FixScr affiliate of FitchRatings

FIX (afiliada de Fitch Ratings) comenta sobre el riesgo de ciberseguridad en los bancos

En los últimos años, los bancos han enfrentado crecientes riesgos asociados a la seguridad cibernética – o ciberseguridad. En 2020 se observó un incremento en el costo global del ciberdelito que casi duplicó el nivel registrado en 2018. Los ataques, cada vez más sofisticados, continúan aumentando en un contexto marcado por una creciente digitalización que fue acelerada con la pandemia de COVID-19, en el que los puntos de acceso adicionales crean mayores vulnerabilidades. Como establece Fitch Ratings en su reporte Exploring Bank Cybersecurity Risk, si bien el riesgo de ciberseguridad se categoriza como un riesgo no financiero, existe un impacto financiero real que implica un nivel de inversión por parte de la entidad para mitigar los riesgos y costos asociados (multas, incumplimiento de normas regulatorias, daños reputacionales, costos directos de la violación de datos, entre otros).

Los riesgos asociados a la seguridad cibernética son relevantes en la evaluación crediticia. En este sentido, una violación cibernética (*cyber breach*) material representaría un evento que podría tener implicancias en las calificaciones de una determinada entidad. Aunque hasta la fecha Fitch Ratings a nivel global no ha bajado ninguna calificación únicamente en respuesta a un evento de ciberseguridad, su ocurrencia ha resultado en sensibilidades de calificación específicas para los bancos. Además, un ataque que vulnere de ciberseguridad debido a, por ejemplo, controles débiles podría tener un impacto negativo en las calificaciones mientras que es menos probable que una buena "seguridad cibernética" y controles fuertes conlleven un impacto positivo en las mismas. Asimismo, los ESG Relevance Scores de Fitch (observaciones sobre los factores ESG en las calificaciones crediticias) reflejan este riesgo. En general, se captura como un elemento Social – bienestar del cliente, seguridad de los productos, seguridad de datos – aunque también podría comprenderse como parte del Gobierno Corporativo.

El análisis realizado por Fitch, basado en los *scores* de ciberseguridad de SecurityScorecard, revela que los bancos con calificaciones crediticias más altas generalmente exhiben mejores *scores* de ciberseguridad (más altos) que los bancos con calificaciones más bajas, y una menor variabilidad en los mismos. Sin embargo, el hecho de que un banco tenga una alta calificación crediticia no implica que automáticamente alcance un buen *score* de ciberseguridad. Asimismo, los bancos de mercados desarrollados obtuvieron un mayor puntaje con menor dispersión que los bancos de mercados emergentes, por lo que las diferencias regionales entre las puntuaciones de ciberseguridad pueden ser significativas. En el caso de los mercados emergentes, se debe tener presente que el menor nivel de los *scores* junto con la mayor variabilidad observada no es uniforme. Por ejemplo, el Medio Oriente es una región de mercados emergentes cuyos bancos mostraron una alta puntuación, la cual podría explicarse dadas las tensiones geopolíticas en la región durante muchos años que podrían haber incentivado a estos bancos a reforzar su postura ante el riesgo cibernético. La brecha existente entre regiones podría reducirse a medida que las entidades bancarias de mercados emergentes avancen en su proceso de transformación digital – siempre que la transición esté correctamente dirigida, ejecutada y controlada.

Por otra parte, si bien podría pensarse que los bancos de mayor tamaño tienen ventajas en el riesgo de ciberseguridad debido a sus más amplios presupuestos tecnológicos, el análisis de Fitch muestra que el tamaño no es necesariamente un buen predictor de la "seguridad cibernética" de una entidad. Ello podría deberse, en primer lugar, al hecho de que es más probable que un banco de mayor tamaño y estructura más compleja tenga una huella digital más grande y, por lo tanto, una "superficie de ataque" mayor. En segundo lugar, los bancos más grandes probablemente tengan una estructura de IT más compleja en comparación con los bancos más pequeños, que podría aumentar el riesgo de ciberseguridad si no se maneja adecuadamente. Por último, también es probable que los bancos de mayor tamaño operen internacionalmente y, por lo tanto, las diferencias en un país o región podrían afectar su postura de riesgo de ciberseguridad, tal como explica Fitch.

En Argentina, el Banco Central (BCRA) establece los siguientes lineamientos en la materia:

-Marco de Referencia de Ciberseguridad y Estrategia: el propósito de contar con una estrategia y un marco de referencia es la de orientar cómo identificar, gestionar, y reducir efectivamente los ciberriesgos de manera integrada. Las entidades financieras, los terceros y todo el sector financiero deberían establecer estrategias y adoptar un marco de ciberseguridad acorde a su tamaño, complejidad, perfil de riesgo y cultura, teniendo en cuenta las amenazas y vulnerabilidades actuales.

