La FCA, el Banco de Inglaterra y la Autoridad de Regulación Prudencial (PRA) han publicado el último informe temático anual de CBEST.



CBEST pone a prueba la resiliencia cibernética de las empresas y las infraestructuras del mercado financiero (FMI) a través de pruebas en vivo que imitan las acciones de los atacantes cibernéticos.

El informe, que contiene buenas prácticas y conocimientos sobre resiliencia cibernética, incluidos los del Centro Nacional de Seguridad Cibernética (NCSC), se publica en su totalidad por primera vez. Destaca la importancia de construir una sólida higiene cibernética y la necesidad de que las empresas simulen una variedad de escenarios de pruebas cibernéticas para seguir siendo resilientes a las amenazas.

La resiliencia cibernética es una prioridad para nosotros, el Banco y la ARP. Las perturbaciones de los ciberataques pueden afectar a la estabilidad financiera, causar daños intolerables a los consumidores u otros participantes en el mercado, o perturbar la confianza del mercado.

Las empresas y las IMF deben leer la [temática de CBEST](http://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/2023-cbest-thematic) y considerar la posibilidad de incorporar los resultados en sus estrategias cibernéticas.



Temática CBEST 2023

La temática anual de CBEST tiene como objetivo informar al sector sobre nuestros hallazgos y lecciones aprendidas de nuestro programa CBEST, que evalúa la resiliencia cibernética de las instituciones financieras sistémicas a través de pruebas en vivo realizadas en sus redes corporativas.



**1: Descripción general**

La resiliencia cibernética es una prioridad para los reguladores. En los últimos años, los reguladores han aumentado significativamente su enfoque en la resiliencia operativa. Por «[**resiliencia operativa**](https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector)» nos referimos a la capacidad de las empresas/IMF y del sector financiero para absorber las perturbaciones y las perturbaciones y adaptarse a ellas, en lugar de contribuir a ellas.

Con el fin de mejorar la resiliencia de las empresas/IMF de importancia sistémica y, por extensión, del sistema financiero en general, llevamos a cabo el programa CBEST para evaluar la ciberresiliencia de los servicios empresariales importantes de las empresas/IMF. [**CBEST**](https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/cbest-threat-intelligence-led-assessments-implementation-guide) promueve un enfoque de pruebas de penetración basado en inteligencia que imita las acciones de los atacantes cibernéticos que intentan comprometer los servicios comerciales importantes de una organización e interrumpir los activos tecnológicos, las personas y los procesos que respaldan esos servicios. Este enfoque significa que existe un "hilo dorado" que vincula las pruebas de seguridad con las amenazas, con las actividades de una organización y el impacto potencial en la economía en general (Figura A).

Como parte de las pruebas CBEST, las instituciones financieras sistémicas se someten a pruebas en vivo que evalúan sus capacidades de detección y respuesta a través de simulaciones de los escenarios cibernéticos más relevantes.

**Figura A: El "hilo dorado" guiado por la inteligencia**



El propósito de CBEST es proporcionar una evaluación priorizada que permita a las empresas/IMF comprender mejor las debilidades y vulnerabilidades en sus entornos. Sobre esta base, pueden adoptar las medidas correctoras adecuadas, mejorando así su resiliencia y, por extensión, la del sistema financiero en general. Como reguladores, extraemos lecciones temáticas para informar nuestras prioridades de supervisión en materia de ciberseguridad y resiliencia cibernética.

Los reguladores están publicando los resultados temáticos del último ciclo de evaluaciones de CBEST sobre los bancos, las aseguradoras, los gestores de activos e inversiones y las IMF participantes.

Esta publicación es el resultado de la colaboración entre los reguladores y el Centro Nacional de Seguridad Cibernética (NCSC), la autoridad cibernética pública del Reino Unido. En las secciones 6 y 7, proporcionamos enlaces a la guía relevante del NCSC para estos temas y otros recursos cibernéticos del NCSC. Estos enlaces representan directrices técnicas recomendadas, pero no pretenden establecer nuevos requisitos reglamentarios.

