SEGUNDO SUPLEMENTO

REGISTRO OFICIAL®
ÓRGANO DE LA REPÚBLICA DEL ECUADOR

SUMARIO:

Págs.

Año I - Nº 155 - 62 páginas
Quito, jueves 30 de octubre de 2025

Secretaría Nacional
de Gestión de Riesgos

RESOLUCION No. SNGR-0357-2025

M.ENG. JORGE CARRILLO TUTIVÉN
SECRETARIO NACIONAL DE GESTION DE RIESGOS

CONSIDERANDO:

Que, el numeral l del artículo 154 de la Constitución de la República del Ecuador, establece, a las ministras y ministros de Estado, además de las atribuciones establecidas en la ley, les corresponde: *"Ejercer la rectoría de las políticas de área a su cargo y expedir los acuerdos y resoluciones administrativas que requiera su gestión."*;

Que, el artículo 225 de la Constitución de la República del Ecuador, señala: *"El sector público comprende:*
1. Los organismos y dependencias de las funciones Ejecutiva, Legislativa, Judicial, Electoral y de Transparencia y Control Social.
2. Las entidades que integran el régimen autónomo descentralizado.
3. Los organismos y entidades creados por la Constitución o la ley para el ejercicio de la potestad estatal, para la prestación de servicios públicos o para desarrollar actividades económicas asumidas por el Estado.
4. Las personas jurídicas creadas por acto normativo de los gobiernos autónomos descentralizados para la prestación de servicios públicos.";

Que, el artículo 226 de la Constitución de la República del Ecuador, señala: *"Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que le sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución.";*

Que, el artículo 227 de la Constitución de la República del Ecuador, manifiesta: *"la administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación.";*

Que, el artículo 229 de la Constitución de la República del Ecuador, indica: *"Serán servidoras o servidores públicos todas las personas que en cualquier forma o a cualquier título trabajen, presten servicios o ejerzan un cargo, función o dignidad dentro del sector público. (...) Las obreras y obreros del sector público estarán sujetos al Código de Trabajo.";*

Que, el artículo 47 del Código Orgánico Administrativo, en relación a la representación legal de las administraciones públicas, señala: *"La máxima autoridad administrativa de la correspondiente entidad pública ejerce su representación para intervenir en todos los actos, contratos y relaciones jurídicas sujetas a su competencia. Esta autoridad no requiere delegación o autorización alguna de un órgano o entidad superior, salvo en los casos expresamente previstos en la ley.";*

Que, el artículo 130 del Código Orgánico Administrativo, en relación a la competencia normativa de carácter administrativo establece: *"Las máximas autoridades administrativas tienen competencia normativa de carácter administrativo únicamente para regular los asuntos internos del órgano a su cargo, salvo los casos en los que la ley prevea esta competencia para la máxima autoridad legislativa de una administración pública. La competencia regulatoria de las actuaciones de las personas debe estar expresamente atribuida en la ley.";*

Que, el artículo 23 de la Ley Orgánica para la Gestión Integral del Riesgo de Desastres; en relación a la rectoría de la política de gestión integral del riesgo de desastres y del Sistema Nacional Descentralizado de Gestión Integral del Riesgo de Desastres, señala: *"La rectoría de la política y del Sistema Nacional Descentralizado de Gestión Integral del Riesgo de Desastres es competencia de la Secretaria Nacional de Gestión de Riesgos, como entidad técnica de derecho público, con rango de ministerio, adscrita a la Función Ejecutiva. La máxima autoridad será ejercida por una secretaria o secretario con rango de ministro, que será nombrado por el presidente de la República y no podrá asumir la rectoría en una materia distinta. (...) Disposición General Primera, se dispone que la actual Secretaría de Gestión de Riesgos se convertirá en Secretaría Nacional de Gestión de Riesgos para lo cual deberá adaptar todas sus normativas institucionales";*

Que, la Norma de Control Interno 401-05, señala: *"Documentación de respaldo y su archivo. - (...) Toda operación institucional deberá estar respaldada con evidencia documental contenida en formatos digitales, registros electrónicos, bases de datos o plataformas interoperables, que permitan su seguimiento, verificación, comprobación y análisis correspondiente. La documentación generada electrónicamente y los archivos digitales serán válidos para efectos del control, siempre que cumplan las condiciones previstas por la Ley.";*

