Informe Final - Recomendaciones para Lograr una Mayor Convergencia en el Reporte de Incidentes Cibernéticos

Disponible como: [PDF](https://www.fsb.org/wp-content/uploads/P130423-1.pdf)

13 abril 2023

La interconexión del sistema financiero global hace posible que un incidente cibernético en una institución financiera (o un incidente en uno de sus proveedores de servicios externos) pueda tener efectos indirectos a través de fronteras y sectores.

Los incidentes cibernéticos están creciendo rápidamente en frecuencia y sofisticación. Al mismo tiempo, el panorama de las amenazas cibernéticas se está expandiendo en medio de la transformación digital, el aumento de la dependencia de proveedores de servicios externos y las tensiones geopolíticas.

Reconociendo que la información oportuna y precisa sobre incidentes cibernéticos es crucial para una respuesta y recuperación efectiva de incidentes y para promover la estabilidad financiera, el G20 solicitó al FSB que entregue un informe sobre cómo lograr una mayor convergencia en el informe de incidentes cibernéticos (CIR).

A partir del cuerpo de trabajo del FSB sobre cibernética, incluido el compromiso con las partes interesadas externas, el informe identifica puntos en común en los marcos de CIR y detalla los problemas prácticos asociados con la recopilación de información sobre incidentes cibernéticos de las IF y el intercambio posterior entre las autoridades financieras. Estas cuestiones prácticas incluyen:

1. desafíos operativos derivados del proceso de presentación de informes a múltiples autoridades;
2. establecer criterios/umbrales cualitativos y cuantitativos apropiados y coherentes para la presentación de informes;
3. establecer una cultura apropiada para reportar incidentes de manera oportuna;
4. definiciones y taxonomía inconsistentes relacionadas con la seguridad cibernética;
5. establecer un mecanismo seguro para comunicar sobre incidentes cibernéticos; y
6. Restricciones legales o de confidencialidad en el intercambio de información con autoridades a través de fronteras y sectores.

Este informe establece 16 recomendaciones para abordar estos problemas con el fin de promover las mejores prácticas en la notificación de incidentes cibernéticos.

Tipo(s) de contenido: [Documentos de política](https://www.fsb.org/content_type/publications/policy-documents/), [Publicaciones](https://www.fsb.org/content_type/publications/), [Informes para el G20](https://www.fsb.org/content_type/publications/reports-to-the-g20/) Fuente(s): [FSB](https://www.fsb.org/source/fsb/) Área(s) de política: [Resiliencia cibernética](https://www.fsb.org/policy_area/cyber-resilience/)



Resumen ejecutivo

Los incidentes cibernéticos están creciendo rápidamente en frecuencia y sofisticación. Al mismo tiempo, el panorama de las amenazas cibernéticas se está expandiendo en medio de la transformación digital, el aumento de la dependencia de proveedores de servicios externos y las tensiones geopolíticas. La interconexión del sistema financiero mundial hace posible que un incidente cibernético en una institución financiera (IF) (o un incidente en uno de sus proveedores de servicios externos) pueda tener efectos indirectos a través de las fronteras y los sectores.

Reconociendo que la información oportuna y precisa sobre incidentes cibernéticos es crucial para una respuesta y recuperación efectivas de incidentes y para promover la estabilidad financiera, el G20 solicitó al FSB que entregue un informe sobre cómo lograr una mayor convergencia en la notificación de incidentes cibernéticos (CIR). Para atender este llamamiento, el FSB llevó a cabo un trabajo para promover una mayor convergencia en el RCDI de tres maneras: (i) estableciendo recomendaciones para abordar los problemas identificados como impedimentos para lograr una mayor armonización en la notificación de incidentes; ii) mejorar el léxico cibernético1 para incluir términos adicionales relacionados con el RCDI como «lenguaje común» es necesario para una mayor convergencia; y iii) identificar tipos comunes de información que las IF presentan a las autoridades con fines de RCDI, lo que culminó en un concepto de formato común para el intercambio de notificación de incidentes (FIRE) para recopilar información sobre incidentes de las IF y utilizarla entre ellas. FIRE sería flexible para permitir una gama de opciones de adopción e incluir los elementos de datos más relevantes para las autoridades financieras.

Basándose en el cuerpo de trabajo del FSB sobre ciberseguridad, incluido el compromiso con las partes interesadas externas, este informe establece recomendaciones que apuntan a promover la convergencia entre los marcos del RCDI, al tiempo que reconoce que un enfoque único para todos no es factible ni preferible. Las autoridades financieras y las instituciones financieras pueden optar por adoptar estas recomendaciones según proceda y sea pertinente, de conformidad con su marco jurídico y reglamentario.

Recomendaciones:

1. Establecer y mantener objetivos para el RCDI. Las autoridades financieras deben tener objetivos claramente definidos para la notificación de incidentes, y evaluar y demostrar periódicamente cómo se pueden lograr estos objetivos de manera eficiente, tanto para las instituciones financieras como para las autoridades.

2. Explorar una mayor convergencia de los marcos CIR. Las autoridades financieras deben seguir estudiando formas de armonizar sus regímenes RCDI con otras autoridades pertinentes, sobre una base transfronteriza e intersectorial, para minimizar la posible fragmentación y mejorar la interoperabilidad.

3. Adoptar requisitos comunes de datos y formatos de presentación de informes. Las autoridades financieras deben identificar individual o colectivamente requisitos comunes en materia de datos y, cuando proceda, desarrollar o adoptar formatos normalizados para el intercambio de información sobre notificación de incidentes.

4. Implementar requisitos de informes por fases e incrementales. Las autoridades financieras deben implementar requisitos de información incrementales de manera gradual, equilibrando la necesidad de la autoridad de informar oportunamente con el objetivo principal de la institución afectada de controlar el incidente.

5. Seleccione los activadores de informes de incidentes apropiados. Las autoridades financieras deberían explorar los beneficios y las implicaciones de una serie de opciones de activación de la presentación de informes como parte del diseño de su régimen de RCDI.

6. Calibre las ventanas de informes iniciales. Las autoridades financieras deben considerar los posibles resultados asociados con el diseño de la ventana o la calibración utilizada para la presentación de informes iniciales.

7. Proporcione detalles suficientes para minimizar el riesgo de interpretación. Las autoridades financieras deben promover una comprensión coherente y minimizar el riesgo de interpretación proporcionando un nivel adecuado de detalle al establecer umbrales de notificación, utilizando terminologías comunes y complementando la orientación del RCDI con ejemplos.

8. Promover la presentación oportuna de informes en el marco de desencadenantes basados en la materialidad. Las autoridades financieras que utilizan umbrales de materialidad deben considerar la posibilidad de ajustar el lenguaje del umbral, o explorar otros enfoques adecuados, para alentar la notificación rápida por parte de las IF de incidentes materiales.

9. Revisar la efectividad del CIR y los procesos de respuesta y recuperación de incidentes cibernéticos (CIRR). Las autoridades financieras deben explorar formas de revisar la eficacia de los procesos y procedimientos CIR y CIRR de las IF como parte de su compromiso supervisor o regulatorio existente.

10. Llevar a cabo la recopilación de datos ad-hoc. Las autoridades financieras deben explorar formas de complementar los marcos del RCDI con medidas de supervisión según sea necesario e involucrar a las instituciones financieras en incidentes cibernéticos, tanto durante como fuera de los incidentes en vivo.

