GESTIÓN INTEGRAL DE RIESGOS 2023

SERVICIOS FINANCIEROS, S.A. DE C.V.

I. INTRODUCCIÓN

Servicios Financieros, S.A de C.V. ha brindado soluciones innovadoras en la industria de pagos, generando ingresos y rentabilidad a comercios afiliados por medio de un sólido conjunto de soluciones de pago, que están a la vanguardia del desarrollo tecnológico. La red supera los 10.000 puntos de aceptación de pago y administra las transacciones electrónicas de más de 900 cajeros automáticos.

II. OBJETIVO

Informar sobre la Gestión Integral de Riesgos, lo relativo a las políticas, metodologías y demás medidas relevantes adoptadas para la gestión de cada tipo de riesgos, de acuerdo con lo indicado en la NRP-20 Norma Técnica para la Gestión Integral de Riesgo de las entidades Financieras.

III. ALCANCE

La información presentada en el Informe hace referencia a la Gestión realizada en el año dos mil veintitrés sobre la Gestión Integral de Riesgo de la entidad y su divulgación en el sitio web para cumplimiento de lo establecido en el artículo veintidós de la norma de Gestión Integral de Riesgos, en lo referente a información relativa a las políticas, metodologías y demás medidas relevantes adoptadas para la gestión de cada tipo de riesgos.

IV. INDICE

Contenido

V. CONTENIDO DEL INFORME

a. Principales riesgos asumidos por las actividades de la entidad

Servicios Financieros, S.A. de C.V. cuenta con un modelo de negocio con un esquema de operación basado en la transaccionalidad de tarjetas de crédito y/o débito de bancos locales, a su vez, un esquema que soporta el manejo de transacciones internacionales y su gestión y administración con las marcas principales. Por lo cual la entidad realiza estudio para identificar los riesgos que sume por las actividades que desarrolla en su modelo de negocio, los cuales se listan a continuación:

- Riesgo Operacional

Es la posibilidad de incurrir en pérdidas, debido a uno de los siguientes factores: fallas en los procesos, personas, los sistemas de información o a causa de acontecimientos externos, dentro de este riesgo se incluye el riesgo legal, riesgo de fraude, riesgo tecnológico y lo relacionado al riesgo estratégico por afectación al cumplimiento de los objetivos del negocio. La entidad asume el riesgo operacional como uno de los principales identificados en los procesos.

- Riesgo Reputacional

Es la posibilidad de incurrir en pérdidas, producto del deterioro de imagen de la entidad, debido al incumplimiento de leyes, normas internas, códigos de gobierno corporativo, códigos de conducta, lavado de dinero, entre otros. Como entidad y bajo el compromiso de brindar a los clientes servicio de calidad, se adopta el riesgo Reputacional y se asume con el nivel de relevancia que implica debido a la afectación a nivel transversal.

- Riesgos de Lavado de Dinero y de Activos, Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva.

Es la posibilidad de pérdida o daño que puede sufrir la entidad por su propensión o vulnerabilidad a ser utilizada directa o indirectamente o a través de sus operaciones como instrumento para el lavado de dinero o activos, canalización de recursos hacia la realización de actividades terroristas, financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva.

- Riesgo de Seguridad de la Información y Ciber riesgo, riesgo cibernético o de ciberseguridad:

El riesgo de Seguridad de la Información hace referencia al conjunto de medidas que permiten resguardar y proteger la información cumpliendo con las propiedades de confidencialidad, integridad y disponibilidad de la misma, con el fin que las amenazas no se materialicen.

