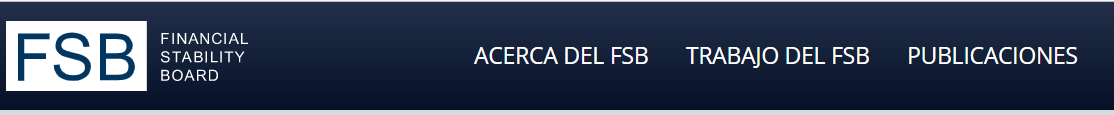
Documento consultivo - Lograr una mayor convergencia en la notificación de incidentes cibernéticos



17 octubre 2022

La información sobre incidentes cibernéticos es crucial para una respuesta y recuperación efectivas de incidentes y para promover la estabilidad financiera.

Los incidentes cibernéticos están creciendo rápidamente en frecuencia y sofisticación, lo que subraya la importancia de fuertes salvaguardas contra el riesgo cibernético. 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 creciente interconexión del sistema financiero aumenta la probabilidad de que un incidente cibernético en una institución financiera, o un incidente en uno de sus proveedores de servicios externos, tenga efectos indirectos a través de las fronteras y los sectores.

La información oportuna y precisa sobre incidentes cibernéticos es crucial para una respuesta y recuperación efectivas de incidentes y para promover la estabilidad financiera. Reconociendo esto, el G20 pidió al FSB que entregara un informe sobre cómo lograr una mayor convergencia en la notificación de incidentes cibernéticos.

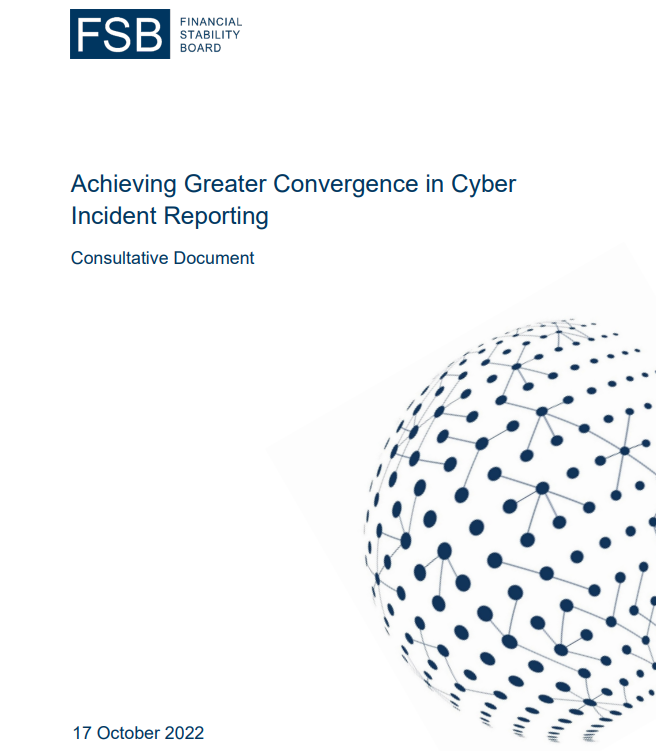
Para informar su trabajo, el FSB realizó una encuesta a los miembros del FSB para: identificar los objetivos de presentación de informes más comunes y los tipos de informes realizados; comprender los problemas prácticos que tienen las autoridades financieras y las instituciones financieras para recopilar o utilizar información sobre incidentes; Identificar los elementos de información que las autoridades recopilan para cumplir los objetivos comunes de presentación de informes, y explorar los mecanismos para que las autoridades financieras compartan información sobre incidentes a través de fronteras y sectores.

Este documento consultivo:

* Formula recomendaciones para abordar los obstáculos que impiden lograr una mayor convergencia en la notificación de incidentes cibernéticos con miras a promover mejores prácticas;
* Avanza en el trabajo para desarrollar terminologías comunes en torno al ciberespacio; y
* Propone el desarrollo de un formato para el intercambio de notificación de incidentes (FIRE) para promover la convergencia, abordar los desafíos operativos derivados de la notificación a múltiples autoridades y fomentar una mejor comunicación.

El FSB está invitando a comentarios sobre este documento consultivo, en particular sobre las preguntas establecidas en el informe. Las respuestas deben enviarse a [fsb@fsb.org](mailto:fsb@fsb.org) a más tardar el 31 de diciembre de 2022 con el asunto «Convergencia RCDI». Las respuestas se publicarán en el sitio web del FSB a menos que los encuestados soliciten expresamente lo contrario.

Tipo(s) de contenido: [Consultas](https://www.fsb.org/content_type/publications/consultations/), [Consultas actuales](https://www.fsb.org/content_type/publications/current-consultations/), [Publicaciones](https://www.fsb.org/content_type/publications/), [Informes al G20](https://www.fsb.org/content_type/publications/reports-to-the-g20/)



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 creciente interconexión del sistema financiero aumenta la probabilidad de que un incidente cibernético en una institución financiera (IF) (o un incidente en uno de sus proveedores de servicios externos) tenga 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 cumplir con este llamado, el FSB buscó comprender los impedimentos para lograr una mayor armonización en la notificación de incidentes y estableció recomendaciones para abordarlos (ver más abajo). El FSB Cyber Lexicon también se actualizó para incluir términos y definiciones relacionados con los incidentes cibernéticos, ya que tener un lenguaje común es esencial para lograr la convergencia en CIR. Estas iniciativas ayudarán a promover la resiliencia cibernética a medida que el panorama de amenazas se vuelve cada vez más complejo.

