Osterman Research

# WHITE PAPER

**White Paper** por Osterman Research
Publicado en **Marzo de 2023**
Patrocinado por **BIO-key International**

# Ciberseguridad en Servicios Financieros: Viewpoint 2022

# Resumen ejecutivo

El sector financiero está bajo ataque cibernético con vectores de amenazas que incluyen violaciones de datos, ataques avanzados que eluden las protecciones de seguridad y servicios en la nube mal configurados. Los reguladores de todo el mundo exigen un estándar más alto de rendimiento de las empresas financieras, al igual que los clientes que requieren un acceso seguro a sus fondos en un mundo cada vez más móvil e impulsado por aplicaciones. La industria seguirá siendo un objetivo clave para los actores de amenazas debido a la oferta de dinero e identidades, junto con oportunidades de sabotaje financiero para paralizar a un país. Las empresas de servicios financieros deben revisar la eficacia de las protecciones de seguridad cibernética actuales, invertir en nuevas soluciones para abordar las amenazas emergentes y desarrollar una sólida postura de seguridad siguiendo las mejores prácticas.

El término “empresa de servicios financieros” cubre una amplia gama de empresas, incluidos bancos (centrales, minoristas, comerciales e Internet), cooperativas de crédito, bancos de inversión, compañías de seguros y casas de bolsa.

## CONCLUSIONES CLAVE

Los puntos clave de esta investigación son:

- **Las empresas de servicios financieros están bajo ataque desde muchos lados**
  Los nuevos bancos entrantes con nuevos modelos comerciales, el alejamiento de la banca en persona, un ecosistema complejo plagado de tecnología heredada y el aumento de las criptomonedas crean un contexto desafiante para las empresas de servicios financieros.

- **Los ciberataques tradicionales se complementan con los emergentes**
  Las violaciones de datos, los ataques de suplantación de identidad y las fechorías internas siguen siendo moneda corriente en el sector. Se están viendo amenazas emergentes contra la infraestructura de la nube, SaaS, tokens de acceso entre aplicaciones e interfaces de programación de aplicaciones.

- **Entorno normativo muy exigente**
  Los organismos gubernamentales y de la industria han impuesto importantes regulaciones de preparación y presentación de informes sobre seguridad cibernética en el sector, además de mandatos más amplios de protección de datos. Los reguladores también están impulsando la resiliencia operativa.

- **Los actores de amenazas encuentran atractivo el sector, y no se espera que eso cambie.**
  Si bien se puede ganar dinero por medios ilícitos, los actores de amenazas seguirán intentándolo. Las pandillas más pequeñas buscan el dinero, pero los actores de amenazas del estado-nación están más interesados en causar un sabotaje financiero para desestabilizar a un enemigo extranjero.

- **Se necesitan soluciones para proteger y defender el sector y sus clientes.** Los servicios en la nube deben estar mejor protegidos, la identidad y la autenticación deben fortalecerse y el acceso con privilegios excesivos debe reducirse sistemáticamente. Los bots deben detenerse, fortalecerse el correo electrónico y los empleados deben estar mejor capacitados para detectar amenazas.

- **Complementar las soluciones con las mejores prácticas de ciberseguridad**
  Comience con una evaluación de riesgos cibernéticos actualizada y rica en contexto para su empresa, junto con marcos de gestión de riesgos mejorados interna y externamente.
  Va más allá del entrenamiento y desarrolle la resiliencia humana para hacer frente a los ataques cibernéticos.

***El sector financiero seguirá siendo un objetivo clave para los actores de amenazas debido al sabotaje financiero.***

## ACERCA DE ESTE DOCUMENTO

Este informe técnico fue patrocinado por BIO-key International. La información sobre BIO-key International se proporciona al final de este documento.

# Servicios financieros: un contexto desafiante

Las firmas de servicios financieros tradicionales están bajo una tremenda presión desde muchas direcciones. Es una industria bajo ataque, y no solo ciberataque. Los factores que hacen que los servicios financieros sean un sector desafiante incluyen:

- **Nuevos bancos entrantes con nuevos modelos de negocio**
  Las nuevas Fintech o los neobancos ofrecen servicios bancarios digitales primero o solo digitales.1 La interacción con el cliente se realiza a través de un sitio web o una aplicación móvil, no de una sucursal física. Las tarifas son bajas, las plataformas tecnológicas son nuevas y la línea de productos está muy enfocada. Su estructura de costos es muy diferente de las empresas tradicionales con décadas de tecnología heredada, una amplia cartera de servicios bancarios y de inversión, y una costosa red de sucursales físicas para dotar de personal y mantener.

- **El alejamiento de la banca en persona**
  El valor de la relación cara a cara tradicional entre un banquero y un cliente se está erosionando rápidamente a medida que los clientes se desplazan hacia la interacción móvil y en línea. Tener una red de sucursales se ve más como un negativo neto cuando los clientes tienen acceso físico a sus servicios bancarios a través de un dispositivo móvil dondequiera que estén, y particularmente en el contexto de la pandemia de salud que ha visto a los clientes no poder o no querer visitar una sucursal. Existe una preferencia cada vez mayor entre los clientes por experiencias móviles y en línea personalizadas, y cuando una institución de servicios financieros tradicional es demasiado lenta para ofrecer, los clientes buscan alternativas más nuevas y dinámicas.

- **Un ecosistema complejo plagado de tecnología heredada**
  El sistema financiero mundial se basa en un ecosistema complejo de cámaras de compensación financiera propiedad de una variedad de actores, cada uno con sus propias interdependencias y requisitos de acceso. Los estándares tecnológicos, los sistemas y los protocolos de intercambio se desarrollaron hace décadas y, aunque las actividades de modernización están en marcha, la infraestructura heredada permanece integrada.

- **El auge de las criptomonedas**
  Las plataformas de criptomonedas ofrecen un medio descentralizado para almacenar e intercambiar valor, y cuando aumentan las valoraciones de esta moneda volátil, las criptomonedas ofrecen rendimientos financieros que superan con creces lo que está disponible en una cuenta de ahorros tradicional. Por ejemplo, el robo de 120 000 bitcoins en 2016 por un valor de 66 millones de dólares valía más de 4500 millones de dólares cuando el Departamento de Justicia confiscó las billeteras robadas en febrero de 2022.2 Ninguna cuenta de ahorros ofrece ese tipo de retorno, y tanto los clientes como los ciberdelincuentes acuden en masa. a los mercados de mayor riesgo en busca de ganancias descomunales (o ilícitas).

*Tener una red de sucursales se parece más a una red negativa cuando los clientes tienen acceso físico a sus servicios bancarios a través de un dispositivo móvil en la mano.*

En combinación, estos factores crean una tormenta perfecta para la ciberseguridad. Los CIO, los directores de IT y los CISO enfrentan demandas urgentes y contrapuestas desde múltiples lados. La empresa demanda urgentemente nuevas tecnologías para abordar las elevadas expectativas de los clientes y ofrecer nuevos productos y servicios al mercado. Las crecientes demandas de los reguladores gubernamentales y de la industria dejan poco espacio para las ofertas que no cumplen con los más altos estándares de seguridad desde el primer día. Los proveedores de seguros cibernéticos están retirando la cobertura cibernética, cambiando drásticamente el cálculo del riesgo. Los ciberataques diarios y las amenazas comerciales, económicas y cibernéticas inmediatas de la guerra rusa contra Ucrania complican aún más las cosas. Priorizar la seguridad cibernética durante tal vorágine depende de los tomadores de decisiones con perspectivas informadas, juicio claro y la voluntad de impulsar un cambio sistémico.

# Las empresas de servicios financieros están bajo ataque cibernético

Los ciberataques vienen en muchas formas y tamaños. En esta sección, analizamos la variedad de ciberataques, ciberfraudes e incidentes de seguridad que preocupan a las empresas de servicios financieros.

### FRAUDE CIBERNÉTICO

Los ataques de fraude digital, como el robo de identidad y el phishing, contra empresas de servicios financieros aumentaron un 109 % a principios de 2021, más de cuatro veces el promedio de la industria. No es sorprendente que el fraude cibernético sea la preocupación más calificada entre los bancos sobre la economía global, con los bancos califican los problemas de la cadena de suministro posteriores a la pandemia y el riesgo de tasa de interés como preocupaciones menores.

### BRECHAS DE DATOS

Los hackers intentan robar o comprometer los datos en poder de las empresas de servicios financieros. En 2021, la industria tuvo una de las tasas más altas de incidentes de violación de datos (la tercera más alta en el Reino Unido, con atención médica en primer lugar y educación y cuidado de niños en segundo lugar), con incidentes exitosos debido a múltiples tipos de ataques. Por ejemplo:

- **Hackeo de un servicio en la nube, por ejemplo, Capital One**
  Capital One almacenó datos de solicitudes de tarjetas de crédito en una cuenta de Amazon Web Services (AWS). Un ex empleado de AWS agraviado escribió un código para identificar las cuentas de AWS con debilidades de configuración y pudo violar los datos de 100 millones de personas que habían solicitado una tarjeta de crédito de Capital One durante un período de 15 años. Capital One recibió una multa de $80 millones por parte de la Oficina del Contralor de la Moneda por no establecer y mantener procesos efectivos de gestión de riesgos antes de pasar a la nube. Capital One también acordó un acuerdo de $190 millones en una demanda colectiva que cubre la violación.

- **Explotación de una vulnerabilidad sin parchear, p. ej., Punjab National Bank**
  La fuga de datos es la consecuencia más común de las vulnerabilidades no resueltas en las aplicaciones.9 Una firma consultora de seguridad de TI en India alegó que un importante banco local expuso los detalles personales y financieros de sus 180 millones de clientes al no resolver una vulnerabilidad conocida en Exchange Server. El banco confirmó la vulnerabilidad sin parchear, pero negó en gran medida cualquier acceso no autorizado.10 En el esquema más amplio de las cosas, un estudio encontró que el 43% de las aplicaciones en el sector de finanzas y seguros estuvieron expuestas perpetuamente durante 2021 debido a al menos una vulnerabilidad explotable grave.

- **Debilidades en los procesos de terceros, por ejemplo, Ascension Data & Analytics**
  Ascension Data & Analytics, una empresa de análisis de datos que atiende a la industria hipotecaria, contrató a una empresa de terceros para proporcionar servicios de reconocimiento de texto. La empresa de terceros almacenó los documentos de Ascension en un servicio en la nube sin controles de acceso, proporcionando acceso abierto a 24 millones de registros durante un año. Los registros mostraron que se accedió a los datos más de 50 veces desde computadoras aparentemente ubicadas en Rusia y China. Ascension no realizó la debida diligencia en las prácticas de seguridad de la empresa de terceros antes de compartir datos personales y financieros con ellos.12 La Comisión Federal de Comercio (FTC) exigió que Ascension reforzara sus protecciones de seguridad, incluidas las que se extienden a terceros. Un comisario protestó enérgicamente pidiendo que se impusiera una pena más severa.

***El fraude cibernético es la preocupación mejor calificada entre los bancos sobre la economía global —mayor que los problemas de la cadena de suministro y el riesgo de tasa de interés.***

- **Debilidades en los controles de seguridad internos, p. ej., First American Financial**
  Un error introducido en 2014 durante una actualización de rutina de la aplicación expuso datos personales y financieros en 885 millones de documentos en First American Financial al acceso no autorizado de cualquier persona con un navegador web. A mediados de 2019, un análisis de un tercero concluyó que se habían violado los datos de solo 32 personas, mientras que otro análisis en 2020 indicó que se había accedido a 350 000 documentos sin autorización. La SEC multó a First American con $ 488,000 por no mantener controles y procedimientos de divulgación de seguridad cibernética (según la Regla 13a-15 (a) de la Ley de Bolsa de Valores de 1934), y el Departamento de Servicios Financieros de Nueva York alegó múltiples cargos bajo el Reglamento de Seguridad Cibernética de Nueva York (23 NYCRR 500), que establece un nivel mucho más alto de sanción por cumplimiento. Aunque la vulnerabilidad ya se había descubierto a través de pruebas internas, se clasificó erróneamente como de bajo riesgo y no se abordó.

