Spread the love

El Consejo de Estabilidad Financiera (FSB) publicó el 13 de octubre de 2017 los resultados de su evaluación de las regulaciones, orientaciones y prácticas de supervisión sobre ciberseguridad. El objetivo último del ejercicio es mejorar la seguridad y la cooperación transfronteriza frente a los riesgos cibernéticos.

Reina-Teuta-de-Iliria-circa-235-200-a-C. Reina Pirata

Subyace a este ejercicio la preocupación por la posible alteración del funcionamiento de los servicios financieros a nivel nacional y también internacional como consecuencia de los ciberataques. Y, la percepción de que estos ataques cibernéticos pueden poner en peligro la estabilidad financiera. La naturaleza cambiante del riesgo cibernético para las instituciones financieras se debe a varios factores como la evolución de la tecnología o las interconexiones entre instituciones financieras y entre instituciones financieras y terceros, así como los métodos cambiantes que se utilizan para atacar y para comprometer los sistemas de tecnología de la información.

Las autoridades de todo el mundo han adoptado medidas de regulación y de supervisión para mitigar el riesgo cibernético que pesa sobre las instituciones financieras, así como para mejorar la respuesta efectiva a los ataques y hacer más eficiente su recuperación.

El informe del FSB del que se da noticia, se compone de dos documentos, uno resumido y un segundo análisis detallado de los resultados de la evaluación que tomaen cuenta las experiencias de las diversas jurisdicciones y organismos internacionales. El informe de resumen establece los temas clave planteados en septiembre de 2017 en un taller organizado por el FSB que reunió a responsables del sector público y del sector privado para discutir la ciberseguridad en el sector financiero.

Entre los resultados destacamos:

- Algunos mecanismos regulatorios actuales adoptan un enfoque específico para la ciberseguridad y / o para el riesgo de la tecnología de la información. El otro tercio se aproxima al problema como un riesgo operativo.
- Algunos ordenamientos regulatorios de la ciberseguridad incluyen la evaluación de riesgos, interconexiones de terceros, controles de acceso al sistema, recuperación después de incidentes, pruebas de sistemas y capacitación de personal.
- El 72% de las jurisdicciones tienen planes para aprobar nuevas regulaciones en 2018, o al menos guías o prácticas de supervisión que aborden la seguridad cibernética para el sector financiero

- Los organismos internacionales también abordan el problema de la ciberseguridad para el sector financiero, desde distintas perspectivas: gobernanza, análisis y evaluación de riesgos, seguridad de la información, fomento y reconocimiento de la experiencia y de la capacitación de su personal, respuesta y recuperación frente a incidentes, intercambio de información y comunicaciones, o la supervisión de las interconexiones.
- Desde el sector privado, los participantes en el taller mencionado enfatizaron que la

> ciberseguridad efectiva requiere un enfoque estratégico, prospectivo, fluido y proactivo, y destacaron la importancia de integrar la seguridad con las operaciones comerciales, así como la importancia de la comunicación de los responsables de ciberseguridad con los órganos de administración de las entidades. Expresaron su apoyo a la regulación proporcional basada en principios y basada en el riesgo, y también destacaron la importancia de un enfoque global coherente que evite múltiples esquemas regulatorios potencialmente conflictivos

Concluimos recordando que estos resultados fueron presentados en la reunión de los ministros de Finanzas del G20 y de los gobernadores de los bancos centrales en Washington DC ya que había sido precisamente el G20 en su reunión de marzo de 2017 quien había encargado al FSB está evaluación. con el objetivo último de mejorar la seguridad y la cooperación trasfronteriza.