Para complementar este trabajo, el FSB presenta un concepto de un formato común para el intercambio de informes de incidentes (FIRE) que las autoridades financieras podrían desarrollar aún más y eventualmente usar para recopilar información de incidentes de las IF, y para que las autoridades lo utilicen para compartir información. Se prevé que FIRE sea flexible para permitir una gama de opciones de adopción e incluir los elementos de datos más relevantes para las autoridades financieras. El concepto de FIRE aprovecha el análisis de varias plantillas de informes de incidentes, que identificaron muchos puntos en común en los datos que las autoridades financieras recopilan para cumplir con sus objetivos de informes.

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. 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 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 formatos comunes 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. 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. 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, incluido el complemento de la orientación del RCDI con ejemplos y la participación de las instituciones financieras.

8. Amplíe los desencadenantes basados en la materialidad para incluir posibles infracciones. Las autoridades financieras que utilizan umbrales de materialidad deben explorar el ajuste del lenguaje del umbral, o utilizar otros enfoques equivalentes, para alentar a las instituciones financieras a notificar incidentes en los que aún no se hayan cumplido los criterios de notificación, pero es probable que se incumplan.

9. Revisar la efectividad de los procesos CIR. Las autoridades financieras deben explorar formas de revisar la efectividad de los procesos y procedimientos del RCDI de las IF como parte de su compromiso supervisor o regulatorio existente.

10. Llevar a cabo la recopilación de datos ad-hoc y la participación de la industria. 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.

1. 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, la creación de un lenguaje común relacionado con la cibernética a través del desarrollo de un léxico cibernético y el establecimiento de un conjunto de herramientas de prácticas efectivas para la respuesta y recuperación de incidentes cibernéticos. En muchas jurisdicciones, las autoridades financieras han introducido requisitos CIR para las IF, 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. Más recientemente, reconociendo la importancia de los desafíos y los beneficios potenciales, el FSB ha llevado a cabo trabajos para lograr una mayor convergencia en el RCDI de tres maneras.

■ En primer lugar, a partir de una encuesta a los miembros del FSB realizada a principios de 2022, el FSB identificó puntos en común en los marcos del RCDI (detallados en el Anexo 1) y cuestiones prácticas asociadas con la recopilación de información sobre incidentes cibernéticos de las IF y el intercambio posterior entre las autoridades financieras (Sección 2). Sobre la base de la experiencia de las autoridades financieras y el compromiso con las instituciones financieras, se formularon 16 recomendaciones (Sección 3) para abordar estas cuestiones prácticas que plantean desafíos para lograr una mayor convergencia en el RCDI: i) desafíos operativos 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.

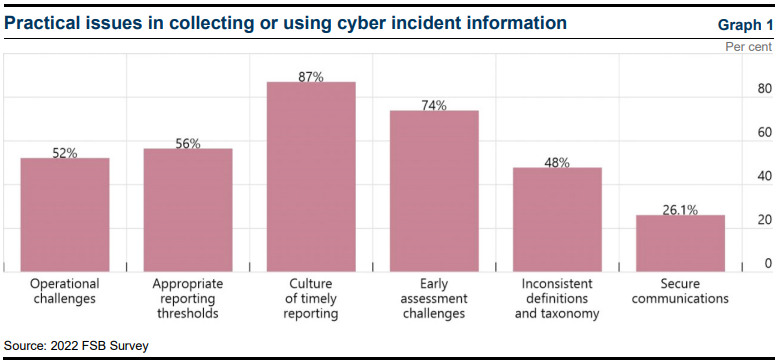
■ En segundo lugar, se mejoró el Cyber Lexicon para incluir términos adicionales relacionados con el RCDI (Sección 4). Los regímenes armonizados de RCDI requieren una «lengua común». En particular, se necesita una definición y comprensión comunes de lo que constituye un «ciber incidente» que evite la notificación excesiva de incidentes que no son significativos para una IF o la estabilidad financiera. De los más de 80 términos que se revisaron para su inclusión o enmienda al Cyber Lexicon, se agregarán cuatro términos (Insider Threat, Phishing, Ransomware, Security Operations Centre) y tres definiciones serán revisadas (Cyber Incident, Cyber Incident Response Plan, Information System).

■ Y, por último, el FSB identificó tipos comunes de información que deben compartirse entre jurisdicciones y sectores (Sección 5), informada por una revisión de los requisitos y plantillas de información de las autoridades financieras. Los tipos de información que las IF deben comunicar se refieren a: quién emitió el informe y a quién se envió; información sobre el incidente; lo que llevó al incidente; evaluación de impacto; y qué medidas correctivas se adoptarán. Para facilitar nuevos desarrollos en el intercambio de información y la convergencia en CIR, el FSB presenta el concepto FIRE que podría considerarse más a fondo entre las IF y las autoridades financieras.

2. Desafíos para lograr una mayor convergencia en el RCDI

La encuesta de 2022 aumentó y refinó el balance en 2021,5 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 (notificación iniciada por la entidad). (Consulte el Anexo 1 para un análisis más detallado de los resultados de la encuesta).

