El *Reglamento (UE) 2022/2554* del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero -DORA-, establece, entre otros, los **requisitos y obligaciones** aplicables a las ESI (en calidad de entidad financiera) en relación con: **(a)** gestión del riesgo relacionado con las tecnologías de la información y la comunicación (TIC), con el fin de proteger, detectar, contener, recuperar y reparar incidentes relacionados con las TIC; **(b)** notificación obligatoria a la autoridad competente de incidentes graves relacionados con las TIC y, con carácter voluntario, de ciberamenazas importantes; **(c)** las pruebas de resiliencia operativa digital; **(d)** el intercambio de información e inteligencia acerca de las ciberamenazas y las vulnerabilidades cibernéticas; y **(e)** las medidas para una adecuada gestión del riesgo relacionado con las TIC derivado de terceros (subcontratación).

## Tipología de ESI a efectos de aplicación de DORA

Teniendo en cuenta el principio de proporcionalidad establecido en el *artículo 4 de DORA* señale el **tipo de ESI** a constituir -*márquese solo 1 de las 3 opciones siguientes y elimine el resto*-:

ESI tipo **A** -SV- o **B** -SV/AV- (*ver contestación a pregunta 2) apartado 1. del capítulo 2 del Manual de autorización de ESI*) considerada **microempresa** (*conforme a la definición del número 61) del artículo 3 de DORA*).

*Si señala esta opción debe cumplimentar el apartado 2 del formulario y eliminar los apartados 3 y 4*

ESI tipo **A** -SV- o **B** -SV/AV- (*ver contestación a pregunta 2) apartado 1. del capítulo 2 del Manual de autorización de ESI*) **no** considerada **microempresa** (*conforme a la definición del número 61) del artículo 3 de DORA*).

*Si señala esta opción debe cumplimentar el apartado 3 del formulario y eliminar los apartados 2 y 4*

ESI tipo **C** -SV/AV/SGC/EAF- (*ver contestación a pregunta 2) apartado 1. del capítulo 2 del Manual de autorización de ESI*).

*Si señala esta opción debe cumplimentar el apartado 4 del formulario y eliminar los apartados 2 y 3*

## Mecanismos y sistemas previstos en materia de gestión de ciberseguridad de ESI tipo A o B que sean microempresas

#### **2.1. Mecanismos y sistemas previstos en materia de gestión y gobernanza de riesgos las TIC**

1. El solicitante de autorización **manifiesta** que:

 La ESI dispondrá de un marco interno de gobernanza y control que garantice una gestión efectiva y prudente del riesgo relacionado con las tecnologías de la información y la comunicación (TIC).

A tal efecto, de conformidad con el modelo interno de gestión y control de riesgos de la ESI, esta garantizará una separación e independencia adecuadas de las personas responsables de la gestión del riesgo relacionado con las TIC y las responsables de las funciones de control y de auditoría interna.

 La ESI contará con un marco de gestión de riesgo relacionado con las TIC - entendido como el conjunto de 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, incluidos el *software*, el *hardware* y los servidores, así como para proteger todos los componentes e infraestructuras físicos pertinentes, como locales, centros de datos y zonas sensibles designadas, a fin de garantizar que todos los activos de información y activos de TIC estén adecuadamente protegidos de los riesgos, incluidos los daños y el acceso o uso no autorizado – sólido, completo y bien documentado, basado en el despliegue de estrategias, políticas, procedimientos, protocolos y herramientas de TIC adecuados (que cumplirán con lo dispuesto al efecto en el *artículo 7 de DORA*), que le permita hacer frente al riesgo relacionado con las TIC de forma rápida, eficiente y exhaustiva y asegurar un alto nivel de resiliencia operativa digital.

 El marco de gestión de riesgo relacionado con las TIC de la ESI cumplirá con lo establecido en el *Reglamento Delegado (UE) 2024/1774 de la Comisión, de 13 de marzo de 2024*, por el que se completa el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo en lo que respecta a las normas técnicas de regulación que especifican las herramientas, métodos, procesos y políticas de gestión del riesgo relacionado con las TIC y el marco simplificado de gestión del riesgo relacionado con las TIC.

 El marco de gestión de riesgo relacionado con las TIC de la ESI incluirá una estrategia de resiliencia operativa digital que, a efectos de establecer cómo se aplica el marco, incluirá métodos para hacer frente al riesgo relacionado con las TIC y alcanzar los objetivos específicos de la ESI en materia de TIC, para lo cual contendrá la información especificada en las *letras a) a h) del artículo 6.8. de DORA*.

 Como parte del marco de gestión de riesgo relacionado con las TIC, la ESI elaborará y documentará una política de seguridad de la información que defina las normas para proteger al confidencialidad, disponibilidad, integridad o autenticidad de los datos, activos de información y activos TIC, aplicando las medidas, protocolos, procedimientos y controles establecidos en el *artículo 9.4. de DORA*.

 La ESI dispondrá de capacidades y personal para recopilar información sobre vulnerabilidades, ciberamenazas e incidentes relacionados con las TIC -en particular ciberataques-, analizar las posibles repercusiones en su resiliencia operativa digital, identificando sus causas y las mejoras necesarias para las operaciones de TIC o en la política de continuidad de la actividad en materia de TIC (*artículo 13 de DORA*).

 La ESI desarrollará programas de sensibilización en materia de seguridad de las TIC y formación sobre resiliencia operativa digital, módulos que serán obligatorios en los programas de formación de personal que la ESI desarrolle.

