Cyber Task Force

Final Report

El Consejo de la ORGANIZACIÓN INTERNACIONAL DE LAS COMISIONES DE VALORES

FR09/2019 JUN 2019

 **Resumen ejecutivo**

Este informe, preparado por el Cyber ​​Task Force (CTF) de IOSCO, recopila información de las jurisdicciones miembros de IOSCO con respecto a sus marcos existentes para la regulación Cyber.[[1]](#footnote-1) Tiene la intención de servir como un recurso para que los reguladores del mercado financiero y las firmas creen conciencia sobre las guías cibernéticas internacionales existentes y para alentar la adopción de buenas prácticas entre la comunidad IOSCO.

El informe examina cómo las jurisdicciones miembros de IOSCO están utilizando tres marcos cibernéticos destacados y reconocidos internacionalmente (como se explica más adelante, los “Estándares básicos”). Para evitar superposiciones o duplicaciones, el informe se centra en estos marcos cibernéticos existentes en lugar de proponer un nuevo marco o una guía prescriptiva. El informe también indica cómo tales marcos cibernéticos existentes podrían ayudar a abordar cualquier brecha identificada en los regímenes actuales de los miembros. Por último, el informe proporciona un conjunto de preguntas fundamentales que las empresas y los reguladores pueden utilizar para promover el conocimiento de las buenas prácticas cibernéticas o mejorar sus prácticas existentes.

Los hallazgos del informe y el análisis correspondiente se basan en una encuesta de las jurisdicciones miembros de IOSCO. Algunas de las principales conclusiones de este informe son:

* Calificación del riesgo cibernético: muchas jurisdicciones miembros de IOSCO consideran al cibernético como al menos uno de los riesgos más importantes que enfrentan las empresas reguladas en su jurisdicción. Sin embargo, un porcentaje significativo de los encuestados considera que Cyber ​​es un riesgo como cualquier otro o no está seguro de su posición relativa en comparación con otros riesgos.
* Coherencia con los Estándares Esenciales: La mayoría de los encuestados indicó que sus regulaciones, guías y / o prácticas de supervisión nacionales eran “generalmente consistentes” o “totalmente consistentes” con uno de los Estándares Esenciales. Si bien los principios subyacentes a los Estándares Básicos han ganado una influencia considerable en las jurisdicciones de IOSCO, no predomina ningún Estándar Básico.
* Referencia expresa a los estándares básicos: casi la mitad de los encuestados indicaron que son flexibles y no prescriptivos en cuanto a los estándares cibernéticos (estándares básicos o de otro tipo) que las empresas pueden utilizar para cumplir con las regulaciones nacionales aplicables.
* Coherencia entre los marcos nacionales de seguridad cibernética: a pesar de las diferencias jurisdiccionales, los marcos cibernéticos de la mayoría de los encuestados comparten ciertos elementos comunes.
* Actualización y mejora de los regímenes cibernéticos: más de un tercio de los encuestados informaron que han declarado públicamente planes para emitir, durante el próximo año, nuevas regulaciones, guías o prácticas de supervisión que aborden la seguridad cibernética[[2]](#footnote-2) para todo o parte de su sector financiero.

**1. Introducción**

**1.1 El panorama del riesgo cibernético**

Riesgo Cibernetico[[3]](#footnote-3) es ampliamente reconocido como una de las principales amenazas para los mercados financieros en la actualidad. Abundan los ejemplos de incidentes cibernéticos,[[4]](#footnote-4) desde violaciones de datos financieros en grandes empresas públicas multinacionales hasta incidentes de alto perfil en bancos centrales y sistemas gubernamentales. Los costos económicos potenciales de tales eventos pueden ser inmensos y el daño a la confianza pública es significativo ya que los incidentes cibernéticos podrían socavar potencialmente la integridad de los mercados financieros globales.

A medida que aumenta este riesgo, también lo han hecho los esfuerzos nacionales e internacionales para abordarlo. Durante los últimos cinco años, las autoridades nacionales, los organismos de establecimiento de normas y las organizaciones del sector privado han lanzado iniciativas para abordar el riesgo cibernético y aumentar la resiliencia cibernética[[5]](#footnote-5) de los mercados financieros y la industria.[[6]](#footnote-6)

IOSCO participa activamente en estos esfuerzos. En 2013, IOSCO publicó un documento de trabajo conjunto con la Federación Mundial de Bolsas, titulado Cyber-Crime Securities Markets and

Riesgo sistémico.[[7]](#footnote-7) En 2014, IOSCO y el Comité de Pagos e Infraestructuras de Mercado (CPMI) establecieron un grupo de trabajo conjunto sobre Ciberresiliencia en infraestructuras de mercados financieros (WGCR) que continúa monitoreando los problemas de implementación asociados con la Ciberresiliencia. Este trabajo condujo a la publicación en 2016 de la Guía CPMI-IOSCO sobre ciberresiliencia para infraestructuras de mercados financieros[[8]](#footnote-8) (Guía CPMI-IOSCO), que proporciona un marco importante para que la industria de servicios financieros aborde e implemente la ciberresiliencia para las infraestructuras de los mercados financieros. En 2016, la IOSCO también publicó un informe sobre enfoques regulatorios de la seguridad cibernética[[9]](#footnote-9) titulado Seguridad cibernética en los mercados de valores: una perspectiva internacional.[[10]](#footnote-10) El Comité Consultivo de Miembros Afiliados de la IOSCO (AMCC) también es muy activo en esta área, ayudando con las publicaciones de la IOSCO y coordinando por separado con industria en cuestiones de ciberresiliencia.

**1.2 Formación y objetivo del Cyber ​​Task Force**

Si bien ha habido un progreso significativo en el aumento de la conciencia global y la acción para abordar el riesgo cibernético, los incidentes cibernéticos continúan ocurriendo con mayor frecuencia y mayor sofisticación. La preparación es importante tanto para las entidades financieras como para los reguladores.

Para abordar estos problemas, IOSCO ha emprendido un trabajo para crear conciencia sobre la orientación cibernética internacional existente y alentar la adopción de buenas prácticas entre la comunidad reguladora de IOSCO. Para llevar a cabo este trabajo, la Junta de IOSCO estableció un Cyber ​​Task Force (CTF) en octubre de 2017.

Al establecer el CTF, la IOSCO determinó que sería más eficaz basarse en el trabajo de expertos existente sobre la orientación cibernética que intentar crear un nuevo marco o un nuevo conjunto de estándares específicamente para los miembros de la IOSCO. Por lo tanto, el CTF tomó como punto de partida el amplio cuerpo de trabajo existente impulsado por la industria creado en consulta con las autoridades del sector público. Entre ellos, identificó tres ejemplos de marcos cibernéticos ampliamente utilizados y bien recibidos (a los que se hace referencia como los “Estándares básicos”)[[11]](#footnote-11)

El objetivo principal del CTF es determinar cómo las jurisdicciones miembros de IOSCO han utilizado los Estándares Básicos y, cuando sea necesario, identificar cómo dichos estándares podrían aplicarse mejor para abordar cualquier brecha identificada entre las jurisdicciones miembros de IOSCO. Al evaluar el uso de los Estándares Básicos, el CTF también tiene como objetivo identificar y promover las prácticas sólidas de Cyber[[12]](#footnote-12) para la comunidad IOSCO.

