Perspectivas de los Grupos de Coordinación Cibernética 2021



**Investigación Publicado:** 08/12/2022 **Última actualización:** 08/12/2022

Esta publicación proporciona una visión general de las ideas que surgen de las discusiones celebradas en las reuniones trimestrales del Grupo de Coordinación Cibernética (CCG) de la FCA a lo largo de 2021.

Introducción

Esta publicación se divide en 3 secciones: la primera destaca el panorama del riesgo cibernético, así como los riesgos cibernéticos emergentes discutidos en los CCG en 2021. Esto es seguido por 2 temas de enfoque en los que resumimos las ideas de los miembros sobre el compromiso de la junta con la seguridad cibernética y el estado de DevSecOps. Los temas de enfoque son acordados antes de cada foro por la industria y los copresidentes de FCA.

Antecedentes de los Grupos de Coordinación Cibernética

Desde que se lanzó el programa CCG en 2017, los CCG han reunido a líderes de seguridad cibernética y riesgo tecnológico de la industria en foros compartidos y los han conectado con múltiples autoridades responsables de la resiliencia cibernética en todo el sector financiero, para discutir temas clave en un entorno seguro.

A las firmas miembro se unieron representantes de las autoridades financieras del Reino Unido y las agencias gubernamentales del Reino Unido (las autoridades), incluidas el Tesoro, la FCA, el Banco de Inglaterra, el Centro Nacional de Seguridad Cibernética (NCSC) y la Agencia Nacional del Crimen (NCA).

Los foros de CCG se celebran trimestralmente con el objetivo de ayudar a las empresas a compartir conocimientos, desafíos y buenas prácticas para proteger al sector financiero de las amenazas cibernéticas. También promueven el compromiso entre el sector financiero y las autoridades.

En 2021, celebramos 30 foros y reunimos a 152 empresas en 7 CCG, y cada CCG representa un subsector específico. Estos subsectores fueron Seguros, Gestión de Inversiones, Gestión de Fondos, Banca Minorista y Empresas de Pagos, Inversiones y Préstamos Minoristas, Brokers/Principales Empresas de Negociación y Comercio/Sociedades de Administración de Índices de Referencia.

La FCA también apoya el foro Trade Association Cyber Information Group (TACIG) que reúne a los principales organismos de la Asociación Comercial del Sector Financiero, para maximizar el intercambio de información relevante para el sector financiero.

Esta es nuestra cuarta publicación anual de perspectivas de CCG. Al igual que en años anteriores, se basa en el conocimiento compartido de las discusiones de CCG del año pasado, con el objetivo de compartir información y buenas prácticas con el sector financiero en general. Las ideas cubren amplios riesgos cibernéticos que abarcan las prioridades del sector, así como los temas clave que fueron discutidos en profundidad por algunos o todos los CCG.

Las ideas clave discutidas en esta publicación incluyen:

1. Actores cibernéticos maliciosos dirigidos a sistemas orientados a Internet, como servidores de correo electrónico y redes privadas virtuales (VPN) con vulnerabilidades recientemente reveladas, ataques de ransomware que utilizan protocolos de escritorio remoto (RDP) y dispositivos sin parches, ataques de denegación de servicio y supervisión inadecuada de la cadena de suministro que conduce al compromiso de la cadena de suministro.
2. La pandemia de coronavirus (Covid-19) continuó afectando al sector en 2021, con los [desafíos planteados por las formas de trabajo remotas e híbridas](https://www.fca.org.uk/publications/research/insights-cyber-coordination-groups-2020#lf-chapter-id-section-2-covid-19-and-remote-working).
3. Las tendencias emergentes en los riesgos de seguridad cibernética incluyen el compromiso de la cadena de suministro y la explotación de vulnerabilidades de día cero.
4. La importancia de la participación de la junta directiva para establecer el apetito de riesgo cibernético de la organización. Esto también se extiende al apoyo de la junta para medir la efectividad de las posturas de seguridad cibernética y la garantía de la junta de que los socios de la cadena de suministro protegen efectivamente la información compartida con ellos.
5. Se pueden utilizar varias buenas prácticas comunes para implementar la seguridad en las primeras etapas del ciclo de desarrollo de software (también conocido como DevSecOps). Esto incluye empoderar en lugar de exigir prácticas de seguridad y dar acceso a herramientas de seguridad a los equipos de desarrollo.