Que, el artículo 17 del Estatuto del Régimen Jurídico y Administrativo de la Función Ejecutiva, en lo relacionado a los Ministerios, establece: *"Los ministros de Estado son competentes para el despacho de todos los asuntos inherentes a sus ministerios sin necesidad de autorización alguna del Presidente de la República, salvo los casos expresamente señalados en leyes especiales.";*

Que, mediante Decreto Ejecutivo Nro. 1046-A de 26 de abril de 2008, publicado en Registro Oficial No. 345, de 26 de mayo de 2008, se reorganiza la Dirección Nacional de Defensa Civil, mediante la figura de la Secretaría Técnica de Gestión de Riesgos, adscrita al Ministerio de Coordinación de Seguridad Interna y Externa, adquiriendo por este mandato, todas las competencias, atribuciones, funciones, representaciones y delegaciones constantes en leyes, reglamentos y demás instrumentos normativos que hasta ese momento le correspondían a la Dirección Nacional de Defensa Civil y a la Secretaría General del COSENA, en materia de Defensa Civil;

Que, mediante Decreto Ejecutivo Nro. 42 de 10 de septiembre de 2009, publicado en Registro Oficial Nro. 31, de 22 de septiembre de 2009, la Secretaría Técnica de Gestión de Riesgos, pasa a denominarse Secretaría Nacional de Gestión de Riesgos que ejercerá sus competencias y funciones de manera independiente, descentralizada y desconcentrada; mediante Decreto Ejecutivo Nro. 103 de 20 de octubre de 2009, publicado en Registro Oficial Nro. 58 de 30 de octubre de 2009, se reforma el Decreto Ejecutivo Nro. 42, por el

cual se le da el rango de Ministro /a de Estado al Secretario/a Nacional de Gestión de Riesgos;

Que, mediante Decreto Ejecutivo Nro. 62 de 05 de agosto de 2013, la Secretaría Nacional de Gestión de Riesgos cambia de denominación a Secretaría de Gestión de Riesgos, considerando que las Secretarías son organismos públicos con facultades de rectoría, planificación, regulación, gestión y control sobre temas específicos de un sector de la administración pública; y, estará representada por un secretario que tendrá rango de ministro de Estado;

Que, mediante Decreto Ejecutivo Nro. 534 de 03 de octubre de 2018, la Secretaría de Gestión de Riesgos se transforma en el Servicio Nacional de Gestión de Riesgos y Emergencias, como entidad de derecho público, con personalidad jurídica, dotada de autonomía administrativa, operativa y financiera, encargada de la gestión, seguimiento y control de las políticas, regulaciones y planes aprobados por su órgano gobernante;

Que, mediante Decreto Ejecutivo Nro. 641 de 06 de enero de 2023, se dispuso la transformación del Servicio Nacional de Gestión de Riesgos y Emergencias a Secretaría de Gestión de Riesgos, dirigida por el/la Secretario/a, con rango de Ministro de Estado; encargada de la rectoría, regulación, planificación, gestión, evaluación, coordinación y control del Sistema Nacional Descentralizados de Gestión de Riesgos;

Que, mediante Decreto Ejecutivo Nro. 42, el 04 de diciembre de 2023, el Presidente Constitucional de la República del Ecuador, designó al Señor. Jorge Raúl Carrillo Tutivén como Secretario de Gestión de Riesgos;

Que, mediante Resolución No. SGR-039-2014, publicada en el Registro Oficial No.163 de 09 de septiembre de 2014, se expidió el Estatuto Orgánico de Gestión Organizacional por Procesos de la Secretaría de Gestión de Riesgos, en el cual se establece la desconcentración de la gestión de riesgos a través de la creación de las Coordinaciones Zonales de Gestión de Riesgos en ocho (8) zonas territoriales;

Que, mediante Resolución Nro. SNGRE-106-2022 de 11 de mayo de 2022, se institucionalizó el FIN-SNGR-PR-06 Procedimiento para registro, custodia y control de vigencia de garantías de contratos de bienes, servicios y obras, versión 1.0;