Cuando el CTF comenzó este trabajo, no había una sola fuente que describiera cómo las jurisdicciones miembros de IOSCO estaban aplicando los Estándares Básicos o que hubiera identificado dónde existen diferencias en su aplicación. Al destacar las diversas aplicaciones de los Estándares Básicos por parte de los miembros de IOSCO, el CTF anticipa que los miembros pueden revisar sus propios estándares Cibernéticos en relación con las prácticas proporcionadas por los Estándares Básicos y, cuando sea relevante, usar los Estándares Básicos como modelo para mejorar aún más su Regímenes cibernéticos.

El informe del CTF está organizado en seis partes: una introducción, revisión de los Estándares Básicos, discusión de la encuesta emitida por el CTF, análisis de los marcos nacionales de Seguridad Cibernética de los miembros de IOSCO, análisis de cómo los miembros de IOSCO están utilizando los Estándares Básicos, y, por último, la conclusión y los próximos pasos.

**1.3 Revisión de los estándares básicos**

Los Estándares Básicos son tres marcos cibernéticos prominentes y ampliamente respetados que se están utilizando en el sector financiero en todo el mundo.[[13]](#footnote-13) A menudo se usan no de forma aislada sino en combinación con otras guías cibernéticas, como COBIT 5 para la seguridad de la información.[[14]](#footnote-14) Los Estándares Básicos también son generalmente consistentes entre sí y con otros principios cibernéticos notables,[[15]](#footnote-15) como el trabajo del Grupo de Expertos Cibernéticos del G-7.[[16]](#footnote-16) Los Estándares Básicos se describen con más detalle a continuación.

**1.3.1 Marco de seguridad cibernética del Instituto Nacional de Estándares y Tecnología (NIST)**

Publicado por primera vez en 2014 y dirigido a los operadores de infraestructuras críticas, el NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework) es un marco voluntario basado en riesgos de estándares de la industria y mejores prácticas diseñado para ayudar a las organizaciones a gestionar los riesgos de ciberseguridad.[[17]](#footnote-17) El marco permite a las organizaciones, independientemente del tamaño, el grado de riesgo de seguridad cibernética o la sofisticación de la seguridad cibernética, aplicar los principios y las mejores prácticas de gestión de riesgos para mejorar la seguridad y la resistencia de la infraestructura crítica. El marco de ciberseguridad del NIST se compone de tres partes:

* **El Núcleo del Marco** Core es un conjunto de actividades de seguridad cibernética, resultados deseados y referencias aplicables que son comunes en los sectores de infraestructura crítica. Framework Core consta de cinco funciones: identificar, proteger, detectar, responder y recuperar. Juntas, estas cinco funciones y la orientación asociada tienen como objetivo proporcionar una visión estratégica de alto nivel del ciclo de vida de la gestión de riesgos de seguridad cibernética de una organización. Luego, el Framework Core identifica categorías y subcategorías clave para cada función y las empareja con ejemplos de referencias informativas, como estándares, pautas y prácticas existentes para cada subcategoría.
* **Los Niveles de Implementación del Marco** están diseñados para definir cómo una organización ve los riesgos de seguridad cibernética y sus procesos para administrar estos riesgos. Los Niveles describen el grado en el que las prácticas de gestión de riesgos de seguridad cibernética de una organización exhiben ciertas características (p. Ej., Conscientes de riesgos y amenazas, repetibles y adaptables) para definir su lugar en un rango, desde Parcial (Nivel 1) hasta Adaptable (Nivel 4). Estos Niveles están destinados a reflejar una progresión desde respuestas informales y reactivas hasta enfoques que son ágiles y están informados sobre los riesgos.
* **El Perfil del Marco** caracteriza la alineación de estándares, pautas y prácticas con el Núcleo del Marco en un escenario de implementación específico. Por lo tanto, los perfiles se pueden utilizar para identificar formas de mejorar la seguridad cibernética comparando un perfil “actual” con un perfil “objetivo” ”. El perfil actual puede respaldar la priorización y medir el progreso hacia el perfil objetivo. Los perfiles se pueden utilizar para realizar autoevaluaciones y facilitar la comunicación dentro de una organización o entre organizaciones.

Tras las consultas, NIST lanzó la versión 1.1 del marco de ciberseguridad de NIST.[[18]](#footnote-18) La versión 1.1 es totalmente compatible con la versión 1.0 e incluye actualizaciones sobre:

* autenticación e identidad;
* autoevaluación del riesgo de seguridad cibernética;
* gestionar la seguridad cibernética dentro de la cadena de suministro; y
* divulgación de vulnerabilidades.

NIST planea lanzar una hoja de ruta actualizada para mejorar la ciberseguridad de la infraestructura crítica, que describe áreas clave de desarrollo, alineación y colaboración.

**1.3.2 Orientación CPMI-IOSCO sobre ciberresiliencia para infraestructuras de mercados financieros (Orientación CPMI-IOSCO)**

Publicada en 2016, la Guía CPMI-IOSCO se desarrolló para que la infraestructura del mercado financiero (FMI) mejore su ciberresiliencia. Dada la naturaleza dinámica de las amenazas cibernéticas, la guía se basa en principios y, en general, es coherente con los otros marcos cibernéticos, incluidos los otros dos estándares básicos. Si bien está dirigida a las FMI, la guía deja abierto a las autoridades pertinentes para que la apliquen a otra infraestructura.[[19]](#footnote-19) La Guía CPMI-IOSCO describe cinco categorías principales de gestión de riesgos y tres componentes generales que deben abordarse en el marco de ciberresiliencia de una FMI. Las cinco categorías principales de gestión de riesgos son:

* **Gobernanza:** Deben establecerse acuerdos para establecer, implementar y revisar el enfoque de la FMI para gestionar los riesgos cibernéticos. Una gobernanza eficaz debe comenzar con un marco de ciberresiliencia claro y completo. En consecuencia, se proporciona orientación sobre los elementos básicos del marco de resiliencia cibernética de una FMI y cómo los acuerdos de gobernanza de una FMI deben respaldar ese marco.
* **Identificación:** Es fundamental que las FMI identifiquen cuáles de sus operaciones críticas y activos de información de apoyo deben, en orden de prioridad, estar protegidos contra compromisos. La Guía CPMI-IOSCO describe cómo una FMI debe identificar y clasificar los procesos comerciales, los activos de información, el acceso al sistema y las dependencias externas.
* **Protección:** la resiliencia cibernética depende de controles y sistemas de seguridad efectivos y del diseño de procesos que protegen la confidencialidad, integridad y disponibilidad de los activos y servicios de una FMI. La Guía CPMI-IOSCO insta a las FMI a implementar controles apropiados y efectivos y diseñar sistemas y procesos en línea con las principales prácticas de ciberresiliencia y seguridad de la información para prevenir, limitar y contener el impacto de un posible ciberincidente.
* **Detección:** la capacidad de una FMI para reconocer signos de un posible incidente cibernético, o detectar que se ha producido una infracción real, es esencial para una fuerte resiliencia cibernética. Dada la naturaleza sigilosa y sofisticada de los incidentes cibernéticos y los múltiples puntos de entrada a través del cual podría producirse un compromiso, se necesitan capacidades avanzadas para monitorear extensivamente las actividades anómalas. El capítulo sobre detección de la Guía CPMIIOSCO describe las herramientas de seguimiento y proceso que debe utilizar una FMI para la detección de incidentes cibernéticos.
* **Respuesta y recuperación**: la estabilidad financiera puede depender de la capacidad de una FMI para liquidar obligaciones a su vencimiento. Por lo tanto, la Guía CPMI-IOSCO establece que los arreglos de una FMI deben diseñarse para permitirle reanudar las operaciones críticas de manera rápida, segura y con datos precisos para mitigar los riesgos potencialmente sistémicos de falla en cumplir con dichas obligaciones.

