10 de marzo de 2022

SGF-0479-2022

SGF-PUBLICO

**Resolución de la Superintendente**

**Dirigida a:**

* **Personas jurídicas, que realicen la actividad de proveedores de servicios de pago, según lo dispuesto en el artículo 6 del “Reglamento del Sistema de Pagos”, que están inscritas o pretendan inscribirse por el Artículo 15 o 15 bis de la Ley 7786.**

**Asunto: Disposiciones para demostrar el cumplimiento de lo requerido en el artículo 6 del Reglamento del Sistema de Pagos del Banco Central de Costa Rica, para obtener la autorización que otorga el BCCR para poder operar como proveedores de servicios de pago en el Sistema Nacional de Pagos Electrónicos (SINPE)**

**La Superintendencia General de Entidades Financieras (SUGEF),**

**Considerando que:**

1. Mediante la Ley 9449 del 10 de mayo del 2017, la Asamblea Legislativa decretó la *“Reforma de los artículos 15, 15 bis, 16, 81 y adición de los artículos 15 ter y 16 bis a la Ley 7786, Ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, actividades conexas, legitimación de capitales y financiamiento al terrorismo, de 30 de abril de 1998”*.
2. Los artículos 15 y 15 bis de la Ley 7786 disponen que las personas que desempeñen las actividades allí indicadas, en adelante conocidas como APNFD (Actividades y Profesiones no Financieras Designadas),“…*deberán someterse a la supervisión de esta Superintendencia, respecto de la materia de prevención de la legitimación de capitales, el financiamiento al terrorismo y el financiamiento de la proliferación de armas de destrucción masiva, bajo un enfoque basado en riesgos, incluyendo el régimen sancionatorio establecido en el artículo 81 de la presente ley, y deberán cumplir con las siguientes obligaciones, además de las que establezca Conassif mediante normativa prudencial de acuerdo con la realidad de cada sector...”.*
3. En el Acuerdo SUGEF 11-18 “*Reglamento para la inscripción y desinscripción ante la SUGEF de los sujetos obligados que realizan alguna o algunas de las actividades descritas en los en los artículos 15 y 15 bis de la Ley sobre Estupefacientes, Sustancias Psicotrópicas, Drogas de Uso no Autorizado, Actividades Conexas, Legitimación de Capitales y Financiamiento al Terrorismo, Ley 7786”* publicado en el diario oficial La Gaceta N°213 del 16 de noviembre de 2018, se establece en el artículo 25 que “*Los sujetos inscritos por los artículos 15 y 15 bis de la Ley 7786 deben cumplir en todos sus extremos con lo dispuesto en esta Ley y sus Reglamentos, así como con la normativa aprobada por el CONASSIF en relación con la citada Ley.”*
4. El 19 de noviembre de 2019 en el Alcance 258 de la Gaceta 220 se publicó el Reglamento para la prevención del riesgo de Legitimación de Capitales, Financiamiento al Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva, aplicable a los sujetos obligados por los artículos 15 y 15 bis de la Ley 7786, Acuerdo SUGEF 13-19.
5. El 13 de agosto de 2021 en el Alcance 159 a La Gaceta 155 se publicó la última modificación del Reglamento del Sistema de Pagos del Banco Central de Costa Rica.
6. El artículo 6 de dicho Reglamento de Pagos indica:

*Artículo 6. Proveedores de servicios de pago. Se refiere a las empresas jurídicas nacionales que realizan actividades de transferencias de fondos, remesas, pagos y cobros a comercios o cualquier otra actividad que requiera la movilización de fondos propios o de terceros, siempre que cumplan con las regulaciones nacionales vigentes en materia de prevención de legitimación de capitales y financiamiento al terrorismo, protección de datos y cualquier otra legislación aplicable a los servicios ofrecidos.*