 El órgano de administración de la ESI, será responsable de definir, aprobar, aplicar y supervisar todas las disposiciones relacionadas con el marco de gestión del riesgo relacionado con las TIC asumiendo, a tal efecto, las funciones y responsabilidades desarrolladas en las *letras a)* a *i) del artículo 5.2. de DORA*.

 La ESI documentará y revisará el marco de gestión de riesgos relacionado con las TIC periódicamente, así como cuando se produzcan incidentes graves relacionados con las TIC, en base a las instrucciones de supervisión o conclusiones derivadas de los procesos de prueba o auditoría de la resiliencia operativa digital.

 La ESI proporcionará a la CNMV, previa petición de esta, información completa y actualizada sobre el riesgo relacionado con las TIC y sobre su marco de gestión de dicho riesgo, así como sobre la revisión periódica que realice del mismo.

1. En el contexto de la estrategia de resiliencia operativa digital que, de conformidad con lo dispuesto en el *artículo 6.8. de DORA*, debe elaborar la ESI, ¿tiene previsto definir una estrategia global multiproveedor en materia de TIC a nivel de grupo o de la ESI?

NO

SI  Detalle

|  |
| --- |
| Insertar información, *detallando posibles dependencias clave de los proveedores terceros de servicios TIC y explicando los motivos subyacentes a la contratación de una combinación de proveedores terceros de servicios TIC* . |

1. ¿Tiene previsto externalizar, en un tercero o en una empresa del grupo, las tareas de verificación del cumplimiento de los requisitos de gestión del riesgo relacionado con las TIC?

NO

SI  Detalle

|  |
| --- |
| Insertar |

1. En relación con el marco de gestión del riesgo relacionado con las TIC que establecerá la ESI:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Identifique:  |  | | --- | | Funciones, cometidos, responsabilidades y áreas de negocio, cuyos procesos están sustentados por las TIC: Insertar | | Activos de información y activos TIC (incluidos los que se encuentren en emplazamientos remotos, recursos de red y equipos de *hardware*) que sustentan dichos procesos: Insertar | | Vínculos e interdependencias entre activos TIC: Insertar | | Procesos que dependan de proveedores terceros de servicios de TIC e interconexiones con proveedores terceros de servicios de TIC que sustenten funciones esenciales o importantes: Insertar |  1. Detalle los criterios de clasificación de los incidentes relacionados con las TIC y las ciberamenazas, (*artículo 18 de DORA*):  |  | | --- | | Insertar *teniendo en cuenta lo dispuesto al efecto en el Reglamento Delegado (UE) 2024/1772: acerca del conjunto de criterios que deben seguir las entidades a la hora de clasificar los incidentes TIC y las ciberamenazas importantes, siguiendo un enfoque basado en el riesgo.* |  1. Informe brevemente de las principales características del modelo (interno o basado en tres líneas de defensa -1ª encargada de la gestión operativa del riesgo; 2ª encargada del control del riesgo y; 3ª la auditoría interna-) que utilizará la ESI para la gestión y control de su riesgo relacionado con las TIC. En particular, aporte información sobre:  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | 1. Las políticas, protocolos, procedimientos y herramientas en materia de seguridad de las TIC que utilizará la ESI al objeto de asegurar la resiliencia, continuidad y disponibilidad de los sistemas TIC (en particular aquellos que sustentan funciones esenciales), así como de mantener elevados niveles de disponibilidad, autenticidad, integridad y confidencialidad de datos (*artículo 9 de DORA*)  |  | | --- | | Insertar |  1. Los mecanismos de detección que tendrá la ESI de actividades anómalas (*artículo 17.3. de DORA*) -incluidos los problemas de rendimiento de las redes de TIC y los incidentes con las TIC (ciberataques), criterios y umbrales de alerta para activar e iniciar procesos de respuesta a incidentes relacionados con las TIC, así como periodicidad de su revisión (*artículo 10 de DORA*)  |  | | --- | | Insertar |  1. Los planes de respuesta y recuperación en materia de TIC, incluyendo planes de prueba, informando sobre la periodicidad de revisión de dichos planes (al menos una vez al año, así como cada vez que se produzca un cambio sustancial en los sistemas TIC que sustenten funciones esenciales o importantes) y de las pruebas. (*artículo 11, apartados 3 y 6 de DORA*)  |  | | --- | | Insertar |  1. La política de continuidad de la actividad en materia de TIC, incluidos planes de prueba, en especial en lo referente a funciones esenciales externalizadas o contratadas con proveedores terceros de servicios TIC, así como el análisis del impacto en el negocio de la ESI de sus exposiciones a perturbaciones graves -teniendo en cuenta criterios cuantitativos y cualitativos-, incluyendo información sobre la periodicidad de revisión de dichos planes (al menos una vez al año, así como cada vez que se produzca un cambio sustancial en los sistemas TIC que sustenten funciones esenciales o importantes) y de las pruebas (*artículo 11, apartados 1, 2,4 ,5 y 6 de DORA*)  |  | | --- | | Insertar |  1. Las políticas y procedimientos de respaldo, así como los procedimientos y métodos de restablecimiento y recuperación, incluidas la realización de pruebas periódicas sobre dichas políticas y procedimientos (*artículo 12 de DORA*) -incluyendo información sobre si la ESI, sobre la base de su perfil de riesgo, mantendrá capacidades de TIC redundantes dotadas de recursos, medios y funciones adecuados para satisfacer las necesidades asociadas a su negocio:  |  | | --- | | Insertar |  1. Los planes previstos en la ESI relativos a la comunicación de crisis, al objeto de una adecuada divulgación, al menos, de los incidentes graves relacionados con las TIC o las vulnerabilidades importantes a clientes y contrapartes (*artículos 14 y 17.3., letras d) y e) de DORA*)  |  | | --- | | Insertar | | |