11. Abordar los impedimentos para el intercambio transfronterizo de información. Las autoridades financieras deben explorar métodos para abordar en colaboración los desafíos legales o de confidencialidad relacionados con el intercambio de información sobre RCDI sobre una base transfronteriza.

12. Fomentar la comprensión mutua de los beneficios de la presentación de informes. Las autoridades financieras deben colaborar regularmente con las IF para crear conciencia sobre el valor y la importancia de la notificación de incidentes, comprender los posibles desafíos que enfrentan las IF e identificar enfoques para superarlos cuando sea necesario.

13. Proporcionar orientación sobre la comunicación efectiva del RCDI. Las autoridades financieras deben explorar formas de desarrollar o fomentar el desarrollo de conjuntos de herramientas y directrices para promover prácticas de comunicación efectivas en los informes de incidentes cibernéticos.

14. Mantener capacidades de respuesta que apoyen el RCDI. Las IF deben identificar y abordar continuamente cualquier laguna en sus capacidades de respuesta a incidentes cibernéticos que apoyen directamente al RCDI, incluida la detección, evaluación y capacitación continuas de incidentes.

15. Reunir conocimientos para identificar eventos cibernéticos relacionados e incidentes cibernéticos. Las autoridades financieras y las instituciones financieras deben colaborar para identificar e implementar mecanismos para compartir proactivamente información sobre eventos, vulnerabilidades e incidentes entre los participantes del sector financiero para combatir la incertidumbre situacional y aunar conocimientos en defensa colectiva del sector financiero.

16. Proteja la información confidencial. Las autoridades financieras deben implementar formas seguras de manejo de información de incidentes para garantizar la protección de la información confidencial en todo momento.

Introducción

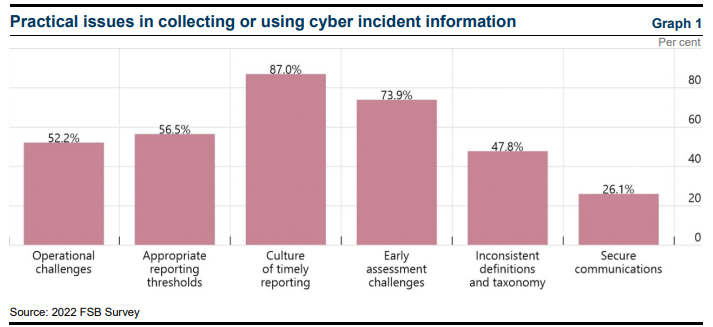
Mejorar la ciber resiliencia es una prioridad clave para las autoridades financieras y las instituciones financieras y ha sido un elemento clave del programa de trabajo del CEF para promover la estabilidad financiera. Este trabajo ha incluido el desarrollo de una mejor comprensión de las prácticas de supervisión y regulación en torno a la seguridad cibernética, 2 la creación de un lenguaje común relacionado con la cibernética a través del desarrollo de un léxico cibernético3 y el establecimiento de un conjunto de herramientas de prácticas efectivas para la respuesta y recuperación de incidentes cibernéticos.4 En muchas jurisdicciones, las autoridades financieras han introducido requisitos de RCDI para las instituciones financieras, que son cruciales para una respuesta política eficaz y para promover la estabilidad financiera. Sin embargo, durante la última década, han surgido y siguen surgiendo diferencias significativas en los requisitos y prácticas asociados con el CIR, que el FSB exploró con mayor detalle en su balance de 2021. 5

A partir de una encuesta de miembros del FSB realizada a principios de 2022, el FSB identificó puntos en común en los marcos CIR (detallados en el Anexo A) y problemas prácticos asociados con la recopilación de información sobre incidentes cibernéticos de las IF y el intercambio posterior entre las autoridades financieras. En la sección 2 se describen las cuestiones prácticas, que incluyen: i) los problemas operacionales derivados del proceso de presentación de informes a múltiples autoridades; ii) establecer criterios/umbrales cualitativos y cuantitativos apropiados y coherentes para la presentación de informes; iii) establecer una cultura apropiada para informar de los incidentes de manera oportuna; iv) definiciones y taxonomías incoherentes relacionadas con la ciberseguridad; v) establecer un mecanismo seguro para comunicarse en caso de incidentes cibernéticos; y vi) limitaciones jurídicas o de confidencialidad en el intercambio de información con las autoridades a través de las fronteras y los sectores. La Sección 3 establece 16 recomendaciones para abordar estas cuestiones prácticas y desafíos para lograr una mayor convergencia en el RCDI. Estas recomendaciones se basaron en las experiencias de las autoridades financieras y el compromiso con las instituciones financieras.

Cuestiones prácticas y desafíos para lograr una mayor convergencia en el RCDI

La encuesta de 2022 aumentó y refinó el balance en 2021,6 profundizando en la comprensión: (i) los objetivos de presentación de informes más comunes para las autoridades financieras; ii) los tipos de notificación de incidentes utilizados para apoyar objetivos comunes; iii) impedimentos para el intercambio de información entre autoridades financieras; iv) los elementos de información intercambiados como parte de la recopilación de datos sobre incidentes; v) los aspectos considerados para los umbrales de impacto/materialidad que activan las obligaciones de información; y (vi) problemas prácticos que tienen las autoridades financieras y las instituciones financieras para recopilar o utilizar la información cibernética reportada. Este trabajo identificó muchos puntos en común en los marcos del RCDI en todas las jurisdicciones y sectores. Esto incluye elementos comunes en los objetivos de notificación, los tipos de datos recopilados sobre incidentes y el uso de criterios o umbrales de materialidad para activar las obligaciones de notificación de las IF (es decir, la notificación iniciada por la entidad). (Véase el Anexo A para un análisis más detallado de los resultados de la encuesta.)

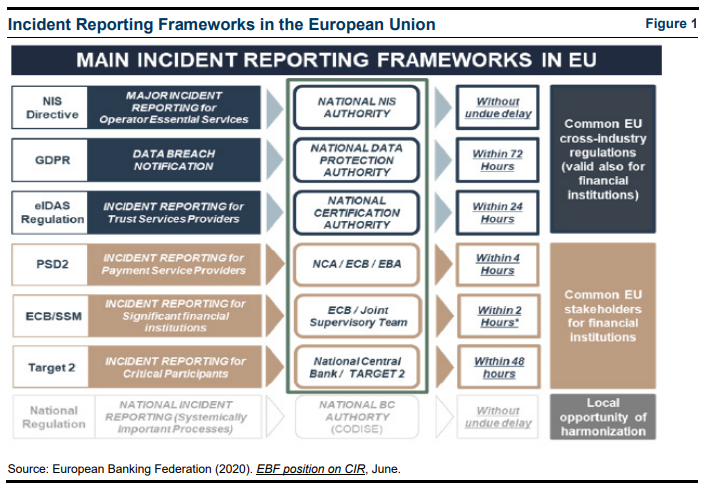
La encuesta también encontró que pueden surgir diferencias en los requisitos de presentación de informes debido a diferentes objetivos y mandatos de política, así como diferencias en el tamaño, las actividades comerciales y los servicios de las instituciones financieras. Los diferentes requisitos de presentación de informes, los diferentes usos de la información y la consiguiente información heterogénea pueden crear desafíos tanto para las instituciones financieras como para las autoridades financieras. El gráfico 1 ilustra los problemas prácticos a los que se enfrentan las autoridades financieras y las instituciones financieras cuando recopilan o utilizan información notificada sobre incidentes cibernéticos.7 Estos problemas están interrelacionados. Por ejemplo, una IF que enfrenta desafíos operativos al presentar informes CIR puede tener más dificultades para desarrollar una cultura que promueva la notificación oportuna de incidentes cibernéticos. Además, las diferencias en los requisitos reglamentarios o la notificación de incidentes cibernéticos, principalmente para las IF que operan en muchas jurisdicciones, podrían dar lugar a desafíos operativos que nuevamente afectan la calidad y la puntualidad de los informes.