- **Robo de tokens de autenticación otorgados a empresas de terceros, por ejemplo, Dave**
  A Dave, un proveedor de una aplicación bancaria en los Estados Unidos, le robaron datos de más de siete millones de clientes después de que los piratas informáticos violaron sus sistemas después de violar primero los sistemas en un proveedor de tecnología con el que Dave había trabajado anteriormente. La infracción utilizó un token de autenticación de OAuth antiguo, pero aún válido que se había creado para Dave.

- **Abuso de cuentas con muchos privilegios, por ejemplo, Desjardins**
  Así como el abuso por parte de empleados bancarios de cuentas financieras inactivas es una forma costosa de fraude financiero, también lo es el abuso de cuentas de usuario inactivas (p. tomados por un empleado actual no son monitoreados por exceso de derechos de acceso, comportamiento inexplicable o acción maliciosa). Un empleado de alto rendimiento, pero descontento de Desjardins, un banco de Canadá, accedió a los datos personales de 9,7 millones de clientes durante un período de dos años. Si bien el empleado no tenía los derechos de acceso a los almacenes de datos que contenían los datos, podía acceder a la unidad compartida donde se almacenaban las copias de los datos. El empleado usó scripts para crear copias adicionales de los datos confidenciales en su computadora de trabajo y llaves USB. Aunque la confianza era un valor importante en Desjardins, la Oficina del Comisionado de Privacidad de Canadá afirmó que el banco necesitaba mejores herramientas y una mayor vigilancia para protegerse contra tales amenazas internas. La falta de supervisión que permitió el abuso de la cuenta sobreprivilegiada le costó a Desjardins más de $ 200 millones para resolver.

## HACKERS QUE SE HACEN PASAR COMO EMPRESAS DE SERVICIOS FINANCIEROS

Las empresas de servicios financieros están intrincadamente entrelazadas con la economía diaria y los hackers que buscan aprovechar la conexión entre los consumidores y su banco para fines maliciosos. Los ataques de phishing contra los consumidores son un enfoque común de los actores de amenazas que se hacen pasar por una empresa de servicios financieros. Miles de personas caen en estafas de phishing supuestamente enviadas desde su banco todos los días. Los datos sobre la amenaza del phishing en el sector de los servicios financieros incluyen:

- **Phishing y filtraciones de datos**
  El phishing ha sido implicado como el principal vector de amenazas en el 90 % de las filtraciones de datos. El sector de servicios financieros es una de las industrias objetivo con más frecuencia y, a menudo, la industria objetivo principal en un año determinado.

***Los controles internos débiles y la falta de protecciones contra empleados maliciosos resultan en filtraciones de datos costosas.***

- **Las marcas de servicios financieros se suplantan comúnmente para los ataques de phishing** Durante la primera mitad de 2021, las marcas de servicios financieros se suplantaron en el 36,4 % de todas las URL de phishing. Las marcas comúnmente suplantadas incluyeron Crédit Agricole, PayPal, Chase y Wells Fargo. Para los esquemas de phishing centrados únicamente en marcas de sistemas de pago financieros, PayPal, Mastercard, American Express y Visa representaron el 70% de dichos ataques de phishing durante 2021.

- **$1 mil millones robados en seis meses en Inglaterra**
  El fraude bancario en línea en Inglaterra le costó a los consumidores $ 1 mil millones en la primera mitad de 2021, lo que le valió al Reino Unido el título de "capital mundial de la estafa bancaria". el banco de la víctima y la Autoridad de Conducta Financiera del Reino Unido, sitios web financieros falsos y el robo de criptobilleteras.

- **USD 10,1 millones perdidos en estafas de phishing en Singapur en un mes para un banco** Los clientes del OCBC Bank en Singapur perdieron un total combinado de USD 10,1 millones en diciembre de 2021 cuando respondieron a alertas por SMS supuestamente provenientes de OCBC para alertar sobre irregularidades en las cuentas. Casi 800 clientes hicieron clic en el enlace de la alerta por SMS e ingresaron las credenciales de su cuenta bancaria por Internet, momento en el cual los estafadores transfirieron fondos de sus cuentas. El banco reembolsó a todas las víctimas afectadas como un “gesto único de buena voluntad”, ataque de phishing a sus clientes es costoso para el banco.

- **Incluso las personas en las empresas de criptomonedas caen en los ataques de phishing**
  bZx, una empresa de criptomonedas, sufrió un ataque de phishing exitoso contra uno de sus desarrolladores en noviembre de 2021, lo que resultó en el robo de $55 millones en criptomonedas. El desarrollador abrió un documento de Word adjunto que contenía una macro maliciosa, lo que comprometió el acceso a su criptomoneda. monedero y los monederos de otros usuarios.Financial services brands are commonly impersonated for phishing attacks

> ***Las marcas de servicios financieros son un objetivo común para la suplantación de identidad en los ataques de phishing.***

## ATAQUES QUE ELUDAN LAS PROTECCIONES DE SEGURIDAD

Los hackers están diseñando activamente ataques que eluden las protecciones de seguridad utilizadas por empresas e individuos, como la autenticación multifactor (MFA). Éste ha sido un método clave para evitar que los ataques de phishing tengan éxito en la obtención de credenciales de cuenta utilizables. Los métodos para eludir las protecciones incluyen:

- **Robo de tokens de sesión a servicios en la nube**
  Los tokens de sesión se crean en un navegador web para brindar y ampliar el acceso a las aplicaciones en la nube; desempeñan un papel facilitador común en las soluciones de inicio de sesión único. Si un actor de amenazas puede capturar el token de sesión de un usuario, obtiene acceso al servicio en la nube en paralelo a lo que sea que esté haciendo el usuario e incluso cuando el usuario cambia su contraseña u obtiene un nuevo código de autenticación. Los tokens de sesión ofrecen acceso persistente a un servicio durante un período de tiempo determinado, a menudo hasta 30 días.

- **Detectar el robo y el uso de tokens de sesión es un desafío porque el token en sí es legítimo y ha sido aprobado por un usuario autorizado.**
  Se agregaron páginas de autenticación falsas frente a las aplicaciones SaaS reales de un usuario. Los ataques de intermediarios buscan formas de capturar el acceso a cuentas o datos sin que el usuario se dé cuenta de que alguien más está involucrado de manera subrepticia. Los actores de amenazas están aumentando la sofisticación de los ataques de phishing, por ejemplo, dando al usuario phishing acceso a su aplicación SaaS real al final de la línea de phishing, aunque también después de robar sus credenciales mediante el uso de páginas de autenticación falsas que se ven y se sienten como las reales. unos. Es menos probable que caer en el phish haga sonar las alarmas para el individuo cuando se le presenta su cuenta real en lugar de llegar a un callejón sin salida o una página de error.

- **Uso creciente de juegos de herramientas de phishing para eludir la autenticación de dos factores (2FA)** Los actores de amenazas utilizan cada vez más juegos de herramientas que eluden las protecciones de 2FA al capturar o interceptar el código 2FA o robar la cookie de autenticación del usuario. Un estudio reciente encontró más de 1,200 sitios de phishing que utilizan enfoques que eluden las protecciones 2FA, frente a los 200 sitios hace solo tres años. Los kits de herramientas de phishing ponen a disposición de cualquier persona herramientas avanzadas contra amenazas.

## ATAQUES DE RELLENO DE CREDENCIALES PARA IRRENAR CUENTAS

Las violaciones de datos causan problemas inmediatos para la empresa violada y sus clientes, pero también existe un problema de mayor duración: a menudo exponen credenciales válidas para su uso en nuevos ataques. Con más de 15 000 millones de credenciales de más de 100 000 filtraciones de datos disponibles para la venta en la dark web, las empresas de servicios financieros se enfrentan a la amenaza de ataques de relleno de credenciales. En estos ataques, las credenciales comprometidas de un sitio se utilizan contra otro sitio para ver si el usuario ha reutilizado el mismo par de credenciales en varios sitios, un enfoque común de los usuarios que luchan por recordar una gran cantidad de contraseñas. Incluso para aplicaciones perfectas sin vulnerabilidades, los ataques de relleno de credenciales funcionan porque las credenciales son válidas. Las empresas de servicios financieros enfrentaron 3400 millones de ataques de este tipo en 2020, un 45 % más que en 2019.33

Los ataques de relleno de credenciales se basan en bots y scripts automatizados. Varios tipos de protecciones de seguridad cibernética han demostrado ser ineficaces para detener los ataques de Credential Stuffing, incluidos los firewalls de aplicaciones web, CAPTCHA y algunos tipos de MFA.

## INCIDENTES DE RANSOMWARE

Los últimos años han sido testigos del aumento continuo de la amenaza del ransomware, el giro hacia el ataque a la infraestructura crítica y los diseños de extorsión de varios niveles destinados a aumentar la probabilidad de pago al actor de la amenaza. En el sector de servicios financieros está sucediendo lo siguiente:

- **Volumen creciente de actividad de ransomware**
  En los primeros seis meses de 2021, la Red de Ejecución de Delitos Financieros en el Departamento del Tesoro de los Estados Unidos observó un aumento en el volumen y el valor de la actividad relacionada con el ransomware en los Estados Unidos, lo que amenaza al sector financiero de los Estados Unidos, junto con las empresas y el público. Tanto el volumen como el valor de la actividad en la primera mitad de 2021 fueron superiores a la actividad equivalente para todo 2020.

- **Crecimiento de ataques de ransomware contra bancos**
  Un estudio encontró que la industria bancaria experimentó un crecimiento interanual del 1318 % en los ataques de ransomware en la primera mitad de 2021. Por el contrario, en todos los sectores, el ransomware creció un 148 % en los primeros tres trimestres de 2021.

- **Crecimiento de los ataques de ransomware contra el sector en general**
  En el tercer trimestre de 2021, los servicios financieros fueron el sector de la industria que enfrentó la mayor cantidad de ataques de ransomware (22 % del total) y los ataques de amenazas persistentes más avanzados (37 % del total). Las amenazas contra el sector aumentaron un 21% durante el segundo trimestre.

- **Ryuk un problema para los servicios financieros**
  La variante de ransomware Ryuk fue un problema particular para las empresas de servicios financieros durante 2020. Ryuk se ha relacionado con grupos de amenazas de estados-nación y se usa a menudo en ataques contra empresas más grandes que se considera que tienen los recursos financieros para pagar un rescate.

***Los ataques de ransomware en el sector de servicios financieros aumentaron 10 veces más que en otros sectores.***

## ATAQUES HACIA LOS SERVICIOS EN LA NUBE

Las instituciones financieras están haciendo un uso cada vez mayor de los servicios en la nube, y se espera que un porcentaje cada vez mayor de las cargas de trabajo se alojen en la nube pública. Los patrones de implementación incluyen el uso de múltiples nubes, modelos híbridos que combinan infraestructura local y múltiples servicios en la nube, y el uso de los servicios en la nube para infraestructura, capacidades de plataforma y servicios empaquetados. La mala configuración de los servicios en la nube ha sido una amenaza importante en los últimos años, lo que ha provocado incidentes como la filtración de datos de Capital One en AWS descrita anteriormente en este documento técnico.

La adopción de aplicaciones SaaS por parte de las instituciones financieras aumenta la huella para los actores de amenazas. Los tipos de datos confidenciales, sensibles y personales se están confiando a estas aplicaciones, con vías de compromiso que incluyen la explotación de vulnerabilidades en los servicios en la nube, la captura de credenciales de cuentas a través de ataques de phishing, el secuestro de tokens de sesión y el movimiento lateral a través de aplicaciones SaaS conectadas después de una violación inicial. Las aplicaciones SaaS a menudo son propiedad de los gerentes de línea de negocios y no del departamento de IT, lo que significa que es menos probable que los propietarios de negocios entiendan y administren las disciplinas de mayor seguridad que se capacitan en los profesionales de IT. A diferencia de la infraestructura local, donde las instituciones financieras tienen todo el peso de garantizar una postura de alta seguridad, el modelo de responsabilidad compartida divide las responsabilidades de seguridad entre los proveedores de la nube y la empresa. El modelo amenaza con descuidos, errores y señalamientos, particularmente cuando la empresa se aferra a la creencia errónea de que la seguridad es responsabilidad del proveedor de la nube. Varias instituciones financieras ya no han logrado garantizar que se cumpla su parte de responsabilidades, con ejemplos de privilegios de acceso. mal configurado o ignorado por completo.