#### **2.2. Notificación de incidentes relacionados con las TIC**

1. El solicitante de autorización **manifiesta** que:

 La ESI notificará a la CNMV los incidentes graves relacionados con las TIC, a través de una notificación inicial, un informe intermedio posterior y un informe final, en la forma y plazos establecidos en el *artículo 19.4. de DORA*, así como en el *Reglamento Delegado (UE) 2025/301 de la Comisión, de 23 de octubre de 2024*, por el que se completa el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo en lo que respecta a *las normas técnicas de regulación que especifican el contenido y los plazos para la notificación inicial y los informes intermedio y final sobre incidentes graves relacionados con las TIC, así como el contenido de la notificación voluntaria de ciberamenazas importantes*, utilizando los formularios, plantillas y procedimientos normalizados establecidos al efecto en el *Reglamento de Ejecución (UE) 2025/302 de la Comisión, de 23 de octubre de 2024*.

1. ¿Tiene intención la ESI de notificar a la CNMV aquellas ciberamenazas que sean importantes, por el impacto que puedan tener para el sistema financiero, los usuarios del servicio o los clientes?

NO

SI   El solicitante de autorización **manifiesta** que la notificación que la ESI remitirá a la CNMV contendrá la información exigida por el [*Reglamento Delegado (UE) 2025/301*](https://www.boe.es/doue/2025/301/L00001-00005.pdf) y se realizará utilizando los formularios, las plantillas y los procedimientos establecidos al efecto en el [*Reglamento de Ejecución (UE) 2025/302*](https://www.boe.es/doue/2025/302/L00001-00044.pdf):

SI

1. ¿Está previsto que la ESI externalice en un proveedor tercero de servicios sus obligaciones de informar a la CNMV de los incidentes graves relacionados con las TIC, así como, en su caso, de las ciberamenazas importantes?

NO

SI   Detalle:

|  |
| --- |
| Insertar |

#### **2.3. Pruebas de resiliencia operativa digital y acuerdos de intercambio de ciber amenazas**

1. El solicitante de autorización **manifiesta** que:

 La ESI realizará las pruebas periódicas de resiliencia operativa digital contempladas en el *artículo 25.1. de DORA* mediante la combinación de un enfoque basado en el riesgo con una planificación estratégica de las pruebas de TIC, teniendo debidamente en cuenta la necesidad de mantener un planteamiento equilibrado entre la dimensión de los recursos y el tiempo que se asigne a las pruebas de TIC previstas, por una parte, y la urgencia, el tipo de riesgo, el carácter esencial de los activos de información y de los servicios prestados, así como cualquier otro factor pertinente, incluida la capacidad de la ESI para asumir riesgos calculados, por otra.

1. ¿Tiene la ESI previsto intercambiar con otras entidades financieras información e inteligencia sobre ciberamenazas, en la medida que dicho intercambio de información e inteligencia cumple las condiciones establecidas en el *artículo 45.1. de DORA*?

NO

SI   Detalle:

|  |
| --- |
| Insertar |

#### **2.4. Gestión de riesgos de terceros (proveedores de servicios de TIC)**

1. ¿Está prevista la externalización por la ESI de servicios TIC (atendiendo a las definiciones establecidas al efecto en los *considerandos (35) y (63) de DORA*) en proveedores terceros de servicios TIC?

NO

SI   El solicitante de autorización **manifiesta** que:

 Como parte de su marco de gestión del riesgo relacionado con las TIC, adoptará y revisará periódicamente una estrategia sobre el riesgo de terceros relacionado con las TIC.

De conformidad con el *artículo 28, apartado 2 de DORA*, dicha estrategia incluirá una política sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes prestados por proveedores terceros de servicios de TIC, cuyo contenido se ajustará a lo dispuesto en el *Reglamento Delegado (UE) 2024/1773 de la Comisión, de 13 de marzo de 2024,* *por el que se completa el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo mediante normas técnicas de regulación que especifican el contenido detallado de la política relativa a los acuerdos contractuales sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes prestados por proveedores terceros de servicios de TIC*.

La ESI dispondrá de acuerdos contractuales para la utilización de servicios de TIC de terceros en el ejercicio de sus operaciones que incluirá, al menos, los elementos establecidos en el *artículo 30 de DORA*.

La ESI mantendrá y actualizará un registro de información en relación con todos los acuerdos contractuales sobre el uso de servicios de TIC prestados por proveedores terceros de TIC (distinguiendo entre los que comprenden servicios de TIC que sustentan funciones esenciales o importantes y los que no), que se ajustará a lo dispuesto al efecto en el *Reglamento de Ejecución (UE) 2024/2956 de la Comisión, de 29 de noviembre de 2024*, *por el que se establecen normas técnicas de ejecución para la aplicación del Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo en lo que respecta a las plantillas normalizadas para el registro de información.*

La ESI comunicará al menos una vez al año a la CNMV información sobre el número de nuevos acuerdos relativos al uso de servicios de TIC, las categorías de proveedores terceros de servicios de TIC, el tipo de acuerdos contractuales y los servicios y funciones prestados en materia de TIC.

La ESI pondrá a disposición de la CNMV, en caso de que esta así lo solicite, el registro completo de información o secciones específicas de este, junto con toda información que se considere necesaria por la CNMV para permitir la supervisión efectiva de la ESI.