Retos operativos

La notificación de incidentes cibernéticos iniciada por las instituciones por parte de las instituciones financieras suele desencadenarse al exceder los criterios implícitos o explícitos y normalmente se asocia con obligaciones específicas de notificación, como el requisito de presentar cartas de notificación, plantillas completas de incidentes o informes a través de otras herramientas/plataformas en línea. Las diferencias significativas en la forma en que las diferentes autoridades determinan sus criterios de notificación de incidentes cibernéticos, utilizan la información de incidentes y establecen sus plazos para informar de un incidente plantean desafíos operativos para las instituciones financieras; particularmente para las IF que operan en muchas jurisdicciones y sectores y están sujetas a múltiples requisitos de notificación para un incidente, y cada informe tiende a desencadenar consultas de seguimiento de cada autoridad financiera. Además, muchas IF deben informar a las fuerzas del orden, seguros cibernéticos, grupos de intercambio de amenazas de la industria, clientes y partes interesadas dentro de plazos establecidos, así como internamente a los equipos de continuidad del negocio, ejecutivos corporativos y equipos de comunicación corporativa. Al mismo tiempo, los equipos de respuesta a incidentes están trabajando para abordar el incidente, minimizar el daño y recuperar las operaciones lo más rápido posible.

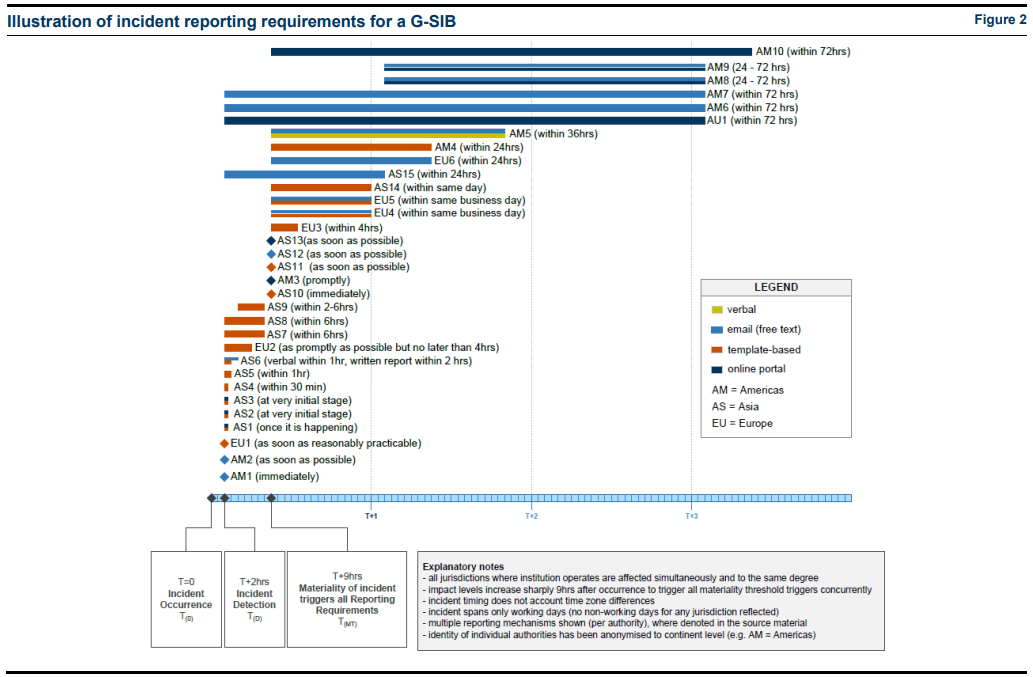
La figura 1 ilustra cómo las instituciones financieras que operan en la Unión Europea (UE) tienen que notificar incidentes a múltiples autoridades en virtud de diferentes reglamentos / directivas de la UE y en diferentes plazos, que van desde "sin demora indebida" hasta "dentro de las 72 horas". El proceso de presentación de informes involucra a las autoridades tanto a nivel nacional como europeo, a menudo aplicando diferentes procedimientos, criterios/umbrales, plantillas y taxonomía. La recientemente desarrollada Ley de Resiliencia Operativa Digital (DORA) es un paso hacia la armonización de los requisitos de notificación de incidentes en toda la UE, allanando el camino hacia un centro centralizado de incidentes de la UE.



La Figura 2 presenta un estudio de caso que se desarrolló en colaboración con un banco de importancia sistémica mundial (G-SIB) con grandes operaciones en Europa y Estados Unidos. En el caso de un incidente cibernético que desencadene requisitos de informes en todas las jurisdicciones en las que opera el G-SIB, el G-SIB, en las primeras 72 horas, tiene que ponerse en contacto verbalmente con cinco o más autoridades, emitir entre 7 y 13 informes escritos, completar y enviar 12-14 formularios iniciales de informes de incidentes e ingresar detalles en 5-9 portales de informes en línea.8 Cada informe es editado y revisado por equipos de respuesta a incidentes para garantizar que sea técnicamente preciso de acuerdo con la información más reciente. a medida que surgen más detalles del incidente, que es particularmente dinámico en las primeras 24 horas de un incidente. Además, el borrador del texto en cada formato, estilo y marco de tiempo de comunicación requerido se itera y finaliza con la información más actualizada disponible, lo que quita un tiempo considerable a los equipos relativamente pequeños de respuesta a incidentes cibernéticos durante el tiempo de investigación inicial más crítico.

También hay diferencias significativas en las plantillas de notificación y los desencadenantes de la notificación (es decir, los umbrales de detección o materialidad), que requieren el juicio del G-SIB, y los mecanismos de presentación de informes (por ejemplo, verbal, por correo electrónico, basado en plantillas, formulario en línea). El desafío de los umbrales de materialidad como desencadenantes para la notificación en las primeras 24 horas se ve exacerbado por la incertidumbre que rodea las primeras horas de la detección de un evento, que ha llevado a varias autoridades financieras a emitir una guía verbal para la notificación proactiva de incidentes con un potencial de estar relacionados con el ciberespacio, o un potencial de impacto material, pero el umbral aún no se ha alcanzado. Además, cada requisito de informes puede tener diferentes procesos de gobernanza, que deben gestionarse mientras se gestiona el incidente en sí.

Finalmente, además de la notificación obligatoria de incidentes, las IF pueden necesitar gestionar solicitudes de información ad hoc de las autoridades financieras tanto sobre incidentes cibernéticos como sobre eventos cibernéticos, lo que podría plantear demandas adicionales a los recursos ya limitados de la IF.