El riesgo de Ciberseguridad se define como posibles resultados negativos derivados de fallas en la seguridad de la infraestructura tecnológica o asociados a ataques cibernéticos, los cuales son gestionados por medio de procesos con el objetivo de prevenir, detectar y responder a la seguridad de la información

b. Políticas y demás medidas relevantes adoptadas para la gestión de cada tipo de riesgos

El Gobierno Corporativo de Servicios Financieros, S.A. de C.V. por medio de las diferentes áreas de control interno creadas para dar seguimiento a los riesgos que afectan las operaciones de la entidad, dan cumplimiento a políticas, metodologías y procedimientos para una adecuada Gestión Integral del Riesgo, las cuales listamos a continuación:

1. Manual de Procedimientos de Auditoría Interna

El objetivo del Manual, es establecer las disposiciones mínimas que deberán considerarse para el ejercicio de la actividad de auditoría interna en Servicios Financieros, S.A. de C.V., para que promueva actividades con valor agregado y así fomentar la adopción de procedimientos y técnicas de trabajo con un enfoque de auditoría basada en riesgos; así como establecer los fundamentos para evaluar el desempeño de la Auditoría Interna y se fomente la mejora continua en los diferentes procesos de la empresa.

2. Política y Manual de Riesgo Operacional

Tiene como objetivo establecer los lineamientos para la gestión de riesgos operativos a los cuales se ve expuesta la entidad de acuerdo con las bases establecidas por los entes reguladores nacionales y seguimiento de las buenas prácticas y estándares internacionales, da cumplimiento a lo establecido en la NRP-42 Normas Técnicas para la Gestión del Riesgo Operacional en las Entidades Financieras.

3. Política de Riesgo Legal

Su objetivo es definir el proceso a ejecutar para una adecuada Gestión del Riesgo Legal en sus diferentes etapas: Identificación, medición, control y mitigación, así como el adecuado monitoreo y comunicación de los riesgos de índole jurídica.

4. Política de Riesgo Reputacional

Define el proceso a ejecutar para una adecuada Gestión del Riesgo Reputacional en sus diferentes etapas: Identificación, medición, control y mitigación, así como el adecuado monitoreo y comunicación de los riesgos de índole Reputacional.

5. Política de Gestión Integral de Riesgo

Establece los lineamientos para la gestión integral de riesgos a los cuales se ve expuesta la entidad de acuerdo con los lineamientos establecidos por los entes reguladores nacionales y seguimiento de las buenas prácticas y estándares internacionales.

6. Política de Continuidad del Negocio

Enfocada a garantizar una respuesta adecuada y oportuna ante la materialización de una amenaza que afecte o atente con la continuidad del negocio o los procesos institucionales críticos, forma parte de los elementos del Sistema de Continuidad del Negocio de acuerdo con la NRP-24 Normas Técnicas para el Sistema de Gestión de la Continuidad del Negocio.

7. Proceso de Análisis de Amenazas a la Continuidad del Negocio

Establece los parámetros que permiten identificar y analizar las amenazas que son capaces de afectar la continuidad del negocio de acuerdo con los procesos, sistemas, personas, partes interesadas, productos o servicios ofrecidos por SERFINSA.

8. Análisis de Impacto al Negocio

Establece el análisis de las posibles consecuencias que puede tener un incidente sobre los productos y servicios críticos, con objeto de elaborar e identificar estrategias de respuesta que permita la continuidad operativa de la entidad.

9. Plan de Continuidad del Negocio y Planes de Respuesta a Eventos de Crisis

Provee las medidas de preparación y recuperación de los servicios de tecnología de información luego de una emergencia producida por eventos intencionales o fortuitos, cubriendo mediante elementos redundantes las eventualidades que pueden afectar el hardware, software y componentes de telecomunicaciones, ya sea bajo una afectación parcial o total de la operación.

10. Manual para la Prevención, Detección y Control de Lavado de Dinero y Activos, Financiación al Terrorismo y Financiación a la Proliferación de Armas de Destrucción Masiva.

Es el documento que establece los conceptos, lineamientos, políticas, roles y responsabilidad frente a la prevención y control de Lavado de Dinero y Activos, Financiación al Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva.

