SUPERINTENDENCIA DE BANCOS
REPÚBLICA DOMINICANA

# CIRCULAR SB: CSB-REG-202400006

**A las** : **Entidades de intermediación financiera (EIF).**

**Asunto** : **Establecer las características y requisitos mínimos de seguridad que deberán cumplir las EIF para acceder al Servicio API de la Central de Riesgos de la Superintendencia de Bancos.**

**Visto** : El literal (e) del artículo 21 de la Ley Núm. 183-02 Monetaria y Financiera del 21 de noviembre de 2002, en lo adelante Ley Monetaria y Financiera, que faculta al Superintendente de Bancos (SB) a emitir Instructivos, Circulares y Reglamentos Internos.

**Vistos** : Los literales (a), (b) y (c) del artículo 55 de la Ley Monetaria y Financiera que establece que las EIF deben contar con políticas administrativas, adecuados sistemas de control de riesgos y de control interno.

**Visto** : El literal (a) del artículo 56 de la Ley Monetaria y Financiera que instruye a la Superintendencia de Bancos establecer un sistema de información de riesgos en el que obligatoriamente participen todas las entidades sujetas a regulación.

**Visto** : El Reglamento de Normas Prudenciales de Adecuación Patrimonial aprobado por la Junta Monetaria mediante la Tercera Resolución del 30 de marzo de 2004 y sus modificaciones.

**Visto** : El Reglamento para el Manejo de los Riesgos de Mercado aprobado por la Junta Monetaria mediante la Tercera Resolución del 29 de marzo de 2005.

**Visto** : El Reglamento Riesgo de Liquidez aprobado por la Junta Monetaria mediante la Cuarta Resolución del 29 de marzo de 2005.

**Visto** : El Reglamento sobre Concentración de Riesgos aprobado por la Junta Monetaria mediante la Quinta Resolución del 19 de diciembre de 2006 y modificaciones.

**Visto** : El Reglamento sobre Riesgo Operacional aprobado por la Junta Monetaria mediante la Quinta Resolución del 2 de abril de 2009 y modificaciones.

**Visto** : El Reglamento sobre Cuentas Inactivas y/o Abandonadas en las Entidades de Intermediación Financiera aprobado por la Junta Monetaria mediante la Segunda Resolución del 12 de julio de 2012.

**Visto** : El Reglamento de Tarjetas de Crédito aprobado por la Junta Monetaria mediante la Primera Resolución del 7 de febrero de 2013.

**Visto** : El Reglamento de Protección al Usuario de los Productos y Servicios Financieros aprobado por la Junta Monetaria mediante la Primera Resolución del 5 de febrero de 2015 y su modificación.

**Visto** : El Reglamento sobre Gobierno Corporativo aprobado por la Junta Monetaria mediante la Primera Resolución del 2 de julio de 2015.

**Visto** : El Reglamento sobre Lineamientos para la Gestión Integral de Riesgos aprobado por la Junta Monetaria mediante la Tercera Resolución del 16 de marzo de 2017.

**Visto** : El Reglamento de Evaluación de Activos (REA) aprobado por la Junta Monetaria mediante la Segunda Resolución del 28 de septiembre de 2017 y modificaciones.

**Visto** : El Reglamento sobre el Programa Monetario e Instrumentos de Política Monetaria aprobado por la Junta Monetaria mediante la Segunda Resolución del 23 de noviembre de 2017.

**Visto** : El Reglamento Unificado de Valores e Instrumentos Hipotecarios aprobado por la Junta Monetaria mediante la Tercera Resolución del 23 de noviembre de 2017.

**Visto** : El Reglamento de Microcréditos aprobado por la Junta Monetaria mediante la Primera Resolución del 17 de mayo de 2018.

**Visto** : El Reglamento de Sistemas de Pago aprobado por la Junta Monetaria mediante la Segunda Resolución del 29 de enero de 2021.

**Vista** : La Circular SB: Núm. 013/21 del primero de septiembre de 2021, que aprueba y pone en vigencia la versión actualizada del Manual de Contabilidad para Entidades Supervisadas.

**Vista** : La Circular SB: Núm. 018/22 del 15 de diciembre de 2022, que aprueba y pone en vigencia la versión actualizada del "Manual de requerimientos de información de la Administración Monetaria y Financiera".

**Considerando** : La necesidad de incrementar la calidad de las informaciones recibidas de las entidades de intermediación financiera, con el interés de disponer de información de alto valor agregado para este ente supervisor poder evaluar los riesgos y exposiciones del sistema financiero nacional.

**Considerando** : Que, como parte de los ejes estratégicos de la SB, la digitalización, innovación y nuevas tecnologías, así como la eficiencia y fortalecimiento institucional, tienen como objetivo mejorar los procesos internos a través del uso de nuevas tecnologías y

aumentar la efectividad y calidad de la gestión con un enfoque orientado a resultados y mejora continua.

