

DORA

Riesgos Tecnológicos y Ciberseguridad

- 
- 01 | Contexto y características
 - 02 | Principales aspectos y requerimientos
 - 03 | ¿Por qué *MS*?
 - A | Anexos

1. Contexto y características. Visión general

El Reglamento sobre Resiliencia Operativa Digital (DORA) vuelve a incidir en buena parte de los requerimientos establecidos en las Guías de la EBA (TIC y Outsourcing), añadiendo nuevos requisitos o reforzando algunos de los ya existentes



Contexto regulatorio

- Este Reglamento es parte del **Paquete de medidas de finanzas digitales** (orientada a impulsar el potencial de las finanzas digitales en términos de innovación y competencia) y **cubre múltiples aspectos de la gestión de TIC** (Disponibilidad y Continuidad, Gestión del Cambio, Seguridad, Externalización).
- Establece un **marco armonizado, detallado y exhaustivo sobre la resiliencia operativa digital** (hasta la fecha recogido de manera limitada en iniciativas nacionales o enfoques de supervisión como las guías EBA o NIS).

Aspectos diferenciales

- Amplía el **perímetro de supervisión a todas las entidades** del sector financiero (bancos, entidades de crédito, aseguradoras, entidades de pago...), así como a **los proveedores terceros de servicios de TIC** (p.e. servicios de nube).
- Establece las características principales de la **clasificación y notificación de incidentes TIC, así como armonizar su gestión en toda la Unión Europea con la creación de un centro al que deben ser notificados.**
- Requiere probar y evaluar todos **los sistemas y aplicaciones TIC críticas al menos una vez al año** (análisis vulnerabilidades, pruebas de rendimiento, etc.), así como realizar **pruebas avanzadas con base trianual** de las herramientas, los sistemas y los procesos de TIC críticos en base a amenazas realizadas **de manera independiente y gestionar las debilidades** encontradas, Todo ello **evaluado por el supervisor.**
- Refuerza la relevancia de la **gestión del riesgo de terceros** (registro de información sobre el uso de servicios TIC prestado por terceros, concentración, planes de continuidad y pruebas, estrategias de salida, etc.) extendiendo el perímetro a otros terceros más allá de lo considerado como *outsourcing* y a todo lo que sea crítico para la resiliencia operativa digital de la entidad.

Ámbitos de DORA

Perímetro y
Gobernanza TIC

Riesgos TIC

Reporte de
incidentes TIC

Intercambio de
información

Riesgos TIC de
terceros

Pruebas de
resiliencia

1. Contexto y características. Ámbitos de la regulación

DORA se divide en seis ámbitos, detallándose los principales impactos de los mismos a continuación

Perímetro y Gobernanza TIC

- Ampliación del **ámbito de aplicación** a cualquier entidad financiera, incluyendo los proveedores de servicios TIC.
- Responsabilidades del **Órgano de Administración** en la gestión de la resiliencia operativa.
- Identificación de un rol a cargo de la **monitorización de acuerdos con terceras partes** de los servicios TIC.

Pruebas de Resiliencia

- **Pruebas anuales** de todos los sistemas y aplicaciones críticos TIC (vulnerabilidades, análisis de código, rendimiento, capacidad,...).
- **Pruebas avanzadas** específicas de amenazas sobre funciones y servicios críticos, validadas por las autoridades supervisoras.
- Dedicación de **recursos** suficientes y garantía de que se evitan conflictos de interés (entre diseño y ejecución de pruebas).

Riesgos TIC de terceros

- Ampliación del **perímetro a todos los proveedores de alto riesgo** (no solo los considerados outsourcing en guías EBA).
- Desarrollo de un **registro de información** que contenga una visión completa de todos los terceros que presten servicios TIC.
- **Reporting** de los **cambios en el registro** al regulador anualmente
- Evaluación de los **riesgos de concentración TIC**.