Los tres componentes generales son:

* **Pruebas:** Todos los elementos de un marco de ciberresiliencia deben probarse rigurosamente para determinar su eficacia general antes de ser implementados dentro de una FMI y, posteriormente, periódicamente.
* **Conciencia situacional:** se refiere a la comprensión de una FMI del entorno de amenazas cibernéticas en el que opera, y las implicaciones de estar en ese entorno para su negocio y la idoneidad de sus medidas de mitigación del riesgo cibernético.
* **Aprendizaje y evolución:** el marco de resiliencia cibernética de una FMI debe lograr una resiliencia cibernética continua dado el entorno de amenazas en constante cambio. Una FMI debe aspirar a inculcar una cultura de conciencia del riesgo cibernético mediante la cual su postura de resiliencia, en todos los niveles, se reevalúe de forma periódica y frecuente.

La Guía CPMI-IOSCO no establece estándares adicionales para las FMI más allá de los establecidos en los Principios para las Infraestructuras del Mercado Financiero (PFMI) de la CPMI-IOSCO.[[20]](#footnote-20) En cambio, la guía complementa la PFMI, en particular, la gobernanza (Principio 2), el marco para la gestión integral de riesgos (Principio 3), la firmeza de la liquidación (Principio 8), el riesgo operacional (Principio 17) y los vínculos FMI (Principio 20)

**1.3.3 Organización Internacional de Normalización (ISO) y Comisión Electrotécnica Internacional (IEC)**

ISO e IEC desarrollaron y publicaron la familia 27000 de estándares sobre sistemas de gestión de seguridad de la información para ayudar a las organizaciones a mantener seguros los activos de información, incluida la información financiera, la propiedad intelectual y los detalles de los empleados, o la información que les confían los clientes o terceros. La serie ISO comprende un conjunto de normas que se han desarrollado desde la década de 1990 y es ampliamente utilizada por corporaciones multinacionales. La versión más reciente se publicó en 2013.[[21]](#footnote-21) Bajo el sistema ISO, una empresa que ha implementado una norma como ISO 27001 puede ser certificada (o registrada) si completa con éxito una auditoría realizada por un organismo de certificación que haya sido acreditado por ISO.

Las normas ISO Cyber ​​más relevantes incluyen ISO 27001, que establece el marco para crear un programa integral de seguridad de TI, e ISO 27002, que luego contiene las "mejores prácticas" para construirlo.

* ISO / IEC 27001 define un conjunto de actividades para gestionar los riesgos de la información (Sistema de Gestión de Seguridad de la Información o “SGSI”). El SGSI es un marco de gestión global a través del cual la organización identifica análisis y aborda los riesgos de la información. El estándar cubre todo tipo de organizaciones de todos los tamaños en todas las industrias o mercados, públicos y privados.

Dada la variedad de entidades que pueden usarlo, ISO / IEC 27001 no adopta un enfoque único para todos ni exige controles particulares. Los controles de seguridad de la información establecidos en el Anexo A de ISO / IEC 27001 actúan como un menú del cual las organizaciones pueden elegir los controles más aplicables dados los riesgos que enfrentan. En consecuencia, impulsa a las organizaciones a realizar una evaluación integral de sus riesgos de información, que es uno de los pasos más importantes en la seguridad de la información y una parte vital del SGSI. El estándar también brinda a las organizaciones la opción de evitar o transferir riesgos de información, en lugar de mitigarlos mediante controles.

* **ISO / IEC 27002** establece un código de buenas prácticas para la seguridad de la información. Es un documento de asesoramiento y no una especificación formal como ISO / IEC 27001. Recomienda buenas prácticas que abordan los objetivos de control de seguridad de la información que surgen de los riesgos para la confidencialidad, integridad y disponibilidad de la información. Las organizaciones deben evaluar sus riesgos de información, aclarar sus objetivos de control y aplicar controles adecuados utilizando el estándar como guía.

Si bien los Estándares Básicos comparten muchos de los mismos objetivos, cada uno ofrece un enfoque diferente tanto en alcance como en detalle.

**Figura 1**

**Comparación de las características clave de los estándares básicos**



**2. Encuesta CTF y análisis de deficiencias**

El CTF realizó una encuesta a los miembros de IOSCO para obtener información sobre cómo se están aplicando los Estándares Básicos a las firmas financieras en las jurisdicciones de IOSCO y para identificar cualquier brecha potencial en la aplicación de los Estándares Básicos.

La encuesta se divide en tres amplias categorías de preguntas: (i) información general de antecedentes; (ii) enfoques regulatorios y de supervisión con respecto a Cyber; y (iii) coherencia con los Estándares Básicos o confianza en ellos. El CTF recibió 59 encuestas respuestas de un total de 128 jurisdicciones miembros, o solo un poco menos de una tasa de respuesta del 50%. A continuación se muestra un resumen del análisis de brechas de las respuestas de la encuesta. Los hallazgos clave están en negrita.

**2.1 Calificación del riesgo cibernético**

Con respecto a la estimación de la importancia del Cyber ​​Risk para las firmas financieras que operan en las jurisdicciones de IOSCO, la mayoría de los encuestados (81%) considera que Cyber ​​Risk es al menos uno de los riesgos más importantes, el riesgo más importante o un riesgo mayor que enfrentan los regulados. firmas en su jurisdicción. Mientras tanto, una minoría de los encuestados (19%) considera que el riesgo cibernético es un riesgo como cualquier otro o no está seguro de su posición relativa en comparación con otros riesgos. Estos datos se reflejan en la Figura 2, a continuación.

**Figura 2**

**Riesgo cibernético en comparación con otros riesgos que enfrentan las empresas reguladas**



Las respuestas de la encuesta también ilustran que ese Cyber Risk se percibe como un riesgo mayor en las jurisdicciones con un PIB per cápita más alto (PIB per cápita superior a $ 30.000). Sin embargo, la relación tiene forma de U, y las jurisdicciones con un PIB per cápita de rango medio (PIB per cápita de $ 10,000- $ 30,000) perciben el riesgo cibernético como el más bajo, mientras que las jurisdicciones con un PIB per cápita más bajo (PIB per cápita de menos de $ 10,000) perciben el riesgo cibernético. Como un riesgo ligeramente menor que los países de ingresos altos. Estos datos se reflejan en la Figura 3, a continuación.

**Figura 3**

**Riesgo cibernético en relación con otros riesgos**



Las jurisdicciones con un PIB per cápita más alto tenían más probabilidades de haber adoptado un marco de seguridad cibernética tanto a nivel nacional como del sector de servicios financieros que las jurisdicciones con un PIB per cápita de rango medio o más bajo. La Figura 4 a continuación refleja esta disparidad.