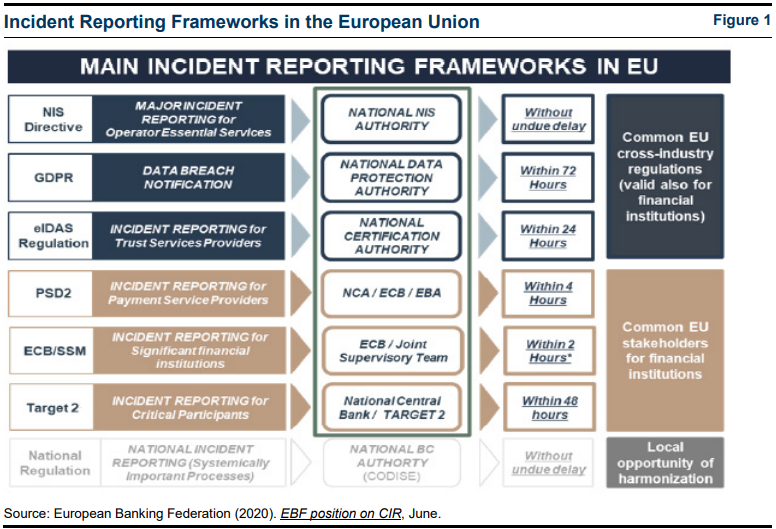
La encuesta también encontró que pueden surgir diferencias en los requisitos de presentación de informes debido a diferentes objetivos y mandatos de política, así como diferencias en el tamaño, las actividades comerciales y los servicios de las instituciones financieras. Los diferentes requisitos de 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 la información notificada sobre incidentes cibernéticos.6 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.



2.1. Retos operativos

La notificación de incidentes cibernéticos iniciada por las instituciones financieras generalmente se desencadena al exceder los criterios implícitos o explícitos y normalmente se asocia con obligaciones específicas de notificación, como el requisito de enviar 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; en particular para las instituciones financieras que operan en muchas jurisdicciones y sectores y están sujetas a múltiples requisitos de notificación para un incidente, y cada notificación tiende a desencadenar consultas de seguimiento de cada autoridad financiera. Además, muchas IF deben notificar a las fuerzas del orden, los seguros cibernéticos, los grupos de intercambio de amenazas de la industria, los clientes y las partes interesadas dentro de los 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 notificaciones escritas, completar y enviar 12-14 formularios iniciales de informe de incidentes e ingresar detalles en 5-9 portales de informes en línea.7 Cada notificación es editada y revisada por los equipos de respuesta a incidentes para garantizar que sea técnicamente precisa 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.

2.2. 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 factores 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 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 punto en el que una autoridad desea ser informada de un incidente cibernético estará impulsado en gran medida por su mandato institucional o enfoque regulatorio o de supervisión general. 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. Dado que los obstáculos a la convergencia son fundamentales por naturaleza, es muy poco probable que puedan superarse. 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.

2.3. 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;

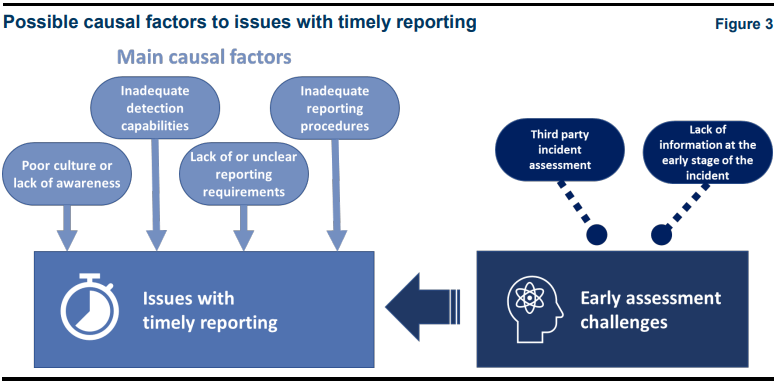
■ temor a daños a la reputación o a un mayor escrutinio por parte del supervisor;

■ capacidades de detección inadecuadas en las instituciones financieras que conduzcan a una detección tardía de los ciber incidentes y a la evaluación de los posibles impactos;

■ 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; o

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

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.



2.4. 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.

Las tensiones 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.

2.5. 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.

3. 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. 11 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.

3.1. Diseño del enfoque del RCDI

Las autoridades financieras deben revisar la cobertura y la idoneidad de los cinco objetivos de información comúnmente identificados (véase el anexo 1) 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 siguen satisfaciendo las necesidades de todas las partes interesadas pertinentes.

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 un formato común de presentación de informes puede ocurrir en tres escalas diferentes que aumentan gradualmente en términos de alcance, complejidad y ambición (que se describe 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. Los formatos comunes para la presentación de informes 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.

Los informes iniciales de incidentes cibernéticos deben tener como objetivo contener un conjunto mínimo de elementos de información que luego pueden 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, los recursos y esfuerzos de la IF afectada se centran principalmente en la respuesta al incidente 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.

Para cada tipo de notificación, el proceso para determinar el desencadenante de la notificación debe tener como objetivo resultados que sean proporcionados, comprensibles y justificables.

■ Para la presentación de informes iniciada por la institución, la principal elección de diseño es si se deben anclar los requisitos de presentación de informes en relación con un punto específico en el tiempo (es decir, ocurrencia o detección) o criterios de umbral predefinidos. 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.

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.

3.2. Compromiso supervisor con las instituciones financieras y entre las autoridades financieras

La revisión periódica de los procesos y procedimientos del RCDI de las IF puede identificar posibles lagunas 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 afín 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.

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.