***The adoption of SaaS apps by financial institutions increases the attack footprint for threat actors.***

## PRÁCTICAS DE SEGURIDAD INSUFICIENTES EN LA CADENA DE SUMINISTRO

Una violación de datos en una empresa de terceros puede implicar los datos de una empresa, incluso cuando se ha llevado a cabo la diligencia debida sobre las prácticas de seguridad en la empresa de terceros. Por ejemplo, Debt-IN Consultants, una firma de recuperación de deuda que subcontrata a empresas de servicios financieros en Sudáfrica, sufrió una violación de datos que comprometió datos personales y financieros de más de 1,4 millones de personas en Sudáfrica provenientes de sus clientes.

## COMPROMISO DE EMAIL EMPRESARIAL (BEC)

Los actores de amenazas buscan ganancias financieras al comprometer las cuentas de email comerciales y los hilos de conversación, intentar cometer fraude de facturas y hacerse pasar por clientes que solicitan transferencias bancarias a cuentas bancarias controladas por los actores de amenazas. Cuando un banco en los Estados Unidos es objeto de fraude con transferencias bancarias, los actores de amenazas solicitan un promedio de 1,5 millones de dólares. En combinación, los ataques exitosos de compromiso de email comercial en los Estados Unidos representan la forma más costosa de ataques cibernéticos contra empresas en todos los sectores.

## CRECIMIENTO DEL FRAUDE DE PRÉSTAMOS POR ROBO DE IDENTIDAD

El uso de identidades personales y comerciales robadas o falsificadas al solicitar un préstamo, junto con el mayor uso de aplicaciones de préstamos móviles, está generando tasas más altas de fraude crediticio. LexisNexis descubrió que los bancos y cooperativas de crédito más pequeños (con menos de $10 mil millones en activos) junto con los prestamistas digitales sufrieron pérdidas del 6,9 % de los ingresos en 2021 debido al fraude crediticio, y los bancos más grandes con más de $10 mil millones en activos enfrentaron pérdidas del 5,9 % de ingresos 2021. Los estafadores están utilizando datos personales y financieros robados para solicitar préstamos que resultan en el robo de fondos de bancos y cooperativas de crédito.

## AMENAZAS DESDE EL INTERIOR

La mayoría de las empresas de servicios financieros también enfrentan amenazas cibernéticas de actores internos y procesos débiles. Las amenazas internas incluyen:

- **Falta de talento en ciberseguridad**
  Ubicar, contratar y retener a profesionales experimentados en seguridad cibernética es un desafío cuesta arriba para las empresas en todos los sectores de la industria, incluidos los servicios financieros. Es más probable que las tareas esenciales se dejen sin hacer o solo se aborden parcialmente cuando no hay suficientes personas para construir y mantener defensas cibernéticas sólidas, por ejemplo, reparar vulnerabilidades, verificar alertas de phishing.

- **Abuso de posición organizacional**
  Cuando los empleados en puestos de confianza actúan con malas intenciones dentro de un banco o cooperativa de crédito, como mínimo causan daños financieros y, en el peor, el cierre de la empresa. Esto sucedió recientemente en una pequeña cooperativa de ahorro y crédito en los Estados Unidos, donde el director ejecutivo abrió varias tarjetas de crédito no autorizadas a su nombre y siguió aumentando el límite de crédito. Solo ella tenía acceso a la base de datos de tarjetas de crédito y manipulaba las tasas de interés y los pagos mensuales a su favor. Los $2.1 millones que cargó a las tarjetas resultaron en el cierre de la cooperativa de ahorro y crédito. Ella era una de los tres únicos empleados de la cooperativa de ahorro y crédito, la junta confiaba en ella por completo y no había controles ni equilibrios para garantizar que sus acciones fueran apropiadas. El CEO fue sentenciado a más de cuatro años en una prisión federal, seguidos de tres años de libertad supervisada, incluido un año de arresto domiciliario.

- **Prácticas de protección de datos insuficientes**
  No diseñar o seguir prácticas sólidas de seguridad de datos, o asegurarse de que se hayan seguido, puede dar lugar a datos violados o expuestos. Morgan Stanley, por ejemplo, se enfrentó a una demanda colectiva después de que se descubriera que su equipo informático fuera de servicio contenía datos personales de más de 15 millones de clientes. Morgan Stanley afirmó que el problema ocurrió debido a una fallo de software. También se culpó a las prácticas insuficientes de protección de datos por la violación masiva de datos en Capital One. Los equipos de seguridad a menudo carecen de visibilidad en los servicios en la nube para saber qué datos deben protegerse, y los internos pueden eludir los controles de seguridad tradicionales exportando datos o copiando archivos o bases de datos.

- **Empleados no suficientemente capacitados en amenazas a la seguridad**
  Los empleados voluntariamente, aunque sin darse cuenta, se convierten en participantes activos en un ciberataque cuando no reconocen los signos reveladores de una amenaza a la seguridad. Por ejemplo, un pirata informático violó los datos personales de más de siete millones de usuarios de la aplicación de corretaje Robinhood al llamar a la línea de atención al cliente y engañar a un empleado de atención al cliente para que entregue las credenciales de su cuenta a varios sistemas de atención al cliente.

- **Empleados que ignoran activamente los deberes de comunicación regulados**
  Las instituciones financieras están obligadas a archivar y supervisar las comunicaciones relacionadas con el trabajo de los empleados. Sin embargo, los empleados pueden eludir fácilmente estos requisitos mediante el uso de herramientas de chat y comunicación no autorizadas, como WhatsApp, cuentas de correo electrónico personales y Telegram. Los reguladores no tienen una visión positiva de tal comportamiento; por ejemplo, la Comisión de Bolsa de Valores (SEC) y la Comisión de Comercio de Futuros de Productos Básicos (CFTC) multaron a JPMorgan Chase & Co. con una suma combinada de $200 millones a fines de 2021 por evitar de manera generalizada y sistemática las responsabilidades de vigilancia mediante el uso de WhatsApp y otras plataformas no autorizadas. Otros bancos también están siendo investigados por la CFTC, incluidos HSBC Holdings y Deutsche Bank.

***Los empleados, sin darse cuenta, se convierten en participantes activos en un ciberataque cuando no reconocen los signos reveladores de una amenaza a la seguridad.***

### DAÑO A LA REPUTACIÓN PERSISTENTE CON APLICACIONES LENTAS

Las empresas de servicios financieros experimentan un daño persistente en su reputación cuando las consecuencias de las filtraciones de datos importantes tardan años en resolverse. Las acciones regulatorias, los casos civiles y las demandas colectivas nunca se resuelven rápidamente, y los plazos prolongados refuerzan la conciencia de falloss anteriores. El acuerdo de una demanda colectiva contra Desjardins por la violación de datos de 2019 solo se propuso en diciembre de 2021. De manera similar, la violación de datos de 2019 en Capital One resultó en una acción regulatoria después de un año y el acuerdo de una demanda colectiva después de más de dos años.

### COMPROMISO DE TOKENS DE ACCESO OAUTH

Los tokens de acceso OAuth brindan conectividad a través de aplicaciones en la nube SaaS, lo que agiliza los flujos de datos y simplifica la integración entre servicios para los clientes. La simplicidad de pedirle a un usuario que apruebe un conjunto duradero de derechos también es atractiva para los actores de amenazas. Comprometer una aplicación, sus datos y derechos resulta de que un usuario, sin saberlo, autorice conexiones OAuth maliciosas después de caer en un ataque de phishing o descargar una aplicación comprometida. También se produce cuando una aplicación de terceros legítima y autorizada se ve comprometida (explotando una vulnerabilidad, obteniendo acceso a través de un ataque de phishing o plantando malware) y moviéndose lateralmente en los entornos del cliente, por ejemplo, SolarWinds, Log4j. Dado que los tokens de OAuth reciben una autorización válida de los usuarios autorizados, la mera presencia de una conexión autorizada es una evaluación de amenaza insuficiente. Las empresas deben adoptar un enfoque matizado y basado en el riesgo para evaluar continuamente cada conexión.

### ATAQUES CONTRA INTERFACES DE PROGRAMACIÓN DE APLICACIONES (APIS)

Las aplicaciones modernas publican API para habilitar funciones del sistema, como crear cuentas, solicitar información e iniciar transacciones. A los actores de amenazas les gustan las API porque contienen vulnerabilidades que pueden explotarse para obtener el control de una cuenta y robar fondos. Un estudio reciente documentó una letanía de problemas de seguridad de API encontrados en aplicaciones móviles proporcionadas por instituciones financieras grandes y pequeñas. En una escala más amplia, al menos el 75 % del total de ataques de inicio de sesión contra instituciones financieras buscan comprometer las API. Los bots y las botnets prevalecen en estos ataques.

***Al menos el 75% del total de ataques de inicio de sesión contra instituciones financieras buscan comprometer las API.***

### ATAQUES DE DENEGACIÓN DE SERVICIO

Los ataques de denegación de servicio (DoS) inundan los servidores de una empresa objetivo con más tráfico del que están configurados para manejar, lo que provoca que las aplicaciones y los servicios se desconecten. Estos pueden lanzarse para causar interrupciones o para obtener ganancias financieras. Por ejemplo, los bancos en Australia han sido amenazados con ataques DoS sostenidos si no pagan un rescate por adelantado, y la bolsa de valores de Nueva Zelanda (NZX) estuvo fuera de línea durante más de seis días en agosto de 2020 debido a un ataque DoS. El ataque contra el NZX fue parte de una campaña de ataque más amplia contra las instituciones financieras de todo el mundo.

### COMPROMISO DE LOS SISTEMAS FINANCIEROS

Comprometer los sistemas financieros de una víctima brinda la oportunidad para que un actor de amenazas cree transacciones fraudulentas directamente en el sistema financiero. Este tipo de ataque permite al actor de amenazas crear una pila de transacciones fraudulentas a lo largo del tiempo. Elephant Beetle, un grupo de actores de amenazas activo en América Latina, está robando millones de dólares de las víctimas en el sector de servicios financieros después de ingresar y establecer persistencia en sus sistemas financieros.

# El entorno regulatorio

En todo el mundo, el sector de los servicios financieros es una de las industrias más reguladas, con controles impuestos por organismos gubernamentales y de la industria en muchos aspectos de las operaciones dentro del sector. En esta sección, analizamos brevemente una muestra de regulaciones relacionadas con la ciberseguridad. Este tratamiento no es exhaustivo.

## ESTADOS UNIDOS

Las regulaciones de seguridad cibernética en los Estados Unidos para las empresas de servicios financieros incluyen requisitos para capturar y retener datos, proteger los datos sensibles y confidenciales de empresas e individuos, y desarrollar un conjunto de protecciones efectivas contra las amenazas de seguridad cibernética. Ejemplos incluyen:

- **SEC (Comisión de Bolsa y Valores)**
  La SEC requiere que las comunicaciones comerciales de ciertos grupos sean capturadas, supervisadas y archivadas. Se permite el mantenimiento de registros electrónicos y existen requisitos estrictos sobre inmutabilidad y accesibilidad. La SEC no ve con buenos ojos que las empresas eludan deliberadamente los requisitos de retención de datos.

- **FINRA (Autoridad Reguladora de la Industria Financiera)**
  FINRA requiere que se establezcan políticas y controles sobre cómo se capturan, administran y protegen los datos. Las empresas deben realizar evaluaciones periódicas de la preparación para la seguridad cibernética, monitorear activamente el uso de información privilegiada (el uso de aplicaciones de comunicaciones no autorizadas puede señalar actividades con malas intenciones) y conservar estrictamente ciertos registros comerciales por hasta siete años, entre otros.

- **PCI-DSS (Estándar de seguridad de datos de la industria de tarjetas de pago)**
  Las empresas que aceptan transacciones con tarjetas de crédito y débito deben cumplir con el estándar PCI, que se enfoca en cómo se protegen los datos de transacciones y tarjetas durante la transmisión y el almacenamiento.

- **Reglamento de Ciberseguridad de Nueva York**
  El Departamento de Servicios Financieros de Nueva York requiere que la mayoría de las instituciones financieras promulguen una política de seguridad cibernética integral, identifiquen todas las amenazas de seguridad cibernética internas y externas y tengan las soluciones adecuadas para defenderse de las amenazas identificadas. También se requieren capacidades de detección y recuperación, junto con informes periódicos.