*Estas empresas deberán estar inscritos ante la SUGEF para efecto de cumplir con lo establecido en el artículo 15 y artículo 15 bis de la Ley 7786, además, esta Superintendencia deberá comunicar al BCCR que dichos sujetos obligados cuentan con adecuados marcos de gobierno corporativo para gestionar los riesgos asociados a la prevención de la legitimación de capitales y que cuentan con plataformas robustas para salvaguardar la información de los usuarios de los servicios financieros que utilizan los servicios de pago de esos sujetos obligados. Lo anterior es una condición necesaria para que el BCCR otorgue la autorización de proveedor de servicios de pago.*

*Los proveedores de servicios de pago deberán suministrar a la División Sistemas de Pago información relacionada con el tipo de servicio, canales e instrumentos de pago que ofrecerá a sus clientes, nicho de mercado al que se dirige, esquema de operación, controles y medidas de seguridad a implementar, esquemas de continuidad del negocio, estadísticas transaccionales y otros datos de interés desde la perspectiva del desarrollo del sistema de pago, según lo especificado en la Serie de Normas y Procedimientos del SINPE. En caso de que producto de su giro de negocio, administren cuentas de fondos, deberán asignarles a estas, un número de cuenta IBAN y registrarlas en el Padrón Único de Cuentas (PUC), cumpliendo con los requerimientos definidos en la Serie de Normas y Procedimientos del SINPE.*

*Asimismo, deberán indicar al BCCR los mecanismos y procedimientos para la publicidad y ofrecimiento de sus productos a los usuarios de sus servicios, lo anterior para garantizar transparencia y claridad.*

1. El Reglamento de Inscripción Acuerdo SUGEF 11-18 en el artículo 14, define las causas de suspensión de los sujetos obligados, entre ellas las siguientes:

*b) Cuando el sujeto obligado no entregue a la SUGEF cualquier información adicional o aclaratoria que le sea requerida, relacionada con la actividad o actividades por las que fue inscrito, en la forma y en los plazos en que la SUGEF, este Reglamento, o el ordenamiento jurídico lo determine.*

*f) Cuando por verificación de la SUGEF se constate que la información y/o documentación suministrada no es coincidente con la información declarada y suministrada.*

1. *El estado "suspendido" es una medida precautoria que se mantendrá publicado en el sitio web de la SUGEF, hasta tanto el sujeto obligado subsane el incumplimiento, o se notifique la revocación de la inscripción. Este estado se podrá mantener, si la causal de la suspensión genera el inicio de un procedimiento administrativo tendiente a la revocación de la inscripción.*

**Dispone:**

1. Comunicar a todas las personas jurídicas, que realicen la actividad de proveedores de servicios de pago, según lo dispuesto en el artículo 6 del Reglamento del Sistema de Pagos, que estén interesados en obtener la autorización que otorga el Banco Central de Costa Rica para poder operar como proveedores de servicios de pago en el Sistema Nacional de Pagos Electrónicos (SINPE), que, para cumplir con el requisito indicado en el artículo señalado, deberán remitir a esta Superintendencia los siguientes documentos:
2. **Informe emitido por auditor externo, para obtener una opinión con certeza razonable del cumplimiento y efectividad de la labor del gobierno corporativo, en la atención de los riesgos de legitimación de capitales, el financiamiento al terrorismo y el financiamiento de la proliferación de armas de destrucción masiva (LC/FT/FPADM);** este informe debe realizarse bajo la norma de Trabajos de atestiguamiento NITA 3000. Para cumplir con el requisito, el informe del auditor externo debe concluir que el sujeto obligado dispone de un **Alto** grado de cumplimiento normativo y de efectividad en la implementación de los controles y de la gestión de prevención de estos riesgos para cada uno de los criterios que más adelante se detallan.

El auditor externo debe estar activo en el Colegio de Contadores Públicos de Costa Rica y contar con la Certificación de Revisión de Control de Calidad que emite ese Colegio; debe además estar inscrito en el Registro de Auditores Externos de la Sugeval. Tales condiciones deben ser demostradas ante la SUGEF.