3.3. Compromiso de la industria

El compromiso continuo entre las autoridades financieras y las empresas puede ayudar a desarrollar un entendimiento común con respecto al marco y los criterios para el RCDI. Las discusiones también pueden cubrir las medidas legales y técnicas establecidas 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. Las orientaciones podrían ayudar a mejorar la claridad de la notificación inicial y ayudar a normalizar la calidad de la información intermedia y final cuando la institución informante disponga de más información (por ejemplo, si incluir indicadores de compromiso u otra información más detallada).

3.4. Desarrollo de capacidades (individuales y compartidas)

El proceso para informar un incidente comienza antes de que ocurra un incidente y, a menudo, está influenciado por elementos del programa y los procesos de respuesta y recuperación de incidentes cibernéticos (CIRR) de una institución. Para fomentar la preparación en torno a la detección y notificación de incidentes, las IF deben considerar la adopción de prácticas descritas en el kit de herramientas de Prácticas Efectivas para la Respuesta y Recuperación de Incidentes Cibernéticos del FSB. 12 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, especialmente 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.

Prácticas relevantes del kit de herramientas del CIRR:

■ 8. Métricas: Las organizaciones establecen métricas para medir el impacto de un incidente cibernético y para informar a la gerencia el desempeño de las actividades de CIRR. Las métricas se pueden utilizar para determinar la gravedad o la prioridad de un incidente. El nivel de gravedad informará qué tan rápido se debe manejar el incidente y a quién se puede escalar.

■ 9. Recursos: Las organizaciones se aseguran de que las funciones del CIRR cuenten con el personal adecuado y de que las competencias del personal pertinente se mantengan y mejoren regularmente.

■ 13. Planificación de escenarios y pruebas de estrés: Los planes y libros de jugadas de las organizaciones incluyen escenarios cibernéticos severos pero plausibles y pruebas de estrés.

■ 15. Centro de operaciones de seguridad (SOC): Dependiendo de su tamaño, complejidad y riesgos, las organizaciones operan un SOC 24x7 o contratan servicios de seguridad de terceros para satisfacer las necesidades de la organización para detectar, identificar, investigar y responder a incidentes cibernéticos que podrían afectar la infraestructura, los servicios y los clientes de la organización. Se utilizan varias herramientas, incluido el aprendizaje automático, para la gestión de vulnerabilidades y el monitoreo del cumplimiento para mejorar la efectividad del análisis de incidentes cibernéticos.

■ 17. Gestión de registros y capacidades forenses. Las organizaciones desarrollan un marco eficaz de gestión y retención de registros que se compone de herramientas para administrar, recopilar y almacenar registros del sistema que serían necesarios para facilitar la investigación y el análisis de incidentes. Los tipos de registros que deben recopilarse y el período de retención de los registros podrían determinarse previamente en función de la reglamentación de supervisión, la ley o la importancia de los datos comerciales mantenidos o transportados a través del sistema. Las organizaciones establecen capacidades técnicas y forenses para preservar la evidencia y analizar fallas de control, identificar problemas de seguridad y otras causas relacionadas con un incidente cibernético. Si la organización no tiene sus propias capacidades forenses, se establecen acuerdos contractuales con proveedores de servicios externos (por ejemplo, servicios de retención forense) para respaldar investigaciones forenses cibernéticas extendidas, que se activan inmediatamente cuando es necesario.

■ 18. Soluciones tecnológicas y proveedores: Las organizaciones implementan tecnologías para hacer cumplir sus políticas y procedimientos. Las organizaciones adquieren proactivamente servicios de terceros si es necesario para aumentar sus capacidades internas de CIRR.

■ 23. Fuentes de información confiables: Las organizaciones correlacionan una variedad de fuentes de información internas y externas para una evaluación rápida de amenazas y un análisis de la causa raíz del incidente cibernético.

4. Terminologías comunes para CIR

Un instrumento clave para lograr la convergencia en el RCDI es el uso de un lenguaje común. En particular, es necesaria una definición común de «ciber incidente» que evite la notificación de incidentes que no sean significativos para una IF, a efectos de supervisión o estabilidad financiera. Las definiciones y taxonomías inconsistentes relacionadas con la seguridad cibernética en las IF se citan como un desafío en la implementación de marcos CIR. 13

En 2018, el FSB publicó el Cyber Lexicon, que tenía una serie de objetivos clave: i) permitir una comprensión común intersectorial de la terminología relevante de ciberseguridad y ciber resiliencia; ii) mejorar el trabajo para evaluar y monitorear los riesgos para la estabilidad financiera de los escenarios de riesgo cibernético; iii) facilitar el intercambio de información según proceda; y iv) ayudar al trabajo del FSB y / o los organismos de establecimiento de estándares para proporcionar orientación relacionada con la seguridad cibernética y la resiliencia cibernética, incluida la identificación de prácticas efectivas.