- **NCUA (Administración Nacional de Cooperativas de Crédito)**
  Las cooperativas de ahorro y crédito que están aseguradas por el gobierno federal deben cumplir con las normas de seguridad cibernética de la NCUA. Las regulaciones cubren áreas tales como el desarrollo de un programa completo de seguridad por escrito (que incluye la confidencialidad y la integridad de los registros de los miembros), la notificación de incidentes y desastres importantes (que se prevé que interrumpan los servicios de los miembros durante más de dos días hábiles consecutivos) y la notificación de incidentes de violación de datos. Las cooperativas de ahorro y crédito con seguro federal se someten a una revisión periódica por parte de la NCUA de su programa de seguridad de la información; la revisión debe tener lugar al menos cada 20 meses.

- **FFIEC (Consejo Federal de Examen de Instituciones Financieras)**
  El FFIEC ofrece orientación a las instituciones financieras sobre una variedad de temas de seguridad cibernética con el espíritu de crear conciencia sobre los riesgos y amenazas de seguridad cibernética. Si bien sus declaraciones generalmente no imponen expectativas regulatorias, sus materiales y enfoques se han convertido en estándares influyentes para las instituciones financieras y se alinean con las regulaciones emitidas por sus agencias miembros en el gobierno federal

***Los servicios financieros son uno de los sectores más regulados, con controles impuestos por organismos del gobierno y las industrias.***

gobierno, incluida la Junta de Gobernadores de la Reserva Federal, la NCUA, la Corporación Federal de Seguros de Depósitos y otros.

• **Reportar violaciones de datos e incidentes cibernéticos dentro de las 36 horas** Una nueva regla federal, en vigencia a partir del 1 de abril de 2022, requiere que los bancos divulguen las violaciones de datos y los incidentes cibernéticos dentro de las 36 horas si interrumpen o degradan, o amenazan con hacerlo, la capacidad del banco para realizar operaciones bancarias o entregar sus productos. y servicios.63 Los proveedores de servicios de los bancos están obligados a notificar a sus clientes bancarios sobre incidentes similares lo antes posible.

• **Requisitos de protección de datos a nivel estatal, p. ej., California, Virginia, Colorado** Si bien no son específicos del sector de servicios financieros, las reglamentaciones emergentes de protección de datos a nivel estatal en California, Virginia y Colorado imponen mayores requisitos sobre cómo se capturan los datos personales de los consumidores almacenados, protegidos y utilizados. Las empresas que tienen datos cubiertos deben extender ciertos derechos a los interesados.

Las instituciones financieras son auditadas regularmente, y la preparación para la seguridad cibernética es un criterio de evaluación clave.

## REINO UNIDO

Las regulaciones de ciberseguridad en el Reino Unido se ocupan de amenazas y riesgos similares a los de los Estados Unidos. Las regulaciones se enfocan en aumentar la resiliencia cibernética de las empresas en el sector financiero. Ejemplos incluyen:

- **PRA (Autoridad de Regulación Prudencial)**
  La principal preocupación de la PRA es mantener la estabilidad financiera del sector financiero del Reino Unido. Los ataques cibernéticos se consideran perjudiciales para alcanzar este objetivo de estabilidad. Un enfoque clave es garantizar que los bancos y otras instituciones financieras que operan en el Reino Unido puedan continuar operando bajo la amenaza de interrupción operativa de los ataques cibernéticos. Un segundo enfoque clave es que las empresas gestionen adecuadamente su riesgo de terceros con los proveedores de la nube.

- **FCA (Autoridad de Conducta Financiera)**
  La FCA se enfoca en proteger a los consumidores y la integridad del mercado financiero.66 Por implicación, la FCA quiere que los participantes del mercado desarrollen una cultura de seguridad, identifiquen sus activos de información y cuenten con protecciones y planes de recuperación para mitigar los incidentes de ciberseguridad. Personal el conocimiento de las amenazas cibernéticas se considera un componente esencial de una postura sólida de seguridad cibernética, junto con la visibilidad de dónde se almacenan y procesan los datos por parte de la propia empresa y a través de socios externos. Las empresas deben realizar revisiones periódicas de seguridad cibernética, desconfiar adecuadamente de los acuerdos de subcontratación de la nube y asegurarse de que las vulnerabilidades en las aplicaciones afectadas se reparen de inmediato. Las empresas deben informar las violaciones de datos y los incidentes cibernéticos cuando se produzca una pérdida de datos, disponibilidad o control.

- **Ley de Protección de Datos**
  La Ley de Protección de Datos de 2018 implementa el Reglamento General de Protección de Datos de Europa en la legislación del Reino Unido. Las empresas deben proteger los datos personales de los clientes, extender un conjunto de derechos de datos a los clientes y avisar sobre violaciones de datos e incidentes cibernéticos que resultan en una menor disponibilidad del sistema.

- **Las empresas deben establecer controles sobre cómo se utilizan los datos personales para la elaboración de perfiles y la toma de decisiones.** Según los informes de empresas sobre incidentes de seguridad de datos, el sector de servicios financieros en el Reino Unido se ubica como el tercer sector más alto en términos de incidentes informados. El sector también tiene la mayor

***Las instituciones financieras son auditadas periódicamente, y preparadas para la seguridad cibernética.***

contar para ransomware e incidentes de mala configuración de acceso y el segundo número más alto de incidentes de phishing.

## REGULACIONES EN OTRAS REGIONES

Las empresas de servicios financieros en otras regiones y países también están sujetas a una variedad de regulaciones relacionadas con la seguridad cibernética. Tres breves ejemplos son:

- **RGPD (Reglamento General de Protección de Datos de la Unión Europea)**
  El RGPD ofrece una regulación intersectorial sobre cómo se capturan, almacenan, gestionan, protegen y utilizan los datos personales. GDPR eleva los derechos disponibles para los interesados y aumenta significativamente las multas administrativas que se pueden imponer a las empresas que no cumplen con sus requisitos. Las violaciones de datos deben notificarse a la autoridad de protección de datos correspondiente dentro de las 72 horas.

- **CPS 234 de Australia sobre la gestión de riesgos de seguridad de la información**
  Publicado a mediados de 2019 por el regulador de servicios financieros de Australia, CPS 234 establece estándares para la seguridad de la información por parte de las entidades cubiertas. evaluaciones, entre otros. El regulador también tiene la intención de adoptar un enfoque activo al evaluar la eficacia de las protecciones de ciberseguridad, en lugar de confiar únicamente en la certificación.

- **Sudáfrica sobre notificación de violación de datos**
  Standard Bank of South Africa tardó nueve días en notificar a los clientes afectados por una violación de datos de su plataforma de propiedad en línea. El Regulador de Información de Sudáfrica dictaminó que nueve días era demasiado tiempo, a pesar de que la Ley de Protección de Información Personal especifica que el estándar de información es "tan pronto como sea razonablemente posible" en lugar de definir la cantidad de horas o días dentro de los cuales debe ocurrir la divulgación.

## EL IMPULSO PARA LA RESILIENCIA OPERATIVA

Los reguladores de la industria de servicios financieros de todo el mundo, como la FCA y sus socios en el Reino Unido, la Reserva Federal y sus socios en los Estados Unidos, y el Comité de Supervisión Bancaria de Basilea, están impulsando una agenda de resiliencia operativa en todo el sector. En los Estados Unidos, la resiliencia operativa se considera “el resultado de una gestión eficaz del riesgo operativo combinada con suficientes recursos financieros y operativos para prepararse, adaptarse, resistir y recuperarse de las interrupciones”.

*Los reguladores de la industria están impulsando una agenda de resiliencia operativa en todo el sector de servicios financieros.*

El crecimiento de los ataques cibernéticos, especialmente el ransomware contra la infraestructura crítica, ha aumentado el riesgo de que el sistema financiero deje de funcionar. Si las aplicaciones financieras se vuelven inútiles debido a ataques distribuidos de denegación de servicio o cifrado no deseado a través de ransomware, los clientes individuales y la economía en general se ven obstaculizados, en el mejor de los casos, o se les impide, en el peor de los casos, completar transacciones financieras. Si bien la resiliencia financiera sigue siendo esencial, lo que significa que los bancos y otras empresas financieras tienen suficientes reservas para funcionar en tiempos difíciles, los dos tipos de resiliencia están cada vez más entrelazados. El sistema financiero de un país puede desestabilizarse más fácilmente al interrumpir la capacidad operativa de sus instituciones financieras y socios tecnológicos, ya sea debido a ataques de actores externos maliciosos o eventos irregulares y devastadores. Tal desestabilización puede ser manipulada en un marco de tiempo más rápido y fácil por parte de los actores de amenazas que esperar a que llegue el próximo ciclo de debilidad financiera sistémica.

# El atractivo del sector financiero como objetivo de los ataques

El sector financiero continúa siendo un objetivo atractivo para los actores de amenazas. Las razones incluyen:

- **Dinero dinero dinero**
  Las instituciones financieras retienen y procesan grandes sumas de dinero, la mayor parte perteneciente a otras personas. Poner en peligro la lógica de las transacciones, obtener credenciales de cuenta para consumidores con saldos bancarios saludables y desviar fondos a una cuenta controlada por un actor de amenazas, todos brindan un día de pago rico.

- **Potencial de sabotaje financiero contra un país**
  Un ataque cibernético exitoso contra una gran institución financiera tiene el potencial de paralizar el sistema financiero de una nación, con posibles efectos indirectos en el sistema financiero global más amplio. Los sistemas financieros no operativos impiden rápidamente la actividad económica, paralizan la vida normal y socavan la confianza de los consumidores y las empresas. Los actores de amenazas ven el potencial de infligir estragos rápidos en una nación al atacar a los jugadores en su sistema financiero, una estrategia que se usó recientemente para disuadir la agresión rusa en su guerra contra Ucrania la urgencia de dictar una resolución rápida.

- **Datos valiosos para el robo de identidad y ataques posteriores**
  Comprometer los datos de los clientes proporciona datos personales actualizados para su uso en el robo de identidad y otros ataques. Los nombres, direcciones, información bancaria, detalles de contacto y documentos hipotecarios ofrecen detalles que pueden usarse en intentos de suplantación de identidad. Los mismos datos subyacentes se pueden usar en intentos de phishing y vishing (phishing de voz) destinados a capturar las credenciales de la cuenta, eludir los controles de autenticación de múltiples factores y robar fondos de clientes desprevenidos. Las regulaciones de la industria exigen que los bancos conserven ciertos tipos de datos durante un máximo de siete años, y los propios bancos suelen optar por conservar los datos durante mucho más tiempo. Por ejemplo, Credit Suisse sufrió una filtración de datos que cubría más de 18.000 cuentas bancarias, incluidas algunas que datan de la década de 1940.

- **La rápida modernización corre el riesgo de socavar la postura de seguridad**
  Las empresas de servicios financieros establecidas están bajo el ataque competitivo de las nuevas empresas de tecnología financiera, las empresas de servicios financieros no tradicionales y las nuevas ofertas de criptomonedas. Los jugadores establecidos se apresuran a modernizar los sistemas, crear nuevos productos y servicios y lanzar ofertas de cuentas actualizadas para reducir la rotación de clientes. Sin embargo, tal velocidad corre el riesgo de crear nuevas deficiencias de seguridad al lanzar aplicaciones vulnerables, depender de servicios en la nube con disposiciones de seguridad insuficientes y no fortalecer los sistemas y procesos lo suficiente antes de lanzarlos al mercado.

- **Actividad delictiva de bajo riesgo, por ejemplo, robo desde la comodidad de un sillón en el otro lado del mundo**
  Los ataques cibernéticos tienen el potencial de que los delincuentes roben fondos significativos desde la relativa seguridad de su hogar u oficina. No requieren camiones, dinamita, armas de fuego, pasaportes falsos o una banda de ladrones con quienes colaborar. Con los ataques de compromiso de email comercial, el escenario ideal es que se ejecute una transferencia bancaria falsificada y el dinero aparezca poco después en la cuenta bancaria del delincuente. Y, con suerte, justo a tiempo para una excursión matutina a la cafetería local.