Riesgos TIC

- Existencia de un **marco interno de gobernanza y control** de los riesgos TIC.
- Identificación y clasificación, según criticidad, de **funciones y activos** soporte TIC y sus interdependencias con terceros.
- Identificación continua de **fuentes de riesgo**.
- **Evaluación anual de riesgos** específicos en todos los sistemas TIC *legacy*.
- Desarrollo de **programas específicos de concienciación y formación** sobre la resiliencia digital.

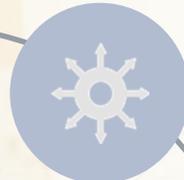
Reporte de incidentes TIC

- Mecanismo de **monitorización y seguimiento de incidentes** hasta erradicar las causas subyacentes.
- Criterios específicos para la **clasificación de incidentes**.
- Ampliación del perímetro de notificación a los **incidentes operativos o relacionados con los pagos**.

Intercambio de información

- Para aumentar la concienciación sobre los riesgos TIC, minimizar su propagación, apoyar las capacidades defensivas de las entidades financieras y sus técnicas de detección de amenazas, la regulación incide en **acuerdos para intercambiar información sobre ciberamenazas**.

Digital Operational Resilience Act (DORA)



2 . Principales aspectos y requerimientos (1/3)

Dora extiende el ámbito de aplicación de los requerimientos sobre resiliencia digital, refuerza los requerimientos de evaluación de riesgos e introduce la necesidad de llevar a cabo un *business impact analysis* (BIA). Otras novedades incluyen:...

Ámbito	Subámbito	Principales aspectos y requerimientos
 <p>Perímetro y Gobernanza TIC</p>	Ámbito de aplicación	<ul style="list-style-type: none"> Extienden el ámbito de aplicación del Reglamento respecto a las Guías de la EBA a prácticamente cualquier entidad financiera (entidades de crédito, aseguradoras, entidades de pago...), incluyendo proveedores de servicios TIC (p.e. servicios de nube).
	Gobernanza y organización	<ul style="list-style-type: none"> Establece las responsabilidades del Órgano de Dirección, exigiendo que deba definir, aprobar, supervisar y responsabilizarse de la implantación de las políticas y procedimientos para la gestión de la resiliencia operativa. Exige la identificación de un rol o figura encargado de monitorizar los acuerdos con proveedores terceros de servicios de TIC. Demanda la asignación de recursos adecuados para satisfacer las necesidades de resiliencia operativa.
 <p>Riesgos TIC (1/2)</p>	Marco de gestión del riesgo TIC	<ul style="list-style-type: none"> Exige la existencia de un marco interno de gobernanza y control de los riesgos de las TIC. El Órgano de Dirección será responsable de la gestión del marco de control y su revisión será al menos anual. Exige un modelo organizacional basado en el esquema de las tres líneas de defensa (123LoD).
	Identificación	<ul style="list-style-type: none"> Demanda la identificación, clasificación y documentación de las funciones relacionadas con TIC, los activos de información que respalden dichas funciones, las configuraciones de los sistemas e interconexiones con sistemas internos y externos y revisar (al menos una vez al año) la idoneidad de la clasificación de los activos y documentación pertinente, así como la identificación continua de fuentes de riesgo (ciberamenazas y vulnerabilidades). Todos los activos de información y los activos de TIC se identificarán y clasificarán según su criticidad, incluidos los de los sitios remotos, los recursos de red y los equipos de hardware. Hace necesario realizar una evaluación específica de los riesgos en todos los sistemas TIC <i>legacy</i> en uso al menos una vez al año y especialmente antes y después de conectar tecnologías, aplicaciones o sistemas antiguos y nuevos.
	Protección y prevención	<ul style="list-style-type: none"> Establece el desarrollo de procedimientos que limiten el acceso físico y virtual a los recursos y datos del sistema a lo estrictamente necesario, una gestión sólida de la red y de la infraestructura, una correcta gestión del parchado de los sistemas, mecanismos de autenticación fuertes, etc.
	Detección	<ul style="list-style-type: none"> Demanda la necesidad de establecer mecanismos para detectar rápidamente las actividades anómalas, incluidos los problemas de rendimiento de la red de TIC y otros incidentes relacionados con las TIC.
	Respuesta y recuperación	<ul style="list-style-type: none"> Mención específica a llevar a cabo un Business Impact Analysis (BIA) de las exposiciones a interrupciones severas del negocio en términos de continuidad para evaluar su impacto potencial mediante criterios cuantitativos y cualitativos, utilizando datos internos y externos y análisis de escenarios, según sea apropiado. Realización pruebas anuales relativas a Planes de Continuidad, Disaster Recovery, incluyendo a terceros que deban involucrarse en las mismas.