Esta publicación no es una guía de la FCA sobre las reglas bajo la sección 139A de la Ley de Servicios y Mercados Financieros de 2000. No establece las expectativas de la FCA para los sistemas y controles que las empresas deberían tener para cumplir con nuestros requisitos reglamentarios.

Todas las ideas han sido compartidas por una o más empresas dentro de los CCG, y gran parte de la discusión apoya la orientación existente del NCSC.

Sección 1: Ciberamenazas y tendencias emergentes

El panorama de las amenazas cibernéticas continúa evolucionando rápidamente. Las amenazas cibernéticas globales, como el abuso de [vulnerabilidades de día cero o el uso de ransomware](https://www.fca.org.uk/publications/research/insights-cyber-coordination-groups-2020) para lanzar ataques contra empresas y cadenas de suministro, plantean desafíos significativos para el sector financiero.

La pandemia continuó presentando a las empresas de servicios financieros muchos desafíos de seguridad de la información, incluido un aumento en las campañas de phishing dirigidas que utilizan correos electrónicos falsificados y objetivos investigados en lugar de correos electrónicos de phishing genéricos, invocando amplios planes de continuidad del negocio, así como cambios significativos en las formas en que las empresas operan día a día.

En esta sección, resumimos los principales riesgos cibernéticos identificados por los miembros de CCG a lo largo de 2021, así como varias tendencias emergentes de seguridad cibernética.

Amenazas actuales

Actores cibernéticos maliciosos

Algunos miembros de CCG destacaron el riesgo de que los actores cibernéticos maliciosos se dirijan a sistemas orientados a Internet, como servidores de correo electrónico y redes privadas virtuales (VPN) con vulnerabilidades recientemente reveladas. Los miembros de CCG discutieron con el NCSC y socios internacionales avisos conjuntos sobre estos temas, como [el asesoramiento de Microsoft Exchange y Fortinet](https://www.ncsc.gov.uk/news/microsoft-exchange-fortinet-vulnerabilities).

Los ataques de ransomware continúan desafiando a las empresas

El [NCSC declaró que para abril de 2021](https://www.ncsc.gov.uk/files/NCSC%20Annual%20Review%202021.pdf), había manejado el número equivalente de incidentes de ransomware como lo había hecho en todo 2020, lo que también fue un aumento del 300% en 2019. El NCSC informó que los puntos de entrada más comunes utilizados por los actores de amenazas para los ataques de ransomware fueron los puertos de protocolos de escritorio remoto (RDP), así como el software, hardware o VPN sin parches.

Los miembros de CCG estuvieron de acuerdo en que la autenticación de usuarios débil y la orientación de puertos fueron 2 de las principales vulnerabilidades presentes en el RDP que condujeron a ataques exitosos de seguridad cibernética.

La supervisión de la cadena de suministro es un desafío de seguridad cada vez más complejo

La supervisión inadecuada de las cadenas de suministro, así como las malas posturas de seguridad de los proveedores, siguen siendo un desafío para las firmas miembro. Los miembros señalaron que, en algunos casos, la supervisión de las cadenas de suministro puede recaer en funciones comerciales separadas, que requieren relaciones de trabajo extremadamente estrechas y colaborativas en toda la organización.

Comprender dónde el software de terceros tiene un amplio acceso es fundamental para el gobierno de TI. Esto podría ser, por ejemplo, con herramientas de punto final y escáneres de vulnerabilidad. Estas utilidades deben ser el foco para mejorar la supervisión y/o los controles de acceso privilegiado.

