CNMV
Comisión Nacional del Mercado de Valores

Ciberseguridad en las infraestructuras de los mercados

Ciberseguridad en las infraestructuras de los mercados

Marzo 2017

Comisión Nacional del Mercado de Valores
Edison, 4
28006 Madrid

Passeig de Grácia, 19
08007 Barcelona

ISBN (edición electrónica): 978-84-87870-99-6

Maqueta: Composiciones Rali, S.A.

Índice

Resumen ejecutivo

Las infraestructuras de los mercados (negociación y postcontratación) se consideran críticas a efectos de ciberseguridad tanto en España como en el resto de países. En particular, un ciberataque a las infraestructuras de postcontratación (registro, pagos y contraparte central) puede generar eventos de importancia sistémica de efectos prolongados con una reversibilidad y recuperación más lenta que si se produjese en los sistemas de contratación.

La tecnología asociada y la interoperabilidad de las infraestructuras de los mercados con otras plataformas y con sus participantes posibilitarían la propagación y ampliación de los efectos de los ciberataques así como las vías de acceso de entrada de amenazas.

La ciberseguridad de las infraestructuras críticas es un asunto de seguridad nacional en la mayoría de países incluida España. Reguladores internacionales como IOSCO y asociaciones de la industria como SIFMA han declarado que la ciberseguridad se encuentra entre sus máximas prioridades. Este hecho, unido al cambio estructural en el sector financiero con la irrupción y consolidación del *Fintech* hacen necesaria una dotación urgente de recursos humanos con marcado perfil tecnológico en las entidades supervisoras.

La naturaleza de las amenazas cibernéticas es cambiante y está en continua evolución por lo que la actuación reguladora y supervisora tiene que ser de la misma dimensión. La cooperación internacional y el intercambio de información y experiencias (*cyber intelligence*) son elementos clave de la estrategia para lograr una mayor seguridad.

Las infraestructuras de los mercados deberían cumplir los requisitos en materia de ciberseguridad establecidos tanto por organismos con competencia nacional en la materia como en el ámbito de los mercados de valores, en concreto:

– El Plan Estratégico Sectorial del Sector Financiero, elaborado por la Comisión Nacional para la Protección de Infraestructuras Críticas (CNPIC), que recoge las principales líneas de un grupo de trabajo creado a tal efecto, en el que ha participado la CNMV. Este plan debería contener, entre otros puntos, las recomendaciones de CPSS-IOSCO para las infraestructuras en materia de ciberseguridad. En el ámbito europeo de ciberseguridad, ya existe una directiva[1] aplicable a las infraestructuras cuya trasposición debería efectuarse antes de mayo de 2018.

1 Directiva (EU) 2016/1148 del Consejo y Parlamento Europeo de 6 de junio de 2016 sobre relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016L1148)

– Una guía[2] del Comité de Pagos e Infraestructuras de Mercado del BIS hecha pública en junio de 2016, que sería de aplicación a las infraestructuras de los mercados y cuyo cumplimiento debería supervisar la CNMV en coordinación con otros organismos encargados de la ciberseguridad.

La CNMV debe seguir de cerca la evolución de las actuaciones del CNPIC en relación con las infraestructuras críticas y sus políticas de ciberseguridad, llevando a cabo aquellas tareas de supervisión que nos asignen en los correspondientes planes.

La realización periódica de ejercicios y simulaciones de ciberataques, que es una herramienta esencial de ciberseguridad y práctica habitual en otros países, se debe de realizar también en España con las infraestructuras que supervisa la CNMV. En el marco de los planes de contingencia de las infraestructuras de los mercados debe tenerse en cuenta que la infraestructura en cuestión dispone de auditorías externas de seguridad de alto nivel, tanto puntuales como permanentes. El documento del Comité de Pagose Infrastructuras de Mercado (CPMI) citado anteriormente puede servir como guía para efectuar una supervisión de las políticas de ciberseguridad de nuestros mercados. En el ámbito de la Unión Europea ya se realizan ejercicios y simulaciones por parte de la European Union Agency for Network and Information Security (ENISA).

Para maximizar la efectividad de los planes de ciberseguridad es necesaria la participación del equipo directivo y de todos los empleados de la compañía ya que cada puesto de trabajo conectado al exterior puede ser una vía de entrada de amenazas.

2 «Guidance on cyber resilience for financial market infraestructures» Committee on Payments and Market Infrastructures. Junio 2016.

1 Definiciones

En este informe se utilizan, de acuerdo con el documento[3] «Guidance on cyber resilience for financial market infraestructures» publicado en junio de 2016 por el Comité de Pagos e Infraestructuras los siguientes conceptos:

– Ciberamenaza (*Cyber threat*): Circunstancia o evento que puede ser o no de naturaleza intencionada con la capacidad potencial de aprovechar una o varias vulnerabilidades de las infraestructuras de los mercados, dando lugar a una pérdida de confidencialidad, integridad o disponibilidad.

– Ciberresiliencia (*Cyber resilience*): La capacidad para anticipar, absorber, adaptarse y/o recuperarse de manera rápida de un ciberataque.

– Ciberseguridad (*Cyber security*): Es un concepto muy general sobre el que aún no existe una definición de consenso. En este documento se referirá a las estrategias, políticas y estándares dirigidos a la reducción de las amenazas, vulnerabilidades, disuasión, compromisos internacionales, respuestas a los ataques, resistencia y actividades de recuperación así como las políticas de seguridad de las infraestructuras de los mercados.

– Ciberinteligencia: La recolección y análisis de la información que permitiría comprender y mitigar el impacto de las ciberamenazas.

3 http://www.bis.org/cpmi/publ/d122.pdf

2 Percepción internacional de los riesgos de un ciberataque a las infraestructuras de los mercados

La mayoría de supervisores y organizaciones internacionales ha reconocido el riesgo que representaría para el sistema financiero un ciberataque a infraestructuras críticas de los mercados y en algunos casos han puesto en marcha diversas iniciativas que van desde mesas redondas a consultas al sector y grupos de trabajo.

En julio de 2015 IOSCO, por medio de su secretario general[4], se refería a los potenciales ciberataques como una de las mayores preocupaciones de los supervisores de valores y cuyo nivel de riesgo se incrementaría en la medida en que los mercados cuenten con un mayor grado de digitalización. IOSCO ha creado un grupo de trabajo que está analizando la ciberseguridad. En noviembre de 2015 hizo público un primer documento que dio lugar a una guía publicada en junio de 2016 con principios a seguir por parte de los administradores de las infraestructuras de los mercados y que se comenta en el punto 6 de este informe.