2 . Principales aspectos y requerimientos (2/3)

...incorporación de los terceros en los programas de formación internos, perímetro ampliado de reporte de incidentes operativos o de seguridad de pagos y notificación voluntaria de ciberamenazas relevantes, promoción del intercambio de información,...

Ámbito	Subámbito	Principales aspectos y requerimientos
 Riesgos TIC (2/2)	Backups	<ul style="list-style-type: none"> En cuanto a las políticas y procedimientos de copia de seguridad y procedimientos y métodos de restauración y recuperación, las entidades deberán, además, mantener los recursos adecuados y disponer de instalaciones de copia de seguridad y restauración para ofrecer y mantener su servicio en todo momento.
	Aprendizaje y evolución	<ul style="list-style-type: none"> Exige el desarrollo de programas específicos de concienciación y formación sobre resiliencia digital (personal y directivos), debiendo incluirse a los terceros proveedores de servicios TIC en los programas de formación pertinentes.
	Comunicación	<ul style="list-style-type: none"> Requiere una estrategia de comunicación de crisis a clientes, supervisores y sociedad en su conjunto con funciones y responsabilidades claras y obligatoriedad de programas de concienciación y formación sobre resiliencia digital. Establece la necesidad de informar a las autoridades competentes de todos los costes y pérdidas causados por las interrupciones e incidentes TIC.
 Reporte de incidentes TIC	Proceso de gestión de incidentes	<ul style="list-style-type: none"> Exige el establecimiento de mecanismos de monitorización y seguimiento de incidentes hasta la erradicación de las causas subyacentes. Amplía el perímetro al reporte de los incidentes operativos o de seguridad relacionados con los pagos.
	Clasificación de incidentes TIC	<ul style="list-style-type: none"> Establece criterios específicos para la clasificación de incidentes (número de usuarios o contrapartes afectados, la duración, la extensión geográfica, las pérdidas de datos, la gravedad del impacto, la criticidad de los sistemas afectados y el impacto económico de la interrupción).
	Notificación de incidentes graves TIC y respuesta de la autoridad de supervisión	<ul style="list-style-type: none"> Los incidentes importantes relacionados con las TIC deben notificarse a un nuevo centro creado por la UE para este fin, utilizando un procedimiento armonizado y una plantilla común. Además, deberá ampliarse esta información con una notificación voluntaria de las ciberamenazas relevantes. El feedback de los supervisores después de un informe sobre un incidente relevante debe evaluarse y proporcionará orientaciones a la entidad financiera, en particular para discutir las soluciones a nivel de la entidad o las formas de minimizar el impacto adverso en todos los sectores.
 Intercambio de información	Intercambio de información sobre ciberamenazas	<ul style="list-style-type: none"> Para aumentar la concienciación sobre el riesgo de las TIC, minimizar su propagación, apoyar las capacidades defensivas de las entidades financieras y las técnicas de detección de amenazas, el reglamento permite y promueve que las entidades financieras establezcan acuerdos para intercambiar entre ellas información e inteligencia sobre ciberamenazas.