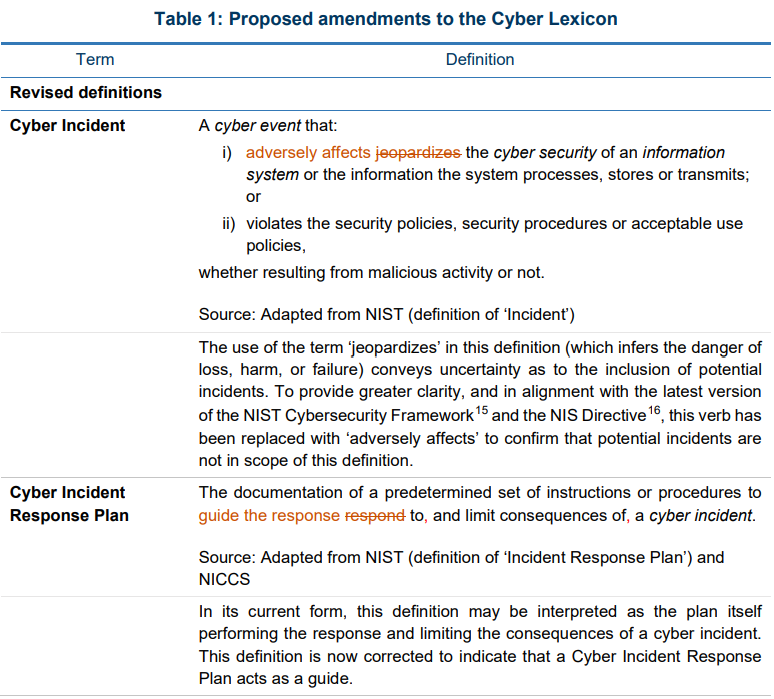
Muchas autoridades utilizan el Cyber Lexicon en sus orientaciones o informes internos, y en menor medida, en sus conversaciones con las instituciones financieras. En algunos casos, el Cyber Lexicon se tiene en cuenta en la redacción de alertas, políticas, procedimientos y orientación de riesgos relacionados con el ciberespacio, así como en las evaluaciones de supervisión y regulación. El Cyber Lexicon es generalmente bien reconocido por las IF y muchos términos son utilizados por las autoridades nacionales en sus comunicaciones y discusiones con las IF. Sin embargo, las IF no necesariamente lo utilizan para sus fines internos de gestión de riesgos, ya que se basan en terminologías y definiciones utilizadas en los estándares de seguridad cibernética que adoptan.

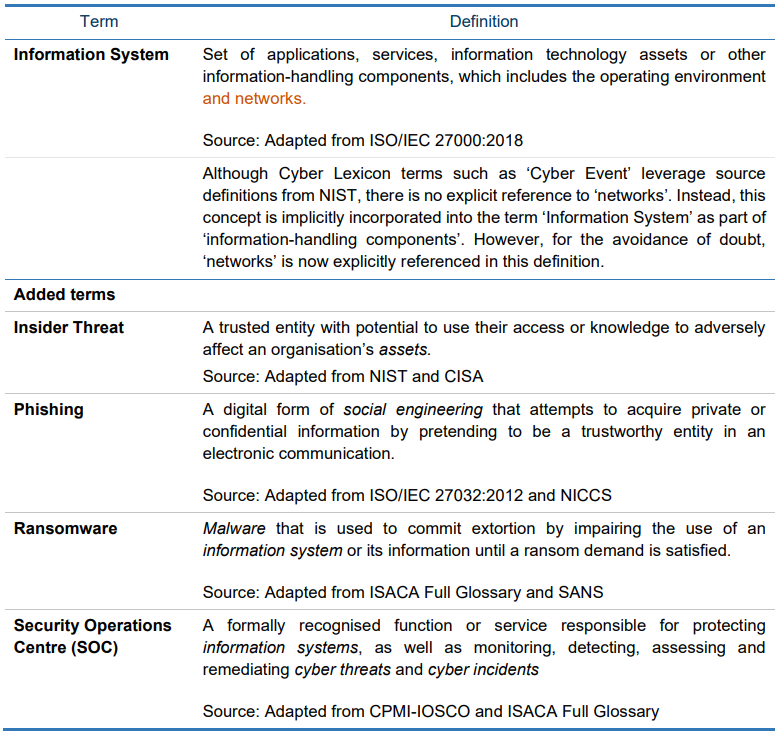
Más específicamente, solo unas pocas autoridades utilizan la definición de "incidente cibernético" del Léxico Cibernético. Todas las demás autoridades utilizan su propia definición, que normalmente se establece en reglamentos o directrices. Estos van desde definiciones de alto nivel, como "un compromiso real o potencial de la seguridad de la información", o "cualquier tipo de interrupción de la prestación de servicios bajo obligaciones de licencia", hasta definiciones más complejas y detalladas.

Algunas autoridades ven la necesidad de actualizar el Léxico Cibernético para mantenerse al día con el panorama cibernético en evolución y el desarrollo de la tecnología de la información. Por ejemplo, dado el aumento de las amenazas cibernéticas debido a los acuerdos prolongados de trabajo remoto a la luz de COVID-19 y el aumento de la dependencia de proveedores de servicios externos, varias autoridades sugirieron incluir términos como 'phishing', 'ransomware' y 'cadena de suministro', junto con otros términos relacionados con dependencias de terceros y resiliencia operativa. Como tal, este trabajo se está realizando en colaboración con el grupo de trabajo del FSB sobre el riesgo de terceros para garantizar que los términos relacionados con el ciberespacio sobre el riesgo de terceros se consideren para su futura inclusión en el Cyber Lexicon o se incluyan en el resultado de ese flujo de trabajo. Esta colaboración es aún más importante dada la creciente prevalencia de incidentes derivados de las cadenas de suministro de las IF.