11. Política “Conozca a su Cliente”.

Constituye el pilar principal y la medida más importante ya que establece el proceso de debida diligencia para conocer a los clientes y la evaluación de riesgo inherente, por lo que ayuda a evaluar y evitar el riesgo de que se involucre y utilicen a la Entidad, como intermediaria en operaciones ilícitas u operaciones de Lavado de Dinero y Activos, Financiación al Terrorismo y Financiación a la Proliferación de Armas de Destrucción Masiva. (Vigencia 2023).

12. Política “Conozca a su Contraparte”.

Establece un mecanismo que permita prevenir, detectar y disminuir el riesgo que involucre a la institución, ya que implica el desarrollo de procedimientos y controles para valorar, identificar y verificar la identidad de sus proveedores y aliados estratégicos

13. Política conozca a su empleado.

Interviene directamente al fortalecimiento del control Interno, a través de lineamientos y procedimientos encaminados a cumplir con un alto nivel de integridad personal del Empleado, así como de sistemas para evaluar sus antecedentes personales, laborales y patrimoniales

14. Política para el uso de Listas de Control y Prevención contra el Lavado de Activos y Delitos Conexos.

Es un instrumento que permitirá prevenir de forma eficaz que ingresen personas consideradas no recomendadas a la institución como cliente, usuarios o accionistas, con la intención de usar la Entidad en actos ilícitos de Lavado de Dinero y el Financiamiento del Terrorismo

15. Política para la Identificación de Operaciones Inusuales y Envío de Reportes de Operaciones Sospechosas a la UIF.

El presente documento desarrolla la política interna para la elaboración y envío de Reportes de Operaciones Sospechosas de SERFINSA, destacando la importancia de poder detectar operaciones inusuales y remitir los Reportes respectivos a la UIF

16. Política para el Archivo y Conservación de Documentación.

Establecer mecanismos, procedimientos y control respecto al resguardo y manejo en forma impresa, digital y/o electrónica de la información de los clientes, documentación de apertura de Servicios

17. Política para la Identificación Personas Expuestas Políticamente (PEP´s)

La política para la identificación de las Personas Expuestas Políticamente y los lineamientos y procedimientos necesarios para cumplir con una debida diligencia de acuerdo con lo que establece el marco regulatorio vigente en materia de prevención de Lavado de Dinero y Activos, Financiación al Terrorismo y Financiación a la Proliferación de Armas de Destrucción Masiva

18. Política de Capacitación al Personal en Prevención de LDTFT

Es contar con un programa óptimo de capacitaciones para todo el personal en general, y más especial, al personal que interviene directamente en los procesos internos de vinculación y control que SERFINSA.

19. Código de Ética

Una serie de pautas de comportamiento que ayudan a la mejora y el mantenimiento de la confianza de nuestros funcionarios, empleados y proveedores

20. Política de Gestión de Riesgos de Lavado de Dinero y de Activos, Financiación al Terrorismo y Financiación a la Proliferación de Armas de Destrucción Masiva y sus Riesgos Asociados.

Brindar una herramienta a los funcionarios y empleados de SERFINSA, para realizar el proceso de identificación, evaluación, control, mitigación y comunicación de los riesgos relacionados a lavado de dinero y activos, financiación al terrorismo y financiación a la proliferación de armas de destrucción masiva

21. Política de Confidencialidad sobre las Transacciones y de la Información.

Describe los lineamientos específicos que permitan tratar con estricta reserva, confidencialidad y fidelidad toda la información concerniente a las operaciones que realizan los Clientes/usuarios tanto internos como externos de nuestros servicios

22. Política de Monitoreo de Transacciones.

Enfocada en llevar un control de las transacciones que se realicen, desde el punto de vista de prevención de lavado de activos/financiamiento al terrorismo, así mismo se regula el envío de Operaciones reguladas a la Unidad de Investigación Financiera.

23. Política Anticorrupción

Promover una cultura de prevención encaminada a mitigar los riesgos de corrupción a nivel interno y en relación con terceros, además de brindar directrices para prevenir, detectar, verificar y remediar de manera efectiva y oportuna los eventos de riesgos.