2 . Principales aspectos y requerimientos (3/3)

... intensificación de requerimientos de ejecución de pruebas normales y avanzadas, deber de identificar las interconexiones con los proveedores que apoyan funciones críticas o importantes, así como de evaluar el riesgo de concentración de las TIC

Ámbito	Subámbito	Principales aspectos y requerimientos
 <p>Pruebas de resiliencia</p>	<p>Pruebas normales</p>	<ul style="list-style-type: none"> • Demanda la ejecución una gama completa de pruebas de resiliencia operativa digital basadas en el riesgo y procedimentadas (<i>pentesting</i>, análisis de código, rendimiento, capacidad, etc.) de los sistemas y aplicaciones críticos TIC al menos una vez al año por partes independientes y remediar los problemas de manera prioritaria. • Dedicar recursos suficientes y asegurarse de que se evitan los conflictos de intereses a lo largo de las fases de diseño y ejecución de las pruebas si éstas son realizadas por testadores internos.
	<p>Pruebas avanzadas</p>	<ul style="list-style-type: none"> • Exige llevar a cabo pruebas específicas avanzadas guiadas por amenazas sobre funciones y servicios críticos (TLTP), incluyendo a terceros y cada 3 años,. Las autoridades competentes validarán la documentación y emitirán un certificado. • Teniendo en cuenta que la frecuencia estándar es cada 3 años para las pruebas avanzadas, la autoridad competente podrá, en caso necesario, solicitar a la entidad financiera que reduzca o amplíe esta frecuencia en función de su perfil de riesgo. • Las entidades financieras clasificadas como significativas sólo podrán utilizar testadores externos. • El marco de referencia para las pruebas avanzadas será desarrollado por las ESAs en colaboración con el ECB, de acuerdo con el marco TIBER-EU.
 <p>Riesgos TIC de terceros</p>	<p>Gestión del Riesgo TIC de terceros</p>	<ul style="list-style-type: none"> • Amplía el perímetro de aplicación a todo proveedor que presente riesgo alto (no solo outsourcing). • Requiere elaborar un registro de información que contenga la visión completa de todos sus proveedores de TIC, los servicios que prestan y las funciones que respaldan. Este registro presenta un reto particular para las grandes entidades con un elevado número de proveedores. • Exige informar cambios en registro al regulador una vez al año. • Establece directrices sobre el contenido de los contratos y las razones para su rescisión (vinculada a un riesgo o prueba de incumplimiento). • Las autoridades competentes podrán exigir que se suspendan temporalmente, de forma parcial o total, el uso o despliegue de un servicio prestado por un tercero proveedor de servicios TIC crítico hasta que se hayan abordado los riesgos identificados en las recomendaciones dirigidas a proveedores terceros de estas características. • Deben identificarse las interconexiones con los proveedores terceros de servicios TIC que apoyan funciones críticas o importantes.
	<p>Proveedores y cadena de subcontratación</p>	<ul style="list-style-type: none"> • Exige una evaluación del riesgo de concentración de las TIC teniendo en cuenta si la celebración de un acuerdo contractual en relación con los servicios TIC que apoyan funciones críticas o importantes daría lugar a alguna de las siguientes situaciones: a) la contratación de un tercero proveedor de servicios TIC que no sea fácilmente sustituible; o b) la celebración de múltiples acuerdos contractuales en relación con la prestación de servicios TIC que apoyen funciones críticas o importantes con el mismo tercer proveedor de servicios TIC o con proveedores terceros de servicios TIC estrechamente vinculados. En este sentido, las cadenas de suministro largas o complejas deben considerarse durante dicha evaluación.

3. ¿Por qué *MS*? Valores diferenciales

Management Solutions posee un conocimiento multisectorial y profundo de los principales *stakeholders*, así como fuertes capacidades para alcanzar resultados prácticos de manera ágil...