Establecimiento de criterios de notificación

El proceso de determinar y articular el punto en el que una obligación de informar se vuelve procesable después de un incidente cibernético plantea desafíos para las autoridades financieras y dificulta la convergencia en CIR.

En primer lugar, la calibración de los criterios de presentación de informes puede presentar problemas prácticos, entre ellos:

■ establecer criterios de notificación que sean independientes de la causa (es decir, pertinentes en todas las circunstancias incidentes) y de naturaleza proporcionada y, por lo tanto, aplicables a una amplia gama de instituciones financieras de diferentes escalas, complejidad y tipos;

■ determinar una duración adecuada para que las instituciones financieras cumplan su obligación de informar una vez que se haya activado;

■ para los desencadenantes basados en la detección, equilibrar el tiempo (en promedio) que puede requerir que las IF comprendan suficientemente la naturaleza de un incidente antes de presentar un informe inicial, frente a la necesidad de la autoridad financiera de ser informada de manera oportuna; y

■ para los desencadenantes basados en la materialidad, superando la dificultad inherente a la hora de describir o medir el impacto y la gravedad, dada la falta de metodologías establecidas para orientar a las autoridades financieras9 y las instituciones financieras.

En segundo lugar, existe la posibilidad de una falta de entendimiento común sobre los criterios de presentación de informes entre las autoridades financieras y sus instituciones financieras reguladas. Este "riesgo de interpretación" puede surgir como resultado de criterios detallados insuficientes, lo que aumenta la probabilidad de que las IF ejecuten de manera incorrecta o inconsistente en contra de las expectativas de la autoridad. En tales circunstancias, es posible que las autoridades experimenten mayores niveles de notificación insuficiente, excesiva o tardía, lo que a su vez puede afectar su capacidad para cumplir sus objetivos de presentación de informes. Por otro lado, tratar de definir demasiados criterios puede aumentar la complejidad operativa con la presentación de informes.

En tercer lugar, la calibración de los criterios de presentación de informes suele ser específica de cada autoridad financiera, lo que limita las oportunidades de convergencia. El momento en el que una autoridad desea ser informada de un incidente cibernético estará influenciado por su mandato institucional o por requisitos intersectoriales. La Figura 2 ilustra esta diversidad de períodos de presentación de informes implementados por 32 autoridades diferentes para la presentación de informes iniciales por parte de las instituciones financieras. La convergencia es menos probable para los impedimentos que son fundamentales en la naturaleza. Sin embargo, otros aspectos de los criterios de notificación que están menos impulsados por mandatos (como la presentación de informes intermedios o finales) pueden presentar oportunidades para la alineación, de modo que el momento de un subconjunto de informes de incidentes puede coincidir con ser recibido por múltiples autoridades simultáneamente.

Cultura de puntualidad en la presentación de informes

La notificación tardía de incidentes cibernéticos por parte de las IF podría retrasar o impedir la evaluación y las respuestas de las autoridades financieras. El impacto resultante podría ser significativo, especialmente cuando existen posibles implicaciones sectoriales o efectos indirectos a otras instituciones financieras que requieren una acción de apoyo de una autoridad. Por ejemplo, un incidente generalizado podría convertirse rápidamente en una crisis, y la autoridad financiera puede decidir emitir declaraciones de prensa al público para mantener su confianza en el sistema financiero. La comunicación efectiva del incidente cibernético solo se puede lograr cuando la autoridad financiera tiene información oportuna y suficiente relacionada con el incidente. Disponer de una notificación oportuna de dicha información también podría ser útil para la coordinación transfronteriza de acciones y respuestas conjuntas.

Establecer una cultura o comportamiento apropiado entre las IF para informar de incidentes cibernéticos de manera oportuna sigue siendo un desafío y puede requerir un cambio de mentalidad. Esto puede deberse a (ver Figura 3):

■ cultura deficiente o falta de conciencia en las instituciones financieras sobre la necesidad de un RCDI oportuno;

■ temor a daños a la reputación o a un mayor control por parte de la autoridad financiera pertinente;

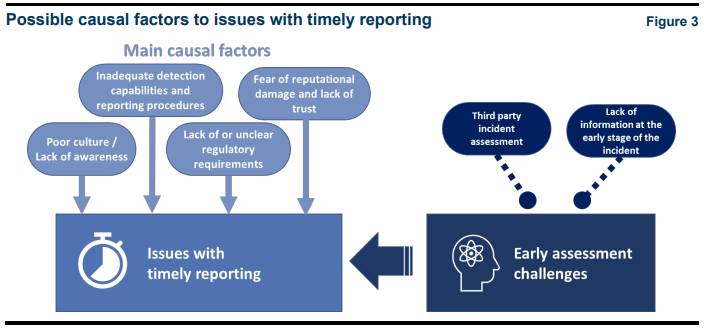
■ retraso en la detección y evaluación de incidentes cibernéticos en las IF debido a capacidades de detección inadecuadas, entornos de TI cada vez más complejos y/o adopción de nuevas tecnologías con las que el personal puede no estar completamente familiarizado;

■ falta de requisitos de información o requisitos de información poco claros que puedan estar abiertos a la interpretación de las instituciones financieras o las autoridades financieras;

■ procedimientos internos inadecuados de escalamiento y presentación de informes en las instituciones financieras; o

■ una falta de confianza por parte de empleados individuales o unidades organizativas en una IF que pueda impedir la escalada oportuna de incidentes cibernéticos.

Al mismo tiempo, las dificultades para realizar evaluaciones precisas durante la etapa inicial de un incidente cibernético, incluso en relación con los incidentes cibernéticos que afectan a proveedores de servicios externos que no comparten información oportuna con las instituciones financieras, también pueden contribuir al problema de la notificación tardía.



Retos de la evaluación temprana

Debido a la naturaleza ambigua de muchos incidentes cibernéticos en general, el verdadero impacto o la causa raíz del incidente pueden no conocerse durante algún tiempo. Esto hace que la obtención de información relevante sobre incidentes cibernéticos en las primeras fases del incidente sea un desafío, lo que dificulta la capacidad de evaluar el impacto de un incidente. Esto crea desafíos para que las autoridades coordinen y comuniquen las respuestas pertinentes de manera oportuna para garantizar la estabilidad del sistema financiero. La información a menudo no se comunica de manera estándar y diferentes autoridades pueden recibir diferentes cantidades de información en diferentes momentos, lo que afecta la capacidad de las autoridades para llegar a una imagen operativa común y una respuesta política cohesiva. Una imagen oportuna y clara de un incidente es importante para las autoridades financieras, ya que constituye la base de cualquier respuesta política; incluyendo respuestas de supervisión o, en el caso de un incidente más importante, comunicación pública o herramientas para abordar posibles impactos sistémicos.

El desafío para las IF es que algunos incidentes cibernéticos a menudo no son fáciles o directos de identificar. La detección de un incidente puede retrasarse significativamente después de la primera ocurrencia y el alcance del impacto puede no ser obvio al principio (por ejemplo, si no hay tiempo de inactividad del servicio). Evaluar el alcance total del impacto de los incidentes cibernéticos puede llevar mucho tiempo y, por lo tanto, puede continuar más allá de los umbrales iniciales y los requisitos de notificación. Las expectativas de completar este tipo de evaluación para fines de presentación de informes desde el principio, si bien son importantes, agregan estrés adicional y desvían recursos de centrarse en resolver el incidente. Los recursos para analizar la causa raíz de un incidente variarán dependiendo de la complejidad del incidente. En el caso de un incidente iniciado con fines maliciosos, la parte instigadora puede tomar medidas para ofuscar el impacto.