-**Gobierno:** la estrategia es responsabilidad del gobierno de la organización. Es necesario contar con estructuras, roles y funciones claramente definidos para hacer frente a esta problemática, así como contar con las previsiones en cada proyecto. Además, fomentar la comunicación entre las unidades de negocio, las distintas áreas de tecnología de la información, las áreas de riesgo, las áreas de fraude y aquellas áreas cuyas actividades se encuentren relacionadas con el control de acuerdo con sus misiones y funciones.

-Evaluación de los controles y el riesgo: analizar el riesgo presentado por las personas, procesos, la tecnología, los datos subyacentes en relación a la propia entidad y también evaluar los riesgos propios de una entidad a partir de sus funciones, actividades, canales, productos y servicios. Las evaluaciones de control deben considerar, los ciberriesgos que la entidad representa o enfrenta para el ecosistema que conforma, tales como los proveedores de servicios, organismos estatales, las personas usuarias de servicios financieros y otras organizaciones con las que interactúa.

-Monitoreo: el proceso de monitoreo debería dar soporte para mantener los niveles de riesgo definidos como aceptables por la dirección de la organización y permitir mejorar o remediar las debilidades que corresponda. Los protocolos de pruebas, de ciberejercicios y auditorías

son esenciales. Dependiendo de la naturaleza de una entidad u organización, su entorno de control y perfil de riesgo, las funciones de prueba y auditoría de los controles deben ser apropiadamente independientes del personal responsable de la implementación acorde al programa de ciberseguridad.

-Respuesta: como parte de sus evaluaciones de riesgo y control, las entidades deben implementar procesos de respuesta a incidentes y otros controles para facilitar una respuesta oportuna y adecuada. Estos controles deben abordar claramente las responsabilidades en la toma de decisiones, definir procedimientos de escalamiento y establecer procesos para comunicarse con las comunidades de intereses internos y externos. Se promueven los ejercicios y la adopción de protocolos internos y entre las entidades u organizaciones del ecosistema. Los ejercicios también permiten a las entidades y las autoridades identificar las situaciones que podrían afectar la capacidad de quienes participan para mantener un nivel de servicio aceptable, funciones y actividades críticas y de otras actividades que pudieran ser relevante para el sistema financiero.

-Recuperación: una vez garantizada la estabilidad y la integridad operativa, la recuperación rápida y efectiva de las operaciones debe basarse en la priorización de los procesos críticos y de acuerdo con los objetivos establecidos por las autoridades responsables de la entidad u organización. La confianza del sector financiero mejora significativamente cuando las entidades u organizaciones y las autoridades tienen la capacidad de ayudarse mutuamente en la reanudación y recuperación de funciones, procesos y actividades críticas. Establecer y probar planes de contingencia para actividades y procesos esenciales puede contribuir a una recuperación más rápida y efectiva.

-Compartir información: compartir información técnica, como indicadores de amenazas o modalidades sobre cómo se aprovecharon las vulnerabilidades, o modalidades de fraudes, permite a las entidades mantenerse actualizadas en sus defensas y aprender sobre los métodos que están siendo más utilizados. Esta práctica facilita la comprensión colectiva de cómo pueden aprovecharse las vulnerabilidades que afecten a todo el sector, a las funciones económicas críticas y hasta poner en peligro la estabilidad financiera. Dada su importancia, las entidades, las organizaciones y las autoridades responsables trabajarán en identificar y abordar los impedimentos para el intercambio de información.

-Aprendizaje continuo: las amenazas y vulnerabilidades del ecosistema ciber evolucionan rápidamente, al igual que las buenas prácticas y los estándares técnicos. La composición del sector financiero también cambia con el tiempo, a medida que surgen nuevos productos y servicios, y se confía cada vez más en proveedores de servicios de terceros. Las estrategias y los marcos de referencia en materia ciberseguridad necesitan revisión periódica y actualización para adaptarse a los cambios en el entorno de control y amenazas, mejorar la concientización de la persona usuaria y desplegar recursos de manera efectiva.

Para la implementación se deben considerar las características particulares, perfiles de riesgo y análisis de impacto en el negocio (BIA) según corresponda. Se espera que estos lineamientos sean adoptados por todos los regulados por el Banco Central en la construcción de un ecosistema financiero comprometido con la ciberseguridad.