**2: Objetivos**

**Esta publicación será útil para los especialistas de SMF24, CISO, CIO, COO, CRO y Cyber de su empresa.**

La intención de esta publicación es hacer que las lecciones aprendidas a través de nuestros programas regulatorios estén ampliamente disponibles para beneficiar a todo el sector financiero del Reino Unido. Le animamos a que utilice estos hallazgos para:

(a) considerar las observaciones de inteligencia de amenazas y las debilidades identificadas y abordar debilidades similares en su organización;

b) sensibilizar a su equipo directivo superior; y

(c) informar al trabajo de sus funciones de auditoría interna y de riesgo.

**3: El proceso temático**

Los hallazgos se basan en los resultados de las pruebas de penetración y la evaluación de detección y respuesta. También compartimos observaciones sobre la inteligencia de amenazas generada a través de CBEST y las tendencias temáticas a través de la [**Herramientas de evaluación de madurez de inteligencia de amenazas cibernéticas Se abre en una ventana nueva**](https://www.crest-approved.org/buying-building-cyber-services/cyber-threat-intelligence-maturity-assessment-tools/). Estas observaciones podrían ser útiles para las empresas/IMF que están considerando sus propios programas de pruebas basados en amenazas.

Los reguladores siguen colaborando con las empresas/FMI, los reguladores internacionales y los organismos gubernamentales para desarrollar CBEST. Agradeceríamos cualquier comentario o sugerencia sobre estos hallazgos temáticos. Por favor, envíelos a **CBEST@bankofengland.co.uk**.

**4: Inteligencia de amenazas en CBEST**

Como marco de pruebas basado en inteligencia de amenazas, CBEST requiere que los evaluadores simulen a los actores de amenazas identificados por expertos en inteligencia de amenazas cibernéticas (CTI). En esta sección, compartimos observaciones sobre la inteligencia de amenazas que podrían ser útiles para las empresas/FMI que están considerando sus propios programas de pruebas basadas en amenazas.

La inteligencia puede mejorar la comprensión de una empresa/FMI del entorno de amenazas específico en el que opera:

**«Un fuerte conocimiento de la situación, adquirido a través de un proceso eficaz de CTI, puede marcar una diferencia significativa en la capacidad del FMI para anticiparse a los eventos cibernéticos o responder a ellos de forma rápida y eficaz. Específicamente, una apreciación aguda del panorama de amenazas puede ayudar a una IMF a comprender mejor las vulnerabilidades en sus funciones comerciales críticas y facilitar la adopción de estrategias adecuadas de mitigación de riesgos".**

Estas observaciones no pretenden, y no deben interpretarse, como un sustituto de las propias actividades de inteligencia interna de una empresa/FMI y no deben utilizarse como una articulación de todo el panorama de amenazas.

**4.1: Observaciones de los actores de amenazas**

Hubo tres tipos principales de actores de amenazas involucrados en las simulaciones de escenarios de CBEST:

* actores estatales, o amenazas persistentes avanzadas (APT);
* grupos delictivos organizados; y
* Amenazas internas.

CBEST continúa demostrando el valor de simular atacantes internos privilegiados, como personas internas malintencionadas y/o ataques a la cadena de suministro. Estos escenarios representan una oportunidad para que una empresa/FMI pruebe los controles dentro de la red en lugar de en el perímetro.

Para mejorar el realismo e introducir complejidad, los escenarios ocasionalmente superponen motivaciones o intensificadores que compiten entre sí (como APT que ejecutan ataques a la cadena de suministro o personal que es chantajeado por ciberdelincuentes). Esta vinculación de múltiples actores en un solo escenario permite realizar pruebas de alto valor, como la exploración de vectores de ataque inusuales o inesperados a lo largo de vías confiables.

Los escenarios tenían una amplia gama de motivaciones de actores de amenazas, en línea con el panorama de amenazas diverso y dinámico. Las motivaciones indicativas fueron:

a) beneficios económicos;

(b) robo de información;

c) perturbación de las operaciones;

d) daños a la reputación; y

(e) Robo de información de identificación personal.