Como parte del trabajo sobre CIR, se revisó el Cyber Lexicon para incluir una serie de términos nuevos y proporcionar aclaraciones sobre algunas definiciones existentes. Para garantizar la coherencia con un documento que se ha implementado desde hace algunos años, se aplicaron los mismos criterios de inclusión y exclusión en el desarrollo del Léxico Cibernético. Para ser incluidos, los términos deben cumplir con los objetivos del Léxico Cibernético (ver arriba) y deben centrarse en los términos básicos necesarios para apoyar estos objetivos. Los términos que se excluyen son generalmente términos técnicos y términos que utilizan los participantes del sector financiero en áreas que van más allá de la seguridad cibernética y la resiliencia cibernética. Las definiciones de los términos en el Cyber Lexicon deben extraerse de fuentes existentes, ser exhaustivas, concisas y utilizar un lenguaje claro y sencillo y evitar términos técnicos y construcciones gramaticales complejas.

A la luz de los recientes desarrollos en el panorama de las amenazas cibernéticas, los términos: "amenaza interna", "phishing" y "ransomware" se consideraron lo suficientemente significativos para su inclusión, en línea con los criterios de inclusión descritos anteriormente. Además, el término "centro de operaciones de seguridad" se consideró una función esencial de muchas instituciones financieras, que desempeñan un papel integral en la detección y gestión de incidentes cibernéticos y beneficiarían la inclusión para avanzar aún más en el trabajo sobre RCDI. Sobre la base de las conversaciones iniciales con la industria, y a través de los comentarios de las autoridades financieras, se consideró importante revisar las siguientes definiciones: «ciber incidente», «plan de respuesta a ciber incidentes» y «sistema de información». En el cuadro 1 se enumeran las modificaciones del Cyber Lexicon.





5. Formato para el intercambio de informes de incidentes (FIRE)

El balance de 2021 de los regímenes RCDI de las autoridades indicó un alto grado de similitud en los requisitos de información para los informes de incidentes cibernéticos. Un examen más detallado de los distintos campos de datos dentro de las plantillas de presentación de informes existentes corroboró aún más esta conclusión, es decir, que los tipos de información notificada no variaban mucho entre las autoridades, en ninguno de los tipos de notificación identificados (por ejemplo, iniciada por la institución, iniciada por la autoridad y presentación periódica).

El alto grado de similitud ofrece una oportunidad para una mayor convergencia que merece una mayor consideración. Concretamente, la convergencia de los requisitos de información sobre incidentes mediante el desarrollo y la adopción de un formato común de presentación de informes podría mejorar en gran medida las prácticas de notificación de incidentes a nivel mundial, abordar los problemas operacionales y fomentar una mejor comunicación.

El concepto FIRE se propone como un enfoque para estandarizar los requisitos comunes de información para la notificación de incidentes, sin dejar de ser flexible a una serie de prácticas de implementación. Ese formato, si se sigue desarrollando, no requeriría una convergencia mundial estricta y podría ser flexible para considerar la coexistencia. Las autoridades pueden decidir en qué medida desean adoptar FIRE, si es que lo hacen, en función de sus circunstancias individuales. Por ejemplo, las autoridades podrían considerar la posibilidad de aprovechar un subconjunto de las características o definiciones, lo que promovería una forma limitada de convergencia. Incluso si no es adoptado por una sola jurisdicción, podría servir como una base de referencia común para que las instituciones financieras se comparen con una serie de requisitos de presentación de informes y ayuden a traducir entre los marcos existentes.

En términos de alcance, FIRE podría abordar los requisitos de información para la presentación de informes iniciada por las instituciones, que es donde se observan con mayor intensidad las cuestiones prácticas. Sin embargo, los requisitos de presentación de informes periódicos e iniciados por la autoridad pueden no aumentar significativamente el trabajo y, por lo tanto, también pueden considerarse desde el principio. FIRE también apoyaría cuatro recomendaciones del CIR: lograr una mayor convergencia en los marcos del CIR, promover la adopción de un formato común de presentación de informes (# 3), apoyar la implementación de requisitos de presentación de informes por fases e incrementales (# 4) y fomentar la comprensión mutua de los beneficios de la presentación de informes (# 12).

El alcance de FIRE sería más sólido si cubriera todas las formas de incidentes operativos, no solo los incidentes cibernéticos. Como se señaló en el balance de 2021, la mayoría de las autoridades no distinguen entre incidentes operativos más amplios e incidentes cibernéticos como parte de sus regímenes de notificación de incidentes. Por lo tanto, la utilidad de FIRE podría verse fuertemente influenciada por su capacidad para satisfacer las necesidades de tales autoridades. De lo contrario, un concepto limitado a los incidentes cibernéticos podría introducir fragmentación y duplicación en el mercado, lo que va en contra de los objetivos de convergencia.

Dadas las implicaciones para el sector financiero, la intención sería utilizar el poder de convocatoria del FSB para reunir a las autoridades financieras, las IF reguladas y otras partes relevantes para explorar la viabilidad de FIRE, aprovechando la experiencia de presentación de informes de todas las partes y teniendo en cuenta esfuerzos similares relacionados con la convergencia de datos en contextos superpuestos para evitar duplicaciones innecesarias. La propiedad y el mantenimiento a largo plazo de FIRE tendrían que ser abordados por las partes interesadas clave, preferiblemente desde el principio, como un factor crítico para el éxito general y la sostenibilidad del proyecto.

5.1. Beneficios, riesgos y costes potenciales

5.1.1. Beneficios potenciales

FIRE estaría diseñado para obtener varios beneficios tanto para las autoridades financieras como para las IF, que incluyen:

■ Flexibilidad para la aplicación por parte de las autoridades. El concepto FIRE se diseñaría con flexibilidad en su núcleo, para permitir un grado de divergencia permisible para satisfacer las necesidades locales y la posible innovación futura en los requisitos de notificación de incidentes.