**Considerando :** Que este ente supervisor tiene como objetivo mantener la adecuada gestión de los objetivos de seguridad (confidencialidad, disponibilidad e integridad) de las informaciones de los clientes y entidades del sistema financiero nacional.

**Considerando** : Que el 18 de enero de 2024, la SB informó a las EIF a través del correo de "Consulta Riesgos", la definición de los nuevos controles de acceso al API de descarga en lotes de la Consulta Crediticia, incluyendo los requisitos a cumplir y el plazo de adecuación de las entidades ante dichos requerimientos, definiendo como fecha límite el 15 de marzo de 2024, e indicando que el no cumplimiento de estos dentro del plazo definido revocaría los accesos, por lo que es necesario establecer los requerimientos mínimos que deberán cumplir los servidores o computadores personales que utilizarán las EIF para obtener y mantener la autorización de descargar y almacenar las informaciones provistas por esta SB a través del Servicio API de la Central de Riesgos.

**POR TANTO:**

El Intendente de Bancos, quien actúa de conformidad con lo que establece el literal (a) del artículo 12 del Reglamento Interno, aprobado mediante la Primera Resolución de la Junta Monetaria del 23 de marzo de 2004 y conforme las atribuciones que le confiere al Superintendente de Bancos el literal (e) del artículo 21 de la Ley Núm. 183-02 Monetaria y Financiera del 21 de noviembre de 2002, dispone lo siguiente:

1. Las entidades deberán asegurarse de que los servidores o computadoras personales cumplan con lo siguiente:

   1.1. Disponer de un equipo físico, servidor o computador personal, exclusivo para la descarga y almacenamiento de las informaciones disponibles en el Servicio API de la Central de Riesgos, provisto por esta SB.

   1.2. Asegurar que el equipo que dispongan para la descarga y almacenamiento de las informaciones en el Servicio API de la Central de Riesgos cumpla, mínimamente, con los aspectos siguientes:

      1.2.1. SISTEMA OPERATIVO

      a) Versión soportada por su fabricante para la corrección de vulnerabilidades.
      b) Mecanismos de autenticación local y de la red que, sin limitarse, incluya contraseñas robustas, combinando longitud y complejidad en los caracteres que la componen.
      c) Bloqueo de todos los puertos que permitan conexión de dispositivos de almacenamiento externo.
      d) Registros (*Logs*) activos y con la política de no eliminar o sobrescribir registros de logs.
      e) El usuario con privilegio de administrador local deberá estar asignado a un representante identificable, perteneciente al área de Seguridad de la Información de la entidad.
      f) Dirección IP (por sus siglas en inglés, Internet Protocol) fija que deberá ser comunicada a la SB.
      g) Bloqueo automático por inactividad de equipo y desbloqueo mediante autenticación.

1.2.2. SISTEMA DE GESTION DE BASE DE DATOS (SGBD)

a) Versión soportada por su fabricante para la corrección de vulnerabilidades.
b) Registros (*Logs*) activos que registre todas las consultas, actualizaciones, inserciones y eliminaciones de datos en las bases de datos existentes en la instancia.
c) Perfiles de usuario debidamente definidos en base a las necesidades que, para el desarrollo de sus funciones formales, tengan los colaboradores que demanden acceso a este recurso.
d) Mecanismos de autenticación sin limitarse a que las contraseñas sean robustas, combinando longitud y complejidad en los caracteres que la componen.

1.2.3. SERVICIOS DE RED

a) Acceso a Internet solo para aquellos sitios que sean utilizados para el adecuado uso o funcionamiento del equipo, sus componentes y el Servicio API.
b) No incluirá unidades o carpetas compartidas que puedan ser accedidas remotamente desde la propia red de la entidad o cualquier otra red.
c) Sin acceso inalámbrica.

1.2.4. OTROS

a) Ubicación física que asegure la integridad del equipo y sus componentes.
b) Software de protección contra código malicioso instalado en el equipo, e incluyendo las características siguientes:

   i. Actualización automática, centralizada y periódica desde la fuente del fabricante.
   ii. No podrá ser desactivado por usuarios sin privilegios administrativos de red o del software.

1.3. Disponer del ambiente de control necesario para:

1.3.1. Implementar controles normativos, mediante políticas y procedimientos, que consideren los aspectos de seguridad de la información del equipo, así como el uso de controles técnicos (p.ej.: herramientas de software) para la prevención de pérdidas de los datos e informaciones relacionadas a la Central de Riesgos. Las EIF dispondrán de un plazo de dieciocho (18) meses para el cumplimiento de esta disposición.

1.3.2. Gestionar que las informaciones provistas a través del Servicio API sean accedidas solo por personal de la entidad cuyas funciones se relacionen con el negocio que esta hará uso de esas informaciones y en pleno cumplimiento con las disposiciones normativas dispuestas por la Administración Monetaria y Financiera.