En octubre de 2015 la Reserva Federal de EEUU coincidía con el supervisor de los mercados de derivados (CFTC) en señalar que el riesgo de ciberataques está en lo más alto de su lista de prioridades[5]. La Securities and Exchange Commission (SEC) organizó en marzo de 2014 una mesa redonda con varios paneles [6] dedicada a la ciberseguridad.

También en EEUU, la CFTC publicó en diciembre de 2015 un documento para consulta «Proposed Enhanced Rules on Cybersecurity for Derivatives Clearing Organizations, Trading Platforms, and Swap Data Repositories». El documento persigue mejorar las normas vigentes en la materia e identifica cinco tipos de pruebas de ciberseguridad esenciales: vulnerabilidad, intrusión, controles, respuesta a incidentes y evaluación de riesgos. La frecuencia de estas pruebas dependerá del tipo de entidad y de la materia a probar y las podrán realizar empresas independientes especializadas en ciberseguridad. Desde octubre de 2016, las citadas pruebas son de aplicación a todas las entidades de contrapartida centralizada y a los registros de operaciones. Otro de los objetivos que pretende y en lo que coincide con las recomendaciones de IOSCO, es la implicación del comité de dirección de las compañías en las políticas de seguridad frente a ciberataques.

---

4 http://www.bloomberg.com/professional/blog/cyber-risk-is-next-black-swan-uneven-across-the-globe-says-ioscos-medcraft/?utm_source=SmartBrief&utm_medium=SBRC&utm_content=Cyber-Risk%20Is%20%E2%80%98Next%20Black%20Swan%2C%E2%80%99%20Uneven%20Across%20the%20Globe%2C%20Says%20Iosco%E2%80%99s%20Medcraft&utm_campaign=Core

5 http://www.thinkadvisor.com/2015/10/14/fed-says-cybersecurity-is-right-at-the-top-of-prio

6 http://www.sec.gov/spotlight/cybersecurity-roundtable/cybersecurity-roundtable-transcript.txt

En el Reino Unido hay una iniciativa conjunta entre el Tesoro, el Banco de Inglaterra y la Financial Conduct Authority (FCA) con el objetivo de proporcionar y reunir información para garantizar la resistencia y continuidad del sector financiero[7]. El Gobierno del Reino Unido publicó en junio de 2014 un documento marco que contiene[8] los 10 principios esenciales que las compañías deben considerar para salvaguardar su ciberseguridad. En su plan estratégico para los años 2015 y 2016 la FCA tenía previsto, de manera coordinada con el Banco de Inglaterra, el Tesoro y la Autoridad de Regulación Prudencial, evaluar la ciberresiliencia de las infraestructuras críticas del sector financiero. Para el Comité de Política Financiera del Banco de Inglaterra las amenazas a la ciberseguridad son un riesgo clave para el año 2015 y advertía de la necesidad de realizar el ejercicio de evaluación de las infraestructuras críticas.

En la reunión del Comité de Estabilidad Financiera (FSB) celebrada en septiembre de 2015 en Londres, varios miembros señalaron la amenaza potencial para la estabilidad financiera que podrían suponer los ciberataques.

7 http://www.bankofengland.co.uk/financialstability/fsc/Pages/default.aspx

8 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317480/Cyber_Essentials_Summary.pdf

3 Estructura orgánica de la ciberseguridad en España

Desde el año 2013, España cuenta con un Plan Estratégico de Ciberseguridad elaborado por el Consejo de Seguridad Nacional. El plan tiene los siguientes objetivos:

1. Garantizar que los sistemas de información y telecomunicaciones que utilizan las Administraciones Públicas posean el adecuado nivel de ciberseguridad y resiliencia.

2. Impulsar la seguridad y resiliencia de los sistemas de información y telecomunicaciones usados por el sector empresarial en general y los operadores de infraestructuras críticas en particular.

3. Potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio.

4. Sensibilizar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio.

5. Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de ciberseguridad.

6. Contribuir a la mejora de la ciberseguridad en el ámbito internacional.

Una de las líneas de actuación del Plan relacionadas con las infraestructuras críticas es la mejora de la seguridad de sus sistemas de información y telecomunicaciones. Para alcanzar este objetico, tiene previsto impulsar la implantación de la normativa (detallada en el punto 5 de este informe) sobre protección de infraestructuras críticas y de las capacidades necesarias para la protección de los servicios esenciales.

De acuerdo con el Plan, la estructura orgánica de la ciberseguridad en España es la siguiente:

a) Consejo de Seguridad Nacional: El Consejo de Seguridad Nacional, configurado como Comisión Delegada del Gobierno para la Seguridad Nacional, asiste al Presidente del Gobierno en la dirección de la Política de Seguridad Nacional.

b) Comité Especializado de Ciberseguridad: El Comité Especializado de Ciberseguridad da apoyo al Consejo de Seguridad Nacional para el cumplimiento de sus funciones y, en particular, asiste al Presidente del Gobierno en la dirección y coordinación de la Política de Seguridad Nacional en el ámbito de la ciberseguridad. Además, refuerza las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas, así como entre los sec-

tores públicos y privado, y facilita la toma de decisiones del propio Consejo mediante el análisis, estudio y propuesta de iniciativas tanto en el ámbito nacional como en el internacional.

c) Comité Especializado de Situación: El Comité Especializado de Situación se convoca para llevar a cabo la gestión de las situaciones de crisis en el ámbito de la ciberseguridad que, atendiendo a la acentuada transversalidad o dimensión e impacto de sus efectos, produzcan el desbordamiento de los límites de capacidad de respuesta eficaz por parte de los mecanismos habituales previstos.

Dentro de este esquema, las infraestructuras de los mercados financieros tienen la consideración de infraestructuras críticas y para ellas se crean varias instituciones que coordinen y supervisen las diferentes actuaciones preventivas y den respuesta en materia de ciberseguridad. No obstante, la CNMV mantiene sus competencias de supervisión de las infraestructuras de los mercados financieros que deberían incluir también la política y procedimientos de ciberseguridad

Previsiones y organización de la ciberseguridad de las infraestructuras críticas en España

Desde 2007 existe un Plan Nacional de Protección de las Infraestructuras Críticas que se considera documento clasificado. Recientemente, se ha llevado a cabo una actualización, a través de la Instrucción 01/2016 de 10 de febrero de la Secretaría de Estado de Seguridad.