**Figura 4**

**Si se ha adoptado un marco cibernético**



En general, los resultados de la encuesta sugieren que, de los miembros de IOSCO que respondieron a la encuesta, la mayoría son muy conscientes de los riesgos cibernéticos y han implementado enfoques cibernéticos (regulaciones, políticas, marcos, etc.) que son total o generalmente consistentes con uno o más de los Estándares Básicos.

**2.2 Coherencia con los estándares básicos**

Las respuestas de la encuesta confirman que los Estándares Básicos han ganado una influencia significativa en los reguladores de todo el mundo y en diferentes sectores de los mercados de valores. En particular, una mayoría sustancial de las jurisdicciones de IOSCO informaron que sus enfoques de la seguridad cibernéticalas regulaciones son consistentes con los Estándares Básicos. Muchas jurisdicciones de IOSCO también informaron que sus enfoques cibernéticos también son consistentes con los principios de alto nivel en los Elementos Fundamentales del G7.

**La mayoría de los encuestados (59%) indicó que sus regulaciones, orientación y / o prácticas de supervisión nacionales eran “generalmente consistentes” o “completamente consistentes” con uno de los Estándares Básicos.**

Los datos de la encuesta también sugieren que las autoridades están influenciadas por una variedad de estándares, en lugar de uno solo. Como muestra la Figura 5, a continuación, el 31% de los encuestados informaron que sus enfoques cibernéticos son generalmente consistentes con NIST, el 39% informó que sus enfoques cibernéticos son generalmente consistentes con ISO y el 31% informó que sus enfoques cibernéticos eran generalmente consistentes con CPMI-IOSCO . Estos resultados sugieren que, **aunque los principios subyacentes a los Estándares Básicos han ganado una influencia considerable en las jurisdicciones de IOSCO, no predomina ningún Estándar Básico.**

**Figura 5**

**Los enfoques cibernéticos son generalmente consistentes con los estándares básicos**



Entre el 37% de los encuestados que no identificaron sus estándares cibernéticos como consistentes con los Estándares Básicos, algunos explicaron por qué este es el caso. Por ejemplo, un encuestado señaló que la Guía CPMI-IOSCO era inaplicable a su marco regulatorio, porque los participantes del mercado en su jurisdicción suelen utilizar infraestructuras de mercado en países vecinos.

**2.3 Referencia expresa a los estándares básicos**

La mayoría de los encuestados (58%) informó que sus regulaciones y guías nacionales se refieren expresamente a elementos de los Estándares Básicos u otros estándares destacados. La Figura 6 ilustra el desglose del tipo de estándar al que se hace referencia. Los resultados sugieren que se hace referencia a ISO un poco más a menudo en las reglamentaciones u orientaciones nacionales que cualquier otro estándar destacado.

**Figura 6**

**Referencia expresa a los estándares básicos u otros estándares destacados**



Estos resultados pueden verse en un contexto más amplio. En particular, la mitad de los encuestados (49%) indicó que son flexibles y no prescriptivos con respecto a los estándares cibernéticos (estándares básicos o de otro tipo) que las empresas pueden utilizar para cumplir con las regulaciones aplicables. De hecho, si un encuestado respondió "sí" a cualquier parte de la pregunta sobre la referencia expresa o la confianza en un Estándar Básico, el encuestado también indicó casi inevitablemente que su jurisdicción adoptó un enfoque flexible. Estos datos sugieren que entre las jurisdicciones encuestadas, la mayoría parece reconocer que no existe un enfoque único para la regulación de la seguridad cibernética y, en cambio, adoptan un enfoque basado en principios. Como señaló un miembro de IOSCO, las empresas reguladas bajo su jurisdicción pueden hacer referencia a cualquiera de los Estándares Básicos para cumplir con los requisitos legales aplicables. Otro miembro de IOSCO señaló que una de sus regulaciones cibernéticas clave no exige que se adopten o sigan estándares de seguridad específicos. Además, en un documento de orientación relacionado, su personal proporcionó ejemplos de estándares que una entidad financiera regulada podría considerar al desarrollar políticas y procedimientos razonables para cumplir con la regulación cibernética relevante.

**2.4 Coherencia entre los marcos nacionales de seguridad cibernética**

El análisis de la encuesta destaca varios elementos comunes entre las estrategias, políticas o marcos nacionales de seguridad cibernética en las jurisdicciones encuestadas.

**A pesar de las diferencias jurisdiccionales, existen elementos comunes en los regímenes cibernéticos de la mayoría de los encuestados.** Estos elementos comunes de estrategias, políticas o marcos de seguridad cibernética son:

* La institucionalización de una agencia nacional que promovió políticas e iniciativas de seguridad cibernética y que tenía la capacidad de brindar apoyo a la infraestructura crítica a través, por lo general, de un Equipo de Respuesta a Emergencias Informáticas (CERT) nacional.
* De aquellos que tenían estrategias, políticas o marcos de seguridad cibernética, alrededor del 30% incluía políticas e iniciativas para la protección de infraestructura crítica.
* Mejorar la resiliencia cibernética de las agencias gubernamentales, la infraestructura crítica y la inversión en investigación para desarrollar capacidades de seguridad cibernética.
* Establecer y / o adoptar estándares de Ciberseguridad e implementar esquemas de certificación y acreditación para profesionales y proveedores de servicios de Ciberseguridad, respectivamente.
* Colaboración entre el gobierno y la industria en iniciativas de seguridad cibernética y desarrollo de ecosistemas, en particular tratando la seguridad cibernética como un facilitador del crecimiento económico.
* Alentar a las organizaciones a establecer sus propios marcos de gestión de riesgos con políticas de seguridad cibernética junto con planes de acción para monitorear la implementación de medidas de seguridad cibernética como la gestión de incidentes cibernéticos.
* Educar al público sobre las prácticas de seguridad cibernética y sensibilizar al público sobre las amenazas a la seguridad cibernética.
* Cooperación internacional entre gobiernos para combatir el ciberdelito

Aproximadamente el 39% de los encuestados informaron que tienen planes públicos para emitir, durante el próximo año, nuevas regulaciones, guías o prácticas de supervisión que aborden la seguridad cibernética para todo o parte del sector financiero. De ese 39%, alrededor del 75% ya ha emitido reglamentos, orientaciones o prácticas de supervisión. Esto puede atribuirse a la necesidad de una guía actualizada a la luz del rápido ritmo de los desarrollos tecnológicos y la creciente sofisticación de las amenazas a la seguridad cibernética.

**2.5 Posibles brechas en la aplicación de los estándares básicos**

Los posibles vacíos que el CTF ha identificado a partir de los resultados de la encuesta son los siguientes:

* Una minoría de los encuestados no ve el riesgo cibernético como un riesgo importante o no está seguro de su gravedad. Esto podría significar que los encuestados aún no aprecian completamente la gravedad de los riesgos cibernéticos.
* Una minoría de los encuestados indicó que sus regímenes cibernéticos no son al menos “generalmente consistentes” con los Estándares Básicos. Como los Estándares Esenciales han sido ampliamente adoptados, las jurisdicciones que tienen regímenes que difieren significativamente de los Estándares Esenciales de manera que su enfoque no es generalmente consistente con los Estándares Esenciales pueden encontrar útil determinar dónde existen brechas materiales entre sus regímenes Cibernéticos y los Estándares Esenciales. Estándares.