Experiencia en Resiliencia Operativa Digital (*DORA*)

- Proyectos de **diagnóstico** del nivel de adecuación de diferentes entidades respecto a exigencias regulatorias marcados por *DORA*
- **Conocimiento normativo** para dar entendimiento a los distintos *stakeholders* de la organización (internos y externos) sobre **Resiliencia Operativa Digital**
- **Conocimiento detallado** de la normativa y análisis de las novedades de la publicación final del documento previo a su aprobación
- **Detección de *gaps* y establecimiento de líneas de mejora** para cumplir con las exigencias de la regulación y elaboración de planes directores
- **Establecimiento de *PMOs* para asegurar** la correcta implementación de planes directores sobre la adecuación a *DORA*
- **Acompañamiento** en procesos de **inspección de supervisores** en materia de **Ciberresiliencia** (compilación del cuestionario *CROE*, recopilación de evidencias, etc.)

Experiencia contrastada en proyectos de Riesgo Tecnológico y relacionados

- **Consultor de referencia en la implementación del modelos de riesgos y controles** (*Info&Data Sec., Physical Sec., Third Party, Technology, Data Mgmt., Processes, Finance, People...*)
- **Análisis de metodologías y frameworks** (*COBIT, ICT, NIST, ITIL, SANS...*) identificación de líneas de mejora y definición de marcos de control adaptados a ellos
- **Dilatada experiencia en proyectos de adecuación normativa, evolución y evaluación de modelos compliance**
- **Apoyando a organizaciones en su revisión de procesos, intervinientes, sistemas, etc. donde se localizan los principales focos de riesgos**
- **Profundo conocimiento de las áreas de TI, plataforma tecnológica (*legacy y next gen*) y proyectos activos** en los principales ámbitos de actuación

Perfiles alto valor, *expertise* y visión *cross*

- Profesionales con grandes capacidades de comprensión, comunicación, *challenge/asesoramiento* de alto valor, *expertise* en *Outsourcing* y Riesgos Tecnológicos, y su relación con la gestión de riesgos y procesos (*visión cross*)
- Entendimiento de los procesos de negocio, conocimiento de metodologías de gestión de riesgos y con capacidades analíticas
- **Conocimiento detallado normativas y mejores prácticas del mercado**