■ Abordar las fuentes de los desafíos operativos: El concepto FIRE tiene el potencial de reducir los desafíos operativos en las IF al promover una mayor convergencia en las siguientes áreas, permitiendo así a las IF dedicar una mayor proporción de recursos a resolver incidentes y abordar sus causas.

■ Mejorar las capacidades para apoyar el objetivo de presentación de informes. Sobre la base de los objetivos comunes de información para las autoridades financieras identificados en el Anexo 1: Sección 2, FIRE tiene el potencial de racionalizar las capacidades comparativas y analíticas que aprovechan los conjuntos de datos de incidentes. En particular, los elementos estructurados de un formato común de notificación facilitan la capacidad de comparar y contrastar los incidentes sobre una base histórica, transfronteriza o intersectorial. Estos atributos podrían ser de particular beneficio en la realización de un análisis más sistemático de la presentación de informes para identificar tendencias o causas profundas comunes y facilitar una cooperación transfronteriza más estrecha a través de una comprensión común de un incidente a medida que se informa.

■ Permitir la automatización. La estandarización propuesta dentro de FIRE puede facilitar una reducción de los gastos generales manuales dentro de los procesos de informes existentes mediante la introducción de la automatización, generando así una mayor eficiencia.

■ Eficiencia en el uso de los recursos: En lugar de que las autoridades individuales gasten recursos para resolver un problema común, FIRE representa un esfuerzo de colaboración que puede beneficiarse del conocimiento y la experiencia colectivos de todos los participantes, para producir un resultado utilizable por todos. Aquellas autoridades que no participen directamente en el desarrollo de FIRE, y que aún no hayan establecido sus propios requisitos de formato de presentación de informes, podrían aprovechar el producto final sin incurrir en los costos asociados. Además, las autoridades financieras y las instituciones financieras pueden implementar soluciones comunes de presentación de informes que se desarrollan posteriormente para respaldar FIRE.

■ Fomentar el cambio a nivel de los ecosistemas. Para instigar el cambio a mayor escala, la iniciativa también se beneficiaría de apoyar soluciones para instituciones financieras pequeñas o medianas que pueden no tener la capacidad interna para implementar FIRE. Para este fin del mercado, es posible que terceros proveedores de servicios o productos de gestión de incidentes puedan diseñar sus sistemas para soportar FIRE, promoviendo así una mayor utilidad en todo el ecosistema financiero. Con ese fin, puede ser beneficioso involucrar a este grupo de partes interesadas como parte del equipo de diseño, de modo que estas soluciones puedan estar disponibles al principio del proceso.

5.1.2. Riesgos y costes potenciales

Un programa de transformación de esta magnitud no está exento de riesgos y costes, y requiere la inversión de tiempo, esfuerzo y recursos para desarrollar plenamente su potencial. A continuación se resumen las posibles fuentes de riesgo y los costos que podrían detener o impedir esta iniciativa propuesta o disminuir sus beneficios previstos.

Riesgos potenciales

■ Falta de patrocinio de proyectos: Falta de apoyo suficiente entre las partes interesadas y compromiso con el programa de transformación plurianual.

■ Niveles de adopción insuficientes: Ya sea por elección o en función de las circunstancias, no se logra alcanzar la masa crítica y, por lo tanto, conferir los máximos beneficios.

■ Desajuste localizado en el apetito: La decisión de no proceder por parte de una autoridad financiera puede ser impugnada localmente por las IF que tienen un mayor deseo de aceptación.

■ Posiciones de diseño irreconciliables: Las opiniones divergentes sobre el diseño de los elementos de FIRE pueden reducir el grado de convergencia o dar lugar a enfoques competitivos.

■ Riesgo de mantenimiento a largo plazo: Sería necesario determinar la propiedad y el proceso para el desarrollo futuro de FIRE.

Costos potenciales

■ Disposiciones transitorias: Es posible que las autoridades financieras tengan que apoyar la recepción de información de notificación de incidentes tanto preexistente como basada en FIRE mientras las IF reguladas migran.

■ Ajustes de políticas: Puede haber costos de implementación involucrados en el cambio de políticas y reglas regulatorias existentes para apoyar la implementación.

■ «coste de entrada» poco atractivo: Los costes generales excepcionales relacionados con la aplicación y la migración pueden ser menos aceptables que los actuales gastos generales recurrentes de los desafíos operativos.

5.2. El concepto FIRE

En esta sección, las opiniones iniciales sobre el concepto FIRE se han limitado a la presentación de informes iniciada por las instituciones, aunque también pueden incorporarse otros tipos de informes. Es importante destacar que las ideas transmitidas en esta sección deben considerarse como material inicial para futuras discusiones sobre cómo se podría construir un concepto.

Además, una articulación basada en texto de los requisitos de datos, con sus reglas de formato y lógica que los acompañan, puede estar abierta a interpretaciones erróneas. Para eliminar este riesgo de interpretación, puede ser necesario codificar el concepto final en uno o más formatos de intercambio de datos de uso común, como JSON o XBRL, lo que también facilitará la implementación técnica.