La falta de profesionales cibernéticos suficientemente capacitados y experimentados también podría afectar la capacidad de una IF para identificar y evaluar la situación de manera oportuna. Los desafíos pueden exacerbarse en las instituciones pequeñas, que pueden carecer de recursos para el monitoreo continuo, la detección automatizada y el análisis forense. Por otro lado, las grandes IF experimentan un mayor volumen de incidentes cibernéticos, muchos de los cuales pueden no ser dignos de mención para la institución o sus autoridades financieras.

Comunicaciones seguras

La información contenida en los informes de incidentes puede ser sensible tanto comercial como del mercado y, por lo tanto, debe ser manejada adecuadamente por todas las partes involucradas. La naturaleza diversa de los mecanismos de presentación de informes utilizados por las autoridades presenta desafíos operativos, como se destaca en la Sección 2.1. Desde una perspectiva de seguridad, las IF deben asegurarse de que pueden cumplir con estos requisitos variados en todo momento. Desde la perspectiva de la IF puede no haber suficiente claridad o confirmación de que ciertas plataformas de notificación de autoridades cumplan con los requisitos de seguridad compartidos, exponiendo así a las IF a posibles fuentes de riesgo, particularmente porque el correo electrónico no cifrado es la forma más común en que las IF informan de un incidente cibernético. Las IF también pueden tener preocupaciones sobre las plataformas de informes que son atacadas activamente por los actores de amenazas.

Cuestiones transfronterizas e intersectoriales

Si bien muchas autoridades financieras tienen acuerdos formales o informales de intercambio de información con autoridades fuera de su jurisdicción,11 existen diferencias en el alcance, la profundidad y la forma de dicho intercambio de información entre jurisdicciones y sectores. A través de la encuesta del FSB, surgieron dos temas como impedimentos para el intercambio de información a través de fronteras y sectores:

■ legal, ya sea que existan las leyes o acuerdos previos para establecer los términos por los cuales la información sobre incidentes puede ser compartida entre las partes; y

■ confidencialidad, es decir, el tratamiento/tratamiento de la información protegida entre las partes.

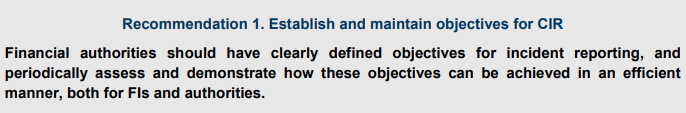
En la mayoría de los casos, siempre que existan acuerdos, como memorandos de entendimiento (MoU) o pasarelas legales, y la información transferida no viole los términos de lo que se puede intercambiar, se observan menos impedimentos.

Los acuerdos transfronterizos están «impulsados por el apetito», se rigen por los deseos de las autoridades individuales de compartir con otras partes y en qué medida, así como por la experiencia histórica. En la mayoría de las circunstancias, las autoridades financieras prefieren celebrar acuerdos bilaterales entre sí, lo que resulta en un mosaico de compromisos idiosincrásicos que, aunque tal vez no sean el resultado eficiente, reflejan la naturaleza / cercanía de las relaciones. Aunque existen acuerdos multilaterales, tienden a alinearse con círculos de confianza predefinidos.

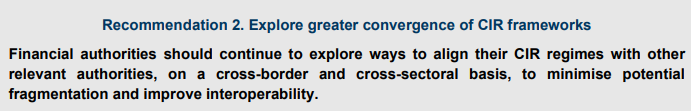
Recomendaciones

Basándose en el cuerpo de trabajo del FSB sobre ciberseguridad, incluido el compromiso con las partes interesadas externas, este informe establece recomendaciones para abordar los impedimentos para lograr una mayor convergencia en el RCDI. 12 Las recomendaciones tienen por objeto promover la convergencia entre los marcos del RCDI, reconociendo al mismo tiempo que no es factible ni preferible un enfoque único para todos. Las autoridades e instituciones financieras pueden optar por adoptar estas recomendaciones según sea apropiado y pertinente, de conformidad con su marco jurídico y reglamentario.

Diseño del enfoque del RCDI



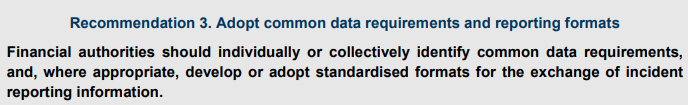
Las autoridades financieras deben revisar la cobertura y la idoneidad de los cinco objetivos de presentación de informes comúnmente identificados (véase el anexo A) dentro de su régimen de RCDI. En algunos casos, los objetivos CIR de una autoridad financiera pueden estar contenidos implícitamente dentro de objetivos más amplios relacionados con la notificación de incidentes, que pueden incluir, en lugar de ser exclusivos, incidentes cibernéticos. Al definir los objetivos, las autoridades financieras deberían, siempre que sea posible, abordar los problemas prácticos comúnmente identificados y los impedimentos asociados con el RCDI (por ejemplo, la reducción de los desafíos operativos). Las autoridades financieras deben revisar sus objetivos RCDI a intervalos regulares para verificar que siguen siendo adecuados para su finalidad y proporcionados, y garantizar que la información solicitada en la notificación de incidentes siga satisfaciendo las necesidades de todas las partes interesadas pertinentes. Las autoridades financieras también podrían involucrar a las IF para aclarar sus objetivos de política de RCDI, de modo que las IF puedan comprender y apoyar esos objetivos.



El establecimiento de un mayor grado de convergencia entre las autoridades financieras facilitará el intercambio de información en puntos críticos y promoverá una mayor eficiencia de los requisitos del RCDI para las IF activas a nivel mundial, promoviendo así la estabilidad financiera. Dicha armonización podría dar cabida a las necesidades de intercambio de información transfronterizas e intersectoriales de autoridades específicas.

En las jurisdicciones donde se designa a más de una autoridad financiera para recibir informes de incidentes cibernéticos, y donde las circunstancias operativas y los marcos legales permitirían dicha racionalización, las autoridades deberían explorar formas de consolidar los procesos CIR superpuestos. Los posibles enfoques incluyen la implementación de RCDI unificado para todas las autoridades pertinentes o la designación de una autoridad principal de notificación para recibir informes de incidentes y difundir esta información a otras autoridades según corresponda. En tales casos, las autoridades deben tratar de utilizar formatos comunes de presentación de informes para la difusión de información, que además pueden apoyar la entrega de instancias de informes individuales a múltiples destinatarios de autoridad.

Las autoridades financieras también deben explorar la armonización de los mecanismos para el intercambio seguro de información sobre notificación de incidentes, incluidas las oportunidades de armonizar los canales de denuncia con otras autoridades financieras que reciben información del RCDI.