Los principales organismos encargados de la protección de las infraestructuras críticas en España son:

– La Comisión Nacional para la Protección de Infraestructuras Críticas (Comisión PIC), órgano colegiado adscrito a la Secretaria de Estado de Seguridad. La Comisión tiene varios miembros y está presidida por el Secretario de Estado de Seguridad. La representación de los ministerios integrados en el sistema corresponderá a una persona de rango igual o superior a director general.

– El Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC) dependiente de la Secretaria de Estado de Seguridad.

Con respecto a las infraestructuras críticas, el CNPIC es el órgano que se encarga de impulsar, coordinar y supervisar todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad del Ministerio del Interior en relación con la protección de las infraestructuras críticas españolas.

De acuerdo con la La Ley 8/2011[9], de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, en España deben ser consideradas como infraestructuras críticas: *Las infraestructuras estratégicas (es decir, aquellas que proporcionan servicios esenciales) cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales*. En el caso del sector finan-

9 https://www.boe.es/boe/dias/2011/04/29/pdfs/BOE-A-2011-7630.pdf

ciero, lo recoge la Ley 44/2002, de 22 de noviembre de Medidas de Reforma del Sistema Financiero.

La Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información suscribieron en 2012 (ratificado en 2015) un acuerdo en el que, entre otros aspectos, se sientan las bases para la colaboración entre el CNPIC y el Instituto Nacional de Ciberseguridad en materia de respuesta a incidentes de las infraestructuras críticas ubicadas en España. En el año 2014, la Secretaría de Estado de Seguridad creó la Oficina de Coordinación Cibernética dependiente del CNPIC [10] como órgano técnico de coordinación en materia de ciberseguridad y que también actuará como enlace con las autoridades nacionales e internacionales.

Ambas entidades han puesto en marcha un equipo de respuesta especializado en el análisis y gestión de incidencias de seguridad tecnológicas. Este equipo de respuesta se convierte, por lo tanto, en el centro especializado en la gestión de incidentes relacionados con las infraestructuras críticas en el ámbito nacional.

En caso de que una infraestructura crítica sufra un problema de seguridad cibernético el operador responsable de la misma podrá beneficiarse de los servicios del equipo de respuesta, informando de la incidencia a través del punto de contacto único habilitado para esta finalidad.

Se han realizado ciberejercicios[11] tanto en el ámbito nacional como en el ámbito europeo, coordinados por la European Union Agency for Network and Information Security (ENISA https://www.enisa.europa.eu/), con la participación de treinta y dos países. Estos ejercicios tienen carácter bienal[12]. Las principales conclusiones obtenidas de los cuatros ejercicios realizados desde 2010 son, por un lado, la necesidad de articular un mecanismo para compartir experiencias sobre ciberataques registrados y las mejores prácticas para aumentar la ciberseguridad, y por otro, mantener su periodicidad, con un calendario prestablecido.

En este sentido, se entiende por problema de seguridad cibernético cualquier incidente que, empleando o estando dirigido a elementos tecnológicos, afecte al correcto funcionamiento de la infraestructura afectada, como por ejemplo ataques que supongan la parada o inutilización de servicios tecnológicos, acceso a información privilegiada, alteración de información para manipular de forma fraudulenta los sistemas tecnológicos y la información que manejan, etc.

Dado su carácter de secreto oficial no se ha podido acceder a información sobre los estándares, procedimientos y pruebas que el CNPIC realiza para salvaguardar la seguridad de las infraestructuras definidas como críticas.

---

10 http://www.academiauniform.es/mediapool/81/814638/data/2014/Instrucc._15_14_Oficina_coordinacion_cibernetica.pdf

11 Un ciberejercicio es una herramienta que permite evaluar el estado de preparación de los participantes frente a crisis de origen cibernético, facilitando además lecciones aprendidas y recomendaciones para el futuro: aspectos de mejora frente un ataque cibernético, para el aumento de la cooperación y la coordinación dentro de los sectores involucrados, para la identificación de interdependencias, para la mejora de la concienciación y la formación. https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/incibe_taxonomia_ciberejercicios.pdf

12 «The 2015 Report on National and International Cyber Security Exercises Survey, Analysis and Recommendations». ENISA.

En el año 2016, se han conocido los resultados de un ejercicio de simulación realizado en septiembre de 2015 por la Securities Industry and Financial Markets Association (SIFMA) de EE.UU y cuya conclusión principal es que, a pesar de los avances, son necesarios mayores esfuerzos en medidas de ciberseguridad. En este ejercicio, participaron más de 650 entidades que incluían, además de instituciones financieras, agencias del gobierno de EEUU como el Departamento del Tesoro, el FBI, el Departamento de Seguridad Nacional y varios reguladores federales. El ejercicio incluyó el teórico cierre de una infraestructura de contrapartida central y ataques a bolsas de valores y a sistemas multilaterales. SIFMA ha hecho públicas sus prioridades estratégicas para el año 2016 entre las que la ciberseguridad está en la primera posición. En diciembre de 2015, el Congreso de EE.UU aprobó la Cybersecurity Information Sharing Act[13], que permite que las empresas y los organismos federales compartan su información sobre ciberataques así como las mejores prácticas en esta materia.

Ciberseguridad en el ámbito de la CNMV

En el ámbito de competencias de la CNMV pueden identificarse los siguientes riesgos derivados de un ciberataque:

- Entidades emisoras/cotizadas. Con diferentes alcances sobre la continuidad de sus operaciones y sus consecuentes repercusiones bursátiles. Especialmente significativos serían los impactos de un ciberataque en empresas proveedoras de infraestructuras estratégicas y críticas como las eléctricas y las comunicaciones, el control aéreo y los sistemas de pago.

- Empresas de servicios de inversión y entidades gestoras y depositarias de instituciones de inversión colectiva. Con efectos negativos sobre el registro de cuentas de valores y efectivo de los clientes.

- El propio supervisor: Con procesos especialmente críticos como la difusión de información relevante, que podrían ver afectado su funcionamiento.

- Difusores de información financiera relevante.

- Infraestructuras de los mercados financieros: negociación, sistemas de liquidación y pagos, cámaras de contrapartida central y registros de valores. Estas infraestructuras están especialmente expuestas a los riesgos de un ciberataque como consecuencia, por un lado, de su dependencia tecnológica ya que los sistemas de compensación y liquidación descansan en las tecnologías de la información y, por otro, por la profunda interconexión con sus miembros, lo que ofrece múltiples puntos de acceso a sus sistemas.