Los Miembros dijeron que algunas de las actuales diligencias debidas de terceros son obsoletas e ineficaces. Los Miembros compartieron que la debida diligencia basada en cuestionarios no identifica necesariamente los riesgos de ataques sofisticados o de software comprometido. Las firmas de los miembros sugirieron que se desarrollara una alternativa, como un organismo independiente que proporcionara garantías a los proveedores del sector financiero a través de un esquema de evaluación compartida.

Trabajar de forma segura durante la pandemia

La pandemia de coronavirus continuó afectando al sector en 2021, con desafíos planteados por formas de trabajo remotas e híbridas y un mayor uso de VPN. Los miembros de CCG también discutieron los desafíos en el monitoreo de los empleados que trabajan de forma remota. Este tema fue ampliamente cubierto en la [publicación Cyber Insights 2020](https://www.fca.org.uk/publications/research/insights-cyber-coordination-groups-2020).

Tendencias emergentes

Los miembros de CCG identificaron el compromiso de la cadena de suministro y las vulnerabilidades de día cero como las 2 principales tendencias emergentes en las que estaban más enfocados.

Compromiso de la cadena de suministro: legado de SolarWinds

El incidente de SolarWinds que se descubrió a fines de diciembre de 2020 fue un tema de interés para las firmas miembro en 2021. En abril de 2021, el NCSC, junto con sus homólogos de seguridad estadounidenses, compartió su opinión de que el Servicio de Inteligencia Exterior de Rusia (SVR) estaba detrás del [ataque de SolarWinds](https://www.ncsc.gov.uk/files/NCSC%20Annual%20Review%202021.pdf).

Es probable que un atacante haya podido agregar una modificación maliciosa y no autorizada a los productos SolarWinds Orion para enviar comandos de nivel de administrador a cualquier instalación afectada. La plataforma de gestión de TI de la plataforma SolarWinds se utilizó posteriormente para realizar ataques posteriores a los sistemas conectados.

Los miembros de CCG discutieron cómo el incidente de SolarWinds afectó la resiliencia de todo el sector y, en particular, la gravedad de los incidentes recientes de la cadena de suministro.

Los miembros estuvieron de acuerdo en que reaccionar rápidamente una vez que se ha producido una violación es fundamental, especialmente en los casos en que un actor del Estado-nación puede estar involucrado.

Los parches rápidos se destacaron como vitales para este tipo de incidentes. Los miembros coincidieron en que la comunicación entre los equipos de Gestión de Crisis y Continuidad del Negocio y los equipos de Seguridad Cibernética es esencial.

Llegar a proveedores y socios críticos y comprender cómo se han visto afectados fue fundamental.

También es importante que las juntas se interesaran mucho en este incidente y buscaran garantías. Sin embargo, las respuestas a SolarWinds fueron generalmente lentas, y muchos proveedores no están regulados en el mismo grado que sus clientes de servicios financieros (por ejemplo, los miembros de CCG).

Los Miembros propusieron establecer acuerdos de nivel de servicio más estrictos en los contratos de las empresas con terceros para ayudar a abordar esta situación.

Los miembros informaron que ha habido pocos cambios en el modelado de amenazas después de SolarWinds. Sin embargo, señalaron que la probabilidad de compromiso de la cadena de suministro puede, de hecho, aumentar, ya que los atacantes habrían visto a SolarWinds como un gran éxito.

Buenas prácticas generales

Las buenas prácticas compartidas por los miembros incluyeron:

* Avanzar hacia la confianza cero en una red ayudará contra los ataques de día cero. Si bien las empresas se adaptan a un enfoque de confianza cero, los miembros sugirieron que una solución práctica a corto plazo es aumentar el uso de firewalls de punto final por parte de las empresas.
* Restringir y monitorear qué datos pueden salir de los servidores, así como restringir los datos entrantes, es crucial para prevenir y responder a los ataques de día cero, en particular limitar el acceso saliente a Internet.
* Segregar ambientes internos para limitar el movimiento lateral. Los miembros propusieron la microsegmentación como una forma de reducir el movimiento lateral también.
* Implemente la administración de acceso privilegiado y limite los privilegios otorgados a los productos del proveedor de forma predeterminada.
* Se dijo que comprender los flujos de tráfico de red (incluido el DNS) para ayudar a establecer una línea de base para la actividad normal y detectar anomalías era más efectivo que confiar en la definición de actividad anormal.
* Algunos miembros señalaron que las soluciones de análisis del comportamiento del usuario eran útiles, especialmente si se pueden extender a las cuentas de servidor.
* Los ejercicios de mesa y los manuales de respuesta a incidentes pueden ser una forma práctica de ayudar a identificar dónde residen las vulnerabilidades y las dependencias clave.