La ESI informará oportunamente a la CNMV cuando se proponga celebrar cualquier acuerdo contractual para el uso de servicios de TIC que sustenten funciones esenciales o importantes y cuando una función se haya convertido en esencial o importante.

Antes de celebrar un acuerdo contractual sobre el uso de servicios de TIC, la ESI llevará a cabo las actuaciones previstas en el *artículo 28.4. de DORA*:

## Mecanismos y sistemas previstos en materia de gestión de ciberseguridad de ESI tipo A o B que no sean microempresas

#### **3.1. Mecanismos y sistemas previstos en materia de gestión y gobernanza de riesgos las TIC**

* 1. El solicitante de autorización **manifiesta** que:

 La ESI dispondrá de un marco interno de gobernanza y control que garantice una gestión efectiva y prudente del riesgo relacionado con las tecnologías de la información y la comunicación (TIC).

A tal efecto, la gestión y la supervisión del riesgo relacionado con las TIC, se encomendará a la siguiente función de control (que tendrá un nivel adecuado de independencia para evitar conflictos de intereses): Insertar

 La ESI contará con un marco de gestión de riesgo relacionado con las TIC - entendido como el conjunto de 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, incluidos el *software*, el *hardware* y los servidores, así como para proteger todos los componentes e infraestructuras físicos pertinentes, como locales, centros de datos y zonas sensibles designadas, a fin de garantizar que todos los activos de información y activos de TIC estén adecuadamente protegidos de los riesgos, incluidos los daños y el acceso o uso no autorizado – sólido, completo y bien documentado, basado en el despliegue de estrategias, políticas, procedimientos, protocolos y herramientas de TIC adecuados (que cumplirán con lo dispuesto al efecto en el *artículo 7 de DORA*), que le permita hacer frente al riesgo relacionado con las TIC de forma rápida, eficiente y exhaustiva y asegurar un alto nivel de resiliencia perativa digital.

 El marco de gestión de riesgo relacionado con las TIC de la ESI cumplirá con lo establecido en el *Reglamento Delegado (UE) 2024/1774 de la Comisión, de 13 de marzo de 2024*, por el que se completa el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo en lo que respecta a las normas técnicas de regulación que especifican las herramientas, métodos, procesos y políticas de gestión del riesgo relacionado con las TIC y el marco simplificado de gestión del riesgo relacionado con las TIC.

 El marco de gestión de riesgo relacionado con las TIC de la ESI incluirá una estrategia de resiliencia operativa digital que, a efectos de establecer cómo se aplica el marco, incluirá métodos para hacer frente al riesgo relacionado con las TIC y alcanzar los objetivos específicos de la ESI en materia de TIC, para lo cual contendrá la información especificada en las *letras a) a h) del artículo 6.8. de DORA*.

 Como parte del marco de gestión de riesgo relacionado con las TIC, la ESI elaborará y documentará una política de seguridad de la información que defina las normas para proteger al confidencialidad, disponibilidad, integridad o autenticidad de los datos, activos de información y activos TIC, aplicando las medidas, protocolos, procedimientos y controles establecidos en el *artículo 9.4. de DORA*.

 La ESI dispondrá de capacidades y personal para recopilar información sobre vulnerabilidades, ciberamenazas e incidentes relacionados con las TIC -en particular ciberataques-, analizar las posibles repercusiones en su resiliencia operativa digital, identificando sus causas y las mejoras necesarias para las operaciones de TIC o en la política de continuidad de la actividad en materia de TIC; asimismo, previa petición de la CNMV, comunicará a esta los cambios que haya introducido después de las revisiones tras incidentes relacionados con las TIC (*artículo 13 de DORA*).

 La ESI desarrollará programas de sensibilización en materia de seguridad de las TIC y formación sobre resiliencia operativa digital, módulos que serán obligatorios en los programas de formación de personal que la ESI desarrolle.

 La ESI supervisará continuamente los avances tecnológicos, con vistas a comprender las posibles repercusiones del despliegue de estas nuevas tecnologías en sus requisitos de seguridad de las TIC y su resiliencia operativa digital.

 El órgano de administración de la ESI, será responsable de definir, aprobar, aplicar y supervisar todas las disposiciones relacionadas con el marco de gestión del riesgo relacionado con las TIC asumiendo, a tal efecto, las funciones y responsabilidades desarrolladas en las *letras a) a i) del artículo 5.2. de DORA*.

 La ESI documentará y revisará el marco de gestión de riesgos relacionado con las TIC al menos una vez a año, así como cuando se produzcan incidentes graves relacionados con las TIC, en base a las instrucciones de supervisión o conclusiones derivadas de los procesos de prueba o auditoría de la resiliencia operativa digital.

 El marco de gestión de riesgos relacionado con las TIC de la ESI será objeto de auditoría interna, llevada a cabo por auditores -que deberán poseer conocimientos, capacidades y pericia, así como gozar de la independencia adecuada- suficientes en materia de riesgo relacionado con las TIC con la periodicidad y el enfoque adoptado por la ESI respecto de sus planes de auditoría, teniendo en cuenta el riesgo relacionado con las TIC de la ESI.

 La ESI proporcionará a la CNMV, previa petición de esta, información completa y actualizada sobre el riesgo relacionado con las TIC y sobre su marco de gestión de dicho riesgo, así como sobre la revisión anual que realice del mismo.