Que, mediante Memorando Nro. SNGR-SGR-2025-0263-M, la Máxima Autoridad de la SNGR, pone en conocimiento el INFORME GENERAL DPGY-0051-2025 CGE, del *"Examen especial a las fases de ejecución y liquidación de los procesos de contratación de bienes y servicios (...), por el período 01 de enero de 2020 al 31 de diciembre de 2024"*, el mismo que en su parte pertinente indica: *"Conclusión.- (...) en dos procesos de contratación, no constó la devolución de las garantías. Debido a que los Administradores de Contratos en sus respectivos períodos de actuación, no aplicaron controles efectivos para comunicar el cumplimiento de las obligaciones contractuales y solicitar a la Tesorería General, la gestión oportuna para su devolución a los contratistas; y, el Tesorero General no aplicó mecanismos adecuados de control para cumplir con la devolución oportuna de las citadas garantías (...) Recomendación Al Tesorero General: 1. Aplicará controles oportunos para garantizar la devolución de las garantías de buen uso del anticipo; al momento en que se haya devengado en su totalidad; y, la garantía de fiel cumplimiento, cuando se hayan*

cumplido las obligaciones contractuales, con la firma del Acta entrega recepción definitiva, de conformidad con lo señalado en las cláusulas contractuales y normativa vigente";

Que, mediante Memorando Nro. SNGR-UF-2025-0514-M de 09 de julio de 2025, la Ing. María Auxiliadora Villacís Morante, Tesorera, solicita a la Mgs. Ariana Lizzette Zúñiga Parada, Directora Financiera, la actualización del procedimiento para registro, custodia y control de vigencia de garantías, incluyendo un lineamiento en reemplazo del Nro.8 y la Plantilla Nro.3 Solicitud para devolución de garantías;

Que, mediante Memorando Nro. SNGR-UF-2025-0515-M de 09 de julio de 2025, la Mgs. Ariana Lizzette Zúñiga Parada, Directora Financiera, solicita al Coordinador General Administrativo Financiero, actualizar el procedimiento para el registro, custodia y control de vigencia de garantías;

Que, mediante Memorando Nro. SNGR-CAF-2025-0576-M de 14 de julio de 2025, el Coordinador General Administrativo Financiero, solicita a la Coordinadora General de Planificación y Gestión Estratégica, disponer a quien corresponda realizar la asesoría metodológica para acompañamiento en la actualización del Procedimiento para registro, custodia y control de vigencia de garantías, en cumplimiento a las recomendaciones emitidas por la Contraloría General del Estado mediante Informe DPGY-0051-2025;

Que, mediante Memorando Nro. SNGR-CGPGE-2025-0384-M de 01 de octubre de 2025, el Mgs. Javier A. Luna Rodríguez, Coordinador General de Planificación y Gestión Estratégica, Subrogante, solicita a la máxima autoridad institucional la autorización para institucionalización del FIN-SNGR-PR-06 Procedimiento para registro, custodia y control de vigencia de garantías de contratos de bienes, servicios y obras, versión 2.0, elaborado y revisado por la Dirección Financiera y la Dirección de Servicios, Procesos y Calidad y aprobado por la Coordinación General Administrativa Financiera y la Coordinación General de Planificación y Gestión Estratégica;

Que, mediante comentario inserto en la Hoja de Ruta del Memorando Nro. SNGR-CGPGE-2025-0384-M, la máxima autoridad institucional, autoriza y dispone a la coordinación General de Asesoría Jurídica, proceder con los trámites legales correspondientes para la institucionalización del FIN-SNGR-PR-06 Procedimiento para registro, custodia y control de vigencia de garantías de contratos de bienes, servicios y obras, versión 2.0;

Que, es necesario contar con la normativa institucional que sustente el procedimiento para registro, custodia y control de vigencia de garantías de contratos de bienes, servicios y obras de la Secretaría Nacional de Gestión de Riesgos; y,

En ejercicio de las atribuciones conferidas en el numeral 1 del artículo 154 de la Constitución de la República del Ecuador, y artículo 17, inciso primero, del Estatuto del Régimen Jurídico y Administrativo de la Función Ejecutiva.