Vulnerabilidades de día cero Log4Shell y Log4j

Un exploit de vulnerabilidad de día cero (también llamado amenaza de día cero) es un ataque que aprovecha una vulnerabilidad de seguridad que no tiene una solución implementada. Se conoce como una amenaza de "día cero" porque una vez que finalmente se descubre la debilidad de seguridad del software, el desarrollador de software o la organización tiene cero días para encontrar una solución. Por definición, no existe ningún parche para una vulnerabilidad de día cero y los sistemas no tienen defensas en su lugar, lo que hace que los ataques tengan muchas probabilidades de éxito.

Log4Shell, una vulnerabilidad crítica que es relativamente fácil de explotar, involucra una pieza de software casi ubicua previamente oscura, Log4j. [Log4j](https://www.apache.org/) es una biblioteca de registro de código abierto.

Casi todo el software tiene funcionalidad de registro para fines de desarrollo, operativos y de seguridad y Log4j es un ejemplo comúnmente utilizado de esto.

La vulnerabilidad inicial de Apache Log4j se identificó el 9 de diciembre de 2021 y se le asignó una puntuación máxima CVSS (sistema de puntuación de vulnerabilidades comunes) [de 10](https://nvd.nist.gov/vuln/detail/CVE-2021-44228). Esto llevó a una actividad masiva de reconocimiento y explotación por parte de actores de amenazas que utilizan el error para explotar vulnerabilidades.

Las organizaciones se enfrentan al desafío de identificar dónde se utiliza Log4j en sus organizaciones, ya que a menudo se incluye como parte de otro software. Como resultado del uso variado de Log4j, no existe una solución universal o parche de software.

* Dependiendo de cómo se incorporó Log4j en un sistema, la solución requerirá diferentes [enfoques](https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd#vp), desde la actualización del sistema, como se hace para algunos enrutadores Cisco, o la actualización a una nueva versión de software o la eliminación manual del código vulnerable.
* Los miembros cuestionaron los métodos de diligencia debida y la medida en que los parches de software de un socio o proveedor de confianza son esencialmente confiables, ya que no pueden verificarse independientemente aparte de su autenticidad (firma de código).

Sección 2: Participación de la Junta Directiva en materia de ciberseguridad

Los miembros de CCG señalaron que la conciencia de la seguridad cibernética ha aumentado significativamente en los últimos 5 a 10 años debido a un aumento en el delito cibernético, más infracciones perjudiciales y una legislación más estricta. La seguridad cibernética se ha convertido en una agenda permanente en muchas reuniones de la junta y las métricas cibernéticas se están volviendo cada vez más populares entre los miembros de la junta como una forma de evaluar el riesgo cibernético.

Los miembros señalaron que uno de los mayores desafíos que enfrentan muchos es tener múltiples juntas y comités, todos con diferentes niveles de conocimiento y comprensión, así como interés, en la seguridad cibernética. El desafío de crear una comprensión consistente de los problemas cibernéticos es complejo.

El apetito por el riesgo cibernético se discutió entre los miembros, centrándose principalmente en la medición de los riesgos y cómo esto se presenta a las juntas. Los miembros señalaron que era necesario aumentar la comprensión técnica dentro de las juntas para minimizar la necesidad de traducir el lenguaje técnico al no técnico.