El CTF sugiere una mayor exploración de estas posibles lagunas como consideraciones de seguimiento.

**3. Iniciativas de la industria**

El CTF consultó con el Comité Consultivo de Miembros Afiliados de IOSCO (AMCC) para comprender cómo la industria y las empresas de varios sectores financieros (gestión de activos, intermediarios e intercambios) abordan los problemas cibernéticos. A continuación se muestra el resumen de alto nivel de AMCC de las iniciativas del sector privado para aumentar la conciencia cibernética.

**Gestión de activos**:[[22]](#footnote-22) El Grupo de trabajo del Grupo de trabajo sobre resiliencia cibernética de AMCC sobre seguridad cibernética de gestión de inversiones realizó una encuesta anual para comparar la postura de seguridad cibernética de la industria de gestión de activos a nivel mundial (Encuesta AMCC).

Los resultados de la encuesta de AMCC muestran que alrededor de un tercio de los encuestados no logran ni siquiera las prácticas de seguridad más rudimentarias y fundamentales. Por ejemplo, el 35% afirma no haber modelado su programa de seguridad de la información contra cualquier marco conocido (como ISO, COBIT, etc.). Si bien las empresas pequeñas e incluso algunas medianas pueden encontrar estos y otros marcos de seguridad cibernética abrumadores, es fundamental una implementación básica de la práctica de seguridad cibernética simple y procesable.

The Center for Internet Security (https://www.cisecurity.org/controls/), que detalla 20 controles de seguridad, es otro recurso valioso para las empresas cuyos programas de seguridad de la información no son consistentes con uno o más marcos establecidos.

**Intermediarios:[[23]](#footnote-23)** Asociación Nacional de Futuros (NFA), Autoridad Reguladora de la Industria Financiera (FINRA), Organización Reguladora de la Industria de Inversiones (IIROC) y la Asociación Brasileña de Mercados Financieros y de Capital (ANBIMA) son organizaciones autorreguladoras que supervisan una población diversa de intermediarios. Aunque estos cuatro SRO no exigen el uso de un estándar de seguridad cibernético en particular, sus programas regulatorios cubren estos temas. Por ejemplo, la NFA requiere que sus miembros adopten un programa escrito de seguridad de sistemas de información (ISSP), mientras que ANBIMA requiere que los miembros implementen Cyber Reglas, procedimientos y controles de seguridad que deben ser consistentes con el tamaño, perfil de riesgo, modelo de negocio y complejidad de las actividades que realiza la institución. IIROC requiere que sus miembros distribuidores realicen encuestas de autoevaluación obligatorias.

Las cuatro SROs reconocen la necesidad de desarrollar asistencia para empresas pequeñas y medianas con recursos limitados para desarrollar programas efectivos de seguridad cibernética. ANBIMA, FINRA, IIROC y NFA también brindan iniciativas educativas sobre seguridad cibernética y varios de estos recursos están personalizados para entidades pequeñas y medianas. Por ejemplo, FINRA ha creado una lista de verificación (derivada principalmente del Informe de seguridad cibernética de NIST y FINRA Prácticas) para ayudar a las pequeñas empresas a establecer un programa de seguridad cibernética. FINRA también ha impartido un seminario web, titulado "Cómo crear un programa cibernético eficaz con recursos limitados".

**Intercambios / Infraestructura de mercado:[[24]](#footnote-24)** En 2017, la Federación Mundial de Intercambios (WFE) publicó un conjunto de estándares de ciberresiliencia para garantizar la alineación y los estándares mínimos comunes en todo el sistema global. En 2018, WFE publicó un conjunto de pautas de mejores prácticas sobre los aspectos de comportamiento y métodos preventivos para alentar a los empleados a cumplir con los protocolos cibernéticos.

WFE estableció el Grupo de trabajo de seguridad cibernética de intercambio global (GLEX) en diciembre de 2013, para actuar como un canal de intercambio de información para conectar el liderazgo de seguridad de la información (es decir, CISO) entre los principales intercambios financieros y CCP del mundo. El propósito principal del GLEX es facilitar el intercambio de información. Además, se creó un subgrupo de inteligencia y respuesta a incidentes más especializado (el subgrupo GLEX.SECOPS) para compartir información y rastrear a los adversarios potenciales que podrían tener interés en apuntar a los intercambios.

**4. Promoción de buenas prácticas cibernéticas**

Como se describe en la Sección 1.2, uno de los objetivos principales del CTF era considerar cómo utilizar los Estándares Básicos para ayudar a promover prácticas sólidas de Seguridad Cibernética en las jurisdicciones miembros de IOSCO. El sector de valores financieros está interconectado y, por lo tanto, las prácticas de seguridad cibernética en una jurisdicción pueden tener consecuencias potenciales para el sector de los mercados de capital en otras jurisdicciones. Para cumplir con este objetivo, el CTF, en consulta con la AMCC y otras partes interesadas de la industria, creó un conjunto de muestra de 15 preguntas destinadas a ayudar a las entidades del sector financiero que operan en las jurisdicciones de IOSCO a comprender ciertos componentes estructurales clave que se encuentran comúnmente en los Estándares Básicos.

Estas preguntas no pretenden ser un atajo o un sustituto del esquema cibernético integral que se encuentra en los Estándares Básicos o el marco regulatorio existente relevante.[[25]](#footnote-25) Más bien, estas preguntas podrían usarse para promover el conocimiento de las prácticas sólidas de Seguridad Cibernética en el sector financiero. Específicamente, las preguntas están destinadas a sugerir líneas de investigación por parte de las entidades del sector financiero mientras revisan sus propias prácticas y no tienen la intención de respaldar ningún marco regulatorio o de supervisión. Finalmente, las preguntas están diseñadas para ser consistentes con ciertas categorías comunes que se encuentran tanto en los Estándares Básicos como en otros marcos, guías y estándares cibernéticos, de la siguiente manera:

* **Prácticas de identificación y protección:** identificación y protección contra incidentes cibernéticos, como la autenticación de usuarios; infraestructura de red segura; pruebas (incluidas pruebas de penetración); y controles de tiempo de espera de sesión y contraseña.
* **Prácticas de detección:** detección de piratería y otros riesgos, y alerta a instituciones, clientes y autoridades para mitigar su impacto y reducir pérdidas financieras.
* **Prácticas de respuesta y recuperación:** desarrollo y gestión de planes de respuesta a incidentes, así como planes de respaldo y de contingencia que incluyen informes de incidentes y gestión de proveedores de servicios externos.

El conjunto de 15 preguntas es el siguiente:

**A. MARCO ESTÁNDAR DE LA INDUSTRIA:**

1. ¿La organización utiliza un estándar de la industria para desarrollar una estrategia y un marco de gestión de riesgos cibernéticos (por ejemplo, ISO, NIST Cyber Security Framework y / u otros)? Identifique los estándares.