1.3.3. Gestionar que no se realicen desde la entidad, acciones que atenten contra la disponibilidad e integridad del Servicio API y las informaciones que se utilizan desde este.

**Párrafo.** Aquellas entidades que no cuenten con lo previamente indicado no podrán obtener o mantener la autorización para la descarga y almacenamiento de las informaciones del Servicio API de la Central de Riesgos de esta SB.

2. Las entidades que a la fecha no tienen acceso al Servicio API de la Central de Riesgos, una vez que hayan cumplido los requerimientos descritos en el numeral 1 que antecede, deberán utilizar la Mesa de Servicio del Portal de Administración Monetaria y Financiera (PAMF) para solicitar la autorización de acceso. Para los fines de la solicitud, las entidades deberán suministrar:

   2.1. Detalle de la marca, modelo y número serial del equipo definido por la entidad para descargar y almacenar las informaciones en el citado servicio.

   2.2. Dirección IP que se ha fijado en el equipo.

   2.3. Descripción de la ubicación física del equipo, incluyendo dirección de la localidad y departamento.

   2.4. Los datos personales (nombre, apellidos, número de cédula de identidad y electoral, cargo dentro de la entidad, número telefónico y extensión, número de flota) del colaborador a quien le serán asignadas las funciones de Administrador de Grupo. Este tipo de usuario será el responsable, a través del canal SB Interactivo, de crear el Usuario de Servicio responsable de descargar las informaciones en el Servicio API de la Central de Riesgos.

   **Párrafo.** Cuando la SB otorgue la autorización, contactará la entidad vía correo electrónico de Consulta Riesgos para coordinar las visitas “in situ” de verificación de los requerimientos.

3. Las entidades que a la fecha de la presente circular tengan autorización para el acceso al Servicio API de la Central de Riesgos, y lo comunicaron vía correo electrónico de Consulta Riesgos, serán contactadas para coordinar las visitas “in situ” de verificación de los requerimientos definidos en la presenta circular.

4. Las disposiciones que se aprueban mediante la presente Circular, entrarán en vigor a partir del 1 de mayo de 2024; y notificado a las entidades a través del correo electrónico consultasriesgos@sb.gob.do.

5. Las EIF deberán notificar a través de la Mesa de Servicio del Portal de Administración Monetaria y Financiera (PAMF), cualquier incidente que represente un riesgo o evento que haya afectado cualquiera de los objetivos de seguridad del equipo utilizado para la descarga y almacenamiento de las informaciones, así como de las informaciones que este contenga.

   **Párrafo.** Esta notificación debe realizarse en un plazo no mayor a 24 horas, luego de haber identificado el riesgo o evento. Además, deberá incluir una descripción, por lo menos preliminar del caso, incluyendo sus posibles causas.

6. Las entidades deberán utilizar la Mesa de Servicio del Portal de la Administración Monetaria y Financiera para solicitar el desbloqueo de los usuarios que tengan definidos para el Servicio API Central de Riesgos.

7. Las entidades que infrinjan las disposiciones contenidas en la presente Circular en cualquiera de sus aspectos serán pasibles de la aplicación de sanciones por la Superintendencia de Bancos, con base en la Ley Núm. 183-02 Monetaria y Financiera del 21 de noviembre del 2002 y el Reglamento de Sanciones aprobado por la Junta Monetaria en la Quinta Resolución del 18 de diciembre del 2003 y su modificación.

8. La presente Circular deberá ser comunicada a las partes interesadas y publicada en la página web de esta Institución <www.sb.gob.do> de conformidad con el literal (h) del artículo 4 de la Ley Núm. 183-02 Monetaria y Financiera y el mecanismo de notificación de los Actos Administrativos de la Superintendencia de Bancos, dispuesto en la Circular SB: No. 015/10 del 21 de septiembre de 2010 emitida por este ente supervisor.

Dada en la ciudad de Santo Domingo de Guzmán, Distrito Nacional, Capital de la República Dominicana, a los veintitrés (23) días del mes de abril del año dos mil veinticuatro (2024).

**Julio Enrique Caminero Sánchez**
INTENDENTE

JECS/YRM/EFCT/OLC/CJRM
**DEPARTAMENTO DE REGULACIÓN**

Documento firmado digitalmente por:
Omar Antonio Lantigua Ceballos (VB) (23/04/2024 AST), Carlos Rijo (VB) (23/04/2024 AST)
Cinthia Vargas De Heredia (En nombre de Elbin Francisco Cuevas) (VB) (23/04/2024 AST)
Yulianna Marie Ramon Martinez (VB) (23/04/2024 AST), Julio Caminero (23/04/2024 AST)
https://www.viafirma.com.do/inbox/app/sib/v/e9a1be58-a805-4eba-ade7-adc04b88f17f