreto-ley 8/2023 de 27 de diciembre extendió adicionalmente las obligaciones de DORA a los operadores de sistemas de pago, los operadores de esquemas de pago, los operadores de acuerdos de pago electrónico, los procesadores de pagos y otros proveedores de servicios tecnológicos o técnicos que presten servicios en España.

[3] Conforme al artículo 6.2 de la Directiva (UE) 2022/2555 del parlamento europeo y del consejo de 14 de diciembre de 2022

- De las entidades financieras, incluyendo los **terceros proveedores de servicios TIC**[4] directos o indirectos.

¿Quién es el responsable último de la resiliencia operativa de las entidades?

El órgano de dirección[5] de la entidad financiera definirá, aprobará y supervisará todas las disposiciones relacionadas con el marco de gestión del riesgo relacionado con las TIC (…) y será responsable de su aplicación.

La responsabilidad, por tanto, afecta al órgano de dirección, que se define[6] como el órgano u órganos nombrados de conformidad con el derecho nacional, habilitados para fijar los objetivos estratégicos y el gobierno en general de la entidad y que supervisan y controlan el proceso de toma de decisiones en materia de gestión e incluyen a las personas que efectivamente dirigen las actividades de la entidad. En el caso español es el **consejo de administración** el que encaja plenamente con esta definición.

El preámbulo del reglamento, ahondando en esta cuestión, específica que debe exigirse a los órganos de dirección de las entidades financieras que desempeñen **un papel central y activo** en la dirección y adaptación del marco de gestión del riesgo relacionado con las TIC y de la estrategia de resiliencia digital general. El enfoque que adopten los órganos de dirección no solo debe centrarse en los medios para garantizar la resiliencia de los sistemas de TIC, sino que también debe abarcar a las personas y los procesos a través de un conjunto de políticas que promuevan, en cada nivel corporativo y para todo el personal, una fuerte concienciación sobre los riesgos de ciberseguridad y el compromiso de respetar una estricta ciber higiene a todos los niveles. La responsabilidad última del órgano de dirección en la gestión del riesgo relacionado con las TIC de una entidad financiera debe ser un principio fundamental de ese enfoque global, que se traducirá además en la **implicación continua** del órgano de dirección en el control del seguimiento de la gestión del riesgo relacionado con las TIC.

¿Cuáles son las responsabilidades del Consejo?

El reglamento establece una enumeración taxativa de obligaciones para el órgano de dirección, cuando indica[7] que el órgano de dirección de la entidad financiera definirá, aprobará y supervisará todas las disposiciones relacionadas con el marco de gestión del riesgo relacionado con las TIC, lo que se concreta en:

[4] Los servicios TIC son los servicios digitales y de datos prestados a través de los sistemas de TIC a uno o varios usuarios internos o externos de forma continua, incluidos el hardware como servicio y los servicios de hardware que incluyen la prestación de asistencia técnica a través de actualizaciones de software o firmware por parte del proveedor de hardware y excluidos los servicios telefónicos analógicos tradicionales.

[5] Artículo 5.2 del reglamento (UE) 2022/2554 de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero (DORA)

[6] Artículo 4.1.36 de la directiva 2014/65/UE, de 15 de mayo de 2014, relativa a los mercados de instrumentos financieros (MiFID)

[7] Artículo 5.2 del reglamento (UE) 2022/2554 de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero (DORA)