***El acceso al dinero, el sabotaje de los sistemas financieros y el robo de datos para el robo de identidad son motivadores clave para los hackers.***

# Perspectivas de la dinámica de amenazas contra los servicios financieros

El sector financiero seguirá siendo un foco clave para los ataques cibernéticos y el fraude cibernético. Algunos actores de amenazas desatan ataques cibernéticos en busca de ganancias financieras a través de medios maliciosos o nefastos; otros buscan desestabilizar el sistema financiero de un país.

Las perspectivas que vemos para el sector financiero son:

- **Protege tus datos; alguien más lo quiere**
  Las empresas de servicios financieros tienen datos valiosos sobre individuos, empresas y agencias gubernamentales. Esto no va a cambiar. Comprometer dichos datos permite a los actores de amenazas recopilar inteligencia para ataques directos contra las víctimas o usar datos actualizados para intentar varios tipos de fraude financiero y de préstamos contra bancos y compañías de seguros a través de la manipulación de identidad.

- **Protege tus recursos financieros; otras personas quieren robarlos**
  Las empresas de servicios financieros son el mecanismo mediante el cual se almacenan, transfieren y protegen los recursos financieros. Esto no va a cambiar, aunque se agregarán nuevas formas de moneda a la mezcla. Los actores de amenazas permanecerán perpetuamente interesados en obtener acceso a fondos que no les pertenecen. Los ataques de phishing y de compromiso de correo electrónico comercial continuarán, junto con los actores de amenazas que se hacen pasar por empresas de servicios financieros confiables y se hacen pasar por ellas para eludir las protecciones de seguridad y la conciencia del consumidor para robar fondos.

- **Proteger la disponibilidad e integridad de tus sistemas**
  Los sistemas financieros, las redes y las interconexiones facilitan las actividades económicas de individuos, empresas y naciones. Paralizar o degradar el desempeño de estos sistemas tiene interés para que los actores del estado-nación inflijan daño económico y presión de represalia a otras naciones. Por ejemplo, el Banco de la Reserva de Australia considera que un ataque cibernético exitoso contra una institución financiera importante en Australia es solo cuestión de tiempo. Hay tanta actividad de amenazas sucediendo que es casi inevitable.

El potencial de las amenazas contra las instituciones financieras para socavar o desestabilizar un país se destacó desde las primeras etapas de la guerra rusa contra Ucrania. Se establecieron varias sanciones financieras contra Rusia, como quitarle el acceso a la red financiera SWIFT. El temor de ataques de represalia por parte de Rusia contra empresas del sector financiero en todo el mundo aumentó considerablemente, y las agencias federales y nacionales advirtieron a los bancos, cooperativas de crédito y empresas de otros sectores que estén en un estado de mayor preparación para contrarrestar los ataques cibernéticos (por ejemplo, CISA en los Estados Unidos). Unidos y el Banco Central Europeo para los bancos europeos).

Finalmente, el seguro cibernético se está volviendo más difícil y costoso de asegurar, y las aseguradoras aumentan las primas por una cobertura mucho menor. El crecimiento de los ataques cibernéticos exitosos, en particular el ransomware, ha tenido un efecto negativo dramático en la rentabilidad de los suscriptores y, por lo tanto, están reequilibrando sus cálculos de riesgo. Las empresas de todos los sectores, incluidos los servicios financieros, deberán asegurarse de contar con las soluciones tecnológicas adecuadas para contrarrestar las amenazas para las que se utilizó anteriormente la cobertura de seguro.

***Dado que los seguros cibernéticos son cada vez más difíciles de asegurar, las empresas se enfrentan a un cálculo de riesgos cambiante.***

# Soluciones de ciberseguridad a considerar

Las empresas de servicios financieros han estado cada vez más bajo el ataque de los actores de amenazas cibernéticas, y es poco probable que esta trayectoria disminuya. Las empresas deben asegurarse de contar con las soluciones adecuadas para protegerse y defenderse a sí mismas, a sus clientes y a los sistemas financieros en los que participan. Es importante tener en cuenta que las soluciones requieren personas con una comprensión avanzada de cómo funcionan juntas las partes de una implementación eficaz de ciberseguridad. Para esto, la gerencia debe asignar fondos, recursos y tiempo de los empleados para aprender, comprender y pensar sobre estas intersecciones. La educación continua es clave, lo que implica más que solo obtener una certificación de seguridad.

En esta sección, hablamos de soluciones.

## SEGURIDAD EN LA NUBE, INCLUYENDO VISIBILIDAD Y VULNERABILIDAD

Garantizar la seguridad de los servicios en la nube es fundamental a medida que aumenta la adopción. Las empresas de todos los sectores, incluidos los servicios financieros, confían cada vez más datos confidenciales a plataformas IaaS críticas para el negocio y aplicaciones SaaS. Estos son sistemas complejos con funcionalidades intrincadas, y diseñar, implementar y extender una sólida postura de seguridad en estas plataformas y aplicaciones es un desafío. Las empresas de servicios financieros se benefician de soluciones especializadas que identifican y mitigan amenazas, fortalecen la postura de seguridad y brindan alertas tempranas de vulnerabilidades.

Las soluciones de seguridad en la nube deben resaltar las configuraciones incorrectas iniciales, las conexiones riesgosas, las autenticaciones cuestionables, la deriva en la configuración a lo largo del tiempo y más. Las ofertas específicas que debe buscar son:

- **CASB (agente de seguridad de acceso a la nube)**
  Las soluciones CASB monitorean a qué servicios en la nube se conectan los usuarios, qué tipos de datos se almacenan en los respectivos servicios y de dónde provienen las conexiones, entre otros. Brindan visibilidad que no está disponible con las soluciones de monitoreo tradicionales y pueden aplicar políticas de seguridad de datos para contenido y conexiones riesgosas. Las soluciones CASB brindan una evaluación continua del riesgo de cada servicio en la nube identificado, lo que ayuda a los equipos de IT y seguridad a priorizar las acciones de mitigación para los servicios en la nube.

- **CSPM (Administración de postura de seguridad en la nube) y SSPM (Administración de postura de seguridad SaaS)**
  Las soluciones de gestión de la postura de seguridad cubren tanto a los proveedores de infraestructura en la nube (CSPM) como a las soluciones SaaS (SSPM). Brindan visibilidad continua y análisis de la configuración de varios servicios de IaaS y SaaS, recomendaciones sobre cómo fortalecer la configuración de seguridad (p. ej., eliminando los derechos de acceso o reduciendo el alcance de acceso para un individuo o grupo de personas) y alertas sobre cambios. en configuraciones de seguridad que socavan la postura objetivo. Con la mayor dependencia de las ofertas en la nube (IaaS y SaaS), es fundamental tener una visión permanente del estado de la seguridad. Estas soluciones buscan prevenir el tipo de ataque que resultó tan costoso para Capital One.

Las soluciones de seguridad en la nube aprovechan los modelos de inteligencia artificial (AI) y aprendizaje automático (ML) para analizar el comportamiento de los usuarios y los datos para detectar amenazas como el compromiso de la cuenta, los infiltrados maliciosos y la explotación de vulnerabilidades.

***Protege los servicios en la nube de amenazas, configuraciones incorrectas y conexiones peligrosas.***

## IDENTIDAD Y AUTENTICACIÓN PARA EMPLEADOS Y CLIENTES

Muévete en la dirección de menos contraseñas y más datos biométricos para procesos de autenticación más sólidos para empleados y clientes. La identificación única de un empleado y la garantía de que la persona que proporciona las credenciales de autenticación es el empleado correcto está condenado a falla
r con nombres de usuario, contraseñas e incluso formas básicas de autenticación de múltiples factores. Las soluciones de identidad gestionada en las que la identificación biométrica mediante huellas dactilares o el reconocimiento facial están vinculadas a una identidad proporcionan una autenticación de alta seguridad para los empleados que realizan su trabajo, junto con claves criptográficas de hardware utilizadas en combinación con la biometría gestionada.

Las empresas de servicios financieros también necesitan fortalecer los flujos de trabajo de identidad y autenticación para los clientes, no solo para los empleados.84 Los clientes forman una parte integral del sistema financiero; acceden e interactúan con cuentas y productos de préstamo, e inician transacciones estándar y de alto valor. Brindar acceso al sistema a los clientes utilizando solo un nombre de usuario y una contraseña es una invitación abierta al compromiso, y son esenciales métodos más sólidos de autenticación dentro de las aplicaciones móviles, biometría para la autenticación de múltiples factores y principios de confianza cero para detectar características anormales de dispositivos y redes. La alta seguridad de que la persona que solicita acceso a una cuenta o inicia una transacción es quien dice ser es fundamental para evitar fraudes y pérdidas. La dependencia de los enfoques básicos de 2FA, como los códigos enviados por SMS o correo electrónico, debe eliminarse en los flujos de trabajo que otorgan acceso al sistema a los clientes porque las protecciones ofrecidas originalmente por estos enfoques son cada vez más fáciles de romper. Hay una creciente digitalización de la experiencia bancaria para los consumidores, impulsada por la fuerza por las órdenes de confinamiento y confinamiento durante la pandemia y el cierre de las sucursales con la erosión adicional de cualquier relación cara a cara restante entre los banqueros y los consumidores. El desarrollo de medios más sólidos de garantía de identidad es clave para la interacción continua con el cliente y las experiencias bancarias.

La identidad y la autorización deben monitorearse para detectar intentos de piratería, ataques de rociado de contraseñas, volcado de credenciales e intentos de usar credenciales robadas. Las soluciones de seguridad en la nube ofrecen capacidades para monitorear de dónde provienen las solicitudes de autorización, al igual que las soluciones de administración de identidad.

***Desarrollar medios más sólidos de garantía de identidad para salvaguardar las interacciones con los clientes y las experiencias bancarias.***

## ABORDAR EL ACCESO EXCESIVAMENTE PRIVILEGIADO

Cualquier empleado o contratista con derechos de acceso a datos y sistemas que excedan lo necesario para sus tareas laborales representa un riesgo para una empresa de servicios financieros. Esto puede resultar en el robo de datos por parte de un empleado malicioso, el uso compartido excesivo accidental por parte de un empleado o el robo de datos por parte de un actor de amenazas externo después de comprometer las credenciales de un empleado. Una encuesta encontró que el 37 % de las empresas había detectado cuentas con privilegios excesivos en su entorno, y el 59 % de las empresas dijeron que las credenciales de las cuentas privilegiadas habían sido suplantadas con éxito.

Los sistemas que monitorean y analizan los niveles de acceso de los empleados (incluidos gerentes, ejecutivos, administradores de IT y contratistas) para identificar los derechos de acceso con privilegios excesivos permiten una intervención temprana para restablecer los derechos a un nivel más apropiado. Tal tamaño correcto reduce la probabilidad de que existan cuentas con niveles de acceso inapropiadamente altos, reduce la deriva de acceso cuando los derechos se extienden por error y disminuye el radio de explosión en caso de un ataque interno o una infracción externa.
Los sistemas que abordan el acceso con privilegios excesivos utilizan modelos de IA y ML para crear una base normalizada de derechos de acceso para los empleados en función de un grupo de referencia; por ejemplo, un analista de marketing debe tener el mismo nivel de derechos que otros analistas de marketing en el departamento de marketing. Las desviaciones de la norma pueden ser

se ajusta automáticamente o se le permite continuar según la autorización del gerente del empleado.

Para las personas que requieren altos niveles de acceso a los sistemas, las soluciones de gestión de acceso privilegiado (PAM) introducen medidas de seguridad adicionales. Por ejemplo, en lugar de activar continuamente los derechos de superusuario en la cuenta, el usuario solicita una concesión de acceso elevado por tiempo limitado o por transacción limitada que debe aprobarse, auditarse y revocarse automáticamente cuando haya transcurrido el tiempo o el se completa la transacción.

Finalmente, el acceso con privilegios excesivos también ocurre cuando las conexiones entre aplicaciones, como los tokens OAuth que se usan ampliamente en entornos SaaS, se otorgan de manera imprudente o inconsciente a actores malintencionados. Utilice soluciones para evaluar continuamente la intención de las conexiones OAuth, detectar amenazas ocultas y fortalecer las configuraciones de seguridad.