RESUELVE:

Artículo 1.- EXPEDIR el FIN-SNGR-PR-06 Procedimiento para registro, custodia y control de vigencia de garantías de contratos de bienes, servicios y obras, versión 2.0 de la Secretaría Nacional de Gestión de Riesgos.

Artículo 2.- DISPONER al/la Coordinador/a General Administrativo/a Financiero/a en el marco de sus competencias, como responsable de la aplicación, control y seguimiento del presente Procedimiento.

Artículo 3.- DISPONER al/la Coordinador/a General Administrativo/a Financiero/a garantizar la difusión continua de los formatos oficiales y actualizados necesarios para la correcta aplicación del presente Procedimiento, a través de los canales institucionales disponibles.

Artículo 4.- DISPONER al/la Coordinador/a General de Asesoría Jurídica la publicación la publicación en el Registro Oficial del documento FIN-SNGR-PR-06 Procedimiento para registro, custodia y control de vigencia de garantías de contratos de bienes, servicios y obras, versión 2.0, con sus anexos que se encuentra en el siguiente enlace: https://nube.gestionderiesgos.gob.ec/index.php/s/jFgnR3osC3s2okY

DISPOSICIÓN DEROGATORIA

Deróguese la Resolución Nro. SNGRE-106-2022 de 11 de mayo de 2022, mediante la cual se institucionalizó el FIN-SNGR-PR-06 Procedimiento para registro, custodia y control de vigencia de garantías de contratos de bienes, servicios y obras, versión 1.0.

DISPOSICIÓN FINAL

El presente Procedimiento entrará en vigencia a partir de su suscripción sin perjuicio de su publicación en el Registro Oficial.

Dado y firmado en el Despacho de la Secretaría Nacional de Gestión de Riesgos, en el cantón Samborondón, a los trece días del mes de octubre de 2025.

Cúmplase, publíquese y socialícese. -

Firmado electrónicamente por:
JORGE RAUL CARRILLO TUTIVEN
Validar únicamente con FirmaEC

M. Eng. Jorge Carrillo Tutivén
Secretario Nacional de Gestión de Riesgos
SECRETARÍA NACIONAL DE GESTIÓN DE RIESGOS

Elaborado por	Dra. Nina Guerrero S.- Analista de Asesoría Jurídica
Aprobado por	Abg. Tania Núñez.- Coordinadora General de Asesoría Jurídica


PROCEDIMIENTO PARA REGISTRO, CUSTODIA Y CONTROL DE VIGENCIA DE GARANTIAS DE CONTRATOS DE BIENES, SERVICIOS Y OBRAS
FIN-SNGR-PR-06
[Versión 2.0]
EL NUEVO ECUADOR
Secretaría Nacional de Gestión de Riesgos

FIRMAS DE REVISIÓN Y APROBACIÓN

Acción	Nombre / Cargo	Firma
Elaborado por:	María Auxiliadora Villacís Morante / Tesorera	Firmado electrónicamente por: MARIA AUXILIADORA VILLACIS MORANTE Validar únicamente con FirmaEC
	Marcos Emilio Aguilera Avilés / Analista de Planificación e Inversión	Firmado electrónicamente por: MARCOS EMILIO AGUILERA AVILES Validar únicamente con FirmaEC
Revisión técnica:	Arianna Lizzette Zúñiga Parada / Directora Financiera	Firmado electrónicamente por: ARIANA LIZZETTE ZUNIGA PARADA Validar únicamente con FirmaEC
	Rosalía Aurora Pasmay Macías / Directora de Servicios, Procesos y Calidad	Firmado electrónicamente por: ROSALIA AURORA PASMAY MACIAS Validar únicamente con FirmaEC
Aprobado por:	Javier Alejandro Luna Rodriguez / Coordinador General de Planificación y Gestión Estratégica (S)	Firmado electrónicamente por: JAVIER ALEJANDRO LUNA RODRIGUEZ Validar únicamente con FirmaEC
	Dennis Daniel Abril Ortiz / Coordinador General Administrativo Financiero	Firmado electrónicamente por: DENNIS DANIEL ABRIL ORTIZ Validar únicamente con FirmaEC