- Asumirá la **responsabilidad última** de gestionar el riesgo relacionado con las TIC de la entidad financiera;
- Adoptará **políticas** encaminadas a garantizar el mantenimiento de unos niveles elevados de **disponibilidad, autenticidad, integridad y confidencialidad** de los datos;
- Definirá claramente los **cometidos y responsabilidades** por lo que respecta a todas las funciones relacionadas con las TIC y establecerá **mecanismos de gobernanza** adecuados para garantizar una comunicación, cooperación y coordinación efectivas y oportunas entre dichas funciones;
- Asumirá la responsabilidad general de establecer y aprobar la **estrategia de resiliencia operativa digital**, lo que incluye determinar el nivel adecuado de tolerancia al riesgo relacionado con las TIC de la entidad financiera;
- Aprobará, supervisará y revisará periódicamente la aplicación de la **política de continuidad de la actividad** en materia de TIC y de los planes de respuesta y recuperación en materia de TIC de la entidad financiera, que podrán ser adoptados como una política específica que forme parte integrante de la política global de continuidad de la actividad y del plan de respuesta y recuperación de la entidad financiera;
- Aprobará y revisará periódicamente los **planes de auditoría internos** de TIC y las auditorías de TIC de la entidad financiera, así como sus modificaciones significativas;
- Asignará y revisará periódicamente el **presupuesto adecuado** para satisfacer las necesidades de resiliencia operativa digital de la entidad financiera con respecto a todos los tipos de recursos, incluidos los programas de sensibilización en materia de seguridad de las TIC y las actividades de formación sobre resiliencia operativa digital pertinentes, y las capacidades en materia de TIC para todo el personal;
- Aprobará y revisará periódicamente la **política** de la entidad financiera sobre los acuerdos relativos al uso de servicios de TIC prestados por **proveedores terceros** de servicios de TIC;
- Establecerá, a escala corporativa, **canales de comunicación** que le permitan estar debidamente informado de lo siguiente:
    - de los acuerdos celebrados con proveedores terceros de servicios de TIC sobre el uso de servicios de TIC,
    - de cualquier cambio sustancial pertinente previsto en relación con los proveedores terceros de servicios de TIC,
    - de las posibles repercusiones de tales cambios en las funciones esenciales o importantes reguladas por dichos acuerdos, incluido un resumen del análisis de riesgos para evaluar las repercusiones de dichos cambios, y al menos de los incidentes graves relacionados con las TIC y sus repercusiones, así como de las medidas de respuesta, recuperación y corrección.

Adicionalmente, las entidades contarán con un **marco de gestión del riesgo relacionado con las TIC** sólido, completo y bien documentado como parte de su sistema global de

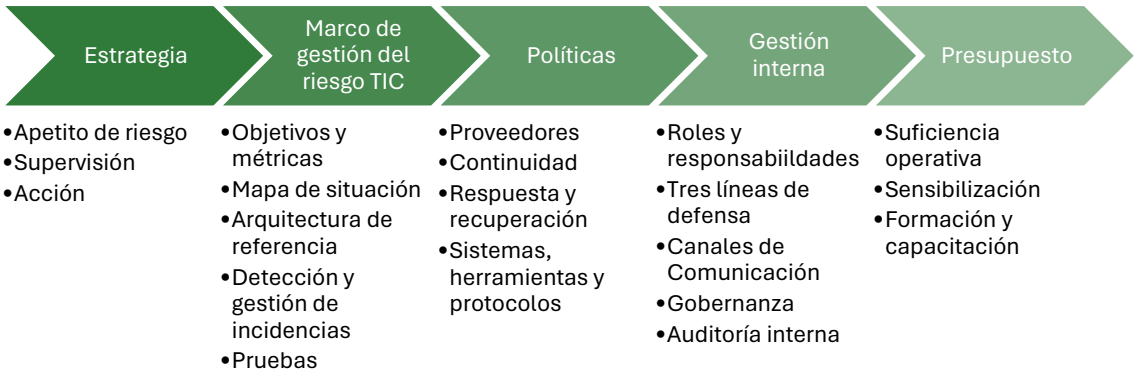
gestión de riesgos, que les permita hacer frente al riesgo relacionado con las TIC de forma rápida, eficiente y exhaustiva y asegurar un alto nivel de resiliencia operativa digital.

Este marco **se documentará y revisará al menos una vez al año**, incluirá al menos las estrategias, las políticas, los procedimientos, y los protocolos y herramientas de TIC que sean necesarios para proteger debida y adecuadamente todos los activos de información y activos de TIC, y **será auditado internamente** de forma regular dentro del plan de auditoría, incluyendo las mejoras y deficiencias identificadas en las sucesivas revisiones.