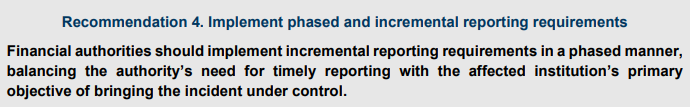
La adopción de requisitos comunes de datos y formatos de presentación de informes puede ocurrir en tres escalas diferentes que se construyen gradualmente en términos de alcance, complejidad y ambición (que se describen a continuación). Las autoridades financieras deben determinar el nivel de adopción, que es apropiado para sus circunstancias, señalando que cualquier cambio en los formatos de presentación de informes probablemente tendría implicaciones de implementación para las instituciones financieras afectadas en su alcance. Se alienta a las autoridades financieras a colaborar con las IF para informar el desarrollo de sus requisitos de datos CIR y formatos de presentación de informes. Los enfoques comunes podrían contribuir a fomentar la confianza y la colaboración y podrían adoptarse:

■ Por una única autoridad, cuando los requisitos de información no están definidos explícitamente actualmente. En tales casos, las IF tendrían un alto grado de flexibilidad, pero podrían carecer de la claridad necesaria para proporcionar a la autoridad financiera información sobre incidentes de manera coherente. La definición de formatos para campos de datos individuales dentro de los informes de incidentes puede generar beneficios adicionales relacionados con el intercambio y procesamiento de la información reportada. En ausencia de una orientación central, los supervisores individuales pueden recurrir a acordar estos requisitos sobre una base bilateral con las instituciones financieras, lo que a su vez podría ser menos eficiente para las autoridades y obstaculizar la capacidad de realizar análisis horizontales.

■ Por autoridades financieras dentro de la misma jurisdicción. La adopción de un formato común de presentación de informes por parte de las autoridades financieras dentro de una sola jurisdicción puede proporcionar una solución más eficiente para los requisitos de información que se originan en esa jurisdicción. Este cambio puede ser particularmente útil para las IF que están reguladas únicamente a nivel nacional.

■ Por (un subconjunto de) autoridades financieras en todas las jurisdicciones. La adopción de un formato común de presentación de informes a través de las fronteras podría beneficiar a las instituciones financieras con una huella global. Además, una adopción más amplia de un formato común puede impulsar la eficiencia para el intercambio transfronterizo de información sobre incidentes entre las autoridades financieras de forma normalizada.

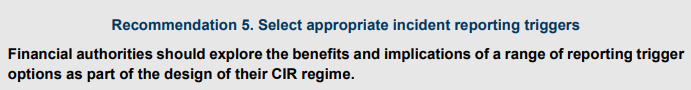
Las autoridades financieras también pueden considerar aceptar el formato y el contenido de un informe de incidente cibernético que las IF deben presentar a su principal autoridad de supervisión o supervisión.



Los informes iniciales de incidentes cibernéticos13 deben tener como objetivo contener un conjunto mínimo de elementos de información que luego puedan complementarse con actualizaciones intermedias más completas y culminar en un informe final que también incluya el análisis posterior al incidente realizado por la IF afectada.

En las primeras etapas de un incidente cibernético, los niveles de confianza sobre las causas y circunstancias del incidente pueden ser bajos y la IF afectada puede no tener una comprensión integral del evento que ha ocurrido. Al comienzo del incidente, la situación podría ser inestable y puede seguir evolucionando. Al mismo tiempo, los recursos y esfuerzos de la IF afectada se centran principalmente en la respuesta a incidentes y la contención del impacto. Por lo tanto, los requisitos de información inicial deben limitarse para facilitar la notificación oportuna y no agravar los desafíos operativos a los que ya se enfrenta la entidad afectada.

A medida que la IF gana mayor claridad y obtiene más detalles en el transcurso de su gestión de incidentes, puede proporcionar más actualizaciones a través de informes intermedios o finales (según el caso) a la autoridad financiera. Para garantizar un cierre adecuado después de que se haya resuelto el incidente, el informe final debe cubrir el análisis de la causa raíz de la IF y la revisión posterior a la acción.

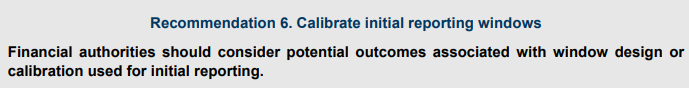


Para cada tipo de notificación14, el proceso para determinar el desencadenante de la notificación debe tener como objetivo resultados que sean proporcionados, comprensibles y justificables. Para cada tipo de informe, las autoridades financieras pueden seleccionar entre una gama de diferentes opciones de activación que afectan el momento y/o el plazo para la presentación de informes.

■ Para la presentación de informes iniciados por la entidad, la principal elección de diseño es si se deben anclar los requisitos de presentación de informes relativos a (1) la ocurrencia o detección de incidentes, o (2) cuando una institución financiera evalúa un incidente para cumplir con un umbral de materialidad predefinido. Los umbrales comunes de materialidad incluyen medidas cuantitativas basadas en el tiempo de inactividad del servicio, el impacto en la rentabilidad o los clientes, aunque estos deben escalarse o implementarse en relación con el tamaño de la institución financiera. Los umbrales de materialidad también pueden ser cualitativos, como los basados en el impacto reputacional. Factores como la facilidad de comprensión, la independencia del escenario, la incertidumbre situacional y la toma de decisiones institucionales deben considerarse como parte de la evaluación de activación.

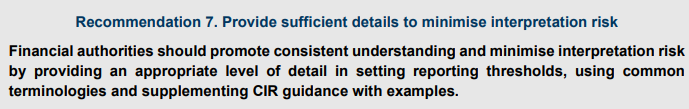
■ Para la presentación de informes iniciada por la autoridad, las autoridades financieras deben tener en cuenta las circunstancias y el proceso necesarios para poner en marcha evaluaciones de impacto sectoriales, ya sea a nivel nacional o transfronterizo.

Las autoridades también pueden recopilar datos de incidentes cibernéticos de forma periódica. Como el desencadenante de la presentación de informes periódicos es impulsado por el tiempo y no por los eventos, las autoridades financieras deben considerar la frecuencia de la recopilación de datos en relación con el volumen de información sobre incidentes recopilada para el período de informe elegido. Las autoridades pueden optar por un intervalo uniforme entre sus instituciones reguladas, o variar la frecuencia de acuerdo con el tipo, la escala y la complejidad de la empresa. El calendario relativo de las recopilaciones masivas de datos de todas las instituciones dentro del alcance puede ser: alineado, aunque esto puede presentar desafíos en el manejo del volumen agregado de información recibida simultáneamente; o se extienden de tal manera que las instituciones individuales informen sobre sus propios ciclos periódicos, lo que podría introducir una complejidad adicional a los mensajes externos.



Al establecer ventanas iniciales de presentación de informes, las autoridades financieras deben considerar una serie de factores que incluyen: (i) el tipo de ventana, es decir, si la ventana está vinculada al inicio, al final o utiliza una ventana definida; ii) la elección del idioma, que puede transmitir un énfasis diferente; y iii) el tamaño de la ventana, que puede verse influido por el tipo de activación de la notificación. Las ventanas de informes deben calibrarse cuidadosamente para no ejercer una presión adicional sobre las IF en la respuesta a los incidentes cibernéticos.