5.2.1. Estructura conceptual

Para determinar una estructura organizativa adecuada para los requisitos de información dentro del concepto propuesto, se utilizó un enfoque de "reunión intermedia" para informar la estructura general:

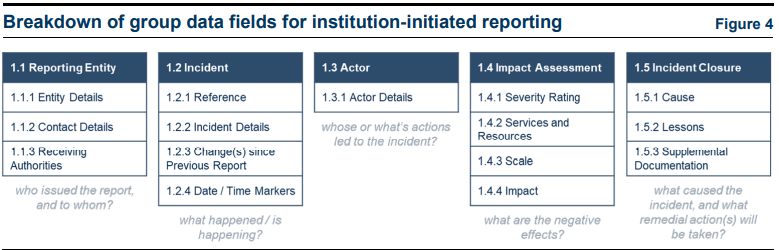
■ Ascendente: utilizando los resultados del ejercicio de mapeo granular de datos sobre el terreno realizado en las plantillas de informes existentes, que identificó el conjunto mínimo de tipos comunes de información.

■ Descendente: puesta en común de los requisitos de información con un objetivo común.

Al agrupar los requisitos comunes de datos, surgieron patrones claros de superposición sobre los cuales se basó la premisa de este concepto. La decisión de centrar inicialmente el diseño FIRE en la presentación de informes iniciados por las instituciones se basó en: (i) ser el tipo de informe más común implementado por las autoridades; y (ii) donde los problemas prácticos se observaron con mayor frecuencia.

Aunque los detalles varían, la premisa subyacente para la notificación iniciada por la institución es compartida por todas las autoridades, es decir, una IF experimenta un incidente que, dependiendo de las circunstancias, da lugar a una obligación de informar a una o más autoridades receptoras. La naturaleza de los flujos de información está impulsada por eventos y es unidireccional desde la entidad informante hasta las autoridades receptoras. Dependiendo de los requisitos de informes individuales, es posible que sea necesario emitir más de un informe de incidente para el mismo incidente.

Desde el punto de vista descendente, los requisitos de información para la presentación de informes iniciados por las instituciones se agruparon en cinco colecciones distintas (como se muestra en la Figura 4). En conjunto, estos campos de datos proporcionan a las autoridades receptoras la información necesaria para comprender los incidentes a medida que evolucionan y actuar en consecuencia. Cada una de las subsecciones subsiguientes desarrolla cada colección y los tipos de información que podrían definirse en un futuro diseño conceptual.



Entidad informante

Los campos de datos asociados a la entidad informante están destinados a describir:

■ Detalles de la entidad. Los campos de datos considerados contienen información básica de referencia y clasificación para la entidad informante. Con la excepción del nombre de la entidad, que refleja la designación legal o más comúnmente utilizada de la entidad, los campos restantes están estructurados para respaldar el análisis en todo el conjunto de datos de la entidad informante, dentro y entre las autoridades informantes. Los sistemas de identificación podrían apoyar tanto los mecanismos mundiales (por ejemplo, el identificador de personas jurídicas (IPJ))17 como las implementaciones locales preexistentes. Para el tipo de entidad, existe una elección de diseño entre: i) utilizar los esquemas de clasificación existentes (por ejemplo, la Clasificación Industrial Internacional Uniforme)18 que pueden actuar como fuente de referencia autorizada pero pueden ser insuficientemente granulares; y ii) desarrollar un sistema de clasificación a medida que proporcione la máxima flexibilidad. La información básica también podría incluir referencias al país donde está domiciliada la entidad afectada.

■ Información de contacto. Por lo general, se requieren puntos de contacto designados dentro de las entidades en caso de que una autoridad receptora requiera más información después de la presentación de un informe de incidente. Por lo tanto, FIRE tendría que apoyar la recopilación de información de contacto para esos representantes.

Incidente

Los siguientes campos de datos consolidan los requisitos de información relacionados con el incidente que se informa, como los identificadores únicos generados por la entidad o la autoridad para el incidente que se informa, u otros incidentes que puedan estar relacionados; la naturaleza y las circunstancias del incidente, que se incrementan y perfeccionan a medida que evoluciona el incidente; las medidas adoptadas o las reacciones al incidente que hayan tenido lugar desde el informe anterior del incidente; e información sobre el calendario de los hitos clave de los incidentes.

■ Referencias. Para apoyar el seguimiento de incidentes individuales y posibles interdependencias, FIRE puede necesitar incluir múltiples campos de referencia de identificación que sirven para diferentes propósitos. Estos campos podrían incluir los identificadores únicos utilizados internamente por la entidad informante para referirse al incidente o cualquier incidente relacionado. Del mismo modo, FIRE puede necesitar almacenar referencias generadas por la autoridad utilizadas para identificar un incidente reportado o crear relaciones entre incidentes reportados por múltiples entidades. Cuando se combinan con el intercambio ulterior entre autoridades, los identificadores proporcionados por la entidad podrían actuar como una clave única entre las autoridades cuando se relacionan con la entidad informante, de forma individual o colectiva.

■ Detalles del incidente. Esta sección describe los posibles atributos básicos para un incidente, que podrían incluir: la fase de los informes de incidentes y el estado del incidente relacionado (como se muestra en la Figura 5); el título y la descripción del incidente, que proporcionan un reflejo general del incidente en diferentes niveles de granularidad; el tipo de incidente, que refleja el evento que ha ocurrido de manera independiente de la causa; el método por el cual la entidad afectada tuvo conocimiento del incidente; el nivel de confianza que la entidad informante tiene en la información facilitada en el informe; los criterios que dieron lugar a la obligación de información; y un tiempo estimado de resolución para cuando se espera que el incidente esté bajo control.

