European Insurance and Occupational Pensions Authority

Observatorio de los Sistemas **Europeos** de Previsión Social Complementaria

EL FUTURO DESARROLLO DE LOS INFORMES SOBRE INCIDENTES RELACIONADOS CON LAS TIC.

Aportación de la Dra. Mercè Claramunt, presidenta del Observatorio de los Sistemas Europeos de Previsión Social Complementaria.

Revisión por el OPSG (Occupational Pensions Stakeholder Group) de EIOPA del artículo 21 de la DORA (siglas en inglés de la Ley de Resiliencia Operativa Digital).

OPINIÓN DE LA DRA. MERCÈ CLARAMUNT, PRESIDENTA DEL COMITÉ CIENTÍFICO DEL OBSERVATORIO DE LOS SISTEMAS EUROPEOS DE PREVISIÓN SOCIAL COMPLEMENTARIA Y MIEMBRO DEL OPSG (EIOPA), SOBRE EL FUTURO DESARROLLO DE LOS INFORMES SOBRE INCIDENTES RELACIONADOS CON LAS TIC.

Aportación realizada en el contexto de la revisión del artículo 21 de la DORA (siglas en inglés de la Ley de Resiliencia Operativa Digital (DORA) – EIOPA.

DORA es un reglamento de la UE que se aplica a partir de 2025 para reforzar la seguridad informática de las entidades financieras y hacerlas resilientes a los ciber incidentes.

Los requisitos legales esenciales que deben analizarse para la creación de un centro de la UE para recoger información sobre incidentes relacionados con las TIC son:

- Requisitos legales (por ejemplo, se necesita una revisión de DORA para crear un único centro de la UE)
- Requisitos de infraestructura y tecnología (incluida la ciberseguridad y la seguridad de los datos)
- Una evaluación del costo potencial total.

Para garantizar la interoperabilidad será necesaria la capacidad necesaria de armonización de datos (utilizar y combinar datos de diferentes fuentes y sistemas).

El elemento crítico de la gestión operativa de un centro de la UE es el procedimiento de gestión de datos

Respecto a las "condiciones de membresía" (por ejemplo, condiciones relacionadas con la posibilidad de acceder y utilizar el centro único de la UE), las más relevantes son los criterios de elegibilidad (tipo de interesado que puede acceder al HUB) y las medidas que garanticen la confidencialidad.

Para ello, las disposiciones técnicas pertinentes en este contexto, será el acceso por las entidades financieras

Los aspectos de la gestión de datos más relevantes son:

- Recopilación de datos (Cómo el HUB apoya la recopilación de incidentes y su validación)
- Difusión y notificación de datos

Porque la recopilación de datos es crucial porque deben recopilarse de diferentes países, lo que establecer criterios de evaluación coherentes es muy importante. Por otro lado, el éxito del HUB depende en gran medida de las mejoras en la difusión y la presentación de informes sobre Incidentes.

Como elemento adicional que debería tenerse en cuenta, está la cuestión del soporte informático, porque si se crea un HUB en la UE, las entidades financieras se verán obligadas primero a adaptarse al sistema de comunicación local, ya que el HUB no estaría operativo hasta principios de 2025, y luego al HUB de la UE, que podría ser de algún modo incompatible con el primero.

Los beneficios generales del escenario base, según el modelo similar al descrito en DORA, son:

- Posibilidad de tiempos de respuesta más rápidos por parte de las CA
- Las ANC como punto de contacto para cuestiones técnicas
- No hay cambios en los canales de notificación (de FE a ANC)

El aspecto más significativo es que el interlocutor de la Entidad Financiera (FE) es directamente su Estado Nacional. La Autoridad Competente (ANC) es responsable de proporcionar orientación, realizar inspecciones y, cuando sea necesario, imponiendo sanciones. Además, la ANC tendrá acceso directo a la información de la FE y poseerá una comprensión integral de la situación.

En un modelo descentralizado, los riesgos generales y las limitaciones del escenario base son:

- Falta de prácticas estandarizadas de presentación de informes (sistemas múltiples)
- Mayor riesgo de problemas en la calidad de los datos

Debido a que con el escenario de referencia es más difícil garantizar informes estandarizados y datos homogéneos de calidad.

Los beneficios generales de un Hub Centralizado, con todas las partes interesadas que informan y consumen datos del mismo, son:

- Potencial para una mejor gestión de la calidad de los datos
- Potencial para el análisis de datos

Debido a que el centro centralizado de la UE tendría la ventaja de aportar un enfoque integrado a la realidad de los ciberataques y las vulnerabilidades cibernéticas relevantes. Cuando se trata de detectar patrones o eventos repetidos, la eficacia de una base de datos centralizada siempre será mayor.

Por el contrario, los riesgos generales y las limitaciones de un centro centralizado, con un HUB central con todos las partes interesadas que informan y consumen datos del mismo, son:

- Mayor exposición a los riesgos de concentración de datos y los riesgos asociados con el "punto único de fallo"
- Mayores costos de implementación inicial
- En términos generales, los riesgos superan los beneficios identificados para los modelos más descentralizados

Dicha opinión se fundamenta en que representará una doble implementación para las entidades financieras, ya que, si se crea un HUB de la UE, estas se verán obligadas primero a adaptarse a la situación local del sistema de comunicación (ya que el HUB no estaría operativo hasta principios de 2025) y, a posteriormente, a un HUB de la UE que podría ser de alguna manera incompatible con el primero.

En consecuencia, los costes de las entidades financieras se duplicarían, hasta los costes iniciales del escenario de referencia a partir de 2025, y luego los costes de adaptación a los requerimientos del HUB centralizado.

Los beneficios generales de un centro de intercambio de datos, como sistema centralizado para todas las Autoridades Competentes de cada estado miembro, a las que las entidades financieras que informan, son:

- Equilibrio entre las opciones anteriores
- Reducción de la exposición al riesgo de concentración de datos / riesgos asociados con el «punto único de fallo» (por ejemplo, confidencialidad, integridad y disponibilidad de los datos)
- Posibilidad de tiempos de respuesta más rápidos por parte de las Autoridades Competentes.
- Las Autoridades Nacionales Competentes (ANC) como punto de contacto para cuestiones técnicas
- No hay cambios en los canales de notificación de las e entidades financieras a las Autoridades Nacionales Competentes
- Potencial de mecanismos seguros de intercambio de datos con múltiple casuística

El riesgo general y la limitación que supone un centro de intercambio de datos, como sistema centralizado para todas las Autoridades Nacionales Competentes, en contacto con las entidades financieras que les reportan las incidencias, es la necesidad de coordinación y la cuestión de la gobernanza, dado que este esquema requiere un gran esfuerzo de colaboración y coordinación entre las distintas ANC, entidades que podrían tener menos agilidad para adaptarse.

De los tres escenarios descritos, el que ofrecería mejor equilibrio entre riesgos y beneficios es el "Data-Sharing HUB", es decir, un sistema centralizado para todas las Autoridades Nacionales Competentes, en el que las entidades financieras reportan a sus respectivas autoridades competentes.

El principal y limitación que tiene esta opción es la necesidad de coordinación y gestión de los datos. En este sentido, la coordinación se verá facilitada si las ANC perciben una mejora y simplificación del proceso de comunicación con el HUB en comparación con el proceso requerido en el escenario de línea base.

Dra. Mercè Claramunt Bielsa
Presidenta del Comité Científico
Observatorio de los Sistemas Europeos de
Previsión Social Complementaria
Miembro del OPSG
EIOPA