Cuando los desencadenantes de la notificación se basan en el tiempo (es decir, la ocurrencia o la detección), podrían implementarse ventanas más largas para permitir que las instituciones financieras evalúen razonablemente la naturaleza del incidente. A la inversa, cuando se utilizan umbrales de importancia relativa, las instituciones financieras ya deberían haber evaluado parcialmente la naturaleza de un incidente y, por lo tanto, podrían aplicarse plazos de notificación más cortos para que las autoridades puedan ser informadas rápidamente y actuar en consecuencia. Al determinar los plazos de presentación de informes, las autoridades financieras también deben velar por que se tengan debidamente en cuenta las ventajas de la presentación temprana de informes, al tiempo que se sopesa con la calidad y la exhaustividad de la información que puede recopilarse razonablemente durante el período de tiempo. Como se contempla en la recomendación 4, la presentación gradual de informes es una forma de equilibrar la carga operativa de las instituciones financieras que pueden no disponer de información completa sobre un incidente desde el principio, garantizando al mismo tiempo que las autoridades financieras estén informadas y preparadas para responder lo antes posible.



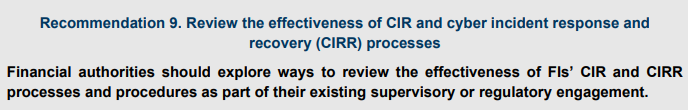
Las autoridades financieras deben considerar enfoques para minimizar el riesgo de interpretación (es decir, una desalineación de las expectativas de la autoridad frente a la comprensión de la institución) a través de la claridad de expresión e ilustrando la intención detrás de la política o la elaboración de normas para los umbrales CIR. Las autoridades también deben considerar la posibilidad de aprovechar las terminologías comunes, que serán particularmente valiosas para las instituciones financieras sujetas a múltiples requisitos de presentación de informes y terminología potencialmente contradictoria. 16 Con independencia de que una autoridad adopte un enfoque cualitativo, cuantitativo o combinado para definir sus criterios de información, el nivel de detalle proporcionado debe tratar de ser lo más informativo posible, teniendo en cuenta al mismo tiempo la introducción de una complejidad indebida.



Las IF requieren tiempo para realizar un análisis sobre si se han superado los umbrales de materialidad, pero no necesitan esperar a que se informe con certeza absoluta. En ciertos casos, las IF pueden tener información que sugiere fuertemente que es razonablemente probable que se supere un umbral de materialidad antes de que eso ocurra. Sobre la base de los detalles iniciales disponibles sobre los incidentes, que pueden ser algo limitados, las autoridades financieras deben alentar a las instituciones financieras a adoptar un enfoque prospectivo para su evaluación y determinación de qué incidentes justificarían la notificación. Este enfoque ayudaría a las autoridades financieras a ser conscientes de las cuestiones que probablemente se convertirán en importantes lo antes posible y a adoptar las medidas oportunas. La IF puede determinar inmediatamente que es poco probable que el incidente se resuelva antes de que se supere el umbral. En consecuencia, la IF podría comenzar el proceso para alertar a las autoridades antes del último período requerido.

A medida que la IF continúa evaluando el impacto, la IF debe poder confirmar o "degradar" el incidente según lo justificado (es decir, informar a las autoridades que la IF ya no cree que el incidente cumpla con el umbral de notificación).

Actividades de supervisión y colaboración entre autoridades



Las revisiones de los procesos y procedimientos del RCDI de las IF pueden identificar posibles brechas que podrían conducir a informes insuficientes, excesivos o tardíos. Siempre que sea posible, las autoridades financieras podrían realizar esos exámenes en el marco de su supervisión permanente, incluyendo, entre otras cosas:

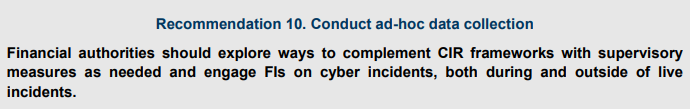
■ simulacros y evaluaciones temáticas para evaluar los planes y procedimientos de las instituciones financieras a fin de alcanzar los niveles requeridos de RCDI (por ejemplo, procedimiento operativo estándar para la comunicación y la coordinación, normas claras de información);

■ inspecciones in situ o revisiones independientes (por ejemplo, comparación de incidentes registrados internamente con incidentes notificados a la autoridad, herramientas adecuadas de respuesta a incidentes cibernéticos);

■ recopilar información sobre incidentes cibernéticos de otras fuentes de información (por ejemplo, informes de incidentes cibernéticos de otras instituciones financieras, terceros u otros sectores; informes de los medios de comunicación; otros acuerdos de intercambio de información).

Las pruebas y ejercicios de ciberseguridad llevados a cabo por las IF también podrían incluir planes y procedimientos CIR para buscar una mejora continua de sus capacidades internas basadas en las lecciones aprendidas. Las IF también podrían contratar a una parte independiente para evaluar sus medidas y procesos de gestión de incidentes, incluidos los procedimientos para la escalada y notificación de incidentes.

Además, el proceso para reportar un incidente comienza antes de que ocurra un incidente y a menudo está influenciado por elementos del programa y los procesos CIRR de una institución. Por lo tanto, también puede haber méritos para que las autoridades financieras revisen estas capacidades como parte de su compromiso de supervisión, lo que podría dar lugar a mejores resultados del RCDI.



Las autoridades financieras pueden utilizar su conjunto de herramientas de supervisión para mejorar la recopilación de información sobre incidentes cibernéticos más allá de cualquier requisito específico de información.

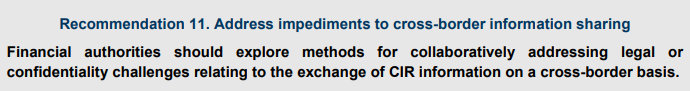
Las posibles situaciones que podrían justificar el uso del conjunto de herramientas de supervisión incluyen:

■ Una autoridad financiera recibe información limitada sobre un incidente cibernético grave que justifique un monitoreo continuo.

■ Una autoridad financiera recibe información sobre un incidente cibernético en una institución, que tiene el potencial de ser replicado en otras instituciones.

■ Una autoridad financiera recibe información (por ejemplo, tal vez a través de informes de prensa u otros canales gubernamentales) sobre una posible vulnerabilidad o evento cibernético y trata de minimizar el impacto en las IF reguladas.

El uso del conjunto de herramientas de supervisión en esta situación, como en otras, depende del juicio de la supervisión y de los hechos y circunstancias específicos en torno a un incidente cibernético, y de la información limitada que los supervisores pueden tener en cualquier momento. Cuando las circunstancias lo permitan, las autoridades financieras deben estudiar formas de aumentar la cooperación transfronteriza e intersectorial con respecto a las instituciones financieras que están sujetas a múltiples reglamentaciones.

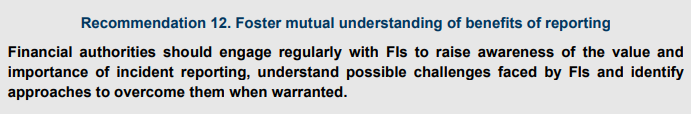


Las autoridades financieras pueden utilizar memorandos de entendimiento u otros acuerdos equivalentes para esbozar la base del intercambio de información entre autoridades, que generalmente incluyen compromisos para mantener la confidencialidad de la información. Sin embargo, en algunos casos, los acuerdos existentes pueden no cubrir claramente el intercambio de información relacionada con cuestiones cibernéticas y la notificación de incidentes, o abordar suficientemente los problemas que pueden impedir que estos intercambios tengan lugar. Las autoridades financieras deberían considerar si el desarrollo colaborativo de cláusulas modelo puede mejorar dichos memorandos de entendimiento e intercambios de información.