Los actores de amenazas actuaron con diferentes objetivos en servicios comerciales importantes. La totalidad de la tríada de confidencialidad, integridad y disponibilidad se observó en la segmentación y la generación de escenarios; todos fueron aproximadamente iguales en su frecuencia general.

**4.2: Observaciones de la evaluación de la madurez de la inteligencia de amenazas**

El proceso CBEST incluye una autoevaluación con respecto a la CREST [**Herramientas de evaluación de madurez de inteligencia de amenazas cibernéticas Se abre en una ventana nueva**](https://www.crest-approved.org/buying-building-cyber-services/cyber-threat-intelligence-maturity-assessment-tools/). La herramienta tiene cuatro temas: gobernanza, planificación y requisitos de programas, operaciones de inteligencia de amenazas y resiliencia.

Las empresas/IMF, en promedio, obtuvieron puntuaciones más altas en **A: Gobernanza** y **D: Resiliencia**. Esto sugiere que las empresas/IMF tienen buenos cimientos (en términos de gestión y sostenibilidad/repetibilidad) detrás de sus modelos operativos de CTI, pero resultados más débiles en la integración con el negocio y la producción y difusión de resultados de inteligencia.

Las empresas/IMF, en promedio, obtuvieron puntajes más bajos en **B: Planificación y requisitos de programas y** **C: Operaciones de inteligencia de amenazas**.

Estos abarcan el enfoque del personal y la gestión de los recursos en una función de CTI, y el ciclo de vida de la inteligencia de extremo a extremo. En conjunto, esto sugiere que las empresas/IMF podrían tender puentes entre sus sólidos cimientos y la aplicación práctica.

**5: Hallazgos temáticos de las pruebas**

**5.1: Gestión de identidades y accesos**

La gestión de acceso débil o ausente para los activos críticos hace que el acceso no autorizado a información, servicios y recursos críticos sea más probable. Los reguladores consideran que la gestión eficaz de la identidad y el acceso es un objetivo clave para la higiene cibernética fundamental.

Ejemplos positivos incluido:

a) el fortalecimiento de Active Directory, un área en la que los ataques son objeto de ataques frecuentes y sostenidos; y

(b) Uso de autenticación reforzada para cuentas humanas.

Entre las brechas más comunes se encuentran:

(c) falta de establecimiento, suficiente fuerza y/o aplicación de políticas y normas que rigen la gestión de la identidad y el acceso;

d) un endurecimiento insuficiente de las cuentas privilegiadas y de servicios; y

e) la falta de una autenticación sólida (multifactor) para los activos críticos, como los servidores.

**5.2: Sensibilización y formación del personal**

El personal es fundamental para la capacidad de cualquier organización para operar de forma segura. Sin la capacitación suficiente, los empleados podrían causar daños accidentales o intencionales a la confidencialidad, integridad o disponibilidad de los activos de información. Como reguladores, observamos el esfuerzo de toda la organización necesario para que las empresas/IMF sigan siendo resilientes. Esto incluye personal altamente técnico, usuarios ordinarios y personal externo.

Algunos ejemplos positivos fueron:

a) la ejecución de una respuesta rápida y de alta calidad por parte de personal especializado en seguridad;

b) la erradicación de las amenazas para proteger importantes servicios prestados a las empresas;

c) la notificación oportuna y proactiva de campañas de phishing simuladas activas; y

(d) el uso de contraseñas seguras que demostraron ser resistentes a los intentos de descifrado de hash.

Entre las brechas más comunes se encuentran:

e) la falta de búsqueda y evaluación de la causa raíz de la disponibilidad de secretos o credenciales que se conservan en repositorios internos de fácil acceso;

f) la falta de revisión y medición suficientes de la higiene cibernética, en particular en el caso de las contraseñas;

g) la exposición excesiva de datos sensibles en los medios de comunicación públicos en los sitios web propiedad de empresas o FMI, así como los de terceros (incluidos los «scrapers» de código abierto); y

(h) información técnica confidencial divulgada en descripciones de puestos, publicaciones en sitios web corporativos o redes sociales.