 El órgano de administración de la ESI, será responsable de definir, aprobar, aplicar y supervisar todas las disposiciones relacionadas con el marco de gestión del riesgo relacionado con las TIC asumiendo, a tal efecto, las funciones y responsabilidades desarrolladas en las *letras a) a i) del artículo 5.2. de DORA*.

* 1. En el contexto de la estrategia de resiliencia operativa digital que, de conformidad con lo dispuesto en el *artículo 6.8. de DORA*, debe elaborar la ESI, ¿tiene previsto definir una estrategia global multiproveedor en materia de TIC a nivel de grupo o de la ESI?

NO

SI  Detalle

|  |
| --- |
| Insertar información, *detallando posibles dependencias clave de los proveedores terceros de servicios TIC y explicando los motivos subyacentes a la contratación de una combinación de proveedores terceros de servicios TIC* . |

* 1. ¿Tiene previsto externalizar, en un tercero o en una empresa del grupo, las tareas de verificación del cumplimiento de los requisitos de gestión del riesgo relacionado con las TIC?

NO

SI  Detalle

|  |
| --- |
| Insertar |

* 1. ¿Está prevista la creación en la ESI de un cargo dedicado al seguimiento de los acuerdos que, en su caso, se celebren con terceros de servicios de TIC sobre el uso de servicios de TIC? -*marque 1 de las 3 opciones y elimine el resto*-

N/A  No está prevista la contratación con terceros de servicios TIC

SI  Detalle:

|  |
| --- |
| Insertar denominación del cargo e identificar dicha posición en el organigrama de la ESI, aportado en la pregunta 2) del apartado 3. del Manual de autorización de ESI. |

NO  Detalle

|  |
| --- |
| Insertar denominación del miembro del órgano de administración, dirección general o cargo asimilado, que será designado como responsable de supervisar la exposición al riesgo correspondiente y la documentación pertinente. |

1. En relación con el marco de gestión del riesgo relacionado con las TIC que establecerá la ESI:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Identifique:  |  | | --- | | Funciones, cometidos, responsabilidades y áreas de negocio, cuyos procesos están sustentados por las TIC: Insertar | | Activos de información y activos TIC (incluidos los que se encuentren en emplazamientos remotos, recursos de red y equipos de *hardware*) que sustentan dichos procesos: Insertar | | Vínculos e interdependencias entre activos TIC: Insertar | | Procesos que dependan de proveedores terceros de servicios de TIC e interconexiones con proveedores terceros de servicios de TIC que sustenten funciones esenciales o importantes: Insertar |  1. Detalle los criterios de clasificación de los incidentes relacionados con las TIC y las ciberamenazas, (*artículo 18 de DORA*):  |  | | --- | | Insertar *teniendo en cuenta lo dispuesto al efecto en el Reglamento Delegado (UE) 2024/1772: acerca del conjunto de criterios que deben seguir las entidades a la hora de clasificar los incidentes TIC y las ciberamenazas importantes, siguiendo un enfoque basado en el riesgo.* |  1. Informe brevemente de las principales características del modelo (interno o basado en tres líneas de defensa -1ª encargada de la gestión operativa del riesgo; 2ª encargada del control del riesgo y; 3ª la auditoría interna-) que utilizará la ESI para la gestión y control de su riesgo relacionado con las TIC. En particular, aporte información sobre:  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | 1. Las políticas, protocolos, procedimientos y herramientas en materia de seguridad de las TIC que utilizará la ESI al objeto de asegurar la resiliencia, continuidad y disponibilidad de los sistemas TIC (en particular aquellos que sustentan funciones esenciales), así como de mantener elevados niveles de disponibilidad, autenticidad, integridad y confidencialidad de datos (*artículo 9 de DORA*)  |  | | --- | | Insertar |  1. Los mecanismos de detección que tendrá la ESI de actividades anómalas (*artículo 17.3. de DORA*) -incluidos los problemas de rendimiento de las redes de TIC y los incidentes con las TIC (ciberataques), criterios y umbrales de alerta para activar e iniciar procesos de respuesta a incidentes relacionados con las TIC, así como periodicidad de su revisión (*artículo 10 de DORA*)  |  | | --- | | Insertar |  1. Los planes de respuesta y recuperación de incidentes en materia de TIC -sujetos a auditoría interna independiente-, incluyendo planes de prueba (que incluirán escenarios de ciberataque y de conmutación entre la infraestructura primario de TIC y la capacidad redundante, las copias de seguridad y las instalaciones redundantes pertinentes), informando sobre la periodicidad de revisión de dichos planes (al menos una vez al año, así como cada vez que se produzca un cambio sustancial en los sistemas TIC que sustenten funciones esenciales o importantes) y de las pruebas. (*artículo 11, apartados 3 y 6 de DORA*)  |  | | --- | | Insertar |  1. La política de continuidad de la actividad en materia de TIC, incluidos planes de prueba (que incluirán escenarios de ciberataque y de conmutación entre la infraestructura primario de TIC y la capacidad redundante, las copias de seguridad y las instalaciones redundantes pertinentes), en especial en lo referente a funciones esenciales externalizadas o contratadas con proveedores terceros de servicios TIC, así como el análisis del impacto en el negocio de la ESI de sus exposiciones a perturbaciones graves -teniendo en cuenta criterios cuantitativos y cualitativos-, incluyendo información sobre la periodicidad de revisión de dichos planes (al menos una vez al año, así como cada vez que se produzca un cambio sustancial en los sistemas TIC que sustenten funciones esenciales o importantes) y de las pruebas (*artículo 11, apartados 1, 2,4 ,5 y 6 de DORA*)  |  | | --- | | Insertar |  1. Las políticas y procedimientos de respaldo, así como los procedimientos y métodos de restablecimiento y recuperación, incluidas la realización de pruebas periódicas sobre dichas políticas y procedimientos (*artículo 12 de DORA*) -incluyendo información sobre el mantenimiento por la ESI de capacidades de TIC redundantes dotadas de recursos, medios y funciones adecuados para satisfacer las necesidades asociadas a su negocio:  |  | | --- | | Insertar |  1. Los planes previstos en la ESI relativos a la comunicación de crisis, al objeto de una adecuada divulgación, al menos, de los incidentes graves relacionados con las TIC o las vulnerabilidades importantes a clientes y contrapartes (*artículos 14 y 17.3., letras d) y e) de DORA*)  |  | | --- | | Insertar | | |