En tanto, las distintas entidades bancarias realizan continuamente diversas campañas de concientización, destacando la importancia de no compartir claves ni datos personales y entrar en contacto únicamente a través de los canales oficiales de atención de los bancos.

Finalmente, se destaca que las Entidades Financieras en Argentina cuentan con distintos desafíos en la materia, incluyendo contar con políticas de seguridad informática basadas en estándares elevados, equipos especializados en la materia, mayor inversión que encarece costos dentro de la entidad vs costos en la pérdida de datos y educación a los usuarios. Estas acciones no garantizan que no sufran ciberataques, sin embargo pueden reducir la frecuencia y el impacto de los mismos en función a la capacidad de respuesta ante eventos de ésta naturaleza.

INFORMES RELACIONADOS

ESG Credit Quarterly: 1Q21

Exploring Bank Cybersecurity Risk

Exploring Bank Cybersecurity Risk (Video)

Bonos Verdes: Actualidad, Evolución y Perspectivas

Fitch Ratings Partners with SecurityScorecard to Assess Cyber Risk

Calificación y Finanzas Sostenibles

CONTACTOS

Responsable del Sector
Gustavo Ávila
Director
gustavo.avila@fixscr.com
+54 11 5235-8142
Sarmiento 663 – 7° piso – C1041AAM
Capital Federal – Argentina

Relación con los Medios: Diego Elespe, Head Comercial y de Desarrollo de Negocios
diego.elespe@fixscr.com
+5411 5235-8100/10

TODAS LAS CALIFICACIONES CREDITICIAS DE FIX SCR S.A. AGENTE DE CALIFICACIÒN DE RIESGO (Afiliada de Fitch Ratings), EN ADELANTE TAMBIEN DENOMINADA "FIX", ESTÁN SUJETAS A CIERTAS LIMITACIONES Y ESTIPULACIONES. POR FAVOR LEA ESTAS LIMITACIONES Y ESTIPULACIONES SIGUIENDO ESTE ENLACE: HTTP://WWW.FIXSCR.COM. ADEMÁS, LAS DEFINICIONES DE CALIFICACIÓN Y LAS CONDICIONES DE USO DE TALES CALIFICACIONES ESTÁN DISPONIBLES EN NUESTRO SITIO WEB WWW.FIXSCR.COM. LAS CALIFICACIONES PÚBLICAS, CRITERIOS Y METODOLOGÍAS ESTÁN DISPONIBLES EN ESTE SITIO EN TODO MOMENTO. EL CÓDIGO DE CONDUCTA DE FIX SCR S.A., Y LAS POLÍTICAS SOBRE CONFIDENCIALIDAD, CONFLICTOS DE INTERÉS, BARRERAS PARA LA INFORMACIÓN PARA CON SUS AFILIADAS, CUMPLIMIENTO, Y DEMÁS POLÍTICAS Y PROCEDIMIENTOS ESTÁN TAMBIÉN DISPONIBLES EN LA SECCIÓN DE CÓDIGO DE CONDUCTA DE ESTE SITIO. FIX SCR S.A. PUEDE HABER PROPORCIONADO OTRO SERVICIO ADMISIBLE A LA ENTIDAD CALIFICADA O A TERCEROS RELACIONADOS. LOS DETALLES DE DICHO SERVICIO DE CALIFICACIONES SOBRE LAS CUALES EL ANALISTA LIDER ESTÁ BASADO EN UNA ENTIDAD REGISTRADA ANTE LA UNIÓN EUROPEA, SE PUEDEN ENCONTRAR EN EL RESUMEN DE LA ENTIDAD EN EL SITIO WEB DE FIX SCR S.A.