**5.3: Configuración segura**

Los activos y sistemas de TI configurados adecuadamente pueden evitar el uso indebido no intencionado o no autorizado de los activos críticos. Asegurarse de que los sistemas se diseñan, aprovisionan y prueban de forma correcta y sólida reduce la superficie de ataque a los atacantes internos y externos. El uso indebido, la explotación, la corrupción y la elusión total de capas enteras de controles pueden ser posibles si un actor de amenazas identifica y explota las configuraciones incorrectas de los activos y servicios. Mientras que los recursos implementados de forma segura y bien administrados podrían ser esenciales para ralentizar o interrumpir la capacidad de los actores de amenazas para avanzar en sus ataques.

Algunos ejemplos positivos fueron:

a) las empresas/FMI que configuraron de forma segura los servicios de infraestructura fundamentales demostraron una mayor resiliencia al interrumpir las rutas de ataque menos sofisticadas adoptadas por atacantes simulados menos cualificados.

Entre las brechas más comunes se encuentran:

b) la configuración insegura, o la falta de pruebas, de las plantillas y certificados clave;

c) la susceptibilidad a los ataques basados en la memoria que explotan las contraseñas almacenadas en caché o almacenadas en los servicios de seguridad; y

d) el incumplimiento del principio de mínimo privilegio/funcionalidad para evitar el uso indebido de una serie de cuentas humanas y no humanas.

**5.4: Seguridad de la red**

Las debilidades en las redes hacen que el acceso no autorizado a datos y sistemas confidenciales sea más probable. Las debilidades también ayudan a un atacante al facilitar el movimiento por la infraestructura objetivo, lo que aumenta el impacto de un ataque. Los reguladores señalan que las debilidades de seguridad en relación con las redes corporativas siguen siendo un problema recurrente en las pruebas de CBEST.

Algunos ejemplos positivos fueron:

a) redes muy segmentadas, en particular en torno a las infraestructuras críticas;

b) la delimitación de los sistemas/servicios básicos dentro de las "zonas bastión" específicas (aunque hay que tener en cuenta que los bastiones pueden ser atacados si no se gestionan adecuadamente); y

c) el uso de normas y buenas prácticas del sector para reforzar la infraestructura o los activos que respaldan importantes servicios empresariales.

Entre las brechas más comunes se encuentran:

d) redes corporativas insuficientemente segregadas;

e) la falta de segregación, que refleje la cartografía de los servicios empresariales importantes de una empresa; y

f) las deficiencias derivadas de la exposición a redes propiedad del grupo o controladas por él (por ejemplo, la limitación de la exposición de las zonas seguras de la red frente a los movimientos laterales de otras entidades del grupo).

**5.5: Respuesta a incidentes y supervisión de la seguridad**

Las brechas en el monitoreo, el registro y la detección de actividades maliciosas significan que los incidentes no se contienen y los actores de amenazas no se erradican de la red. Esto expone a los sistemas que prestan servicios empresariales importantes a daños o interrupciones. Los hallazgos de CBEST continúan ilustrando la importancia de un monitoreo de seguridad suficiente, integral y oportuno.

Algunos ejemplos positivos fueron:

a) flujos de trabajo eficientes y flexibles que permitan que la inteligencia alimente nuevos controles preventivos y/o casos de uso de detección para evitar que se repitan los riesgos; y

b) Capacidades de respuesta amplias y rápidas (ya sea mediante la automatización o mediante personal cualificado) capaces de erradicar los ataques activos antes de que puedan afectar a servicios empresariales importantes.

Entre las brechas más comunes se encuentran:

(c) sistemas inseguros, excesivamente permisivos o de fácil acceso para la emisión de tickets, el seguimiento y el escalamiento de incidentes;

d) la falta de personal especializado preparado para llevar a cabo actividades complejas de respuesta; y

e) la falta de registro (tanto en entornos de producción como en los que no son de producción) o la retención insuficiente de registros.