#### **3.2. Notificación de incidentes relacionados con las TIC**

1. El solicitante de autorización **manifiesta** que:

 La ESI notificará a la CNMV los incidentes graves relacionados con las TIC, a través de una notificación inicial, un informe intermedio posterior y un informe final, en la forma y plazos establecidos en el *artículo 19.4. de DORA*, así como en el *Reglamento Delegado (UE) 2025/301 de la Comisión, de 23 de octubre de 2024*, por el que se completa el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo en lo que respecta a *las normas técnicas de regulación que especifican el contenido y los plazos para la notificación inicial y los informes intermedio y final sobre incidentes graves relacionados con las TIC, así como el contenido de la notificación voluntaria de ciberamenazas importantes*, utilizando los formularios, plantillas y procedimientos normalizados establecidos al efecto en el *Reglamento de Ejecución (UE) 2025/302 de la Comisión, de 23 de octubre de 2024*.

1. ¿Tiene intención la ESI de notificar a la CNMV aquellas ciberamenazas que sean importantes, por el impacto que puedan tener para el sistema financiero, los usuarios del servicio o los clientes?

NO

SI   El solicitante de autorización **manifiesta** que la notificación que la ESI remitirá a la CNMV contendrá la información exigida por el [*Reglamento Delegado (UE) 2025/301*](https://www.boe.es/doue/2025/301/L00001-00005.pdf) y se realizará utilizando los formularios, las plantillas y los procedimientos establecidos al efecto en el [*Reglamento de Ejecución (UE) 2025/302*](https://www.boe.es/doue/2025/302/L00001-00044.pdf):

SI

1. ¿Está previsto que la ESI externalice en un proveedor tercero de servicios sus obligaciones de informar a la CNMV de los incidentes graves relacionados con las TIC, así como, en su caso, de las ciberamenazas importantes?

NO

SI   Detalle:

|  |
| --- |
| Insertar |

#### **3.3. Pruebas de resiliencia operativa y acuerdos de intercambio de ciber amenazas**

1. El solicitante de autorización **manifiesta** que:

 La ESI establecerá, mantendrá y revisará un programa sólido y completo de pruebas de resiliencia operativa digital, que formará parte del marco de gestión del riesgo relacionado con las TIC.

 El programa de pruebas de resiliencia operativa digital incluirá las evaluaciones, pruebas, metodologías, prácticas y herramientas necesarias, que se aplicarán de conformidad con lo dispuesto en los artículos 25.1. - evaluaciones y exploraciones de vulnerabilidad, análisis del *software* de código abierto, evaluaciones de seguridad de la red, análisis de carencias, exámenes de la seguridad física, cuestionarios y soluciones de *software* de detección, revisiones del código fuente cuando sea posible, pruebas basadas en escenarios, pruebas de compatibilidad, pruebas de rendimiento, pruebas de extremo a extremo y pruebas de penetración- y 26 -pruebas avanzadas de penetración basadas en amenazas- de DORA.

 La ESI garantizará que las pruebas serán realizadas por partes independientes, ya sean internas o externas. En caso de que un probador interno se encargue de realizar las pruebas, la ESI dedicará los recursos suficientes y garantizará que se evitan los conflictos de intereses durante todas las fases de constitución y ejecución de las pruebas.

 Los probadores, internos o externos, que utilizará la ESI para la realización de pruebas avanzadas de penetración basadas en amenazas cumplirán lo establecido al efecto en el *artículo 27 de DORA*.

 La ESI establecerá procedimientos y políticas para ordenar por prioridades, clasificar y corregir todos los problemas descubiertos durante la realización de las pruebas y establecerá métodos de validación internos para asegurarse de que todas las debilidades, deficiencias o carencias sean tratadas de manera exhaustiva.

 La ESI efectuará, al menos una vez al año, las pruebas apropiadas de todos los sistemas y aplicaciones de TIC que sustenten funciones esenciales o importantes.

 La ESI llevará a cabo, al menos cada tres años, pruebas avanzadas de penetración basadas en el nivel de amenaza (*artículo 26 de DORA*) basadas en su perfil de riesgo y teniendo en cuenta las circunstancias operativas y únicamente utilizará evaluadores que estén certificados, posean la experiencia e idoneidad necesarias y tengan un seguro de responsabilidad profesional.

1. ¿Tiene la ESI previsto intercambiar con otras entidades financieras información e inteligencia sobre ciberamenazas, en la medida que dicho intercambio de información e inteligencia cumple las condiciones establecidas en el *artículo 45.1. de DORA*?