Firma de referencia, con capacidades globales

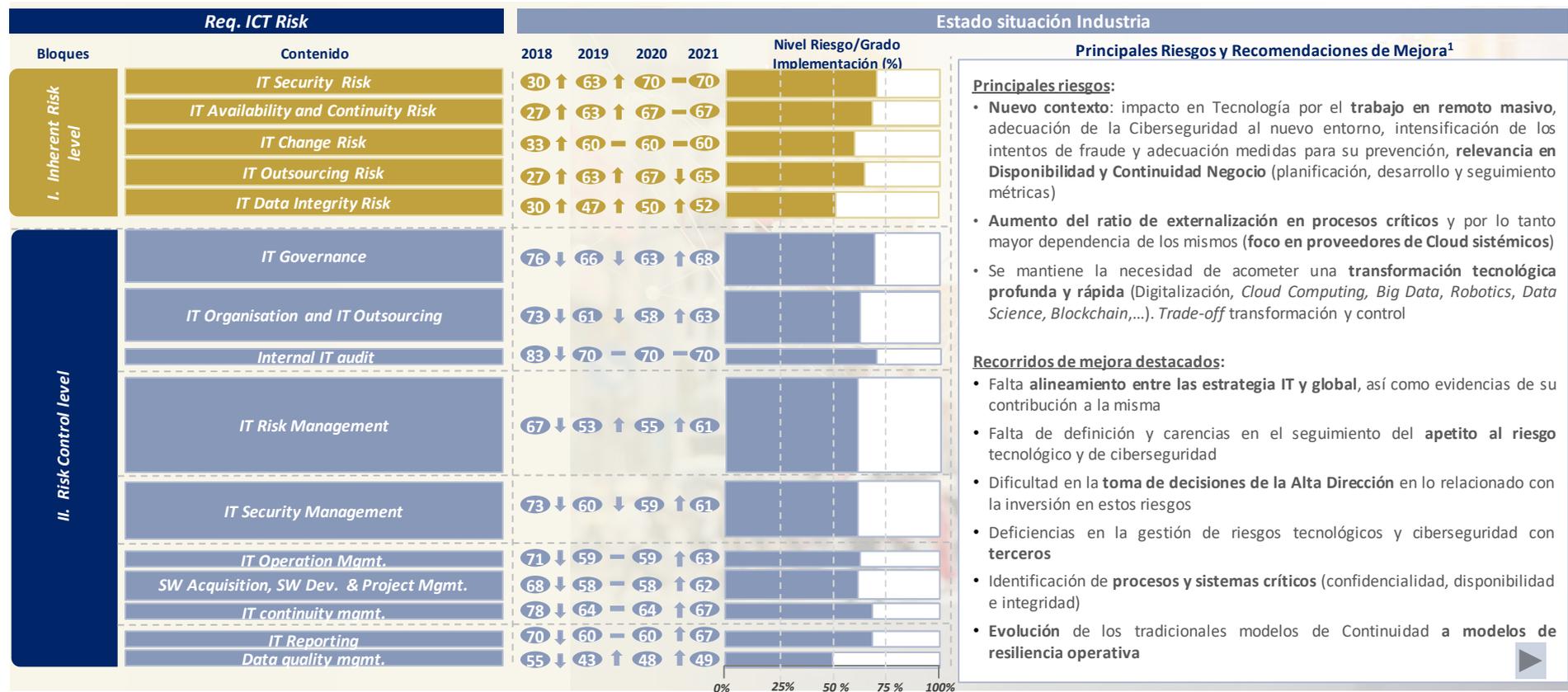
- **Firma global, independiente e internacional** (+40 países), con profundo conocimiento de los negocios en los que operan nuestros clientes (+1.500 globales y locales) seleccionando los recursos más apropiados para cada proyecto, independientemente de donde estén ubicados
- **Equipo multidisciplinar** con fuertes capacidades analíticas y conocimiento especialista. Organizados de forma matricial (cliente, industria, competencia y geografía)
- Consultor acreditado por **supervisores y organismos supranacionales**
- **Una fuerte cultura corporativa:** compromiso, vocación de servicio y búsqueda constante de la excelencia
- **Una trayectoria que nos avala:** probada capacidad de entrega, que se ha sustanciado en un importante crecimiento orgánico (x38 en 20 años)
- Capacidad de **benchmark** (presencia en clientes *Top* en TI en todas las geografías)

Acceso a criterios reguladores y supervisores

- Acompañamos a los **supervisores en sus inspecciones *on-site*** en organizaciones
- **Apoyamos directamente a las organizaciones en la superación de los procesos de supervisión *on-site*, auditoría interna y externa**, en materia de riesgos *TIC*
- **Oficina en Frankfurt como *Hub* de análisis normativo y de relación con el regulador** para contrastar aspectos regulatorios, dudas y anticipar requerimientos

Anexo. Retos para la gestión de Riesgos Tecnológicos y Ciberseguridad

Las organizaciones están evolucionando sus marcos de gestión de Riesgos Tecnológicos y Ciberseguridad, también promovidas por el refuerzo del marco supervisor, si bien todavía se identifican una serie de debilidades y recorridos de mejora





**International
One Firm**



**Multiscope
Team**



**Best Practice
Know-How**



**Proven
Experience**



**Maximum
Commitment**



Jorge Monge Alonso

Socio en Management Solutions

jorge.monge.alonso@managementsolutions.com

Alejandro Iglesias Rodríguez

Socio en Management Solutions

alejandro.iglesias@msspain.com