Para mejorar aún más la cooperación transfronteriza, las autoridades financieras deben explorar los beneficios y la aplicabilidad de los marcos de presentación de informes regionales o mundiales. Los acuerdos transfronterizos, como el Mecanismo Único de Supervisión del Banco Central Europeo (MUS del BCE) y los marcos de información de la Autoridad Bancaria Europea (ABE) en la UE, el acuerdo de cooperación con los países del Golfo y la DTN-CRISP demuestran los beneficios para los participantes, independientemente del marco que se utilice.

Además, las autoridades financieras pueden tomar medidas para evitar la inclusión de información protegida a menos que puedan cumplir con la legislación de protección de datos relevante en todas las jurisdicciones involucradas. En la mayoría de los casos, ese nivel de detalle solo sería necesario si se intercambiara información sobre la respuesta técnica al incidente.

Compromiso de la industria

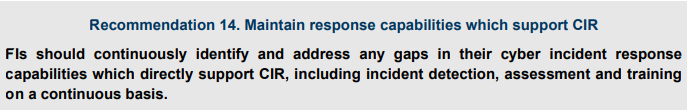


El compromiso continuo entre las autoridades financieras y las instituciones financieras puede ayudar a desarrollar un entendimiento común con respecto al marco y los criterios para el RCDI, incluidos los objetivos políticos del RCDI. Las discusiones también pueden cubrir las medidas legales y técnicas implementadas para proteger la información que se informa a las autoridades financieras, incluida la forma y las circunstancias en las que esta información sobre incidentes puede compartirse nuevamente. Las autoridades financieras deben considerar la posibilidad de revisar periódicamente sus requisitos y procesos de RCDI e incorporar la retroalimentación de las instituciones financieras, según corresponda. Tales compromisos podrían tener lugar en forma de talleres y seminarios de la industria, o diálogos con asociaciones industriales y instituciones financieras. Por último, compartir los resultados (de forma agregada y anónima) sobre los informes de ciberincidentes, es decir, sobre las tendencias de los incidentes sectoriales, podría proporcionar un ciclo de retroalimentación beneficioso a las instituciones financieras.

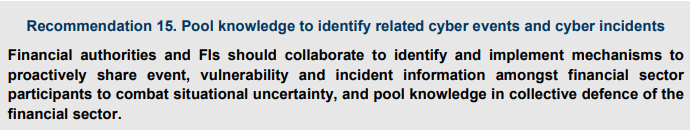


Las instituciones financieras pueden beneficiarse de una mayor orientación de las autoridades sobre prácticas eficaces en términos de los diferentes tipos de informes asociados con incidentes cibernéticos específicos. La orientación podría ayudar a mejorar la claridad de la presentación de informes iniciales. Las orientaciones también podrían ayudar a normalizar la calidad de los informes intermedios y finales cuando la institución informante disponga de más información (por ejemplo, si incluir indicadores de compromiso u otra información más detallada).

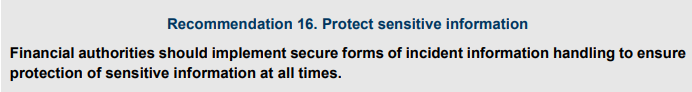
Desarrollo de capacidades (individuales y compartidas)



Para fomentar la preparación en torno a la detección y notificación de incidentes, las IF deben considerar la adopción de prácticas efectivas, como las descritas en el conjunto de herramientas de Prácticas Efectivas para la Respuesta y Recuperación de Incidentes Cibernéticos del FSB (ver Recuadro 5). 17 En muchos casos, el conjunto de herramientas del FSB reconoce que determinadas capacidades especializadas de respuesta a incidentes y notificación no siempre pueden conservarse internamente, en particular para las instituciones más pequeñas, y pueden obtenerse de terceros u organizaciones afiliadas. En particular, los proveedores o consultores externos pueden ayudar con soluciones tecnológicas, monitoreo de seguridad, capacidades forenses y recursos de información confiables para proporcionar capacidades adicionales a una IF antes de un incidente, y pueden escalarse rápidamente en la respuesta a incidentes más complejos. Debido a que los incidentes pueden manifestarse debido a relaciones con terceros, las IF deben evaluar la necesidad y la capacidad de obtener información relevante de proveedores externos para un informe de incidente relevante (por ejemplo, a través de contratos o acuerdos de nivel de servicio). Cuando proceda, las IF deben alentar a sus proveedores externos a compartir información sobre incidentes que afecten a los servicios prestados. Esto facilitaría la evaluación temprana de los incidentes cibernéticos por parte de las instituciones financieras, así como las actividades de respuesta y recuperación.



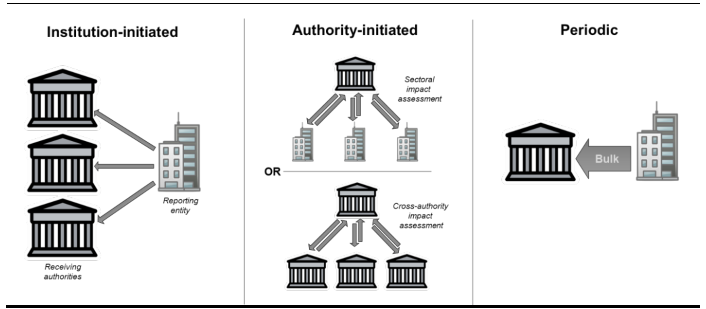
Cuando proceda, las autoridades financieras deben considerar su papel en el establecimiento del entorno de colaboración para fomentar nuevos mecanismos de intercambio de información o mejorar los existentes para los incidentes cibernéticos dentro de las jurisdicciones y entre ellas. En virtud de tales acuerdos, las instituciones afectadas pueden aprovechar el conocimiento colectivo y las capacidades de otras instituciones financieras para ayudar a contener y resolver incidentes en vivo, y proporcionar recíprocamente información crucial para evitar futuros sucesos o limitar la propagación a otras partes del sector financiero. Las autoridades financieras también pueden aprovechar estos mecanismos para proporcionar un circuito de retroalimentación a las IF para mejorar la resiliencia cibernética en todo el sector financiero, generar confianza con las IF y fomentar un enfoque constructivo para intercambiar información sobre incidentes.



Las autoridades financieras deben verificar periódicamente que los mecanismos utilizados para recopilar, procesar y almacenar información RCDI mantengan un nivel adecuado de seguridad en las diferentes fases o actividades (por ejemplo, recopilación, uso, intercambio, eliminación) y que la información sensible se maneje de conformidad con las prácticas comunes de seguridad y las obligaciones legales de las autoridades financieras pertinentes. Las autoridades financieras también pueden considerar riesgos de seguridad relevantes en sus mecanismos utilizados para recopilar información sobre incidentes.

Los mecanismos incluyen el uso de plataformas, portales o canales seguros; cuentas de correo electrónico certificadas; o protocolos de cifrado y otras medidas técnicas, para proteger la información tanto en reposo como en tránsito. Además, para aumentar la fiabilidad del proceso de presentación de informes, las autoridades financieras deben considerar la posibilidad de establecer canales de comunicación de respaldo, según proceda, para cubrir situaciones en las que el canal principal no esté disponible o no pueda ser utilizado por las instituciones informantes.

**Ilustración de los tipos de informes**



**Mapeo de los objetivos y tipos de información de las autoridades financieras**

