Encender un FUEGO bajo informes de incidentes cibernéticos: ¿se necesita un formato digital?



Publicado el octubre 21, 2022 por [**Editor**](https://www.xbrl.org/news/lighting-a-fire-under-cyber-incident-reporting-digital-first-format-needed/)

El Consejo de Estabilidad Financiera (FSB) ha publicado un documento consultivo sobre cómo lograr una mayor convergencia en la notificación de incidentes cibernéticos. *"La información oportuna y precisa sobre incidentes cibernéticos es crucial para una respuesta y recuperación efectivas de incidentes y para promover la estabilidad financiera",*observa.

Un aspecto importante de las propuestas del FSB es el desarrollo de un formato común para el intercambio de informes de incidentes (FIRE). Ya ha encontrado un alto grado de similitud en los requisitos de información para los informes de incidentes cibernéticos. *"Sobre la base de estos puntos en común, el FSB propone el desarrollo de un formato de información común que podría ser considerado más a fondo entre las instituciones financieras y las autoridades financieras".*

El documento consultivo ofrece una estructura preliminar para el concepto FIRE como material semilla para futuras discusiones. Fundamentalmente, señala que: *"una articulación basada en texto de los requisitos de datos, con su formato y reglas lógicas, 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".*

Por supuesto, en XBRL International recomendamos encarecidamente el uso de XBRL para garantizar la comparabilidad global de los datos de incidentes cibernéticos, así como para facilitar un análisis rápido, efectivo y dinámico. XBRL es ahora también un formato de informes muy familiar para la mayoría de las instituciones financieras. Alentamos a los miembros interesados de la comunidad de informes digitales a responder a la consulta, e instamos al FSB a no perder tiempo en adoptar un enfoque digital. Las respuestas deben presentarse antes del 31 de diciembre de 2022.

Lea más aquí y [aquí](https://www.fsb.org/2022/10/fsb-makes-proposals-to-achieve-greater-convergence-in-cyber-incident-reporting/).

[DIGITALIZACIÓN DE CIBERSEGURIDAD](https://www.xbrl.org/tag/cybersecurity/) [FSB](https://www.xbrl.org/tag/fsb/) [REPORTING](https://www.xbrl.org/tag/reporting/) [XBRL](https://www.xbrl.org/tag/xbrl/)

FSB hace propuestas para lograr una mayor convergencia en la notificación de incidentes cibernéticos

17 octubre 2022

Consultas de prensa: +41 61 280 8477
press@fsb.org
Ref: 31/2022

El Consejo de Estabilidad Financiera (FSB) publicó hoy un [documento consultivo sobre cómo lograr una mayor convergencia en la notificación de incidentes cibernéticos](https://www.fsb.org/2022/10/achieving-greater-convergence-in-cyber-incident-reporting-consultative-document/). La información oportuna y precisa sobre incidentes cibernéticos es crucial para una respuesta y recuperación efectivas de incidentes y para promover la estabilidad financiera. Las propuestas adoptan un enfoque integral e incluyen:

* **Recomendaciones para abordar los desafíos para lograr una mayor convergencia en la notificación de incidentes cibernéticos.**Basándose en la experiencia de las autoridades financieras y el compromiso con las instituciones financieras, el FSB ha establecido 16 recomendaciones para abordar los problemas prácticos asociados con la recopilación de información sobre incidentes cibernéticos de las instituciones financieras y el intercambio posterior entre las autoridades financieras.
* **Seguir trabajando en el establecimiento de terminologías comunes relacionadas con los incidentes cibernéticos.**Un instrumento clave para lograr la convergencia en la notificación de incidentes cibernéticos es el uso de un lenguaje 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 las autoridades financieras o la estabilidad financiera.
* **Propuesta para desarrollar un formato común para el intercambio de notificación de incidentes (FIRE).**Un examen de las plantillas de notificación de incidentes y un inventario de los regímenes de notificación de incidentes cibernéticos de las autoridades indicaron un alto grado de similitud en los requisitos de información para los informes de incidentes cibernéticos. Sobre la base de estos puntos en común, el FSB propone el desarrollo de un formato de información común que podría ser considerado más a fondo entre las instituciones financieras y las autoridades financieras.

El FSB está invitando a comentarios sobre este documento consultivo, en particular sobre las preguntas que ha planteado. Las respuestas deben enviarse a fsb@fsb.org antes del 31 de diciembre de 2022 con el asunto «Convergencia CIR». Las respuestas se publicarán en el sitio web del FSB a menos que los encuestados soliciten expresamente lo contrario.

**Notas para los editores**

El FSB publicó un informe sobre [*Informes de incidentes cibernéticos: enfoques existentes y próximos pasos para una convergencia más amplia*](https://www.fsb.org/2021/10/cyber-incident-reporting-existing-approaches-and-next-steps-for-broader-convergence/) en octubre de 2021. El informe encontró que existe fragmentación entre sectores y jurisdicciones en el alcance de lo que debe informarse por un incidente cibernético; metodologías para medir la gravedad y el impacto de un incidente; plazos para informar sobre incidentes cibernéticos; y cómo se utiliza la información sobre incidentes cibernéticos. Esto somete a las instituciones financieras que operan a través de fronteras o sectores a múltiples requisitos de informes para un incidente cibernético. Al mismo tiempo, las autoridades financieras reciben información heterogénea para un incidente determinado, lo que podría socavar la respuesta y las acciones de recuperación de una institución financiera. Reconociendo que la información sobre incidentes cibernéticos es crucial para acciones efectivas y promover la estabilidad financiera, el G20 solicitó al FSB que avance el trabajo para lograr una mayor convergencia en la notificación de incidentes cibernéticos.

En 2018, el FSB desarrolló un [léxico cibernético](https://www.fsb.org/2018/11/cyber-lexicon/) para fomentar una comprensión común de la terminología relevante de ciberseguridad y resiliencia cibernética en todo el sector financiero, incluida la banca, las infraestructuras del mercado financiero, los seguros y los mercados de capitales, y con otros sectores de la industria. Un léxico común podría fomentar un entendimiento común con otros sectores de la industria y facilitar la cooperación adecuada para mejorar la ciberseguridad y la ciber resiliencia.

El FSB coordina a nivel internacional el trabajo de las autoridades financieras nacionales y los organismos internacionales de normalización y desarrolla y promueve la implementación de políticas efectivas de regulación, supervisión y otras políticas del sector financiero en interés de la estabilidad financiera. Reúne a las autoridades nacionales responsables de la estabilidad financiera en 24 países y jurisdicciones, instituciones financieras internacionales, agrupaciones internacionales de reguladores y supervisores específicos del sector y comités de expertos de bancos centrales. El FSB también lleva a cabo actividades de divulgación con aproximadamente otras 70 jurisdicciones a través de sus seis Grupos Consultivos Regionales.

El FSB está presidido por Klaas Knot, presidente de De Nederlandsche Bank. La Secretaría del FSB se encuentra en Basilea, Suiza, y está alojada por el Banco de Pagos Internacionales.

Comunicado de prensa disponible como: [PDF](https://www.fsb.org/wp-content/uploads/R171022.pdf)

Tipo(s) de contenido: [Prensa](https://www.fsb.org/content_type/press/), [Comunicados de prensa](https://www.fsb.org/content_type/press/press-releases/) Fuente(s): [FSB](https://www.fsb.org/source/fsb/) Área(s) política(s): [Resiliencia cibernética](https://www.fsb.org/policy_area/cyber-resilience/)