Recordemos que el marco global de gestión de riesgos es una de las principales responsabilidades del Consejo. Dicho marco incluirá una estrategia de resiliencia operativa digital que establezca cómo se aplicará el marco. A tal fin, la estrategia de resiliencia operativa digital incluirá métodos para hacer frente al riesgo relacionado con las TIC y alcanzar los objetivos específicos en materia de TIC, para lo cual:

- Explicará cómo apoya el marco de gestión del riesgo relacionado con las TIC la estrategia y los objetivos empresariales de la entidad financiera;
- Establecerá el **nivel de tolerancia al riesgo (apetito de riesgo)** relacionado con las TIC, de acuerdo con la propensión al riesgo de la entidad financiera, y analizará la tolerancia al impacto de las perturbaciones de las TIC;
- Establecerá **objetivos claros** en materia de seguridad de la información, incluidos indicadores clave de rendimiento y parámetros clave de medición del riesgo;
- Explicará la **arquitectura de referencia** de TIC y cualquier cambio necesario para alcanzar objetivos empresariales específicos;
- Esbozará los diferentes mecanismos establecidos para **detectar incidentes** relacionados con las TIC, prevenir su impacto y protegerse de sus efectos;
- Hará constar la **situación actual** de la resiliencia operativa digital sobre la base del número de incidentes graves relacionados con las TIC notificados y la eficacia de las medidas preventivas;
- Efectuará **pruebas de resiliencia** operativa digital;
- Esbozará una **estrategia de comunicación** en caso de aquellos incidentes relacionados con las TIC que sea obligatorio divulgar.

De forma esquemática, las obligaciones generales del Consejo quedarían enmarcadas en el siguiente esquema:



Otras obligaciones relevantes para el Consejo

Adicionalmente, los miembros del órgano de dirección mantendrán al día de manera activa los conocimientos y capacidades suficientes para comprender y evaluar el riesgo relacionado con las TIC y sus repercusiones en las operaciones de la entidad financiera, también siguiendo periódicamente una **formación específica** que sea acorde al riesgo relacionado con las TIC que se esté gestionando.

Aplicación simplificada

El reglamento permite una gestión simplificada para determinado tipo de entidades, como las empresas de servicios de inversión pequeñas y no interconectadas, las entidades de pago exentas en virtud de la Directiva (UE) 2015/2366, las entidades de dinero electrónico exentas en virtud de la Directiva 2009/110/CE; o los fondos de pensiones de empleo pequeños.

Elementos complementarios del reglamento

El reglamento desarrolla adicionalmente cuatro piezas relevantes para reforzar el marco de resiliencia digital:

- La gestión, clasificación y notificación de incidentes relacionados con las TIC.
- Las pruebas de resiliencia operativa digital.
- La gestión del riesgo relacionado con las TIC derivado de terceros.
- Los acuerdos de intercambio de información entre entidades.

Por otro lado, determinadas obligaciones requieren el desarrollo de normas técnicas de armonización que, en estos momentos, todavía están en desarrollo por parte de las autoridades competentes.

Dichas normas incluyen:

- Normas técnicas de regulación (RTS) sobre el **marco de gestión del riesgo de las TIC** y sobre el marco simplificado de gestión del riesgo de las TIC[8], que incluye detalles complementarios sobre los instrumentos, métodos, procesos y políticas necesarios, así como desarrolla el marco simplificado.
- RTS sobre **criterios para la clasificación de incidentes** relacionados con las TIC[9], que desarrolla criterios y umbrales para determinar la importancia relativa de los incidentes graves y amenazas significativas, así como los detalles de los datos a compartir de determinados incidentes.
- RTS para especificar la política sobre los servicios de TIC que respaldan **funciones críticas o importantes prestadas por proveedores terceros** de servicios de TIC

[8] Disponible en https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/operational-resilience/regulatory-technical-0, adoptado por la EBA y pendiente de aprobación por la Comisión.
[9] Disponible en https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/operational-resilience/regulatory-technical, adoptado por la EBA y pendiente de aprobación por la Comisión.