NO

SI   Detalle:

|  |
| --- |
| Insertar |

#### **3.4. Gestión de riesgos de terceros (proveedores de servicios de TIC)**

1. ¿Está prevista la externalización por la ESI de servicios TIC (atendiendo a las definiciones establecidas al efecto en los *considerandos (35) y (63) de DORA*) en proveedores terceros de servicios TIC?

NO

SI   El solicitante de autorización **manifiesta** que:

 Como parte de su marco de gestión del riesgo relacionado con las TIC, adoptará y revisará periódicamente una estrategia sobre el riesgo de terceros relacionado con las TIC.

De conformidad con el *artículo 28, apartado 2 de DORA*, dicha estrategia incluirá una política sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes prestados por proveedores terceros de servicios de TIC, cuyo contenido se ajustará a lo dispuesto en el *Reglamento Delegado (UE) 2024/1773 de la Comisión, de 13 de marzo de 2024,* *por el que se completa el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo mediante normas técnicas de regulación que especifican el contenido detallado de la política relativa a los acuerdos contractuales sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes prestados por proveedores terceros de servicios de TIC*.

La ESI dispondrá de acuerdos contractuales para la utilización de servicios de TIC de terceros en el ejercicio de sus operaciones que incluirá, al menos, los elementos establecidos en el *artículo 30 de DORA*.

La ESI mantendrá y actualizará un registro de información en relación con todos los acuerdos contractuales sobre el uso de servicios de TIC prestados por proveedores terceros de TIC (distinguiendo entre los que comprenden servicios de TIC que sustentan funciones esenciales o importantes y los que no), que se ajustará a lo dispuesto al efecto en el *Reglamento de Ejecución (UE) 2024/2956 de la Comisión, de 29 de noviembre de 2024*, *por el que se establecen normas técnicas de ejecución para la aplicación del Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo en lo que respecta a las plantillas normalizadas para el registro de información.*

La ESI comunicará al menos una vez al año a la CNMV información sobre el número de nuevos acuerdos relativos al uso de servicios de TIC, las categorías de proveedores terceros de servicios de TIC, el tipo de acuerdos contractuales y los servicios y funciones prestados en materia de TIC.

La ESI pondrá a disposición de la CNMV, en caso de que esta así lo solicite, el registro completo de información o secciones específicas de este, junto con toda información que se considere necesaria por la CNMV para permitir la supervisión efectiva de la ESI.

La ESI informará oportunamente a la CNMV cuando se proponga celebrar cualquier acuerdo contractual para el uso de servicios de TIC que sustenten funciones esenciales o importantes y cuando una función se haya convertido en esencial o importante.

Antes de celebrar un acuerdo contractual sobre el uso de servicios de TIC, la ESI llevará a cabo las actuaciones previstas en el *artículo 28.4. de DORA*.

## Mecanismos y sistemas previstos en materia de gestión de ciberseguridad de ESI tipo C

#### **4.1. Mecanismos y sistemas previstos en materia de gestión y gobernanza de riesgos las TIC**

1. El solicitante de autorización **manifiesta** que:

 La ESI creará y mantendrá un marco simplificado de gestión de riesgo relacionado con las TIC sólido y documentado, en el que se detallarán los mecanismos y las medidas encaminados a procurar una gestión rápida, efectiva y global del riesgo relacionado con las TIC, incluyendo la protección de las infraestructuras y los componentes físicos pertinentes; la eficacia de dichas medidas de control será sometida a pruebas periódicas. Dicho marco simplificado de gestión del riesgo relacionado con las TIC cumplirá con lo establecido al efecto en el *Reglamento Delegado (UE) 2024/1774 de la Comisión, de 13 de marzo de 2024*, por el que se completa el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo en lo que respecta a las *normas técnicas de regulación que especifican las herramientas, métodos, procesos y políticas de gestión del riesgo relacionado con las TIC y el marco simplificado de gestión del riesgo relacionado con las TIC*

 La ESI supervisará de manera permanentemente la seguridad y el funcionamiento de todos los sistemas de TIC.

 La ESI minimizará las consecuencias del riesgo relacionado con las TIC mediante el uso de sistemas, protocolos y herramientas de TIC sólidos, resilientes y actualizados que sean apropiados para sustentar el desempeño de sus actividades y la prestación de servicios y para proteger adecuadamente la disponibilidad, autenticidad, integridad y confidencialidad de los datos en las redes y sistemas de información; la eficacia de dichas medidas de control será sometidos a prueba periódica

 La ESI deberá permitir que las fuentes de riesgo relacionado con las TIC y las anomalías en las redes y sistemas de información se identifiquen y detecten de inmediato y que los incidentes relacionados con las TIC se gestionen con rapidez.

 La ESI identificará las dependencias clave de proveedores terceros de servicios de TIC.

 La ESI garantizará la continuidad de las funciones esenciales o importantes mediante planes de continuidad de la actividad y medidas de respuesta y recuperación que incluyan, al menos, medidas de respaldo y restablecimiento de datos, planes y medidas que serán sometidos a pruebas periódicas.

 La ESI documentará y revisará el marco simplificado de gestión de riesgos relacionado con las TIC periódicamente, así como cuando se produzcan incidentes graves relacionados con las TIC, en base a las instrucciones de supervisión.