La reproducción o distribución total o parcial de este informe por terceros está prohibida, salvo con permiso. Todos los derechos reservados. En la asignación y el mantenimiento de sus calificaciones, FIX SCR S.A. se basa en información fáctica que recibe de los emisores y sus agentes y de otras fuentes que FIX SCR S.A. considera creíbles. FIX SCR S.A. lleva a cabo una investigación razonable de la información fáctica sobre la que se basa de acuerdo con sus metodologías de calificación y obtiene verificación razonable de dicha información de fuentes independientes, en la medida de que dichas fuentes se encuentren disponibles para una emisión dada o en una determinada jurisdicción. La forma en que FIX SCR S.A. lleve a cabo la investigación factual y el alcance de la verificación por parte de terceros que se obtenga, variará dependiendo de la naturaleza de la emisión calificada y el emisor, los requisitos y prácticas en la jurisdicción en que se ofrece y coloca la emisión y/o donde el emisor se encuentra, la disponibilidad y la naturaleza de la información pública relevante, el acceso a representantes de la administración del emisor y sus asesores, la disponibilidad de verificaciones preexistentes de terceros tales como los informes de auditoría, cartas de procedimientos acordadas, evaluaciones, informes actuariales, informes técnicos, dictámenes legales y otros informes proporcionados por terceros, la disponibilidad de fuentes de verificación independientes y competentes de terceros con respecto a la emisión en particular o en la jurisdicción del emisor y una variedad de otros factores. Los usuarios de calificaciones de FIX SCR S.A. deben entender que ni una investigación mayor de hechos, ni la verificación por terceros, puede asegurar que toda la información en la que FIX SCR S.A.se basa en relación con una calificación será exacta y completa. El emisor y sus asesores son responsables de la exactitud de la información que proporcionan a FIX SCR S.A. y al mercado en los documentos de oferta y otros informes. Al emitir sus calificaciones, FIX SCR S.A. debe confiar en la labor de los expertos, incluyendo los auditores independientes, con respecto a los estados financieros y abogados con respecto a los aspectos legales y fiscales. Además, las calificaciones son intrínsecamente una visión hacia el futuro e incorporan las hipótesis y predicciones sobre acontecimientos que pueden suceder y que por su naturaleza no se pueden comprobar como hechos. Como resultado, a pesar de la comprobación de los hechos actuales, las calificaciones pueden verse afectadas por eventos futuros o condiciones que no se previeron en el momento en que se emitió o afirmó una calificación.

La información contenida en este informe, recibida del emisor", se proporciona sin ninguna representación o garantía de ningún tipo. Una calificación de FIX SCR S.A. es una opinión en cuanto a la calidad crediticia de una emisión. Esta opinión se basa en criterios establecidos y metodologías que FIX SCR S.A. evalúa y actualiza en forma continua. Por lo tanto, las calificaciones son un producto de trabajo colectivo de FIX SCR S.A. y ningún individuo, o grupo de individuos, es únicamente responsable por la calificación. La calificación no incorpora el riesgo de pérdida debido a los riesgos que no sean relacionados a riesgo de crédito, a menos que dichos riesgos sean mencionados específicamente, como son riesgos de precio o de mercado. FIX SCR S.A. no está comprometido en la oferta o venta de ningún título. Todos los informes de FIX SCR S.A. son de autoría compartida. Los individuos identificados en un informe de FIX SCR S.A. estuvieron involucrados en, pero no son individualmente responsables por, las opiniones vertidas en él. Los individuos son nombrados solo con el propósito de ser contactados. Un informe con una calificación de FIX SCR S.A. no es un prospecto de emisión ni un substituto de la información elaborada, verificada y presentada a los inversores por el emisor y sus agentes en relación con la venta de los títulos. Las calificaciones pueden ser modificadas, suspendidas, o retiradas en cualquier momento por cualquier razón a sola discreción de FIX SCR S.A. FIX SCR S.A. no proporciona asesoramiento de inversión de ningún tipo.

Las calificaciones representan una opinión y no son una recomendación para comprar, vender o mantener cualquier título. Las calificaciones no hacen ningún comentario sobre la adecuación del precio de mercado, la conveniencia de cualquier título para un inversor particular o la naturaleza impositiva o fiscal de los pagos efectuados en relación a los títulos. FIX SCR S.A. recibe honorarios por parte de los emisores, aseguradores, garantes, otros agentes y originadores de títulos, por las calificaciones. Dichos honorarios generalmente varían desde USD 1.000 a USD 200.000 (u otras monedas aplicables) por emisión. En algunos casos, FIX SCR S.A. calificará todas o algunas de las emisiones de un emisor en particular, o emisiones aseguradas o garantizadas por un asegurador o garante en particular, por una cuota anual. Se espera que dichos honorarios varíen entre USD 1.000 y USD 200.000 (u otras monedas aplicables). La asignación, publicación o diseminación de una calificación de FIX SCR S.A. no constituye el consentimiento de FIX SCR S.A. a usar su nombre como un experto en conexión con cualquier declaración de registro presentada bajo las leyes de cualquier jurisdicción, incluyendo, pero no excluyente, las leyes del mercado de títulos y valores de Estados Unidos de América y la "Financial Services and Markets Act of 2000" del Reino Unido. Debido a la relativa eficiencia de la publicación y distribución electrónica, los informes de FIX SCR S.A. pueden estar disponibles hasta tres días antes para los suscriptores electrónicos que para otros suscriptores de imprenta.