Buenas prácticas generales

* Las estrategias para aumentar la participación de la junta identificadas por los miembros incluyeron la traducción de los riesgos cibernéticos en riesgos comerciales, tener comunicación frecuente e informes regulares con la junta y transmitir mensajes consistentes a las juntas cuando se informa sobre el riesgo cibernético. Las juntas pueden encontrar métricas de riesgo cibernético que relacionan la postura de seguridad cibernética con la madurez cibernética para ser inteligencia de gestión efectiva (MI), especialmente si se divide en áreas comerciales clave.
* Otra herramienta efectiva para promover la participación de la junta es ejecutar campañas de spear-phishing en los miembros de la junta y ejercicios de mesa cibernéticos.
* Algunos miembros compartieron que el uso del kit de herramientas de la Junta NCSC ha sido útil para educar a la junta sobre el riesgo cibernético y también ha sido útil para obtener una visión consistente del riesgo en todas las estructuras grupales de la organización. Los miembros también señalaron que las discusiones sobre ciberseguridad con pares impulsan la participación de la junta. Otras herramientas efectivas para la participación de la junta incluyeron presentaciones sobre el panorama actual de amenazas a través de CISO externos que compartieron sus experiencias y desafíos y sesiones informativas enfocadas en estrategias cibernéticas efectivas.
* Las juntas actualmente tienen un gran enfoque en cuestiones cibernéticas relacionadas con la cadena de suministro. Esto se debe al alto número de incidentes cibernéticos en la cadena de suministro y la gran cantidad de publicidad reciente que han creado. Los miembros declararon que estaban siendo desafiados cada vez más por los miembros de la Junta sobre este tema después de eventos como [Solarwinds](https://www.ncsc.gov.uk/guidance/dealing-with-the-solarwinds-orion-compromise%22%20%5Ct%20%22_blank).

Sección 3: Desarrollo, seguridad y operaciones (DevSecOps)

Los miembros de CCG discutieron los principios de desarrollo de software seguro y el nivel de madurez de DevSecOps en sus organizaciones y subsectores.

DevSecOps es una práctica de tendencia en seguridad de aplicaciones que implica introducir seguridad más temprano en el ciclo de vida de desarrollo de software (SDLC). También amplía la colaboración entre los equipos de desarrollo y operaciones basándose en la automatización y el diseño de plataformas que integran la seguridad como una responsabilidad compartida en todo el SDLC.

Los debates abarcaron los siguientes temas:

* **Gobernanza y política:** Garantizar que el proceso y el marco de toma de decisiones que rodean a DevOps sean explicables y sólidos. Crear políticas y procedimientos de ciberseguridad transparentes que sean fáciles de entender e implementar para los desarrolladores y otros miembros del equipo en entornos ágiles también ayudará.
* **Automatización y monitorización:** Escalar los controles de seguridad mientras se alinea con el ritmo de los procesos de DevOps mediante el uso de herramientas de seguridad automatizadas para el análisis de código, la gestión de la configuración, la aplicación de parches y la gestión de vulnerabilidades.
* **Protección de los entornos de desarrollo:** Proporcionar a los ingenieros entornos que se adapten a sus necesidades y a las necesidades del negocio, al tiempo que promueve las prácticas de seguridad y protege la cadena de suministro de software. Acceso y gestión secreta.
* **Implementación de DevSecOps y cultura:**Desarrollar la cultura adecuada para permitir equipos multifuncionales y responsabilidad compartida por la seguridad de la información. Analizar las barreras clave para la adopción y cómo los miembros las han manejado.