#### **4.2. Notificación de incidentes relacionados con las TIC**

1. El solicitante de autorización **manifiesta** que:

 La ESI notificará a la CNMV los incidentes graves relacionados con las TIC, a través de una notificación inicial, un informe intermedio posterior y un informe final, en la forma y plazos establecidos en el *artículo 19.4. de DORA*, así como en el *Reglamento Delegado (UE) 2025/301 de la Comisión, de 23 de octubre de 2024*, por el que se completa el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo en lo que respecta a *las normas técnicas de regulación que especifican el contenido y los plazos para la notificación inicial y los informes intermedio y final sobre incidentes graves relacionados con las TIC, así como el contenido de la notificación voluntaria de ciberamenazas importantes*, utilizando los formularios, plantillas y procedimientos normalizados establecidos al efecto en el *Reglamento de Ejecución (UE) 2025/302 de la Comisión, de 23 de octubre de 2024*.

1. ¿Tiene intención la ESI de notificar a la CNMV aquellas ciberamenazas que sean importantes, por el impacto que puedan tener para el sistema financiero, los usuarios del servicio o los clientes?

NO

SI   El solicitante de autorización **manifiesta** que la notificación que la ESI remitirá a la CNMV contendrá la información exigida por el [*Reglamento Delegado (UE) 2025/301*](https://www.boe.es/doue/2025/301/L00001-00005.pdf) y se realizará utilizando los formularios, las plantillas y los procedimientos establecidos al efecto en el [*Reglamento de Ejecución (UE) 2025/302*](https://www.boe.es/doue/2025/302/L00001-00044.pdf):

SI

1. ¿Está previsto que la ESI externalice en un proveedor tercero de servicios sus obligaciones de informar a la CNMV de los incidentes graves relacionados con las TIC, así como, en su caso, de las ciberamenazas importantes?

NO

SI   Detalle:

|  |
| --- |
| Insertar |

#### **4.3. Pruebas de resiliencia operativa y acuerdos de intercambio de ciber amenazas**

1. El solicitante de autorización **manifiesta** que:

 La ESI establecerá y aplicará un programa de pruebas de seguridad de las TIC (*artículo 36 del Reglamento Delegado (UE) 2024/1774 de la Comisión, de 13 de marzo de 2024*) que tendrá en cuenta las amenazas y vulnerabilidades detectadas dentro del marco simplificado de gestión del riesgo relacionado con las TIC de la ESI

 La ESI revisará, evaluará y someterá a prueba las medidas de seguridad de las TIC, tomando en consideración el perfil de riesgo general de sus activos de TIC.

 La ESI hará un seguimiento y una evaluación de los resultados de las pruebas de seguridad y actualizará sus medidas de seguridad en consecuencia y sin demora indebida en el caso de los sistemas de TIC que sustenten funciones esenciales o importantes.

1. ¿Tiene la ESI previsto intercambiar con otras entidades financieras información e inteligencia sobre ciberamenazas, en la medida que dicho intercambio de información e inteligencia cumple las condiciones establecidas en el *artículo 45.1. de DORA*?

NO

SI   Detalle:

|  |
| --- |
| Insertar |

#### **4.4. Gestión de riesgos de terceros (proveedores de servicios de TIC)**

1. ¿Está prevista la externalización por la ESI de servicios TIC (atendiendo a las definiciones establecidas al efecto en los *considerandos (35) y (63) de DORA*) en proveedores terceros de servicios TIC?

NO

SI   El solicitante de autorización **manifiesta** que:

 Como parte de su marco de gestión del riesgo relacionado con las TIC, adoptará y revisará periódicamente una estrategia sobre el riesgo de terceros relacionado con las TIC.

De conformidad con el *artículo 28, apartado 2 de DORA*, dicha estrategia incluirá una política sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes prestados por proveedores terceros de servicios de TIC, cuyo contenido se ajustará a lo dispuesto en el *Reglamento Delegado (UE) 2024/1773 de la Comisión, de 13 de marzo de 2024,* *por el que se completa el Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo mediante normas técnicas de regulación que especifican el contenido detallado de la política relativa a los acuerdos contractuales sobre el uso de servicios de TIC que sustenten funciones esenciales o importantes prestados por proveedores terceros de servicios de TIC*.

La ESI dispondrá de acuerdos contractuales para la utilización de servicios de TIC de terceros en el ejercicio de sus operaciones que incluirá, al menos, los elementos establecidos en el *artículo 30 de DORA*.

La ESI mantendrá y actualizará un registro de información en relación con todos los acuerdos contractuales sobre el uso de servicios de TIC prestados por proveedores terceros de TIC (distinguiendo entre los que comprenden servicios de TIC que sustentan funciones esenciales o importantes y los que no), que se ajustará a lo dispuesto al efecto en el *Reglamento de Ejecución (UE) 2024/2956 de la Comisión, de 29 de noviembre de 2024*, *por el que se establecen normas técnicas de ejecución para la aplicación del Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo en lo que respecta a las plantillas normalizadas para el registro de información.*

La ESI comunicará al menos una vez al año a la CNMV información sobre el número de nuevos acuerdos relativos al uso de servicios de TIC, las categorías de proveedores terceros de servicios de TIC, el tipo de acuerdos contractuales y los servicios y funciones prestados en materia de TIC.

La ESI pondrá a disposición de la CNMV, en caso de que esta así lo solicite, el registro completo de información o secciones específicas de este, junto con toda información que se considere necesaria por la CNMV para permitir la supervisión efectiva de la ESI.

La ESI informará oportunamente a la CNMV cuando se proponga celebrar cualquier acuerdo contractual para el uso de servicios de TIC que sustenten funciones esenciales o importantes y cuando una función se haya convertido en esencial o importante.

Antes de celebrar un acuerdo contractual sobre el uso de servicios de TIC, la ESI llevará a cabo las actuaciones previstas en el *artículo 28.4. de DORA*.