(TPP)[10], que especifican partes de los acuerdos de gobernanza, la gestión de riesgos y el marco de control interno que las entidades financieras deben tener en vigor en relación con el uso de proveedores terceros de servicios de TIC.

- Las Normas Técnicas de Implementación (ITS) para establecer las plantillas para el **registro de información de acuerdos con terceros**.
- RTS[11] conjunta que especifican los elementos relacionados con las **pruebas de penetración basadas en amenazas.**
- RTS conjunta sobre **notificación de incidentes graves**.
- RTS conjunta sobre la **subcontratación de servicios de TIC que apoyan funciones esenciales** o importantes.

Conexiones adicionales (NIS 2)

Es importante recordar aquí el texto de la directiva (UE) 2022/2555 de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (NIS 2).

Este documento, aunque en formato de directiva y pendiente de su transposición (la fecha límite para ello, en teoría, es el 17 de octubre de 2024), establece algunas claves relevantes para entender la responsabilidad del Consejo en la materia.

El aspecto más relevante es que establece un principio general de responsabilidad del Consejo en materias de ciberseguridad, donde su rol debe ser necesariamente activo.

> *Será el mismo consejo de administración el directamente responsable del daño. Por ello, sí será de aplicación la "**culpa in vigilando**", a diferencia de la anterior directiva que eximía de posible responsabilidad a la empresa por el mero hecho de tener un plan de contingencia activado en caso de ciberataque.*
>
> *Carmen Segovia Blázquez, directora Ciberriesgos en Willis Towers Watson; y Pedro Fernández-Villamea Alemán, responsable Legal & Compliance Grupo Gees-Spain y asesor en Estrategia Corporativa.*
>
> *Cinco Días (19 enero 2023)*

Así, el artículo 21 de la directiva exige que los Estados miembros velen por que las entidades esenciales e importantes **tomen las medidas técnicas, operativas y de organización adecuadas y proporcionadas para gestionar los riesgos** que se planteen para la seguridad de los sistemas de redes y de información que utilizan dichas entidades en sus operaciones o en la prestación de sus servicios y prevenir o minimizar las repercusiones de los incidentes en los destinatarios de sus servicios y en otros servicios.

Además, dicha obligación **se hace extensible a la cadena de producción**, de forma que las entidades deben tener en cuenta las vulnerabilidades específicas de cada proveedor y

[10] Disponible en https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/operational-resilience/regulatory-technical-1, adoptado por la EBA y pendiente de aprobación por la Comisión.

[11] Las tres últimas RTS se encuentran en proceso de consulta y revisión previo a la versión final que se enviará a la Comisión el 17 de julio de 2024.

prestador de servicios directo y la calidad general de los productos y las prácticas en materia de ciberseguridad de sus proveedores y prestadores de servicios, incluidos sus procedimientos de desarrollo seguro.

De forma más específica y **referido al Consejo**, el artículo 20 señala que los órganos de dirección de las entidades esenciales e importantes **aprueben** las medidas para la gestión de riesgos de ciberseguridad adoptadas por dichas entidades para dar cumplimiento al artículo 21, **supervisen** su puesta en práctica **y respondan por el incumplimiento** por parte de las entidades de dicho artículo.

Por último, señalar el énfasis que pone la directiva en la **comunicación** y gestión inmediata de los incidentes graves de ciberseguridad y la necesidad de transparencia y colaboración en la materia.