En este ámbito deberían diferenciarse los efectos y el alcance de un ataque sobre las infraestructuras de negociación de las consecuencias sobre las infraestructuras de postcontratación.

Un ataque sobre las infraestructuras de negociación tendría una notoriedad inmediata y significativa si tuviese como consecuencia una interrupción o perturbaciones

13 https://www.congress.gov/bill/114th-congress/senate-bill/754

Ejemplos de vulnerabilidades de ciberseguridad en las IMF CUADRO 1

Proceso	Amenazas potenciales
Prenegociación	Accesos no autorizados, utilización fraudulenta de algoritmos de negociación automatizada de miembros del mercado. Carga de virus y ficheros dañados desde intermediarios a los sistemas de negociación. Difusión de información falsa, interrupción de la difusión de información relevante. Ruptura del sistema de negociación con introducción de ordenes falsa y/o erróneas, imposibilidad de transmitir órdenes. Manipulación en el cálculo del índice.
Ejecución	Distorsiones en el proceso de formación de precios en la preapertura, sesión o subastas. Manipulación del protocolo FIX (Financial Information Exchange). Interferencias en al algoritmo de casación de órdenes. Interrupciones en las conexiones de los miembros al sistema de negociación.
Compensación y liquidación	Transferencias fraudulentas de fondos o activos a otros miembros. Manipulación de los registros de liquidación. Accesos no detectados a información reservada sobre posiciones abiertas y carteras de miembros y clientes que permitan obtener ventajas. Imposibilidad de realizar las liquidaciones diarias y ajustes de garantías.
Difusión información	Bloqueo de las redes de comunicación de información relevante y de operaciones.
Supervisión de las operaciones	Indisponibilidad de los sistemas de supervisión. Falta de integridad de los ficheros de operaciones.

Fuente: IOSCO y elaboración propia.

en las sesiones de contratación, si bien los potenciales efectos sistémicos serían reversibles en un lapso reducido de tiempo.

Una intrusión en las infraestructuras de postcontratación sí podría tener consecuencias importantes sobre la estabilidad financiera si con ella se imposibilitasen las funciones de pagos, liquidación y contrapartida central. Otra consecuencia potencialmente muy dañina para las infraestructuras de postcontratación sería la vulneración de datos sobre operaciones, lo que concedería significativas ventajas a aquellos que cuenten de manera ilícita con información reservada sobre posiciones abiertas y de carteras de otras instituciones financieras.

Es importante destacar que de acuerdo con un artículo publicado por el semanario The Economist en noviembre de 2015[14], el periodo medio de días desde que una red es atacada hasta que su «propietario» es consciente del ataque es de 205 días. En ese periodo de tiempo, la integridad de los mercados podría estar amenazada si un atacante dispusiese de información confidencial depositada en los registros de operaciones, depositarios centrales y cámaras de contrapartida central. Por este motivo, los análisis y pruebas de intrusión juegan un papel crítico en la detección temprana de ataques que puedan comprometer la confidencialidad de los registros centrales y las consecuentes fugas de información reservada.

Cabría analizar si las nuevas tendencias en lo que respecta a sistemas o estrategias de negociación (negociación algorítmica) y a la compensación y liquidación de valores (libro electrónico descentralizado, *distibuted ledger technology* o *blockchain*) suponen una reducción o por el contrario aumentan la posibilidad de ciberataques.

14 http://www.economist.com/news/business/21677639-business-protecting-against-computer-hacking-booming-cost-immaturity

Las tradicionales entidades de contrapartica central con un registro (libro) centralizado suponen en teoría una facilidad de acceso para los ciberataques al existir un único punto de entrada al sistema. Por el contrario, el carácter descentralizado del sistema de encriptado para cada transacción y la imposibilidad de alterar los registros por un único participante sin la autorización del resto, lo haría, en teoría, más resiliente a los ciberataques.

En el año 2015, Interpol logró introducir un software maligno (proof-of-concept malware) en un *blockchain* para demostrar que era posible realizar un ciberataque a una entidad descentralizada. En este caso, por la propia estructura del registro la propagación sería más fácil e inmediata.

En el documento de IOSCO «Cyber security in securities markets-An international perspective» de abril de 2016 se incluye un cuadro con las principales amenazas para las infraestructuras de mercado (IMF) en cada una de las partes de su cadena de valor.

Es imprescindible la dotación, formación y actualización continua de técnicos especializados en el área tecnológica que permitan a los supervisores de valores analizar y revisar los procedimientos de ciberseguridad puestos en práctica por las infraestructuras críticas sujetas a su supervisión, en el caso de la CNMV los mercados y las entidades de contrapartida central integradas en BME. Su presencia es también esencial en las tareas de coordinación con las entidades encargadas de la ciberseguridad de las infraestructuras críticas en cada país, en el caso de España el Centro Nacional para la Protección de Infraestructuras Críticas.

4 Directiva (EU) 2016/1148 del Consejo y Parlamento Europeo de 6 de junio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea

Esta directiva será de aplicación a las infraestructuras de los mercados bajo el ámbito de supervisión de la CNMV ya que se consideran como operadores de servicios esenciales.

Los artículos 4 y 5 de la directiva definen un operador de servicios esenciales como aquel cuya actividad es crítica para las actividades económicas. Los Estados miembros deberán identificar, antes de noviembre de 2018, los operadores de servicios esenciales y actualizar el listado cada dos años a partir de mayo de 2018.

El anexo II de la directiva incluye un listado de operadores de servicios esenciales con un apartado 4 específico, denominado infraestructuras de los mercados, que incorpora a los operadores de sistemas de negociación (mercados regulados, SMN o SON) [15] y a las entidades de contrapartida central[16]. Aunque no se recogen los depositarios centrales, los registros de operaciones (*trade repositories*) ni los sistemas de pagos, también deberían ser considerados esenciales y críticos.

La directiva entrará en vigor el 10 de mayo de 2018. Para entonces, deberá de estar traspuesta junto con el desarrollo de las normas y previsiones administrativas necesarias para garantizar su funcionamiento y cumplimiento.

Entre los requisitos de seguridad detallados en el artículo 14 de la directiva, figura que:

– Los operadores de mercado tomarán las apropiadas medidas técnicas y organizativas para hacer frente a los riesgos de seguridad de sus redes y sistemas de información. Estas medidas deberán garantizar un nivel de seguridad apropiado a los riesgos potenciales. En particular, se tomarán medidas para prevenir y minimizar el impacto de incidentes que afecten a las redes y sistemas de información en servicios esenciales y deberán garantizar la continuidad en la operatividad de los sistemas.