CONTROL E HISTORIAL DE CAMBIOS

Versión	Descripción del cambio	Fecha de Actualización
0.1	Emisión inicial.	14 /07/2025
0.1	Emisión por regularización de observaciones dadas por la Dirección Financiera y la Dirección de Servicios, Procesos y Calidad.	28/08/2025
0.2	Emisión por regularización de observaciones dadas por la Dirección Financiera.	16/09/2025
0.5	Emisión final luego de la validación técnica de la Directora Financiera.	29/09/2025
1.0	Emisión final luego de la aprobación del Coordinador General Administrativo Financiero	29/09/2025

CONTENIDO

1. INFORMACIÓN DEL PROCESO

Código:	**FIN-SNGR-PR-06**
Versión:	**2.0**
Nombre:	Procedimiento para registro, custodia y control de vigencia de garantías de contratos de bienes, servicios y obras.
Alcance:	Este procedimiento se aplicará en Matriz y Coordinaciones Zonales, y abarca el conjunto de actividades requeridas desde la solicitud de revisión de garantías del contrato por parte del/a Coordinador(a) General de Asesoría Jurídica / Analista de compras públicas delegado(a) en Coordinación Zonal hasta la devolución de garantías del contrato al proveedor o contratista.
Responsable:	Director(a) Financiero(a)
Descripción:	**PROPÓSITO:** Establecer bajo un enfoque de administración por procesos las actividades involucradas en el registro, custodia y control de vigencia de garantías otorgadas a la Institución por conceptos contractuales de bienes, servicios y obras, a fin de mantener el orden adecuado y la calidad en el manejo de la información. **DISPARADOR:** ❖ Garantía de fiel cumplimiento de contrato ❖ Garantía de buen uso de anticipo **PROVEEDORES:** ❖ Coordinador(a) General de Asesoría Jurídica / Analista de compras públicas delegado(a) en Coordinación Zonal ❖ Director(a) Financiero(a) o quien haga sus veces en Coordinación Zonal ❖ Tesorero(a) o quien haga sus veces en la Coordinación Zonal ❖ Responsable de Contabilidad o quien haga sus veces en Coordinación Zonal ❖ Administrador(a) de Contrato **ENTRADAS:** ❖ Documentos habilitantes ❖ Plantilla 1: Base de datos para el control de garantías vigentes ❖ Plantilla 3: Acta de entrega - recepción de garantías **SALIDAS:** ❖ Plantilla 1: Base de datos para el control de garantías vigentes ❖ Plantilla 2: Solicitud para devolución de garantías

	❖ Plantilla 3: Acta de entrega – recepción de garantías ❖ Garantías renovadas
Tipo de usuario:	Interno
Controles:	**Requisitos legales:** ❖ Constitución de la República del Ecuador ❖ Ley Orgánica del Sistema Nacional de Contratación Pública ❖ Ley Orgánica de la Contraloría General del Estado ❖ Código Orgánico Monetario y Financiero Libro III Ley General de Seguros ❖ Ley de Compañías ❖ Reglamento a la Ley Orgánica de la Contraloría General del Estado ❖ Normas de Control del Sector Público y Jurídicas de Derecho Privado **Requisitos internos:** ❖ Estatuto Orgánico de Gestión Organizacional por Procesos de la Secretaría Nacional de Gestión de Riesgos. ❖ Delegaciones y autorizaciones para la administración del talento humano; la ejecución de procesos administrativos, contractuales, financieros y de planificación y gestión estratégica, institucional; y, para actuaciones jurídicas en la Secretaría Nacional de Gestión de Riesgos.
Recursos:	❖ Tecnológicos ❖ Infraestructura ❖ Equipamiento y materiales ❖ Talento humano ❖ Financieros