Código de buen gobierno de la ciberseguridad

Como complemento, en España, el Foro Nacional de Ciberseguridad ha publicado en junio de 2023 un código de buen gobierno de la ciberseguridad[12]. Estructurado en principios y recomendaciones, sirve de guía general de actuación en la materia, destacando las siguientes cuestiones:

- El principio de proporcionalidad.
- La importancia del encaje de la ciberseguridad en la estrategia general.
- La necesidad de asignar responsabilidades y de establecer con claridad las diferentes líneas de defensa.
- La relevancia de las buenas prácticas y la ética.
- La transversalidad de la cuestión.
- La necesidad de asignar recursos adecuados.
- Foco en la gestión de incidencias y la resiliencia operativa.
- Necesidad de formar y concienciar.
- La actualización y mejora permanente.
- La importancia de la anticipación y el reporte periódico.
- El encaje con el plan de continuidad de negocio.
- La inclusión de este riesgo en el mapa de gestión de riesgos.

Reflexiones para el Consejo

Tanto de la normativa en vigor, como del creciente foco reputacional en torno a la resiliencia y ciberseguridad de las empresas, es necesario que el Consejo revise en detalle su aproximación al riesgo digital, para lo que proponemos una breve lista de cuestiones a valorar en cada organización:

- ☐ Dedicar tiempo en los consejos a la materia, incluyendo la puesta a disposición de mapas de riesgos e indicadores de control.
- ☐ Revisar la estructura de responsabilidades en la organización y asegurar la debida ubicación de las líneas de defensa.

[12] Disponible en http://cnmv.es/DocPortal/Ciberseguridad/CBG_Ciberseguridad.pdf

- ☐ Valorar y aprobar, en su caso, la propuesta de tolerancia al riesgo y el modelo de control necesario para no sobrepasar los umbrales establecidos.
- ☐ Reclamar informes de análisis de riesgos específicos.
- ☐ Solicitar que se desarrollen indicadores de control ácidos[13].
- ☐ Mantener reuniones con los directivos responsables de las áreas de seguridad, tecnología y control de riesgos que les permitan entender los riesgos más relevantes y las medidas de mitigación existentes.
- ☐ Seguir los planes y métricas sobre nivel de cultura de gestión de riesgos[14] en la organización.
- ☐ Ubicar en una comisión especializada (por ejemplo, la de riesgos) el análisis detallado de estos riesgos.
- ☐ Acometer planes de formación específicos en la materia.
- ☐ Asegurar la existencia de políticas de escalado claras y efectivas[15].
- ☐ Disponer de un plan detallado de comunicación y gestión de crisis ante eventos relevantes de ciberseguridad o fallos operativos significativos.
- ☐ Disponer de asesoramiento externo recurrente que les permita obtener una actualización del entorno y poder obtener acompañamiento puntual en determinados temas.
- ☐ Asegurar la documentación[16] y las pruebas de los diferentes planes de contingencia y recuperación. Ver *in situ* las pruebas en aspectos de especial criticidad y asegurar que se simulan escenarios suficientemente críticos.

[13] Existen ciertas medidas que pueden enmascarar problemas relevantes. Por ejemplo, es muy habitual hablar del porcentaje de disponibilidad de los sistemas, con porcentajes cercanos al 99,7% del tiempo en pleno funcionamiento. Sin embargo, ese diferencial supone 26 horas en el año de fallo del sistema. Por ejemplo, si nos referimos a una red de pagos, quizás sea más realista hablar del número de transacciones que no fue posible realizar. Una caída de unas pocas horas puede significar varios millones de transacciones que no pueden realizarse, dependiendo del día y el horario y con un impacto directo en las ventas de los clientes del sistema.

[14] La identificación de riesgos y su evaluación debe ser una tarea que nace desde la primera línea de defensa y debe existir una cultura de incentivación adecuada para ello.

[15] La tendencia natural de cualquier organización es a una relajación de estándares con el tiempo. La ausencia de incidentes percibidos genera una falsa sensación de seguridad.

[16] La documentación es una de las herramientas más poderosas para la identificación y gestión del riesgo, pero necesita un claro apoyo desde la Alta Dirección y el propio Consejo. Requiere atención y dedicación. Documentar es poner en un espejo como se hacen las cosas; al vernos reflejados enseguida nos damos cuenta si realmente queremos ser como se describe en el documento.

ETHALO

Ethics & Algorithms

Boosting a healthful data driven society

www.ethalo.es

info@ethalo.es