## GESTIÓN DE BOTS

Los actores de amenazas aprovechan los bots y las redes de bots para permitir los ataques cibernéticos, incluidos los ataques distribuidos de denegación de servicio, relleno de credenciales y API. Las soluciones de administración de bots que identifican, bloquean y mitigan el tráfico de bots permiten a las empresas evitar el tiempo de inactividad, proteger las cuentas de los clientes del compromiso de credenciales oportunistas, garantizar que las API no revelen datos protegidos o confidenciales y evitar la introducción de malware para facilitar el acceso persistente por parte de los actores de amenazas. Las soluciones de administración de bots que detienen el tráfico de bots permiten una mayor capacidad de respuesta para los clientes válidos, detienen la creación de cuentas de usuario falsas que pueden usarse para ataques posteriores y evitan transacciones falsas cuando los detalles de la tarjeta de crédito son forzados.

***Identifica y bloquea el tráfico de bots maliciosos para proteger las cuentas de los clientes y salvaguardar las API.***

## SEGURIDAD AVANZADA DE CORREO ELECTRÓNICO PARA PROTEGER CONTRA PHISHING, MALWARE Y BEC

Proteja su sistema de correo electrónico y el canal de comunicación por correo electrónico de suplantación de identidad, amenazas transmitidas por correo electrónico y ataques de compromiso de email comercial. Las siguientes soluciones fortalecen las protecciones en estas áreas:

- **Analizar mensajes, archivos adjuntos y enlaces en busca de contenido malicioso**
  El email es un canal muy común para la entrega de amenazas maliciosas, con archivos adjuntos y enlaces incrustados particularmente perniciosos. Todo el contenido entrante debe escanearse en busca de amenazas, al igual que los mensajes enviados para capturar amenazas enviadas desde cuentas o dispositivos comprometidos.
  Los proveedores de soluciones de seguridad de email buscan diferenciarse en función de características tales como tasas de captura, niveles de análisis (es decir, desempaquetar y examinar recursivamente cada componente individual en un mensaje o archivo adjunto incrustado) y escaneo de enlaces en uso para capturar el armamento posterior a la entrega que se pierde si el escaneo de enlaces se realiza solo en la entrega inicial.

- **Asegúrate de que SPF, DKIM y DMARC estén configurados y alineados**
  Hay tres estándares básicos de Internet disponibles para proteger los sistemas de correo electrónico de la suplantación de identidad, la suplantación de identidad y el uso de ataques de phishing contra otras empresas. SPF (Sender Policy Framework) especifica los hosts de correo electrónico en los que se confía para enviar email para un dominio. DKIM (DomainKeys Identified Mail) firma mensajes usando criptografía para afirmar su validez. DMARC (Autenticación, informes y conformidad de mensajes basados en dominios) establece qué deben hacer las empresas cuando reciben mensajes con atributos sospechosos e incluye opciones de informes para identificar flujos de mensajes fraudulentos. En combinación, estos controles aumentan la autenticidad del canal de email.

Realizar cambios en estos controles normalmente requiere actualizar los registros DNS, pero existen enfoques más nuevos y dinámicos que simplifican la configuración

- **Track potential brand abuse**
  El uso indebido de nombres de marca permite que los actores de amenazas se hagan pasar por una entidad financiera confiable, por ejemplo, al registrar el mismo nombre de dominio con una extensión diferente o con una ortografía ligeramente diferente para crear un nombre de dominio parecido o registrar un nuevo nombre de dominio que suene como un dominio confiable. Use los servicios de monitoreo de dominio para rastrear y alertar sobre la creación de nombres de dominio que podrían usarse en ataques contra clientes.

- **Supervise los servicios de correo electrónico en la nube en busca de vulnerabilidades**
  Las empresas que usan servicios de correo electrónico en la nube, como Microsoft 365, deben monitorear las vulnerabilidades en la configuración y el uso. Esto incluye el uso de protocolos de autenticación heredados, estándares de correo electrónico heredados para acceder a los mensajes (p. ej., POP e IMAP), la creación de reglas de eliminación y reenvío de correo (que a menudo sucede cuando un actor de amenazas se apodera de la bandeja de entrada de un empleado) y el reenvío de correo electrónico a cuentas personales. Las soluciones SaaS Security Posture Management (SSPM) brindan visibilidad para identificar y rectificar tales vulnerabilidade.

## VULNERABILIDAD Y PATCHING

Las aplicaciones sin parches envían una señal de "abierto para compromiso" a los actores de amenazas. Reducir la amplitud y la frecuencia de las aplicaciones sin parches es una estrategia clave para reducir la fuga y las filtraciones de datos. Los sistemas que monitorean nuevos avisos de vulnerabilidad de los proveedores de aplicaciones, comparan los avisos con un catálogo en tiempo real de aplicaciones y versiones implementadas, y ofrecen una lista priorizada de parches para implementar, brindan a las empresas de servicios financieros los datos necesarios para mantener su panorama de aplicaciones actualizado. Los parches automatizados ayudan a reducir el tiempo transcurrido entre la identificación y la mitigación de una vulnerabilidad, y las soluciones de parches virtuales protegen las aplicaciones de posibles amenazas a la seguridad mientras el proveedor desarrolla y prueba un parche real.

## EXTERNAL ATTACK SURFACE MANAGEMENT

Los actores de amenazas realizan un reconocimiento para encontrar vulnerabilidades sin parches, datos desprotegidos y puertos expuestos para el acceso remoto a la red de una víctima objetivo y a los repositorios de datos en la nube. Las soluciones de gestión de superficie de ataque externo brindan a las empresas de servicios financieros la capacidad de auditar y evaluar de manera consistente las debilidades en los sistemas y los controles de seguridad cibernética. Estas soluciones detectan, identifican, categorizan, priorizan, mitigan y abordan las debilidades directamente o mediante notificación al equipo de seguridad. La postura de seguridad se evalúa continuamente a medida que los proveedores informan sobre la vulnerabilidad del nuevo sistema, las unidades comerciales agregan nuevos sistemas SaaS y de IT, y la actividad de fusión y adquisición trae nuevas redes y riesgos al ámbito más amplio de la seguridad.

***Protege el email de suplantación de identidad, amenazas transmitidas por email y ataques de compromiso de email comercial.***

## FORMACIÓN DE CONCIENTIZACIÓN DE SEGURIDAD

Los empleados de las empresas de servicios financieros tienen las llaves de importantes sistemas financieros. Si un actor de amenazas puede comprometer a un empleado a través de un ataque de phishing, vishing, smishing o compromiso de correo electrónico comercial, entonces se pueden robar las credenciales y los fondos. Los empleados necesitan capacitación periódica sobre las señales de advertencia de las amenazas cibernéticas, los trucos comunes de ingeniería social y las mejores prácticas de higiene de seguridad para reducir la probabilidad de un ataque exitoso.

Los mejores programas de capacitación en concientización sobre seguridad de su clase incluyen métodos de evaluación además del contenido de capacitación para medir la eficacia de los empleados en la detección y mitigación de ataques. A los empleados o grupos de empleados que muestren poca eficacia a pesar de las intervenciones de capacitación recientes se les puede ofrecer capacitación adicional, protecciones de procesos más sólidas y mejores tecnologías de seguridad. Si los empleados se niegan a seguir las políticas de seguridad, vuelva a evaluar el estado de empleo en curso.

## SERVICIOS DE SEGURIDAD GESTIONADOS

Los servicios de seguridad administrados ofrecen una vía para que las empresas obtengan acceso a servicios de seguridad avanzados, aborden la grave escasez de talento en seguridad cibernética y agreguen capas de prevención y detección para aumentar la postura general de seguridad. Algunos servicios ofrecen una colección integral de servicios, incluidos los proveedores de servicios de seguridad administrados (MSSP) y los servicios de detección y respuesta administrada (MDR). Otros servicios adoptan un enfoque más limitado pero especializado para complementar las actividades internas con servicios externos especializados, como la protección contra ataques DDoS.

## AUTOMATIZACIÓN DE LA SEGURIDAD, CIFRADO Y SOLUCIONES DE GOBERNANZA DE LA INFORMACIÓN

Las entidades de servicios financieros deben considerar una variedad de otras medidas de seguridad cibernética para mejorar su postura de seguridad. Éstos incluyen:

- **Automatización de seguridad para triaje y respuesta**
  Los equipos de seguridad con frecuencia tienen exceso de trabajo y recursos insuficientes, lo que hace que las alertas de seguridad no se aborden. Las soluciones de automatización de seguridad ofrecen herramientas para clasificar alertas para asignar una prioridad relativa, guías para seguir automáticamente al responder a ciertos tipos de amenazas y agregación de alertas aisladas en casos más integrales y cohesivos. Las soluciones de automatización de la seguridad reducen la cantidad de esfuerzo manual que requieren los profesionales de la ciberseguridad para superar el ruido.

- **Fuerte cifrado de datos**
  Las soluciones criptográficas modernas permiten cifrar los datos cuando se almacenan, cuando están en tránsito y cuando están en uso. Diseñar el uso de un cifrado fuerte en los sistemas financieros y las aplicaciones significa que los actores de amenazas internos o externos no pueden acceder a los datos de texto claro.

- **Soluciones de gobierno de la información**
  Muchas regulaciones exigen que los datos se conserven de forma segura durante un cierto período de tiempo y estén protegidos contra el acceso, la modificación y la eliminación no autorizados.

- **Las soluciones de control de la información permiten que se definan y apliquen políticas de retención de datos en varios repositorios,** con la eliminación automática o previa aprobación de los datos después de que haya transcurrido el período de tiempo requerido. Minimizar la retención de datos más antiguos reduce la huella de datos disponible para la filtración.

***Los empleados necesitan capacitación periódica sobre las señales de advertencia de las ciberamenazas, los trucos comunes de ingeniería social y las mejores prácticas de higiene de la seguridad.***

# Mejores Prácticas en Ciberseguridad

La preparación para manejar las amenazas de seguridad cibernética requiere una combinación saludable de la tecnología adecuada, personas atentas y bien capacitadas, y procesos sólidos. En esta sección, analizamos una variedad de prácticas que combinan y aprovechan los tres factores.

## REVISAR Y ACTUALIZAR LA EVALUACIÓN DE RIESGO CIBERNÉTICO

Si bien las empresas de servicios financieros tienen atributos comunes y deben cumplir con una variedad de regulaciones similares, cada empresa enfrenta un conjunto diferente de amenazas, riesgos e inquietudes de seguridad cibernética específicos. Una orientación amplia y general, como se describe en este informe técnico y otras fuentes, es buena para provocar una reconsideración del riesgo cibernético, pero no para enumerar el contexto de riesgo específico de una empresa determinada. Liderar dicha revisión es responsabilidad del Director de Seguridad de la Información (CISO) o alguien que tenga un rol equivalente.

Toda empresa que actúe o apoye a otras en el sector de los servicios financieros debe revisar y actualizar su evaluación del riesgo cibernético. Especificar los pasos para realizar una evaluación de riesgos cibernéticos está más allá del alcance de este documento técnico, y hay suficientes listas de verificación de evaluación de riesgos por parte de agencias gubernamentales y reguladores de la industria que hacerlo es innecesario. La mejor práctica que mencionamos es garantizar que su evaluación del riesgo cibernético sea actual, integral y relevante para su empresa.

## FORTALECER LAS PRÁCTICAS DE INTERACCIÓN CON LOS CLIENTES

Los clientes de las empresas de servicios financieros también están bajo ataque, con actores de amenazas que aprovechan los canales de comunicación válidos con fines maliciosos. Los ejemplos incluyen correos electrónicos de phishing que pretenden provenir de su banco, llamadas de telemercadeo para "advertir" sobre actividad sospechosa en la cuenta y revisiones de la cuenta para "medir la satisfacción" con los productos bancarios. Cuando a los clientes les resulta cada vez más difícil diferenciar los mensajes de correo electrónico y las llamadas telefónicas válidos de los maliciosos, los problemas aumentan.

***Revisar cómo los clientes se autentican con productos financieros y cómo se puede hacer más seguro el contacto con los clientes.***

Todas las empresas de servicios financieros deben revisar cómo los clientes se autentican con sus productos financieros y cómo las instituciones financieras contactan a los clientes sobre sus cuentas. Los métodos más nuevos y sólidos para garantizar la autenticidad y la integridad de los canales de comunicación son esenciales para evitar la pérdida de fondos, el compromiso de los datos personales y la degradación de la confianza con los proveedores financieros. La creciente disponibilidad de controles biométricos integrados en teléfonos inteligentes y dispositivos móviles está aumentando la conciencia entre los clientes sobre nuevas formas de autenticación.