2. DEFINICIONES Y ABREVIATURAS

TÉRMINO	DEFINICIÓN
Control de vigencia:	Verificación y seguimiento al vencimiento de las garantías.
CUR:	Comprobante Único de Registro
Custodia:	Responsabilidad que se tiene sobre el cuidado de una cosa.
Garantía de buen uso del anticipo	Si por la forma de pago establecida en el contrato, la entidad contratante debiera otorgar anticipos de cualquier naturaleza, el contratista para recibir el anticipo deberá rendir previamente

	garantías por igual valor del anticipo, que se reducirán en la proporción que se vaya amortizando aquél o se reciban provisionalmente las obras, bienes o servicios. Las cartas de crédito no se considerarán anticipo si su pago está condicionado a la entrega - recepción de los bienes u obras materia del contrato.
Garantía de fiel cumplimiento de contrato:	Para seguridad del cumplimiento del contrato y para responder por las obligaciones que contrajeren a favor de terceros, relacionadas con el contrato, el adjudicatario, antes o al momento de la firma del contrato, rendirá garantías por un monto equivalente al cinco (5%) por ciento del valor de aquel. En los contratos de obra, así como en los contratos integrales por precio fijo, esta garantía se constituirá para garantizar el cumplimiento del contrato y las obligaciones contraídas a favor de terceros y para asegurar la debida ejecución de la obra y la buena calidad de los materiales, asegurando con ello las reparaciones o cambios de aquellas partes de la obra en la que se descubran defectos de construcción, mala calidad o incumplimiento de las especificaciones, imputables al proveedor.
Registro:	Ingreso contable de las garantías en las cuentas de orden del sistema financiero.
RGLOSNCP:	Reglamento General a Ley Orgánica del Sistema Nacional de Contratación Pública
SNGR:	Secretaría Nacional de Gestión de Riesgos
Vencimiento:	Cumplimiento del plazo o fin de un período determinado.

3. LINEAMIENTOS DEL PROCESO

LINEAMIENTOS GENERALES

1. La Dirección Financiera deberá observar las "*Normas de Control del Sector Público y Jurídicas de Derecho Privado"* en el procedimiento para registro, custodia y control de vigencia de garantías de contratos de bienes, servicios y obras.

2. El(a) Coordinador(a) General de Asesoría Jurídica / Analista de compras públicas delegado(a) en Coordinación Zonal, en el ámbito de sus competencias, coordinará con el oferente adjudicado la entrega de las garantías (nuevos contratos), cuyas formas se encuentran contempladas en el *Art. 73 de la Ley Orgánica del Sistema Nacional de Contratación Pública* y cuyos montos se establecerán de acuerdo con las condiciones de pago y monto del contrato.

3. El(a) Tesorero(a) o quien haga sus veces en Coordinación Zonal, al revisar las garantías entregadas deberá considerar lo siguiente:

- Las garantías deberán corresponder a cualquiera de las formas previstas en la normativa legal vigente.
- Deberán contener la fecha, el plazo, el nombre del contratista, el beneficiario y el número de identificación.
- Los montos y formas de las garantías deberán ajustarse a lo dispuesto en la *Ley Orgánica del Sistema Nacional de Contratación Pública*, a la *Norma de Control Interno 403-12 referente al control y custodia de garantías*; así como a lo establecido en las bases y términos contractuales. Esta información deberá verificarse junto con el contrato.
- La autenticidad de la garantía deberá confirmarse a través de correo electrónico institucional con la compañía aseguradora.

4. El(a) Tesorero(a) o quien haga sus veces en Coordinación Zonal gestionará la suscripción de garantías nuevas o renovadas con el servidor(a) público(a) delegado(a) en la *Resolución de delegaciones y autorizaciones para la administración del talento humano; la ejecución de procesos administrativos, contractuales, financieros y de planificación y gestión estratégica, institucional; y, para actuaciones jurídicas en la Secretaría Nacional de Gestión de Riesgos* que se encuentre vigente.

5. El(a) Administrador(a) del Contrato, una vez concluido el mismo con la firma del Acta de Recepción definitiva, de manera inmediata, en cumplimiento del *Art. 263 Devolución de garantías del RGLOSNCP*, mediante oficio dirigido al(a) Tesorero(a) o quien haga sus veces en Coordinación Zonal deberá solicitar la devolución de las garantías, adjuntando el acta de recepción definitiva, para el efecto utilizará la ***Plantilla No.2 Solicitud para devolución de garantías.***

6. El(a) Tesorero(a) o quien haga sus veces en Coordinación Zonal, para la devolución de garantías, deberá considerar lo siguiente:
   - Garantía de fiel cumplimiento de contrato: en los contratos de ejecución de obras, la garantía se devolverá al momento de la entrega recepción definitiva, real o presunta. En los demás contratos, las garantías se devolverán a la firma del acta de recepción única o según lo estipulado en el contrato. *(Art.77 Ley Orgánica del Sistema Nacional de Contratación pública).*
   - Garantía de buen uso de anticipo: se devolverá cuando el anticipo haya sido amortizado en su totalidad.