**B. IDENTIFICAR Y PROTEGER:**

1. ¿La organización mantiene un inventario de su software, hardware, aplicaciones y proveedores?
2. ¿La organización identifica los riesgos cibernéticos y las vulnerabilidades[[26]](#footnote-26) que pueden afectar las operaciones comerciales?
3. ¿Tiene la organización un programa de gestión de identificación[[27]](#footnote-27) y acceso diseñado para limitar el acceso y eliminar el acceso de sus usuarios de manera oportuna?
4. ¿Tiene la organización un programa de capacitación y concientización sobre seguridad que les permita a las personas comprender sus roles dentro de la seguridad cibernética y aprender más sobre las amenazas emergentes?
5. ¿La organización emplea un programa de administración de parches[[28]](#footnote-28) para abordar las vulnerabilidades de software conocidas? ¿La organización emplea hardware (por ejemplo, cortafuegos, sistemas de detección de intrusiones en la red) y software (por ejemplo, anti-malware, sistemas de detección de intrusos en el host) para proteger sus sistemas de información?
6. ¿Tiene la organización procedimientos escritos para asegurar que las copias de seguridad de la información se realicen, mantengan y prueben periódicamente

**C. DETECTAR:**

1. ¿La organización detecta y analiza posibles eventos cibernéticos para comprender la naturaleza, el alcance y los métodos de un actor de amenazas?[[29]](#footnote-29)
2. ¿La organización implementa mecanismos de protección de correo electrónico para escanear, detectar y bloquear automáticamente malware o enlaces maliciosos en el correo electrónico?
3. ¿Tiene la organización un programa de pruebas para validar la eficacia de los procesos y controles de detección de incidentes de la organización?

**D. RESPONDER / RECUPERAR:**

1. ¿Tiene la organización un plan de respuesta a incidentes que contenga ciberincidentes y aplicaciones y procesos para garantizar la alerta y activación del plan?
2. ¿El plan de respuesta a incidentes de la organización aborda el intercambio de información, incluida la gestión de divulgaciones de vulnerabilidades y otras comunicaciones, y la presentación de informes sobre incidentes cibernéticos a partes interesadas internas y externas, terceros, reguladores y aplicación de la ley, según corresponda?
3. ¿La organización prueba su plan de respuesta a incidentes con regularidad y lo actualiza según sea necesario en función de los incidentes cibernéticos que han ocurrido y la inteligencia de amenazas?[[30]](#footnote-30)
4. ¿Tiene la organización un plan de recuperación para garantizar una recuperación oportuna de los incidentes cibernéticos?
5. ¿La organización revisa y actualiza periódicamente su plan de recuperación?

**5. Asignaciones a los estándares básicos**

Las asignaciones entre los Estándares Básicos y los marcos regulatorios cibernéticos también pueden promover cibernéticas sólidas o mejorar las prácticas cibernéticas existentes al proporcionar ejemplos de cómo incorporar los Estándares Básicos en diferentes tipos de regímenes cibernéticos nacionales.

Se pidió a los encuestados que proporcionaran un “mapa” entre su enfoque regulatorio o supervisor y los Estándares Esenciales, de modo que puedan ilustrar cuáles de sus reglas, guías y prácticas son consistentes con los diversos subcomponentes de los Estándares Esenciales. Dieciocho jurisdicciones de IOSCO proporcionaron “asignaciones” que están disponibles para los miembros de IOSCO a través del Cyber Portal establecido en la sección exclusiva para miembros del sitio web de IOSCO.

**6. Conclusión y próximos pasos**

Este informe intenta proporcionar una perspectiva sobre el panorama de las regulaciones cibernéticas entre las autoridades miembros de IOSCO. Examina cómo los miembros están usando los Estándares Básicos y otras guías cibernéticas prominentes en sus respectivos regímenes regulatorios e identifica las brechas potenciales en la aplicación de estos estándares que pueden necesitar ser abordadas. Además, proporciona un conjunto de preguntas que podrían usarse para promover el conocimiento de las prácticas sólidas de seguridad cibernética dentro de la comunidad IOSCO.

Al centrarse en los Estándares Esenciales e identificar posibles brechas regulatorias en relación con estos marcos ya establecidos, el informe subraya en primer lugar que IOSCO no propone nuevos estándares u orientaciones cibernéticas en este informe. En cambio, el camino óptimo a seguir, dada la confianza de muchos miembros de IOSCO en los Estándares Básicos, es continuar basándose en los marcos cibernéticos prominentes y existentes desarrollados por expertos en este espacio. Este enfoque garantiza la coherencia y evita la superposición, la duplicación y el conflicto entre los marcos cibernéticos, todo lo cual puede impedir el progreso en esta área.

En segundo lugar, el informe subraya que, debido al alto grado de interconectividad entre los mercados de valores, las infraestructuras y las empresas, los mercados financieros mundiales son tan fuertes como su eslabón más débil. Por lo tanto, si bien el informe encuentra que los miembros de IOSCO han logrado un buen progreso en el establecimiento de regímenes cibernéticos apropiados, todavía queda trabajo por hacer en áreas clave.

En este sentido, el CTF recomienda que se considere trabajar más a fin de explorar los hallazgos de este informe. En particular, con respecto a las posibles brechas identificadas en la Sección 2.5. recomendamos que el CTF considere explorar el uso de encuestas organizacionales en todo el sector como parte de la siguiente fase de su trabajo para obtener una mejor comprensión de dónde se encuentran las brechas.

**Anexo**

**Estándares, guías y marcos cibernéticos destacados adicionales.**

De las jurisdicciones que han adoptado una estrategia, política o marco nacional de seguridad cibernética, muchas también hacen referencia o siguen expresamente las herramientas y buenas prácticas en otros marcos u orientaciones cibernéticos. Estos otros estándares cibernéticos incluyen:

* Elementos fundamentales de ciberseguridad del G7 para el sector financiero.[[31]](#footnote-31)
* Orientación y estándares proporcionados por las agencias gubernamentales locales y las asociaciones industriales de las jurisdicciones.
* Centro de controles de seguridad críticos (CSC) de seguridad de Internet (CIS).[[32]](#footnote-32)
* Herramienta de evaluación de ciberseguridad del Consejo de examen de instituciones financieras federales de EE. UU. (FFIEC).[[33]](#footnote-33)
* Perfil de ciberseguridad del sector de servicios financieros (FSSCP), versión 1.0.[[34]](#footnote-34)
* Principios clave de la Asociación de Mercados Financieros Globales para un marco de pruebas de penetración de la ciberseguridad comúnmente aceptado.[[35]](#footnote-35)

Además, existen varios marcos generales de tecnología de la información que incluyen, dentro de ellos, una guía sustancial sobre seguridad cibernética y resiliencia cibernética. Éstas incluyen:

* COBIT 5 para la seguridad de la información.[[36]](#footnote-36)
* Biblioteca de infraestructura de tecnología de la información (ITIL).[[37]](#footnote-37)

**• TOGAF[[38]](#footnote-38)**

Además, existen importantes recursos en línea para respaldar estos diversos marcos y orientación cibernéticos. Ejemplos incluyen:

* Página de recursos de infraestructura crítica del marco de seguridad cibernética del NIST, página web de recursos de infraestructura crítica del marco de seguridad cibernética.[[39]](#footnote-39)
* Publicación especial de la serie 800 del NIST y Publicación especial de la serie 1800.[[40]](#footnote-40)
* Biblioteca de investigación del Information Security Forum (ISF).[[41]](#footnote-41)

Para las jurisdicciones que tienen la intención de crear o mejorar los estándares cibernéticos nacionales y desearían recibir orientación además de los estándares básicos, es posible que deseen considerar la posibilidad de revisar estos estándares cibernéticos adicionales.