## FORTALECER LOS MARCOS DE GESTIÓN DE RIESGOS AL TRABAJAR CON EMPRESAS DE TERCEROS

El compromiso de terceros y los incidentes en la cadena de suministro están proyectando un impacto más significativo afecta a las empresas de servicios financieros, como hemos destacado en este libro blanco. Sin embargo, trabajar con empresas de terceros está aquí para quedarse porque ofrecen eficiencias de costos y procesos que son inalcanzables utilizando recursos y sistemas internos. Sin embargo, lo que puede cambiar es alejarse de los arreglos de seguridad de datos flexibles al contratar con empresas de terceros y aplicar procedimientos de auditoría sistemáticos proactivos para identificar áreas de debilidad y vulnerabilidad antes de que lo haga un actor de amenazas. Este enfoque se basa más estridentemente tanto en la certificación por parte de un tercero de buenas prácticas de seguridad como en el cumplimiento auditado.

### REFORZAR LOS PROCESOS INTERNOS DE GESTIÓN DE RIESGOS

Si bien la mayoría de las empresas de servicios financieros tienen sólidos procesos internos de gestión de riesgos, varios incidentes de seguridad cibernética recientes han señalado debilidades críticas que permanecen sin abordar durante demasiado tiempo. Por ejemplo, las revisiones de seguridad interna tanto en First American Financial como en el Banco de la Reserva de Nueva Zelanda identificaron debilidades meses antes de que la vulnerabilidad se divulgara públicamente (First American) o se explotara (el Banco de la Reserva de Nueva Zelanda). Ambas instituciones tuvieron la oportunidad de resolver el problema antes de que se produjera un incumplimiento, pero ninguna asignó la prioridad o los recursos suficientes para hacerlo.

Vale la pena volver a hacer la pregunta: ¿qué temas críticos han destacado nuestros procesos internos que aún no han sido resueltos? Para mayor seguridad, encargue una revisión externa del actual proceso interno de gestión de riesgos para descubrir debilidades sistemáticas en la identificación y priorización de riesgos.

### DISEÑO PARA INTERRUPCIONES REPETIDAS, NO SOLO PRUEBAS

El impulso cada vez mayor para garantizar la resiliencia operativa frente a las amenazas cibernéticas implacables significa que las instituciones financieras deben pensar más allá de la planificación de escenarios en cómo se diseñan los sistemas para aceptar la interrupción sistemática. Los conceptos de generaciones anteriores de conmutación por error, recuperación ante desastres y conexiones de red redundantes se pueden aprovechar para crear sistemas resistentes en plataformas híbridas y de múltiples nubes. Las empresas deberían estar creando de manera sistemática, pero impredecible puntos de fallo e interrupción en sus sistemas para garantizar que la resiliencia sea una realidad. Practicar para la disrupción del mundo real utilizando redes definidas por software y técnicas de conmutación por error del sistema permite una mayor seguridad que la que jamás ofrecerán las pruebas de escenarios anuales.

### LA FORMACIÓN EN CIBERSEGURIDAD ES BUENA, LA RESILIENCIA HUMANA ES MEJOR

Abordar el factor humano es una parte integral del aumento de la resiliencia cibernética en la industria de servicios financieros. Las personas con formación, conciencia, competencia y habilidad inadecuadas para lidiar con incidentes de seguridad cibernética estresantes obstaculizarán los esfuerzos de recuperación. La exposición intencional y proactiva de las personas clave a la interrupción sistemática pero impredecible desarrolla la resiliencia mental, física y emocional para responder adecuadamente cuando se enfrenta al calor de un evento real. Las instituciones de servicios financieros se beneficiarán al adoptar las prácticas de capacitación, simulación y escenarios utilizadas en las fuerzas armadas para desarrollar la resiliencia humana.

***¿Qué problemas críticos de ciberseguridad han sido destacados por los procesos internos que siguen sin resolverse?***

## Conclusión

Los servicios financieros son un sector demasiado importante como para dejarlo desprotegido frente a las ciberamenazas persistentes y emergentes. Las empresas del sector deben advertir la naturaleza cambiante de las amenazas, evaluar la próxima ola de debilidades y vulnerabilidades e implementar soluciones y mejores prácticas para protegerse y defenderse a sí mismas, a sus clientes y al sistema financiero en general.

# Patrocinado por BIO-key Internacional

BIO-key es un proveedor confiable de administración de acceso e identidad (IAM) y soluciones biométricas vinculadas a la identidad (IBB) que ofrecen una forma fácil y segura de autenticar la identidad de empleados, clientes y proveedores mientras administran su acceso a través de dispositivos y aplicaciones.


www.BIO-key.com

info@BIO-key.com

Más de 1000 clientes globales, incluido el gobierno federal y más de 200 instituciones de educación superior, confían en BIO-key PortalGuard IDaaS, una galardonada plataforma de IAM, para reducir las llamadas a la mesa de ayuda relacionadas con contraseñas hasta en un 95 %, eliminar contraseñas y asegurar el acceso remoto. , prevenir ataques de phishing y mejorar la productividad del equipo de IT. PortalGuard proporciona la simplicidad y la flexibilidad necesarias para asegurar la experiencia digital moderna con opciones de inicio de sesión único, restablecimiento de contraseña de autoservicio y autenticación de múltiples factores, y es la única plataforma IAM que ofrece biometría vinculada a la identidad.

Con el respaldo de décadas de experiencia, BIO-key tiene un historial comprobado de entrega exitosa de proyectos de administración de acceso e identidad IAM y sólidas relaciones con los clientes.

Más información www.BIO-key.com.

---

[1] Stephanie Walden and Mitch Strohm, What Is a Neobank?, June 2021, at https://www.forbes.com/advisor/banking/what-is-a-neobank/

[2] US Department of Justice, Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency: Government Seized $3.6 Billion in Stolen Cryptocurrency Directly Linked to 2016 Hack of Virtual Currency Exchange, February 2022, at https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency

[3] Mason Wilder, Are You Ready to Seize Some Cryptocurrency?, March 2022, at https://www.acfeinsights.com/acfe-insights/2022/3/7/are-you-ready-to-seize-some-cryptocurrency

[4] Megan Leonhardt, Online fraud attempts are up 25% in the US - here's why, June 2021, at https://www.cnbc.com/2021/06/03/why-online-fraud-attempts-are-up-25percent-in-the-us.html

[5] ABA Banking Journal, Survey: Cyber Fraud Tops List of Bank Concerns about Global Economy, January 2022, at https://bankingjournal.aba.com/2022/01/survey-cyber-fraud-tops-list-of-bank-concerns-about-global-economy/ and World Economic Forum, What are the biggest business risks of 2022? Experts explain, January 2022, at https://www.weforum.org/agenda/2022/01/biggest-business-risks-2022

[6] ICO, Data security incident trends: Q2 2021-22, October 2021, at https://ico.org.uk/action-weve-taken/data-security-incident-trends/

[7] Office of the Comptroller of the Currency, OCC Assesses $80 Million Civil Money Penalty Against Capital One, August 2020, at https://www.occ.treas.gov/news-issuances/news-releases/2020/nr-occ-2020-101.html

[8] Karen Hoffman, The high cost of mishandling data breaches, security reporting for financial services, January 2022, at https://www.scmagazine.com/analysis/breach/the-high-cost-of-mishandling-data-breaches-security-reporting-for-financial-services

[9] NTT Application Security, AppSec Stats Flash - 2021 Year in Review, February 2022, at https://info.whitehatsec.com/stats-flash-year-in-review.html

[10] Regina Mihindukulasuriya, PNB denies cybersecurity firm's claim that 180 million customers' data was breached, November 2021, at https://theprint.in/tech/pnb-denies-cybersecurity-firms-claim-that-180-million-customers-data-was-breached/770455/

[11] NTT Application Security, AppSec Stats Flash - 2021 Year in Review, February 2022, at https://info.whitehatsec.com/stats-flash-year-in-review.html

[12] Zach Whittaker, FTC settles with data analytics firm after millions of Americans' mortgage files exposed, January 2022, at https://techcrunch.com/2022/01/05/ftc-settle-mortgage-files-exposed/

[13] Commissioner Rebecca Kelly Slaughter, Dissenting Statement of Commissioner Rebecca Kelly Slaughter, December 2021, at https://www.ftc.gov/system/files/documents/public_statements/1599131/1923126ascensionslaughterdissent.pdf

[14] Brian Krebs, NY Charges First American Financial for Massive Data Leak, July 2020, at https://krebsonsecurity.com/2020/07/ny-charges-first-american-financial-for-massive-data-leak/

[15] Jaclyn Jaeger, First American Financial settles SEC charges for cyber-security failures, June 2021, at https://www.complianceweek.com/regulatory-enforcement/first-american-financial-settles-sec-charges-for-cyber-security-failures/30480.article

[16] New York State Department of Financial Services, Department of Financial Services Announces Cybersecurity Charges Against a Leading Title Insurance Provider for Exposing Millions of Documents

With Consumers' Personal Information, July 2020, at https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202007221
[17] Dave, Security incident at Dave, July 2020, at https://www.dave.com/blog/post/
[18] Karl Flinders, Digital bank customer data breached through third party, July 2020, at https://www.computerweekly.com/news/252486767/Digital-bank-customer-data-breached-through-third-party
[19] U.S. Risk, The Risk of Employee Theft and Crime in Financial Institutions, February 2020, at https://www.usrisk.com/about-us-risk/news-and-articles-all/2-11-20-the-risk-of-employee-theft-and-crime-in-financial-institutions/
[20] Frederic Tomesco, Desjardins Says Data Breach Also Affects 1.8-Million Credit-Card Accounts, December 2019, at https://montrealgazette.com/business/local-business/desjardins-says-data-breach-also-affects-1-8-million-credit-cardholders
[21] Office of the Privacy Commissioner of Canada, Investigation into Desjardins' compliance with PIPEDA following a breach of personal information between 2017 and 2019, December 2020, at https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-005/
[22] Kugler Kandestin, Settlement of Class Actions Related to the Personal Information Breach Announced by Desjardins in 2019, December 2021, at https://www.newswire.ca/news-releases/settlement-of-class-actions-related-to-the-personal-information-breach-announced-by-desjardins-in-2019-844138744.html
[23] American Bankers Association, Phishing Scams, February 2022, at https://www.aba.com/advocacy/community-programs/consumer-resources/protect-your-money/phishing
[24] Cisco Umbrella, 2021 Cybersecurity Threat Trends: Phishing, Crypto Top the List, April 2021, at https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list
[25] Vade, Vade Report Reveals Meteoric Rise in Phishing in H1 2021, July 2021, at https://www.vadesecure.com/en/company/news/vade-report-reveals-meteoric-rise-in-phishing-in-h1-2021
[26] AtlasVPN, PayPal and Mastercard most impersonated in financial phishing schemes in 2021, March 2022, at https://atlasvpn.com/blog/paypal-and-mastercard-most-impersonated-in-financial-phishing-schemes-in-2021
[27] Lawrence White and Iain Withers, Welcome to Britain, the bank scam capital of the world, October 2021, at https://www.reuters.com/world/uk/welcome-britain-bank-scam-capital-world-2021-10-14/
[28] Marc Shoffman, UK is branded the 'bank scam capital of the world' with a lack of police resources blamed for rampant fraud, December 2021, at https://inews.co.uk/inews-lifestyle/money/saving-and-banking/uk-bank-scam-capital-world-lack-police-resources-1351256
[29] Philip Heijmans, OCBC to Give S$13.7 Million of Goodwill Payouts After Scam, January 2022, at https://www.bloomberg.com/news/articles/2022-01-30/ocbc-completes-s-13-7-million-of-goodwill-payouts-from-sms-scams
[30] Kevin Shalvey, A hacker stole more than $55 million in crypto after a bZx developer fell for a phishing attack, November 2021, at https://www.businessinsider.com.au/hacker-steals-55-million-in-crypto-after-bzx-phishing-attack-2021-11
[31] Catalin Cimpanu, More than 1,200 phishing toolkits capable of intercepting 2FA detected in the wild, December 2021, at https://therecord.media/more-than-1200-phishing-toolkits-capable-of-intercepting-2fa-detected-in-the-wild/
[32] Digital Shadows, 15 Billion Usernames And Passwords For Internet Services Including Bank And Social Media Accounts On Offer To Cyber Criminals, Finds New Research From Digital Shadows, SOURCE, 20200707, at https://www.digitalshadows.com/press-releases/15-billion-usernames-and-passwords-for-internet-services-including-bank-and-social-media-accounts-on-offer-to-cyber-criminals/
[33] Akamai, Financial Services, Credential Stuff & Web Application Attacks, May 2021, at https://www.akamai.com/newsroom/press-release/-akamai-security-research--financial-services-continues-getting-
[34] Office of the New York State Attorney General Letitia James, Business Guide for Credential Stuffing Attacks, January 2022, at https://ag.ny.gov/sites/default/files/businessguide-credentialstuffingattacks.pdf
[35] Financial Crimes Enforcement Network, Financial Trends Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021, October 2021, at https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf
[36] Trend Micro, Attacks Surge in 1H 2021 as Trend Micro Blocks 41 Billion Cyber Threats, September 2021, at https://newsroom.trendmicro.com/2021-09-14-Attacks-Surge-in-1H-2021-as-Trend-Micro-Blocks-41-Billion-Cyber-Threats
[37] SonicWall, Sonicwall: 'The Year of Ransomware' Continues With Unprecedented Late-Summer Surge, October 2021, at https://www.sonicwall.com/news/sonicwall-the-year-of-ransomware-continues-with-unprecedented-late-summer-surge/
[38] Trellix, Trellix Advanced Threat Research Report: January 2022, January 2022, at https://www.trellix.com/en-us/threat-center/threat-reports/jan-2022.html