Se entiende por gobierno corporativo la forma mediante la cual las entidades se organizan para llevar a cabo la administración y el control de su gestión. Está constituido por las estructuras de dirección de la entidad, las de gestión tal como la alta gerencia y las de control incluyendo la Auditoría Interna, así como por el conjunto de prácticas adoptadas para llevar adelante la dirección, monitoreo y control diario del negocio conocido como Gestión de operaciones, en el marco de las leyes y regulaciones aplicables, lo que representa el cumplimiento legal y regulatorio.

Las prácticas citadas deberán permitir establecer los objetivos institucionales, determinar los medios para alcanzarlos y supervisar su observancia, donde se demuestre un alto cumplimiento y efectividad en la implementación de los controles y de la gestión de prevención del riesgo de legitimación de capitales, el financiamiento al terrorismo y el financiamiento de la proliferación de armas de destrucción masiva, según lo dispuesto en el Reglamento para la inscripción y desinscripción, Acuerdo Sugef 11-18 y en el Reglamento para la prevención del riesgo de LC/FT/FPADM, Acuerdo Sugef 13-19.

El informe emitido por el Auditor Externo debe contemplar la evaluación del cumplimiento y efectividad de los siguientes criterios:

1. **Del Reglamento de Inscripción, Acuerdo SUGEF 11-18:**

Secciones I y II del Capítulo de “Disposiciones Varias”, en lo que aplica a los sujetos obligados por los artículos 15 y 15 bis de la Ley 7786. Referirse en particular al uso de cuentas de uso exclusivo y al cumplimiento de las disposiciones sobre publicidad.

1. **Del Reglamento de Prevención del Riesgo de LC/FT/FPADM, Acuerdo SUGEF 13-19:**

Capítulos del II al X de este cuerpo normativo, incluyendo lo que se dispone en los Lineamientos correspondientes. Referirse a cada capítulo como un criterio individual.

El informe del Auditor Externo debe referirse al grado de: a) cumplimiento normativo y b) efectividad de los controles, sobre cada uno de los criterios anteriores, cuyo resultado debe ser calificado según la siguiente escala:

**Alto**: se minimiza la posibilidad de que se presenten eventos que expondrían a la entidad a los riesgos de LC/FT/FPADM.

**Medio Alto**: Se podrían presentar situaciones que expondrían a la entidad a ser utilizada para LC/FT/FPADM.

**Medio Bajo:** Se presentan debilidades importantes que exponen a la entidad a ser utilizada para LC/FT/FPADM.

**Bajo:** No se cuenta con controles mínimos que protejan a la entidad de ser utilizada para LC/FT/FPADM.

En cada caso, la calificación asignada a cada criterio debe acompañarse de la fundamentación correspondiente, refiriéndose a las fortalezas o debilidades identificadas.

1. **Informe emitido por un Auditor Externo de Tecnologías de Información (TI), CISA**, el cual debe estar activo en la Asociación de Auditoría y Control de los Sistemas de Información (Information System Audit and Control Association/ ISACA) e inscrito en el Registro de Auditores Externos de la Sugeval. Para cumplir con el requisito, el informe del auditor externo de TI debe concluir que el sujeto obligado dispone de un **Aceptable** grado (o superior) en la gestión de los riesgos de TI para cada uno de los criterios que más adelante se detallan.

La auditoría de TI que se realice por el auditor CISA debe utilizar como criterios de evaluación las mejores prácticas y controles de TI descritos en COBIT 5 o superior, con el objetivo de auditar y validar si el sujeto obligado cuenta con plataformas tecnológicas robustas, seguras y cuenta con un adecuado sistema de gestión tecnológica para salvaguardar la información de los usuarios que utilizan los servicios de pago.

