Recuadro 5
CIBERATAQUES A LAS INFRAESTRUCTURAS DEL MERCADO FINANCIERO

El documento "*Guidance on Cyber Resilience for Financial Markets Infrastructures*", elaborado por el *Committee on Payments and Market Infrastructures* (CPMI) del *Bank for International Settlements* (BIS), presenta una guía para fortalecer a las infraestructuras frente a los ciberataques. El BIS enfatiza que el objetivo es lograr que el tiempo de recuperación de una infraestructura ante un ciberataque sea de dos horas. El documento propone 5 categorías que se deben tomar en cuenta para la administración de riesgos:

a. Gobernabilidad: Consiste en la creación de un marco de resistencia ante ciberataques que debe definir objetivos, requerimientos (personas, procesos y tecnologías) y la comunicación y colaboración de los involucrados.

b. Identificación: Las infraestructuras deben identificar sus funciones críticas de negocio y sus activos de información por orden de prioridad. La identificación de las funciones permitirá reconocer su importancia para ser protegidos y la identificación de activos de información permitirá mantener un inventario y conocer qué activos soportan las funciones del negocio.

c. Protección: La resistencia a ciberataques depende de la efectividad de la seguridad en proteger la confidencialidad, integridad y accesibilidad a los activos y servicios mediante controles y diseño de resistencia en tecnologías de comunicación. Los controles de seguridad tienen como función minimizar la probabilidad y el impacto de un ciberataque sobre una función de negocio o activo de información identificada.

d. Detección: La detección de un ciberataque provee tiempo para contrarrestarlo e implementar mecanismos de seguridad apropiados. El monitoreo es una herramienta importante para detectar actividades anómalas y su alcance debe incluir la línea de negocio y funciones y transacciones administrativas. Su cobertura debe incluir personas, procesos y tecnología.

e. Respuesta y recuperación: Las infraestructuras deben ser capaces de reasumir los sistemas críticos de forma rápida, segura y con información exacta para mitigar el riesgo sistémico. Una infraestructura debe reasumir actividades críticas y habilitar sus operaciones en aproximadamente dos horas después del ciberataque y habilitar hacia el final del día la liquidación completa.

Asimismo, se analizan 3 componentes que se deben tomar en cuenta en la elaboración del marco de resistencia ante ciberataques:

a. Pruebas: Una infraestructura debe establecer un programa de pruebas para validar todos los elementos del marco de resistencia a ciberataques. Emplear metodologías y prácticas de testeo que contengan la evaluación de vulnerabilidades, escenario base para simulación de ciberataques extremos, test de penetración de los sistemas, etc.

b. Conocimiento de la situación: Se refiere al entendimiento completo de las amenazas a ciberataques. Este entendimiento permite reevaluar la dirección de la estrategia, la asignación de recursos, procesos, procedimientos y controles.

c. Aprendizaje y evolución: Una infraestructura debe implementar un marco de resistencia adaptativo que evolucione con la naturaleza dinámica de los riesgos cibernéticos. Se debe identificar y aprender de eventos cibernéticos que han ocurrido dentro y fuera de la organización y se debe trabajar para lograr capacidades predictivas y proactivas capturando información de múltiples fuentes internas y externas.

Debido al avance tecnológico y a la mayor importancia que tienen las infraestructuras en la estabilidad del Sistema Financiero, cada vez se hace más necesario fortalecer y revisar continuamente los aspectos relacionados a la administración de riesgos cibernéticos, esfuerzo que no puede ser aislado sino que debe involucrar a empresas y regulados que participan.