En línea con lo anterior, los Estados desarrollarán de manera coordinada estándares y principios de seguridad aplicables a las redes y a los sistemas de información. La

15 Definidas en el punto 24 del artículo 4 de la Directiva 2014/65/EU del Consejo y Parlamento Europeo

16 Definidas de acuerdo con el punto 1 del artículo 2 del Reglamento EU 648/2012 del Consejo y Parlamento Europeo.

Comisión Europea publicará una lista de principios de seguridad aplicables a los operadores de mercado.

– Los operadores de mercado deberán comunicar a la autoridad competente aquellos incidentes que tengan un impacto significativo sobre la seguridad de los servicios que provean.

Están previstas tanto la supervisión periódica, por parte de la autoridad competente del cumplimiento de las obligaciones de información de incidentes, como las sanciones en caso de incumplimiento. También la autoridad podrá requerir a los operadores cualquier información necesaria para evaluar la seguridad así como la realización de auditorías de seguridad.

En el ámbito de actuación de los Estados miembros, se requiere la constitución de un equipo de respuesta de emergencia (Computer Emergency Response Team), función que en España realizarían el Centro Nacional para la Protección de Infraestructuras Críticas y el Instituto Nacional de Ciberseguridad referenciados en el punto 3 de este informe.

La CNMV, y en particular su dirección general de mercados asistida por la dirección de sistemas de información, debe establecer contactos con estas dos entidades para evaluar y supervisar los planes de ciberseguridad de las infraestructuras críticas de los mercados financieros bajo el ámbito de supervisión de la CNMV. En el ámbito de la UE funciona la European Union Agency for Network and Information Security (ENISA) que cuenta con una unidad para para la protección y resiliencia de infraestructuras críticas (Critical Information Infrastructure Protection). Esta unidad tiene encomendada la asistencia a las agencias competentes de cada Estado miembro, al sector privado y a la Comisión Europea en el desarrollo de un plan de medidas de respuesta y recuperación de amenazas contra infraestructuras críticas de información.

Una de las tareas de esta unidad es el desarrollo de buenas prácticas en áreas como la elaboración de planes de contingencia, estrategias y medidas mínimas de ciberseguridad, ejercicios de simulación dentro de cada país e intercambio de información.

ENISA creó en julio de 2014 un grupo de trabajo dedicado a la seguridad de las redes de información del sector financiero. El objetivo de este grupo es:

– Elevar la concienciación del sector financiero sobre los riesgos de ciberataques.

– Promover buenas prácticas y su control en toda la organización de las entidades.

– Desarrollar medidas mínimas de seguridad para las infraestructuras de tecnologías de información y en concreto medidas específicas para el sector bancario.

La Directiva 2008/114 sobre la identificación y designación de Infraestructuras Críticas Europeas obliga a los Estados miembros a definir un sistema organizativo de protección de dichas infraestructuras, lo que dio lugar a la creación del Centro Nacional para la protección de Infraestructuras Críticas (CNPIC).

5 Normativa aplicable en España

En lo que respecta a la CNMV, existen dos fuentes de ordenamiento jurídico de la ciberseguridad. Por un lado, dentro de la regulación general aplicable a la ciberseguridad se encuentran dos directivas, una ley y un real decreto que contienen previsiones específicas aplicables a los operadores de servicios esenciales.

Por otro lado, y en el ámbito estricto de la regulación sectorial internacional de valores, existe una guía de CPSS-IOSCO cuyo objetivo es reforzar la resiliencia de las infraestructuras de mercado.

La ciberseguridad de las infraestructuras críticas en España, es una materia de seguridad nacional y el órgano político de mayor rango competente es la Comisión Nacional para la Protección de las Infraestructuras Críticas, adscrito a la Secretaría de Estado de Seguridad. Esta secretaría además es competente para aprobar los diferentes planes estratégicos sectoriales así como para designar los a los operadores críticos.

Actualmente, se encuentran en vigor las siguientes disposiciones:

– La Ley 8/2011[17], de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. Se define como infraestructura crítica, una infraestructura estratégica cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría grave impacto sobre los servicios esenciales.

– Real Decreto 704/2011[18], de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

Además, existen los siguientes planes: Plan Nacional de Protección de Infraestructuras Críticas, Planes Sectoriales Estratégicos, Planes de Seguridad de los Operadores, Planes Específicos de Protección y Planes de Apoyo Operativo.

Plan Estratégico Sectorial del Sector Financiero

De acuerdo con el art. 20 del RD 704/2011, los planes estratégicos sectoriales están clasificados como secretos oficiales y serán custodiados por la Comisión Nacional para la Protección de las Infraestructuras Críticas, si bien tendrán acceso a ellos los ministerios, en este caso, el de Economía, Industria y Competitividad. Estos planes deben de ser revisados cada dos años.

17 https://www.boe.es/boe/dias/2011/04/29/pdfs/BOE-A-2011-7630.pdf

18 http://www.cnpic.es/Biblioteca/Legislacion/Generico/REAL_DECRETO_704-2011_BOE-A-2011-8849.pdf

Para todos aquellos departamentos y organismos que cuenten con una copia de los planes estratégicos sectoriales será exigible el cumplimiento de las condiciones de seguridad de la Autoridad Nacional de Seguridad.

De acuerdo con el RD 704/2011, cada plan estratégico contendrá al menos los siguientes aspectos:

– Análisis de riesgos, vulnerabilidades y consecuencias.

– Propuestas de implantación de medidas organizativas y técnicas para prevenir, reaccionar y en su caso, paliar las posibles consecuencias de los diferentes escenarios que se prevean.

– Propuestas de actuación de otras medidas preventivas y de mantenimiento (simulacros, formación del personal, canales de comunicación y planes para abordar escenarios adversos).

– Medidas de coordinación con el Plan Nacional de Protección de Infraestructuras Críticas.

Los planes sectoriales están organizados en cuatro capítulos:[19]

– Capítulo 1. Normativa del sector.

– Capítulo 2. Estructura del sector.

– Capítulo 3. Análisis general de riesgos. Incluye la identificación de amenazas, planteamiento de escenarios de impacto y diseño de mapa de vulnerabilidades.

– Capítulo 4. Propuesta de medidas estratégicas: organizativas y técnicas, de mantenimiento y coordinación con el Plan Nacional del Infraestructuras Críticas.