**Background References**

Office of Financial Research, 2017, “Cybersecurity and Financial Stability: Risks and Resilience” OFR Viewpoint, February.

ITU, Global Cyber Security Index (2017), <https://www.itu.int/dms_pub/itu-d/opb/str/D-STRGCI.01-2017-R1-PDF-E.pdf>

Securities and Exchange Commission, 2018, “Commission Statement and Guidance on Public Company Cybersecurity Disclosures”

World Bank Group Financial Sector Advisory Committee, Financial Sector’s Cybersecurity: A Regulatory Digest World Bank (2017), [http://pubdocs.worldbank.org/en/524901513362019919/FinSAC-CybersecDigestOct-2017- Dec2017.pdf](http://pubdocs.worldbank.org/en/524901513362019919/FinSAC-CybersecDigestOct-2017-%20Dec2017.pdf)

Sultan Almuhammadi and Majeed Alsaleh “Information Security Maturity Model for NIST Cyber Security Framework” (2015)

Marsh and Mcllean – Cyber Threats: A Perfect Storm about to hit Europe 2017

Marsh Global Cyber Risk Perception Survey February 2018 “By the Numbers: Global Cyber Risk Perception Survey”

WEF The Global Risks Report 2018 13th Edition

Financial Stability Board, Cyber Lexicon (November 12, 2018), <http://www.fsb.org/wpcontent/uploads/P121118-1.pdf>

1. Este informe utiliza términos y definiciones tal como se definen en el Cyber ​​Lexicon of the Financial Stability Board (12 de 2018) (el Cyber ​​Lexicon) disponible en:

http://www.fsb.org/wp-content/uploads/P121118-1.pdf . Al crear el Cyber ​​Lexicon, el FSB se basó en las fuentes existentes para desarrollar la terminología basándose en el extenso trabajo que han realizado previamente o están realizando otros grupos en el desarrollo de léxicos y glosarios relacionados con la ciberseguridad y la ciberresiliencia, como la terminología definida. en los Estándares Básicos (definidos a continuación), así como en otros marcos y guías cibernéticos. Los términos del Cyber ​​Lexicon están escritos con mayúscula en el informe de CTF.

Cibernético se define para relacionarse con, dentro oa través del medio de la infraestructura de información interconectada de interacciones entre personas, procesos, datos y sistemas de información. Ver el Cyber

Léxico. [↑](#footnote-ref-1)
2. La seguridad cibernética se define como la preservación de la confidencialidad, integridad y disponibilidad de la información y / o sistemas de información a través del medio cibernético. Además, también pueden estar involucradas otras propiedades, como la autenticidad, la responsabilidad, el no repudio y la confiabilidad. Léxico cibernético [↑](#footnote-ref-2)
3. El riesgo cibernético se define como la combinación de la probabilidad de que ocurran incidentes cibernéticos y su impacto [↑](#footnote-ref-3)
4. Los incidentes cibernéticos se definen como un evento cibernético que (i) pone en peligro la seguridad cibernética de un sistema de información o la información que el sistema procesa, almacena o transmite; o (ii) viole las políticas de seguridad, los procedimientos de seguridad o las políticas de uso aceptable, ya sea como resultado de una actividad maliciosa o no. Ver el Cyber ​​Lexicon [↑](#footnote-ref-4)
5. Cyber ​​Resilience es la capacidad de una organización para continuar llevando a cabo su misión anticipándose y adaptándose a las amenazas cibernéticas y otros cambios relevantes en el entorno y resistiendo, conteniendo y recuperándose rápidamente de los incidentes cibernéticos. Ver el Cyber ​​Lexicon [↑](#footnote-ref-5)
6. Las contribuciones destacadas incluyen el trabajo del FSB sobre el Cyber ​​Lexicon, mencionado anteriormente, y del Consejo de Coordinación del Sector de Servicios Financieros (FSSC) sobre el Perfil de Ciberseguridad del Sector de Servicios Financieros (Perfil). El perfil proporciona un marco para la evaluación de la gestión del riesgo cibernético por parte de las empresas financieras y para demostrar el cumplimiento normativo. Disponible en : <https://www.fsscc.org/Financial-SectorCybersecurity-Profile>.

Otro trabajo notable del FSB incluye el Inventario de normas, directrices y prácticas de supervisión de ciberseguridad de divulgación pública (13 de octubre de 2017) (Inventario del FSB de 2017), en el que IOSCO presentó respuestas a la encuesta. Disponible en: <https://www.fsb.org/2017/10/fsb-publishes-stocktake-on-cybersecurity-regulatory-and-supervisorypractices/> [↑](#footnote-ref-6)
7. http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf [↑](#footnote-ref-7)
8. <http://www.bis.org/cpmi/publ/d146.pdf> [↑](#footnote-ref-8)
9. La seguridad cibernética se define como la preservación de la confidencialidad, integridad y disponibilidad de la información y / o sistemas de información a través del medio cibernético. Además, también pueden estar involucradas otras propiedades, como autenticidad, responsabilidad, no repudio y confiabilidad. Ver el Cyber ​​Lexicon [↑](#footnote-ref-9)
10. <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf> [↑](#footnote-ref-10)
11. Si bien Cyber ​​es un riesgo común, una miríada de regímenes diversos podría socavar las iniciativas cibernéticas, confundir los mercados y crear inconsistencias donde varios enfoques son conflictivos o inconsistentes, lo que dificulta o imposibilita el cumplimiento de los diferentes regímenes. En este sentido, los Estándares Básicos podrían usarse como referencia para reducir la probabilidad de que se sigan o apliquen estándares cibernéticos inconsistentes en todas las jurisdicciones a nivel internacional. [↑](#footnote-ref-11)
12. Cibernético se define para relacionarse con, dentro o a través del medio de la infraestructura de información interconectada de interacciones entre personas, procesos, datos y sistemas de información. Consulte el Cyber ​​léxico. [↑](#footnote-ref-12)
13. El balance de 2017 del FSB encontró que los Estándares Básicos eran la guía existente más ampliamente útil sobre seguridad cibernética para las jurisdicciones del FSB, y que una aceptación tan amplia de estos estándares ayuda a promover un grado de convergencia internacional con respecto a la regulación de seguridad cibernética en el sector financiero. [↑](#footnote-ref-13)
14. El marco de Control Objectives for Information and Related Technology (COBIT) fue creado por el IT Governance Institute y la Information Systems Audit and Control Association (ISACA) para ayudar a las organizaciones a crear, monitorear y mantener la tecnología de la información en general. [↑](#footnote-ref-14)
15. See generally Annex, infra. [↑](#footnote-ref-15)
16. El grupo G-7 se estableció en 2015 con el mandato de estudiar los enfoques de las jurisdicciones miembros sobre la ciberseguridad del sector financiero y emitir recomendaciones para los ministros de finanzas y los gobernadores de los bancos centrales del G-7. En octubre de 2016, el G-7 publicó Elementos Fundamentales de Ciberseguridad para el Sector Financiero. Disponible en: https://www.treasury.gov/resource-center/international/g7- g20/Documents/G7%20Fundamental%20Elements%20Oct%202016.pdf [↑](#footnote-ref-16)
17. U.S. National Institute of Standards and Technology (NIST) at, <https://www.nist.gov/cyberframework/critical-infrastructure-resources> [↑](#footnote-ref-17)
18. NIST en 2018 actualizado a la versión 1.1 de su popular marco, comúnmente conocido en NISTCybersecurity Framework, que incluye actualizaciones de autenticación e identidad; autoevaluación del riesgo de ciberseguridad; gestionar la ciberseguridad con la cadena de suministro; y divulgación de vulnerabilidades. Disponible en: <https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework> [↑](#footnote-ref-18)
19. Según se define en la Guía CPMI-IOSCO, y de conformidad con los Principios para las Infraestructuras del Mercado Financiero (PFMI) de CPMI-IOSCO, las FMI son sistemas de pago de importancia sistémica, depósitos centrales de valores, sistemas de liquidación de valores, contrapartes centrales y registros de operaciones. Las autoridades pertinentes, sin embargo, pueden decidir aplicar la guía a otros tipos de infraestructura, como entidades de importancia no sistémica, no cubiertas específicamente por la Guía CPMI-IOSCO. La guía complementa los estándares internacionales en el 2012 CPMI-IOSCO PFMI. [↑](#footnote-ref-19)
20. Disponible en: <https://www.bis.org/cpmi/publ/d101a.pdf> [↑](#footnote-ref-20)
21. Por ejemplo, una parte de la serie ISO se actualizó en 2018. Ver:

<https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip> [↑](#footnote-ref-21)
22. Response provided by the Investment Company Institute. [↑](#footnote-ref-22)
23. Response provided by ANBIMA, FINRA, IIROC and NFA. [↑](#footnote-ref-23)
24. Response provided by the World Federation of Exchanges. [↑](#footnote-ref-24)
25. Tampoco suplantan mapeos sofisticados que rastrean la relación entre los Estándares Básicos, como el análisis integrado en el Perfil de Ciberseguridad del Sector de Servicios Financieros (FSSCP), Versión 1.0. Disponible en https://www.fsscc.org/Financial-Sector-Cybersecurity-Profile.

El FSSCP es una personalización del Marco de Ciberseguridad del NIST que las instituciones financieras pueden usar para la evaluación interna y externa de la gestión del riesgo cibernético y como evidencia de cumplimiento, que abarca las relaciones entre los marcos cibernéticos, incluidos los Estándares Básicos. Además, la herramienta del perfil de seguridad cibernética de la FSSCC abarca los tres estándares básicos de este informe, así como otros, y detalla cómo las diferentes subsecciones de cada uno de los tres estándares básicos (el marco de seguridad cibernética del NIST, ISO y la guía CPMI-IOSCO), así como otros marcos pueden superponerse o ser funcionalmente equivalentes entre sí. [↑](#footnote-ref-25)
26. Las vulnerabilidades se definen como una debilidad, susceptibilidad o falla de un activo o control que puede ser explotado por una o más amenazas. Consulte el Cyber ​​Lexicon. [↑](#footnote-ref-26)
27. Identificar se define como desarrollar la comprensión organizacional para gestionar el riesgo cibernético de los activos y las capacidades. Ver el Cyber ​​Lexicon [↑](#footnote-ref-27)
28. La administración de parches se define como la notificación, identificación, implementación, instalación y verificación sistémicas del sistema operativo y las revisiones del código del software de la aplicación. Estas revisiones se conocen como parches, correcciones urgentes y paquetes de servicios. Consulte el Cyber Lexicon. [↑](#footnote-ref-28)
29. Actor de amenazas se define como un individuo, un grupo o una organización que se cree que opera con intenciones maliciosas. Consulte el Cyber ​​Lexicon. [↑](#footnote-ref-29)
30. Inteligencia de amenazas se define como información sobre amenazas que se ha agregado, transformado, analizado, interpretado o enriquecido para proporcionar el contexto necesario para los procesos de toma de decisiones. Consulte el Cyber ​​Lexicon. [↑](#footnote-ref-30)
31. Fundamental Elements of Cybersecurity for the Financial Sector. Available at: https://www.treasury.gov/resource-center/international/g7- g20/Documents/G7%20Fundamental%20Elements%20Oct%202016.pdf (October 2016). See n.14. [↑](#footnote-ref-31)
32. El CSC es un conjunto de acciones recomendadas para identificar, proteger y responder a las amenazas cibernéticas y los incidentes cibernéticos. https://www.cisecurity.org/controls/. Estos controles son consistentes con el Marco de Ciberseguridad del NIST, pero priorizan y se enfocan en un número menor de controles procesables con "altos beneficios", identificando prioridades clave para la Ciberseguridad y la Ciberresiliencia. [↑](#footnote-ref-32)
33. <https://www.ffiec.gov/cyberassessmenttool.htm>(diseñado para ayudar a las instituciones financieras a identificar riesgos y determinar la preparación para la seguridad cibernética y la resiliencia cibernética) (actualizado en 2017) [↑](#footnote-ref-33)
34. [https://www.fsscc.org/Financial-Sector-Cybersecurity-Profile. See n. 5](https://www.fsscc.org/Financial-Sector-Cybersecurity-Profile.%20See%20n.%205). [↑](#footnote-ref-34)
35. http://gfma.org/uploadedFiles/News/GFMA\_in\_the\_News/2017/GFMA-Penetration-TestingPrinciples.pdf (Diciembre 2017). De acuerdo con el enfoque de este informe en los marcos existentes, esta publicación de la GFMA señala específicamente los riesgos que plantea la participación del sector público en las pruebas de penetración, incluido el riesgo de "métodos y marcos de pruebas de penetración duplicados y prescriptivos" que exigen "mayores recursos dentro de la industria para responder de manera adecuada a todas y cada una de las pruebas ", recursos que" podrían utilizarse de manera más eficiente para proteger a las empresas y sus clientes ". Identificación. a las 2. [↑](#footnote-ref-35)
36. El marco de Control Objectives for Information and Related Technology (COBIT) fue creado por el IT Governance Institute y la Information Systems Audit and Control Association (ISACA) para ayudar a las organizaciones a crear, monitorear y mantener la tecnología de la información en general. [↑](#footnote-ref-36)
37. ITIL es un conjunto de prácticas detalladas para la gestión de la tecnología de la información, que incluye, entre otros, problemas cibernéticos. AXELOS la debe como una empresa de propiedad conjunta entre Capita y la Oficina del Gabinete del Reino Unido. Investigó su libro básico de ITIL 4 más reciente en febrero de 2019. [↑](#footnote-ref-37)
38. Open Group Architecture Framework (TOGAF) es un marco popular para la arquitectura empresarial, que incluye un conjunto de herramientas de apoyo. <https://www.isaca.org/JOURNAL/ARCHIVES/2017/VOLUME4/Pages/enterprise-security-architecture-a-top-down-approach.aspx?utm_referrer>= [↑](#footnote-ref-38)
39. <https://www.nist.gov/cyberframework/critical-infrastructure-resources>, [↑](#footnote-ref-39)
40. NIST publica una serie de pautas, recomendaciones y especificaciones de interés general para la comunidad de seguridad informática. <https://www.nist.gov/itl/nist-special-publication-800-series-generalinformation> [↑](#footnote-ref-40)
41. <https://www.securityforum.org/research/> [↑](#footnote-ref-41)