[39] Cisco Umbrella, 2021 Cybersecurity Threat Trends: Phishing, Crypto Top the List, April 2021, at https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list
[40] Ron Shevlin, Banks' False Sense of Cybersecurity Will Be Shattered by Cloud Computing, Forbes, August 2020, at https://www.forbes.com/sites/ronshevlin/2020/08/17/cloud-computing-raises-new-cybersecurity-concerns-for-banking/
[41] Prasad Chaudhari, Recognizing the Customer's Responsibily in a Shared Responsibility Model, January 2022, at https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/recognizing-the-customers-responsibility-in-a-shared-responsibility-model
[42] Jessica Haworth, Millions of South Africans caught up in security incident after debt recovery firm suffers 'significant data breach', September 2021, at https://portswigger.net/daily-swig/millions-of-south-africans-caught-up-in-security-incident-after-debt-recovery-firm-suffers-significant-data-breach
[43] David Heun, Banks confront new type of phishing: 'Salami' attacks, September 2021, at https://www.americanbanker.com/news/banks-contend-with-new-type-of-phishing-salami-attacks
[44] FBI, FBI Releases the Internet Crime Complaint Center 2020 Internet Crime Report, Including COVID-19 Scam Statistics, March 2021, at https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics
[45] LexisNexis, Small and Mid-sized Business Lending Fraud Study Results, February 2022, at https://risk.lexisnexis.com/insights-resources/research/smb-lending-fraud-study
[46] Kyle Wiggers, Studies show cybersecurity skills gap is widening as the cost of breaches rises, July 2021, at https://venturebeat.com/2021/07/28/studies-show-cybersecurity-skills-gap-is-widening-as-the-cost-of-breaches-rises/
[47] FBI, CEO's Theft Leads to Closure of Credit Union: Leader Spent $2.1 Million on Personal Purchases, Including a Pig Farm, February 2022, at https://www.fbi.gov/news/stories/ceos-theft-leads-to-closure-of-credit-union-021722
[48] United States Department of Justice, Former Federal Credit Union President Sentenced to More than Four Years in Prison for Embezzlement and Failing to File Taxes, January 2022, at https://www.justice.gov/usao-wdpa/pr/former-federal-credit-union-president-sentenced-more-four-years-prison-embezzlement-and
[49] Bob Van Voris, Morgan Stanley to Pay $60 Million to Settle Data-Breach Suit, January 2022, at https://www.bloomberg.com/news/articles/2022-01-03/morgan-stanley-to-pay-60-million-to-settle-data-breach-claims
[50] Annie Massa, Robinhood Data Breach Nightmare Hinged on Customer Service Slip, November 2021, at https://www.bloomberg.com/news/articles/2021-11-08/robinhood-data-breach-exposes-data-on-millions-of-customers
[51] Hannah Levitt and Benjamin Bain, JPMorgan Bosses Hooked on WhatsApp Fuel $200 Million Penalty, December 2021, at https://www.bloomberg.com/news/articles/2021-12-17/jpmorgan-bosses-addicted-to-whatsapp-fuel-200-million-in-fines
[52] Harry Wilson, HSBC Under Investigation in U.S. Over WhatsApp Use, February 2022, at https://www.bloomberg.com/news/articles/2022-02-22/hsbc-says-it-s-under-investigation-in-u-s-over-whatsapp-use
[53] Steven Arons and Macarena Munoz Montijano, Deutsche Bank Warns Staff Not to Delete WhatsApps Amid Scrutiny, February 2022, at https://www.bloomberg.com/news/articles/2022-02-21/deutsche-bank-warns-staff-not-to-delete-whatsapps-amid-scrutiny
[54] Kugler Kandestin, Settlement of Class Actions Related to the Personal Information Breach Announced by Desjardins in 2019, December 2021, at https://www.newswire.ca/news-releases/settlement-of-class-actions-related-to-the-personal-information-breach-announced-by-desjardins-in-2019-844138744.html
[55] Help Net Security, Financial services need to prioritize API security to protect their customers, November 2021, at https://www.helpnetsecurity.com/2021/11/01/financial-services-api-security/
[56] Australian Cyber Security Centre, ACSC Aware of DDoS Threats Being Made Against Australian Organisations, February 2020, at https://www.cyber.gov.au/threats/acsc-aware-ddos-threats-being-made-against-australian-organisations
[57] John Anthony and Tom Pullar-Strecker, NZX back online as Government assists in helping it address cyberattacks, August 2020, at https://www.stuff.co.nz/business/industries/122593041/nzx-back-online-as-government-assists-in-helping-it-address-cyberattacks
[58] Catalin Cimpanu, DDoS extortionists target NZX, Moneygram, Braintree, and other financial services, August 2020, at https://www.zdnet.com/article/ddos-extortionists-target-nzx-moneygram-braintree-and-other-financial-services/
[59] Sygnia, Elephant Beetle: Uncovering an Organized Financial-Theft Operation, January 2022, at https://blog.sygnia.co/elephant-beetle-an-organized-financial-theft-operation?hsLang=en
[60] Karen Hoffman, The high cost of mishandling data breaches, security reporting for financial services, January 2022, at https://www.scmagazine.com/analysis/breach/the-high-cost-of-mishandling-data-breaches-security-reporting-for-financial-services
[61] National Credit Union Administration, Catastrophic and Incident Reporting, October 2021, at https://www.ncua.gov/regulation-supervision/regulatory-compliance-resources/cybersecurity-resources/catastrophic-and-incident-reporting
[62] National Credit Union Administration, NCUA's Information Security Examination and Cybersecurity Assessment Program, October 2021, at https://www.ncua.gov/regulation-supervision/regulatory-

compliance-resources/cybersecurity-resources/ncuas-information-security-examination-and-cybersecurity-assessment

[63] Federal Register, Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, November 2021, at https://www.fdic.gov/news/board-matters/2021/2021-11-17-notational-fr.pdf and David Heun, Report data breaches within 36 hours? Banks are OK with that, November 2021, at https://www.americanbanker.com/news/report-data-breaches-within-36-hours-banks-are-ok-with-that

[64] Bank of England, Prudential regulation, February 2022, at https://www.bankofengland.co.uk/prudential-regulation

[65] Bank of England, Letter from Nathanael Benjamin and Rebecca Jackson 'International banks active in the UK: 2022 priorities', January 2022, at https://www.bankofengland.co.uk/prudential-regulation/letter/2022/january/artis-2022-priorities

[66] Financial Conduct Authority, About us, February 2022, at https://www.fca.org.uk/about

[67] Norton Rose Fulbright, Cybersecurity: Not just an IT issue, but a regulatory one too, August 2020, at https://www.nortonrosefulbright.com/en/knowledge/publications/b8178be8/cybersecurity-not-just-an-it-issue-but-a-regulatory-one-too

[68] Financial Conduct Authority, Apache Log4j cyber vulnerability, December 2021, at https://www.fca.org.uk/news/statements/apache-log4j-cyber-vulnerability

[69] Gov.uk, Data protection, at https://www.gov.uk/data-protection

[70] ICO, Data security incident trends, October 2021, at https://ico.org.uk/action-weve-taken/data-security-incident-trends/

[71] Australian Prudential Regulation Authority, Information security requirements for all APRA-regulated entities, June 2019, at https://www.apra.gov.au/information-security-requirements-for-all-apra-regulated-entities

[72] Australian Prudential Regulation Authority, APRA sets out policy and supervision priorities for 2020, January 2020, at https://www.apra.gov.au/news-and-publications/apra-sets-out-policy-and-supervision-priorities-for-2020

[73] Londiwe Buthelezi, Standard Bank on delay in telling public about data breach: 'We complied with the law', December 2021, at https://www.news24.com/fin24/Companies/Banks/standard-bank-on-delay-in-telling-public-about-data-breach-we-complied-with-the-law-20211213

[74] Osterman Research, Achieving the Operational Resilience Agenda in Financial Services, November 2021, at https://ostermanresearch.com/2021/11/01/whitepaper-operational-resilience-nutanix/

[75] Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation, Sound Practices to Strengthen Operational Resilience, October 2020, at https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20201030a1.pdf

[76] Kaitlan Collins, Phil Mattingly, Kevin Liptak, and Donald Judd, White House and EU nations announce expulsion of 'selected Russian banks' from SWIFT, February 2022, at https://edition.cnn.com/2022/02/26/politics/biden-ukraine-russia-swift/index.html

[77] BBC, Credit Suisse denies wrongdoing after big banking data leak, February 2022, at https://www.bbc.com/news/business-60456196

[78] Reserve Bank of Australia, Financial Stability Review - October 2021, October 2021, at https://www.rba.gov.au/publications/fsr/2021/oct/pdf/financial-stability-review-2021-10.pdf

[79] Russell Hotten, Ukraine conflict: What is Swift and why is banning Russia so significant?, February 2022, at https://www.bbc.com/news/business-60521822

[80] CISA, Shields Up, February 2022, at https://www.cisa.gov/shields-up

[81] Reuters, ECB tells banks to step up defences against hacks, February 2022, at https://www.reuters.com/business/finance/ecb-says-six-banks-come-up-short-its-capital-demands-2022-02-10/

[82] Carolyn Cohn, Insurers run from ransomware cover as losses mount, November 2021, at https://www.itnews.com.au/news/insurers-run-from-ransomware-cover-as-losses-mount-572963

[83] Aon, 2021 Cyber Security Risk Report, January 2021, at https://www.aon.com/2021-cyber-security-risk-report/

[84] FFIEC, Authentication and Access to Financial Institution Services and Systems, August 2021, at https://www.ffiec.gov/press/pdf/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf

[85] Robert Lemos, Enterprises Remain Riddled With Overprivileged Users -- and Attackers Know It, April 2021, at https://www.darkreading.com/vulnerabilities---threats/insider-threats/enterprises-remain-riddled-with-overprivileged-users--and-attackers-know-it/d/d-id/1340576

[86] David Heun, Weary of passwords, mobile banking users warm to biometrics, August 2021, at https://www.americanbanker.com/news/weary-of-passwords-mobile-banking-users-warm-to-biometrics

[87] Brian Krebs, NY Charges First American Financial for Massive Data Leak, July 2020, at https://krebsonsecurity.com/2020/07/ny-charges-first-american-financial-for-massive-data-leak/

[88] Chris Keall, Reserve Bank hit with compliance notice from Privacy Commissioner over data breach, September 2021, at https://www.nzherald.co.nz/business/reserve-bank-hit-with-compliance-notice-from-privacy-commissioner-over-data-breach/GSMMPOPR2SCWIIYFFPR36OGAEU/