Los planes estratégicos sectoriales surgen de los análisis de un grupo de trabajo que en el caso del sector financiero ha estado integrado por la Comisión PIC, el Ministerio de Economía y Competitividad (la Secretaría General del Tesoro y Política Financiera), la Dirección General de Seguros y Planes de Pensiones, el Banco de España y la CNMV con apoyo de una entidad de consultoría. Comparando el contenido de estos planes estratégicos con las recomendaciones de IOSCO se encuentran muchas similitudes, como por otra parte era previsible.

Los operadores críticos entre los que previsiblemente se encuentren los mercados regulados gestionados por BME y las entidades de contrapartida central, tendrán que designar ante la Comisión Nacional para la Protección de las Infraestructuras Críticas un responsable de seguridad y enlace que actuará como interlocutor ante las autoridades competentes en materia de ciberseguridad. Este requisito coincide con la guía de CPSS-IOSCO («Guidance on cyber resilience for financial market infraestructures») que se resume en el apartado 6 de este informe. En concreto, el

19 De acuerdo con el artículo Protección de infraestructuras críticas: El sistema de planeamiento como herramienta de implantación (I). Sánchez Gómez (2014). Seguridad y Ciudadanía. Ministerio del Interior http://www.interior.gob.es/documents/642317/1203831/Seguridad_y_Ciudadania_N_12_web_126140536.pdf/30e4e817-4105-47e6-8cc0-d32ece569845

punto 2.3.4 de la guía incluye que las infraestructuras deberán nombrar a un directivo senior como responsable de ejecutar la política de ciberseguridad dentro de la organización.

Los operadores críticos tienen que remitir una propuesta de plan de seguridad a la Comisión Nacional para la Protección de las Infraestructuras Críticas para su evaluación.

6 Trabajos sobre ciberseguridad del Comité de Pagos e Infraestructuras de Mercado, del Banco Internacional de Pagos

El Comité de Pagos e Infrastructuras del BIS creó un grupo de trabajo con el objetivo de evaluar la importancia de la ciberseguridad para las infraestructuras de los mercados financieros utilizando el marco de los principios para las infraestructuras de los mercados[20]. Estos principios intentan reducir los diferentes riesgos a los que se enfrentan las infraestructuras de los mercados entre los que se encuentran el de tipo legal, de mercado, de contraparte, de negocio y operacional.

El cumplimiento de las recomendaciones del mencionado Comité es ya una responsabilidad directa de la CNMV, en especial de cara a futuras evaluaciones del sector financiero (FSAP) que realiza el Fondo Monetario Internacional.

En este contexto, el trabajo del Comité ya cuenta con una restricción inicial puesto que ninguno de los principios fue desarrollado específicamente para considerar los riesgos de ciberataques. Por ello, la adecuación e idoneidad de las infraestructuras de los mercados para prevenir y hacer frente a un ciberataque se enmarca dentro de los principios orientados a reducir de manera prioritaria el riesgo operacional, en concreto el principio 17. De acuerdo con este principio *una infraestructura de mercado debe identificar las fuentes plausibles de riesgo operacional, tanto internas como externas, y mitigar su impacto mediante la utilización de políticas, procedimientos y controles*. Para ello, deben de ser diseñados sistemas que aseguren un alto grado de seguridad y fiabilidad operativa y contar con una capacidad adecuada y graduable. La gestión de la continuidad de las operaciones debe tener como finalidad recuperar la operatividad en un periodo lo más breve posible, prestablecido en dos horas.

En junio de 2016, CPSS-IOSCO hizo público el documento «Guidance on cyber resilience for financial market infraestructures», cuyo objetivo es proveer una guía para mejorar la ciberresiliencia de las infraestructuras de los mercados. El documento deja claro que no busca establecer nuevos principios a las infraestructuras sino proporcionar una mejor guía y una concreción de los principios ya existentes sobre gobierno (principio 2), marco de gestión de riesgos (principio 3), finalidad (principio 8), riesgo operacional (principio 17) e interconexiones (principio 20). Esta guía complementa otro informe previo de IOSCO publicado en abril de 2016 «Cyber Security in securities markets-An international perspective» que ofrece una visión de las diferentes aproximaciones reguladoras que los miembros de IOSCO han puesto en práctica hasta la fecha. España no se encuentra entre los países que han participado en el informe. La guía de IOSCO describe un marco de ciberseguridad en cinco apar-

20 Committee on Payment and Settlement Systems Technical Committee of the International Organization of Securities Commissions Principles for financial market infrastructures. April 2012 http://www.bis.org/cpmi/publ/d101a.pdf

tados para los que desarrolla una serie de prácticas cuyo cumplimiento reforzaría la ciberseguridad de las infraestructuras. Este marco está sujeto a continuos cambios por la propia naturaleza evolutiva de las amenazas:

1. **Gobernanza.** Se refiere a todos los acuerdos y procedimientos que la infraestructura ha puesto en práctica para gestionar los ciberriesgos. Las medidas no deben limitarse a aspectos técnicos sino que deben incluir personas, en concreto la dirección y el consejo de la entidad serán los responsables últimos de establecer y hacer cumplir el plan de ciberseguridad.

   Debe fomentarse en la cultura empresarial un elevado grado de compromiso y concienciación sobre aspectos de ciberseguridad. Para garantizarlos, el consejo de administración deberá contar con personas con la capacitación y conocimientos técnicos necesarios. La cultura corporativa deberá tener alineada y comprometida con la ciberresiliencia y hacer partícipes de ello al resto de la organización.

   Se incluye el ya citado requisito de nombrar a un directivo senior como responsable de la puesta en práctica y supervisión de las políticas de ciberseguridad, con autoridad, independencia y acceso al consejo.

   Se recomienda la realización de auditorías externas que evalúen de manera periódica la ciberresiliencia de la infraestructura.

2. **Identificación**. El objetivo es detectar aquellos procesos y operaciones críticas de la infraestructura que deben protegerse de manera prioritaria frente a los ciberataques, lo que permitirá priorizar la utilización de los recursos. Los sistemas de gestión y ejecución de órdenes, los sistemas de gestión de riesgos, de supervisión y de difusión de información se deberán incluir como procesos críticos.