24. Política de Gestión de Acceso y Equipo Informático

Regula la gestión de los diferentes tipos de accesos disponibles en SERFINSA, desde accesos lógicos a aplicaciones informáticas, sistemas operativos, dispositivos de red, además considerando los accesos físicos controlados por los accesos biométricos.

25. Política de Seguridad de la Información.

Garantiza el cumplimiento de la confidencialidad, integridad y disponibilidad de los sistemas informáticos y/o la información de ellos contenida.

26. Política de Gestión de Infraestructura.

Garantiza una gestión adecuada de la Infraestructura tecnológica que forma parte de SERFINSA para cumplir con los niveles de confidencialidad y de seguridad demandados por los clientes.

c. Descripción de las metodologías utilizadas para la Gestión de riesgos.

Para la Gestión de los riesgos, Servicios Financieros, S.A de C.V. desarrolla una metodología basada en el proceso conformado de cuatro etapas:

- Identificación: reconocemos y entendemos los riesgos a los que está expuesta la entidad, clasificándolos según criterios que apoyan a su seguimiento.
- Medición: los riesgos identificados son evaluados en probabilidad e impacto para determinar su riesgo inherente en la operativa de los procesos, según el apetito de riesgo propuesto por el Comité de Riesgo y aprobado por Junta Directiva.
- Control y mitigación: tiene como objetivo asegurar que las políticas, límites y procedimientos establecidos para el tratamiento y mitigación de los riesgos son apropiados.

- Monitoreo y comunicación: etapa que da seguimiento a las exposiciones de riesgo y a los resultados de las acciones adoptadas para mitigar los riesgos identificados.

En cuanto a la gestión de riesgos relacionados a la Seguridad de la Información, se fundamenta en el Sistema de Gestión de la Seguridad de la Información, en adelante SGSI, en aplicación de la NRP-23 Norma para la Seguridad de la Información de las Entidades Financieras.

El proceso de gestión de los diferentes tipos de riesgos es reforzado por las políticas establecidas en la entidad, donde se establecen criterios y lineamientos para dar cumplimiento a los procesos, así como métricas de evaluación de la gestión entre otros aspectos.
Adicionalmente, se cuenta con refuerzos de auditorías internas, cuyas etapas se detallan a continuación:

a) Planeación de la Auditoría

Se listan los procesos de la compañía, se prioriza unidades auditables (procesos) con base en evaluación de factores riesgos, definiendo niveles de riesgo para cada factor, se incluyen actividades auditables de cumplimiento legal normativo, el resto de los procesos, se consideran siempre y cuando cumplan el ciclo de auditoría definido y en general, nos aseguramos de que el Plan de Trabajo Anual, cumpla los requerimientos de la NRP15 y los aspectos definidos por el Marco Internacional para la Práctica Profesional de la Auditoría Interna (MIPP) del Instituto Internacional de Auditores (IIA).

b) Ejecución de la Auditoría

Se informa el inicio de la auditoría a áreas involucradas, a continuación; se definen reuniones para conocer detalladamente el proceso a examinar, se prepara planificación del proceso o actividad a examinar, se elabora procedimientos de auditoría y requerimiento inicial, se ejecutan dichos procedimientos, obteniendo evidencia suficiente y adecuada, se elabora y se comunica el informe borrador a las áreas involucradas, se reciben planes de acción y se procede a emitir informe final.

c) Seguimiento de Hallazgos

Se cuenta con matriz de hallazgos, en la cual se van incorporando los puntos observados en cada proceso o actividad auditable, incluyendo las observaciones que hayan sido reportadas por auditores externos, auditorías de la Superintendencia y de cualquier otro ente regulador, estos puntos son monitoreados de forma mensual con cada área responsable y son presentados al comité de auditoría en las fechas programadas y junta directiva de forma trimestral.