7. Toda actualización requerida por el(a) Director(a) Financiero(a) en el presente documento o en los formatos del mismo deberá ser autorizada por el(a) Coordinador(a) General Administrativo(a) Financiero(a) y comunicada al(a) Coordinador(a) General de Planificación y Gestión Estratégica para que a través del(a) Director(a) de Servicios, Procesos y Calidad se realice el registro y control correspondiente.

8. Los responsables de la aplicación del Procedimiento para registro, custodia y control de vigencia de garantías de contratos de bienes, servicios y obras, deberán observar las

normativas vigentes aplicables para realizar las actividades descritas en el presente documento.

LINEAMIENTOS ESPECÍFICO

1. El(a) Coordinador(a) General de Asesoría Jurídica / Analista de compras públicas delegado(a) en Coordinación Zonal, solicitará mediante correo Institucional dirigido al(a) Director(a) Financiero(a) o quien haga sus veces en Coordinación Zonal, la revisión de garantías de contratos nuevos, adjuntando el documento original de las garantías y copia del contrato, quien dispondrá al(a) Tesorero(a) o quien haga sus veces en Coordinación Zonal, la revisión de las mismas.

2. El(a) Tesorero(a) o quien haga sus veces en Coordinación Zonal gestionará la suscripción de garantías y una vez suscritas entregará una copia al(a) Administrador(a) de Contrato.

3. El(a) Tesorero(a) o quien haga sus veces en Coordinación Zonal mantendrá un registro de las garantías para lo cual hará uso de la ***Plantilla 1: Base de datos para el control de garantías vigentes*** y abrirá un expediente para su custodia, en el que constará la póliza original, la copia del contrato, los comprobantes de pago y las actas de recepción provisionales y/o definitivas al finalizar el mismo.

4. El(a) Tesorero(a) o quien haga sus veces en Coordinación Zonal entregará copia del contrato y copia de las garantías al(a) Responsable de Contabilidad o quien haga sus veces en la Coordinación Zonal para su respectivo registro en las cuentas de orden en el sistema financiero; de igual manera para el registro de la baja de una garantía se entregará copia de actas de recepción o documentos que respalden la baja de la misma.

5. El(a) Tesorero(a) o quien haga sus veces en Coordinación Zonal será responsable de efectuar el control permanente de la vigencia de las garantías de los contratos, haciendo uso de la ***Plantilla 1. Base de datos para el control de garantías vigentes*** y, deberá comunicar al(a) Director(a) Financiero(a) o quien haga sus veces en Coordinación Zonal aquellas que estén próximas a vencer.

6. El(a) Tesorero(a) o quien haga sus veces en Coordinación Zonal por intermedio del(a) Director(a) Financiero(a) o quien haga sus veces en Coordinación Zonal, deberá comunicar al(a) Administrador(a) del Contrato, con *veinte (20) días de anticipación al vencimiento* de la garantía, mediante sistema de gestión documental, a fin de que se adopten las decisiones correspondientes respecto a su continuidad o renovación. En caso de no requerirse la renovación, el(a) Administrador(a) del Contrato deberá notificarlo por el mismo medio, adjuntando la siguiente documentación:
   a. Solicitud de no renovación de la garantía, remitida por el(a) Administrador(a) del Contrato;
   b. Informe del(a) Administrador del Contrato;
   c. Actas de ingreso a bodega, en caso de bienes;

d. Actas de recepción parcial y/o definitiva del contrato.
e. ***Plantilla 2: Solicitud para devolución de garantías***

7. El(a) Tesorero(a) o quien haga sus veces en Coordinación Zonal será responsable de gestionar la solicitud de renovación de las garantías ante las compañías aseguradoras, con un mínimo de quince (15) días de anticipación a su vencimiento. En caso de no obtener respuesta, deberá realizar insistencias mediante correo electrónico institucional, llamadas telefónicas y, de ser necesario, a través de oficio, hasta la obtención del documento renovado. Si, pese a las gestiones realizadas, la garantía no fuese renovada por falta de respuesta de la compañía aseguradora, el(a) Tesorero(a) o quien haga sus veces en Coordinación Zonal deberá informar al(a) Coordinador(a) General de Asesoría Jurídica / Coordinador(a) Zonal para que se adopten las acciones legales correspondientes.