   De nuevo se destaca la necesidad de involucrar en las tareas de ciberseguridad al mayor número de personas de la organización e incluso crear un comité con representantes de sistemas de información, de líneas de negocio, jurídicos, de recursos humanos, comunicación y gestión de riesgos. La mayoría de las plataformas de negociación incluidas en el informe cuentan con la figura de un director de seguridad de la información (Chief Information Security Officer)

3. **Protección.** Las infraestructuras deben implantar mecanismos de control en línea con los estándares más exigentes en materia de ciberseguridad. Las medidas pueden ser organizativas como la creación de centros de seguridad de las operaciones o técnicas como antivirus y sistemas de prevención de intrusos.

   a. Protección de los procesos y activos críticos. Con especial énfasis en la salvaguarda de información e identificación de debilidades. Además se recomienda rediseñar los procesos para incorporar mayor segmentación y puntos de control y permitir aislar posibles problemas.

   b. Interconexiones. Implantación de medidas protectoras para mitigar los riesgos y exigir a proveedores de servicios y participantes elevados estándares de ciberseguridad.

   c. Amenazas internas. Detección de comportamientos anómalos del personal y controles de acceso para limitarlo al personal autorizado.

d. Formación. Con especial incidencia e intensidad al grupo de empleados con acceso a sistemas y procesos de carácter restringido.

El siguiente cuadro resume las principales medidas y mecanismos de protección puestos en práctica por las infraestructuras participantes (34) que corresponden a 22 países miembros de IOSCO:

Ejemplos de medidas de protección frente a ciberriesgos adoptadas por las IMF CUADRO 2

Gestión y control IT	Controles de seguridad	Tecnologías de protección
Cumplimiento con los estándares globales como ISO, COBIT, SANS Top 20 controls, NIST Cyber security framework y otros estándares de ciber seguridad de la NIST. Practicas seguras de desarrollo de software.	Medidas de seguridad física. Investigaciones al personal. Política integral de contraseñas y controles de acceso a la red. Segregación de los sistemas y almacenamiento. Pruebas de vulnerabilidad y protección antes de lanzar nuevos programas, servidores y conexiones. Puntos de seguridad.	Web applications firewalls (WAF). Sistemas de prevención de intrusos/ sistemas de detección avanzados de amenazas. Sistemas defensa contra Distributed Denial of Service (DDoS). Plan de prevención de perdida de datos. Filtro antispam. Antivirus y antimalware. Encriptado. Bloqueo de puertos, IP y filtros de red. Herramientas forenses y de respuesta ante incidentes. Análisis de software maligno.

Fuente: IOSCO «Cyber Security in securities markets-An international perspective».

4. **Detección.** Capacidad para reconocer potenciales incidentes o detectar que se ha cometido una ruptura de seguridad en los sistemas.

   a. Supervisión continua en tiempo real o con la menor latencia posible con objeto de detectar actividades anómalas.

   b. Supervisión de amplio rango de factores externos e internos.

   c. Controles en varios niveles (*multi-layered*) que incluyan personas y procesos y con cada nivel actuando como red de seguridad de los precedentes.

5. **Respuesta y recuperación.** La capacidad de la infraestructura para continuar con sus funciones, restaurar los sistemas críticos tras un ataque y reducir el riesgo sistémico que generaría una interrupción en su actividad.

   a. Plan de respuesta. Para determinar los daños y el alcance de un posible ataque y tomar las medidas de contención.

   b. Reinicio de actividad en un periodo de dos horas. Los procesos y operaciones críticas deben de ser reanudadas en un margen de dos horas tras el ataque y completar la liquidación de las operaciones antes de la sesión siguiente de negociación.

   c. Plan de contingencia. En el caso de que no sea posible reanudar las operaciones críticas en un periodo de dos horas debe de existir un plan alternativo con varios escenarios.

d. Planificación y preparación. La infraestructura debe de tener preparado y comprobado regularmente un plan de respuesta y recuperación frente a ataques.

e. Interconexiones. En caso de ataques que pudiesen comprometer la integridad de los datos e hiciesen insegura incluso la utilización de *back up*, se recomienda la posibilidad de obtener los datos de una tercera entidad. Las infraestructuras de los mercados están abiertas para sus miembros, que acceden en tiempo real tanto a los sistemas de negociación como a los registros de operaciones. Por ello, las entidades financieras miembros pueden ser tanto una fuente de contagio como verse afectadas por las amenazas.

Además se destacan varias prácticas que mejoran la ciberresiliencia de las entidades entre las que se incluyen las simulaciones y pruebas y la ciberinteligencia.

Este marco de ciberseguridad, es idéntico al planteado por la National Institute of Standarts and Technology (NIST) del Departamento de Comercio de EE.UU[21] y recoge buena parte de los estándares, guías y principios detallados en el documento «Framework for Improving Critical Infrastructure Cybersecurity» de febrero de 2014.

Pruebas y simulaciones

Las pruebas constituyen uno de los pilares fundamentales del marco de la ciberseguridad. Todos los elementos del programa de ciberseguridad deben de ser probados de manera rigurosa para comprobar su efectividad e identificar fallos y debilidades. Dicho programa de pruebas debe incorporar:

– Evaluación de la vulnerabilidad con soluciones a los fallos potenciales detectados.

– Pruebas basadas en escenarios, en las que se evalúen los planes de respuesta, resolución y recuperación y se contemplen escenarios extremos pero posibles. Deben utilizarse incluso modelos que contemplen posibles amenazas.

– Pruebas de intrusión en los sistemas, redes, procesos y personal. Deben de realizarse regularmente y siempre que se acometa una actualización o mejora de los sistemas.

En relación con el siguiente punto, las infraestructuras deberían participar en grupos sectoriales, con carácter internacional y con los supervisores sectoriales con competencias en ciberseguridad para reunir, distribuir y analizar información sobre prácticas de ciberseguridad, amenazas e indicadores adelantados que permitan anticipar posibles ataques.

Recolección de información sobre ciberamenazas (*cyber intelligence*)

El entorno de las ciberamenazas tiene un carácter de permanente cambio y evolución. Por poner un ejemplo asimilable, podría asimilarse a los algoritmos empleados

21 https://www.nist.gov/sites/default/files/documents/cyberframework/framework_orientation_20160405.pdf

por los negociadores de alta frecuencia que necesitan ser continuamente revisados para adaptarlos a las reacciones de los competidores.

Por ello, debería recolectarse e intercambiar información con el resto de infraestructuras y con los gobiernos sobre los ciberataques sufridos. El objetivo es crear una base de datos con las recientes y mayores amenazas así como posibles soluciones.

Una vez superado un ataque es conveniente dar a conocer las vías de acceso utilizadas para el ataque y las soluciones planteadas para su resolución.

– Acceso a nuevos conocimientos y capacidades.

– Capacidad de predicción.

– Elaboración de métricas para evaluar la resiliencia de los sistemas de información.