Algunos ejemplos de prácticas de DevSecOps incluyen el análisis de repositorios en busca de vulnerabilidades de seguridad, modelado temprano de amenazas, revisiones de diseño de seguridad, revisiones de código estático y de código dinámico:

* El escaneo de vulnerabilidades, en particular el escaneo de vulnerabilidades de código abierto para software que puede haber sido creado sin buenas prácticas de seguridad, analiza los componentes de código abierto, las bibliotecas y las dependencias en el código fuente.
* En un proceso DevSecOps, el análisis de riesgos de seguridad se puede utilizar durante la etapa de planificación para identificar qué componentes son más seguros o están libres de vulnerabilidades que pondrían en riesgo el proyecto. Luego, los escaneos de vulnerabilidades ocurren en múltiples etapas de los procesos de desarrollo y compilación para garantizar que no se introduzcan nuevas vulnerabilidades después de la etapa de planificación inicial.
* El modelado temprano de amenazas es el enfoque de evaluar y mitigar el riesgo de seguridad de la aplicación mediante el análisis del entorno empresarial donde se implementará la aplicación y el establecimiento de cómo se pueden explotar las debilidades potenciales. El objetivo es permitir que los equipos tomen rápidamente decisiones proactivas y basadas en datos para minimizar la exposición al riesgo de seguridad.
* Hay muchas herramientas disponibles, por ejemplo, paneles visuales y soluciones que utilizan datos para crear automáticamente modelos de amenazas.
* Las revisiones de código estático permiten a los desarrolladores escanear el código fuente en busca de código débil o inseguro, cuantificando la vulnerabilidad y priorizando la corrección. El nivel de gravedad evitará que un componente pase a la siguiente etapa del desarrollo.
* La revisión dinámica del código se puede realizar mediante aplicaciones automatizadas, probando una variedad de amenazas sin la necesidad de acceder al código fuente de desarrollo.

Los miembros hablaron muy positivamente sobre los beneficios de DevOps para la seguridad, particularmente los conceptos de automatización, autoservicio y software como código. La automatización madura de DevSecOps implica proporcionar a los desarrolladores herramientas de seguridad de autoservicio que remedian las vulnerabilidades identificadas sin la necesidad de interactuar directamente con el personal de seguridad.

Entre los ejemplos examinados figuraban los siguientes:

* Reducción del esfuerzo manual y, en consecuencia, reducción de errores al girar compilaciones definidas consistentemente
* Tener la configuración de seguridad aplicada de forma inmediata y coherente a través de canalizaciones codificadas, ya que esto permite la automatización de las fases de compilación, prueba e implementación del proceso de lanzamiento cada vez que hay un cambio de código, según el modelo de lanzamiento definido por el desarrollador
* La capacidad de definir de forma proactiva patrones de seguridad para su uso en implementaciones en la nube

El principal desafío en la implementación de una cultura DevSecOps es que los equipos de seguridad de la información a menudo no están integrados con los equipos de desarrollo y tecnología. En algunos casos, el desarrollo se realiza en unidades de ciencia de datos o se subcontrata a terceros.

Los miembros señalaron que puede ser un proceso lento implementar DevSecOps en una empresa establecida. Una solución es el uso de sprints ágiles para proyectos, pero se observó que persisten los desafíos con esta metodología, especialmente para proyectos más grandes. Se sugirió que la metodología de cascada puede ser más eficaz para proyectos más estratégicos.

Buenas prácticas generales

* Un cambio cultural para permitir que la responsabilidad de la seguridad se comparta en toda una organización es crucial para que DevSecOps se use de manera efectiva. Se señaló que el empoderamiento de los equipos de desarrollo para tomar decisiones de seguridad y la integración de la experiencia en seguridad en los equipos de desarrollo eran buenas estrategias para avanzar hacia DevSecOps.
* También se señaló que dar a los desarrolladores acceso a herramientas de seguridad para que las usen ellos mismos puede ser una estrategia efectiva tanto para mejorar las habilidades de los desarrolladores como para crear bucles de retroalimentación de seguridad más rápidos.
* Una práctica ideal para los desarrolladores de código de software es comenzar a contribuir a los estándares de seguridad del código, en lugar de que estos sean obligatorios por los equipos de seguridad. Los estándares de codificación segura son conjuntos de reglas y directrices utilizadas por una organización para reducir las vulnerabilidades y errores de seguridad durante el desarrollo.

Agradecemos a todos los miembros de los Grupos de Coordinación Cibernética que han contribuido a las discusiones y cuyas ideas se reflejan en esta publicación.