**5.6: Seguridad de los datos**

La protección de la confidencialidad, integridad y disponibilidad de los datos críticos es fundamental para la seguridad y la solidez de los servicios empresariales importantes. La seguridad de los datos puede ser la última línea de defensa, incluso cuando los controles perimetrales y de red han fallado.

Algunos ejemplos positivos fueron:

a) el despliegue de algoritmos de cifrados sólidos; y

(b) el uso de cifrado de unidad completa para mitigar los ataques en los que los activos estaban físicamente fuera del control de una organización.

Entre las brechas más comunes se encuentran:

c) niveles inadecuados de protección para el descanso y el tránsito; y

d) incoherencias en los niveles de protección de datos, por ejemplo, en la forma en que se crean y almacenan las copias de seguridad de los datos.

**6: Perspectivas del NCSC**

**6.1: Gestión de identidades y accesos**

Las organizaciones necesitan comprender, documentar y gestionar el acceso a las redes y los sistemas de información. Esto debe incluir garantizar que los usuarios que pueden acceder a datos o servicios estén debidamente verificados, autenticados y autorizados. Las actividades de apoyo a esta esfera incluyen la formulación de políticas, el establecimiento de identidades, la gestión del acceso privilegiado, el diseño arquitectónico y la supervisión.

**6.2: Sensibilización y formación del personal**

Las organizaciones deben asegurarse de que el personal tenga la conciencia, los conocimientos y las habilidades adecuados para llevar a cabo sus funciones organizativas de forma eficaz. Las actividades para apoyar esto incluyen el desarrollo de una cultura de seguridad positiva y la participación activa del personal para comunicarse sobre la seguridad de las redes y los sistemas de información, y cómo se relaciona con sus trabajos.

**6.3: Configuración segura**

La arquitectura y la configuración de los activos/sistemas son de vital importancia, ya sea al comienzo de cualquier desarrollo, hasta el final de su vida útil. Obtener la seguridad desde el principio ayuda a crear sistemas que son más fáciles de mantener seguros y pueden reducir la necesidad de costosos retrabajos en el futuro.

Las organizaciones deben comprender el contexto y los riesgos a los que se enfrentan y decidir si pueden aceptarlos. Un enfoque de seguridad por capas dificulta el compromiso y la interrupción para los posibles atacantes. Esto incluye reducir el impacto del compromiso para evitar que los atacantes se muevan lateralmente dentro de los sistemas, evitar que el malware se ejecute en los dispositivos si los atacantes llegan a los puntos finales y planificar la copia de seguridad y la recuperación. También es importante facilitar la detección y la investigación de los riesgos a través de métodos de comunicación definidos y estrictamente controlados, y la recopilación de registros para la supervisión del sistema.

**6.4: Seguridad de la red**

La seguridad de la red es un componente crítico para evitar el acceso no autorizado al sistema o la interrupción. Las actividades para respaldar esto incluyen la creación de arquitecturas de seguridad más sólidas, la segregación de los servicios y sistemas más críticos en zonas de mayor seguridad y la protección de los límites de la red. Además, reducir la superficie de ataque limitando los flujos y componentes solo a los que son necesarios, asegurando la plataforma de forma predeterminada y creando una capa de administración separada a través de equipos dedicados y separación de redes.

**6.5: Respuesta a incidentes y supervisión de la seguridad**

La respuesta a incidentes y la supervisión de la seguridad ayudan a facilitar la detección de riesgos y a reducir el impacto de los riesgos. Dentro de la respuesta a incidentes, las organizaciones deben implementar procesos bien definidos de gestión y mitigación de incidentes. Estos deben probarse para garantizar la continuidad de las funciones esenciales en caso de falla del sistema o del servicio. También debe haber actividades de mitigación para limitar el impacto del compromiso.

Para la supervisión de la seguridad, las organizaciones deben supervisar el estado de seguridad de las redes y los sistemas que soportan las funciones esenciales, detectar posibles problemas de seguridad y realizar un seguimiento de la eficacia continua de las medidas de seguridad de protección.