El alcance de auditoría de TI debe contemplar la evaluación de los procesos de TI descritos en la tabla siguiente:

**Tabla de procesos TI**

| Id | Proceso | Id | Proceso |
| --- | --- | --- | --- |
| EDM 03 | Asegurar la Optimización del Riesgo | BAI 05 | Gestionar los Cambios |
| EMD 04 | Asegurar la Optimización de Recursos | BAI 08 | Gestionar la Configuración |
| EDM 05 | Asegurar la Transparencia hacia las Partes Interesadas | BAI 09 | Gestionar los Activos |
| APO 08 | Gestionar los acuerdos de servicio | DSS 01 | Gestionar Operaciones |
| APO 11 | Gestionar el Riesgo | DSS 02 | Gestionar Peticiones e Incidentes de Servicio |
| APO 12 | Gestionar la Seguridad | DSS 03 | Gestionar Problemas |
| BAI 01 | Gestión de Programas y Proyectos | DSS 04 | Gestionar la Continuidad |
| BAI 03 | Gestionar la Identificación y Construcción de Soluciones | DSS 05 | Gestionar Servicios de Seguridad |
| BAI 04 | Gestionar la Disponibilidad y la Capacidad | DSS 06 | Gestionar Controles de Proceso de Negocio |

Esta tabla se fundamenta en COBIT 5, en caso de usar COBIT 2019 se deben utilizar los equivalentes.

Además, el auditor externo de TI debe considerar en su evaluación la revisión de los siguientes lineamientos:

* + - * Determinar el perfil tecnológico de la entidad: Descripción de la estructura organizacional, los procesos y la infraestructura de TI del sujeto obligado, así como, del nivel de automatización de sus procesos de negocio y gestión del riesgo.
      * Verificar si la entidad cuenta con una adecuada gestión del riesgo de TI y controles para la protección de los datos.

El informe del Auditor Externo debe referirse a la gestión de los riesgos de TI sobre cada uno de los criterios anteriores, cuyo resultado debe ser calificado según la siguiente escala:

**Fuerte**: Las características de la función tales como las responsabilidades, estructura, recursos, metodologías y prácticas, superan lo que se considera necesario, dada la naturaleza, complejidad y perfil de riesgo de la entidad y su desempeño ha sido altamente efectivo y consistente.

**Aceptable**: Las características de la función tales como las responsabilidades, estructura, recursos, metodologías y prácticas, cumplen con lo que se considera necesario, dada la naturaleza, complejidad y perfil de riesgo de la entidad y su desempeño ha sido altamente efectivo y consistente.

**Mejorable:** Las características de la función tales como las responsabilidades, estructura, recursos, metodologías y prácticas, generalmente cumplen con lo que se considera necesario, dada la naturaleza, complejidad y perfil de riesgo de la entidad. El desempeño de la funsión ha sido generalmente efectivo, pero existen áreas que necesitan mejoras.

**Débil:** Las características de la función tales como las responsabilidades, estructura, recursos, metodologías y prácticas, no cumplen de manera significativa con lo que se considera necesario, dada la naturaleza, complejidad y perfil de riesgo de la entidad. El desempeño de la funsión ha demostrado serias debilidades.

En cada caso, la calificación asignada a cada criterio debe acompañarse de la fundamentación correspondiente, refiriéndose a las fortalezas o debilidades identificadas.

Cuando la unidad de TI no forme parte de la entidad supervisada o cuando existan proveedores de TI, la entidad debe establecer un contrato con esa unidad de TI, en la que deben observarse los instrumentos legales en que se pacten los servicios de TI, los cuales deben indicarse en la certificación.

Cuando las bases de datos o las aplicaciones vigentes que procesan o dan accesos a estas bases de datos, se mantengan en la nube, deben cumplir con los requisitos legales, de seguridad y de acceso a los datos para el supervisor en caso de requerirlo. Estos elementos deberán indicarse en el informe.

En caso de que el sujeto obligado ya cuente con una certificación emitida por un organismo o entidad reconocida internacionalmente (lo cual deberá demostrar de esa manera), podrá solicitar su reconocimiento ante la SUGEF, en sustitución del informe de auditor CISA requerido. No obstante, para esto deberá hacer la solicitud ante la SUGEF, demostrando que tal certificación cumple con lo requerido en esta resolución y que la certificación se encuentra actualizada. En caso de que la certificación y documentos relacionados se hayan emitido en un idioma diferente del español, se deberá acompañar de su traducción formal.