Es precisamente la recolección, tratamiento y puesta en común de la información sobre amenazas y ataques uno de los puntos clave que de manera recurrente y por parte de todos los organismos y expertos en ciberseguridad se destaca como crucial. La naturaleza de las ciberamenazas de carácter global, en muchas ocasiones alentadas por determinados Estados y la interconexión que posibilita su rápida propagación hace imprescindible contar con una actualizada base de datos sobre ataques y medidas para evitarlos. Es lo que se denomina *cyberthreat intelligence sharing.* En el caso de España y de acuerdo con el informe Ciberamenazas 2015/Tendencias 2016 del Centro Criptologico Nacional[22], el 90% de los cibertaques más graves contra las administraciones públicas y las empresas de interés estratégico provienen de gobiernos extranjeros.

Existen varias iniciativas de empresas del sector que han puesto a disposición pública información sobre ciberamenazas, como http://cyberthreatalliance.org/, http://www.brightcloud.com/, https://exchange.xforce.ibmcloud.com/

Por otra parte, en España el CNPIC viene estableciendo una política de colaboración con diversos CERT (Computer Emergency Response Teams), con objeto establecer una política de colaboración, coordinación y compartición de toda información relativa a amenazas e incidentes sobre ciberseguridad, como herramienta de reacción y respuesta ante incidentes de seguridad informática y proporcionar servicios de análisis y alerta temprana de amenazas y riesgos cibernéticos. Entre los CERT con los que se han fijado políticas de colaboración figuran, CCN-CERT, CERTSI o INCIBE.

El documento de IOSCO anteriormente citado «Cyber Security in securities markets-An international perspective», reconoce que aunque los riesgos de ciberataques pueden tratarse dentro de las políticas globales de riesgo operacional, el principio 17 aplicable a las infraestructuras de los mercados, destaca que existen particularidades que deben de considerarse:

– Los ciberataques más sofisticados suelen ser de carácter persistente y de difícil detección y eliminación. Además, estos ataques pueden tener capacidad de

22 https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1483-ccn-cert-ia-0916-ciberamenazas-2015-tendencias-2016-resumen-ejecutivo/file.html

propagación silenciosa dentro de una red de sistemas de información a otras infraestructuras y/o miembros participantes.

– Pueden existir ataques frente a los cuales los planes de contingencia y de gestión de riesgos sean inefectivos y extenderse a los sistemas de *backup* lo que haría que la restauración de la actividad de la infraestructura pudiese propagar el riesgo a los participantes.

– Existen múltiples puntos de entrada de los ciberataques y además las infraestructuras están conectadas entre si y con los participantes lo que extiende la potencial vulnerabilidad a agentes externos. Por ello, la vía de entrada de los ataques podría ser un miembro de pequeño tamaño y con escasas medidas de protección.

En el ámbito internacional, IOSCO apunta, en su ya citado documento de 2016, la posibilidad de centralizar toda la información sobre ataques y amenazas. Para ello, ha analizado la viabilidad e idoneidad del IOSCO's Multilateral Memorandum of Understanding (MMoU) como instrumento que facilite el intercambio de información entre supervisores.

Una versión preliminar de la guía de IOSCO preveía tres escenarios con un nivel ascendente de gravedad en los ataques a las infraestructuras:

Escenario 1: Ruptura de la confidencialidad.

– Robo de información confidencial sobre activos, posiciones y clientes que mantiene la infraestructura.

– El ataque puede ser la primera fase de una oleada de sucesivos incidentes, una vez vulnerado el sistema de seguridad.

– Puede ser de difícil detección y resolución.

– Puede suponer daños reputacionales para la infraestructura.

Escenario 2: Ruptura de la disponibilidad

– Los servicios de la infraestructura no están disponibles.

– La comunicación entre la infraestructura y sus miembros/participantes y proveedores de información está afectada.

– Los efectos del ataque empeoran con el transcurso del tiempo.

Escenario 3: Ruptura de la integridad

– Los datos clave de la infraestructura están afectados por el ataque.

– No es posible garantizar la integridad de los sistemas y de la información almacenada en la infraestructura.

– Los sistemas de respaldo (*backup*) también están afectados o no cuentan con total integridad.

- En un principio los sistemas parecen funcionar correctamente.
- Decidir si es necesario, parar el funcionamiento de la infraestructura, llevar a cabo un reinicio a un estado previo en el que exista confianza en la seguridad de las operaciones.
- El tiempo necesario para detectar y analizar el problema de seguridad puede ser muy considerable.
- Potencial impacto sistémico debido a que las posiciones en instrumentos financieros de los participantes pueden quedar bloqueadas o no estar correctamente identificadas.
- Se puede generar desconfianza en los mercados financieros debido a la imposibilidad de asignar la titularidad de las acciones, bonos y resto de instrumentos financieros.
- Posibilidad de contagio a otras infraestructuras y participantes con efectos sobre la liquidez.

Una de las claves destacadas en el documento para conseguir una resiliencia a los ciberataques es contar con una estrategia de defensa que implique a toda la organización y no sólo a aquellos directamente vinculados a los sistemas e información y tecnología. No puede olvidarse que cada puesto de trabajo conectado con el exterior es una vía potencial de entrada de ciberamenazas por lo que es vital concienciar y hacer partícipes a todos los empleados de las medidas de protección. Un reciente ataque a los sistemas de una de las mayores aseguradoras de salud de EE.UU (Anthem) tuvo su entrada a través de un correo basura (*pishing*) que un empleado abrió y permitió con ello el acceso a los sistemas de la compañía[23].

El informe propone medidas que se agrupan en tres ámbitos: prevención, detección y recuperación tras un ciberataque. Para ello es necesario actuaciones en el ámbito internacional que incluyan:

1. Armonizar las actuaciones de las diferentes jurisdicciones y en concreto apoyar los esfuerzos en países emergentes.
2. Promover y facilitar los intercambios de información sobre ciberataques registrados en las diferentes jurisdicciones.
3. Crear una «biblioteca» de conocimiento sobre ciberseguridad y respuesta a los ciberataques a disposición de las autoridades e infraestructuras.
4. Desarrollar principios de ciberseguridad y resiliencia junto con una normativa sancionadora de las conductas delictivas.
5. Establecer una guía de emergencia para poner en práctica en caso de ciberataques en gran escala a infraestructuras de los mercados.

23 http://www.ft.com/intl/cms/s/2/f3cbda3e-a027-11e5-8613-08e211ea5317.html#axzz3uxoWO0PZ