**6.6: Seguridad de los datos**

La seguridad eficaz de los datos garantiza que los datos almacenados o transmitidos electrónicamente estén protegidos de acciones que causen un impacto adverso en las funciones esenciales. Las organizaciones deben tener en cuenta la protección de los datos en tránsito, los datos en reposo, la protección de los datos en los dispositivos móviles, la eliminación segura y la arquitectura del diseño de los sistemas para proteger los datos importantes.







**7: Recursos adicionales de seguridad cibernética del NCSC**

**7.1: Recomendaciones y orientaciones generales del NCSC**

* Regístrese para el NCSC [**Servicio de Alerta Temprana Se abre en una ventana nueva**](https://www.ncsc.gov.uk/information/early-warning-service). Este servicio gratuito ayuda a las organizaciones a investigar los ciberataques notificándoles la actividad maliciosa que se ha detectado en las fuentes de información. Si ya está registrado, utilice el portal de alerta temprana para ver y realizar cambios en los activos registrados y los datos de contacto.
* Regístrese para el [**Asociación para compartir información de seguridad cibernética Se abre en una ventana nueva**](https://www.ncsc.gov.uk/section/keep-up-to-date/cisp) es un servicio digital conjunto de la industria y el gobierno que permite a las organizaciones del Reino Unido compartir información sobre amenazas cibernéticas en un entorno seguro y confidencial.
* Asegúrese de que su organización sepa cómo informar de un incidente de ciberseguridad. Ver [**NCSC para reportar un incidente Se abre en una ventana nueva**](https://report.ncsc.gov.uk/).
* Implementar la guía del NCSC sobre [**Acciones a tomar cuando la amenaza cibernética se intensifica Se abre en una ventana nueva**](https://www.ncsc.gov.uk/guidance/actions-to-take-when-the-cyber-threat-is-heightened) y así sucesivamente [**Mantener una postura de ciberseguridad reforzada y sostenible Se abre en una ventana nueva**](https://www.ncsc.gov.uk/guidance/maintaining-a-sustainable-strengthened-cyber-security-posture).
* Buscar generales y específicos [**asesoramiento y orientación en el sitio web del NCSC Se abre en una ventana nueva**](https://www.ncsc.gov.uk/section/advice-guidance/all-topics), para ayudar a mejorar la ciberseguridad de su organización. Entre sus publicaciones recientes se encuentran:
	+ Construcción a partir de modelos de lenguaje grandes: [**Tenga cuidado al construir a partir de LLM Se abre en una ventana nueva**](https://www.ncsc.gov.uk/blog-post/exercise-caution-building-off-llms).
	+ Guía actualizada sobre la creación de un [**Construcción de un Centro de Operaciones de Seguridad (SOC)Se abre en una ventana nueva**](https://www.ncsc.gov.uk/collection/building-a-security-operations-centre).
	+ [**Cómo evaluar y ganar confianza en la ciberseguridad de su cadena de suministro Se abre en una ventana nueva**](https://www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security).
* Asistir [**CYBERUK Se abre en una ventana nueva**](https://www.ncsc.gov.uk/section/keep-up-to-date/cyberuk), el evento insignia del gobierno del Reino Unido en materia de ciberseguridad.
* Las empresas/FMI del sector financiero pueden contratar al equipo del sector financiero del NCSC en: **cnifinance@ncsc.gov.uk**.
1. PRA PS6/21 | CP29/19 | DP1/18 – [**Resiliencia operativa: tolerancias de impacto para servicios empresariales importantes**](https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper), marzo de 2021.
2. Banco de Inglaterra – [**Resiliencia operativa del sector financiero**](https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector).
3. PRA PS6/21 | CP29/19 | DP1/18 – [**Resiliencia operativa: tolerancias de impacto para servicios empresariales importantes**](https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper), marzo de 2021.
4. CPMI-IOSCO FR07/2016 – [**Orientaciones sobre ciberresiliencia para las infraestructuras de los mercados financieros Se abre en una ventana nueva**](https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf), junio de 2016.
5. Los ejemplos citados se han tomado de hallazgos individuales o ejemplos que los reguladores han observado.