**Ambos informes indicados en los puntos a) y b) anteriores, deben tener una fecha de emisión no mayor a tres meses al momento de presentar ante esta Superintendencia, la solicitud de la certificación dispuesta en el artículo 6 del Reglamento del Sistema de Pagos.**

El contrato suscrito con cada auditor externo debe incluir una cláusula que obligue a entregar al supervisor, copia de la información recopilada y procesada que sirve como respaldo de las labores para emitir dicho informe, así como los papeles de trabajo en un plazo no mayor a 5 días hábiles. Lo anterior, será por previa solicitud de este ente supervisor.

En caso de que el supervisor identifique en los papeles de trabajo o como parte de su labor de supervisión, situaciones contrarias a las declaradas en el informe emitido, o situaciones que no sustenten tales declaraciones, será notificado al sujeto obligado y al BCCR, indicando que no se cumple con el requisito de cumplimiento y efectividad dispuesto, para que se inhabilite la prestación del servicio.

1. El sujeto interesado deberá suministrar los documentos indicados por medio del correo institucional, [articulo15bis-crm@sugef.fi.cr](mailto:articulo15bis-crm@sugef.fi.cr), u otro(s) medio(s) que disponga la Superintendencia.
2. Las entidades deben demostrar que se encuentran registradas en la plataforma del Instituto Costarricense de Drogas (ICD), ***UIF Reportes***, el cual es el *Sistema de Registro y Reporte de Sujetos Obligados*, que desarrollan alguna de las actividades descritas en el artículo 15 y 15bis de la Ley 8204, para el reporte de operaciones sospechosas. El acceso a la plataforma lo puede ubicar en el siguiente enlace: <https://apps.icd.go.cr/uifreportes/Autenticacion.aspx>
3. Esta Superintendencia, estará haciendo la comunicación correspondiente al BCCR con base en los resultados obtenidos, sin embargo, no se estarán reenviando los informes emitidos por dichos profesionales por cuanto son documentos confidenciales asociados al proceso de Supervisión.
4. La lista de participantes autorizados ante la Sugeval, para prestar sus servicios como auditores externos, puede ser consultada en el siguiente enlace: <https://aplicaciones.sugeval.fi.cr/Participantes/AuditoresExternos>
5. Ambos informes deben actualizarse de forma anual con corte al 30 de junio, debiendo presentarse a esta Superintendencia en el mes de setiembre de cada año, para verificar que se mantienen las condiciones que le dieron origen, salvo que la certificación emitida por esta Superintendencia que dio origen a la autorización por parte del Banco Central de Costa Rica como proveedor de servicios de pago, tenga una fecha de emisión menor a seis meses a la fecha de corte para la correspondiente renovación. Si el sujeto obligado no presenta la actualización anual, tal situación será notificada al BCCR para que se inhabilite la prestación del servicio.
6. En cualquier momento que esta Superintendencia evidencie que no se está cumpliendo con los requerimientos reglamentarios establecidos o las condiciones óptimas en la gestión de tecnologías de información, lo podrá comunicar de forma general al BCCR, para que se inhabilite la prestación del servicio.
7. Para los sujetos obligados que ya se encuentren inscritos ante Sugef y que a la fecha ya se encuentren autorizados por el Banco Central de Costa Rica como proveedores de servicios de pago, **contarán con un plazo de 8 meses a partir del presente comunicado**, para suministrar la información requerida en los puntos 1.a) y 1.b), y en adelante proceder con su actualización de conformidad con el punto 5. En caso de que no se cumpla con lo requerido, tal situación será comunicada al BCCR, para que se inhabilite la prestación del servicio.

Atentamente,



Rocío Aguilar Montoya

Superintendente General de Entidades Financieras

*RAM/RCA/GAM/JCB/RBS.*