8. El(a) Tesorero(a) o quien haga sus veces en Coordinación Zonal previo a la devolución de garantías deberá constatar la siguiente documentación:

   a. ***Plantilla 2: Solicitud para devolución de garantías*** remitida por el(a) administrador(a) de contrato;
   b. Acta de entrega - recepción de contrato y/o Anticipo amortizado.

9. El(a) Tesorero(a) o quien haga sus veces en Coordinación Zonal una vez verificado el cumplimiento de la documentación habilitante para la no renovación y devolución de garantías, deberá solicitar al(a) Responsable de Contabilidad o quien haga sus veces en Coordinación Zonal, el registro contable de baja de garantías, mediante correo electrónico institucional.

10. El(a) Tesorero(a) o quien haga sus veces en Coordinación Zonal realizará la devolución de garantías haciendo uso de la ***Plantilla 3: Acta de entrega - recepción de garantías***, donde incluirá el detalle de la garantía original y sus renovaciones, este documento deberá ser suscrito por el(a) Tesorero(a) o quien haga sus veces en Coordinación Zonal y el Representante Legal de la Compañía que las solicita o la persona autorizada para el retiro.

4. DESCRIPCIÓN DE ACTIVIDADES

No.	Rol	Actividad	Descripción	Documento y/o Registro
1.	Coordinador(a) General de Asesoría Jurídica / Analista de compras públicas delegado(a) en Coordinación Zonal	Solicitar revisión de garantías del contrato	Solicita la revisión de las garantías del contrato. Ver lineamiento general No. 2, y lineamiento específico No. 1.	Correo electrónico institucional; Garantías; Copia del contrato.
2.	Director(a) Financiero(a) o quien haga sus veces en Coordinación Zonal	Disponer revisión de garantías de contrato	Dispone la revisión de las garantías del contrato. Ver lineamiento específico No. 1.	Correo electrónico institucional
3.	Tesorero(a) o quien haga sus veces en Coordinación Zonal	Revisar garantías y confirmar autenticidad	Revisa las garantías y confirma su autenticidad con la compañía aseguradora. Ver lineamiento general No. 3.	Garantías; Copia del contrato; Correo electrónico institucional.
4.	Tesorero(a) o quien haga sus veces en la Coordinación Zonal	¿Documentación de respaldo correcta?	Verifica que la documentación de respaldo se encuentre correcta. Si la documentación no se encuentra correcta continua en la actividad No. 4.1, caso contrario continua en la actividad No. 4.2.	No aplica
4.1	Tesorero(a) o quien haga sus veces en la Coordinación Zonal	Comunicar observaciones	Comunica las observaciones encontradas en la documentación de respaldo.	Correo electrónico institucional; Garantías;

No.	Rol	Actividad	Descripción	Documento y/o Registro
				Copia del contrato.
4.1.1.	Director(a) Financiero(a) o quien haga sus veces en Coordinación Zonal	Realizar devolución de documentación y solicitar ajustes	Realiza la devolución de la documentación de respaldo y solicita ajustes.	Correo electrónico institucional; Garantías; Copia del contrato.
4.1.2.	Coordinador(a) General de Asesoría Jurídica / Analista de compras públicas delegado(a) en Coordinación Zonal	Subsanar observaciones a documentación	Subsana las observaciones en la documentación de respaldo. Regresa a la actividad No. 1.	Correo electrónico institucional; Garantías; Copia del contrato.
4.2	Tesorero(a) o quien haga sus veces en la Coordinación Zonal	Gestionar suscripción de garantías	Gestiona la suscripción de las garantías. Ver lineamiento general No. 4 y lineamiento específico No. 2.	Correo electrónico institucional; Garantías suscritas; Copias de garantías suscritas distribuidas.
5.	Tesorero(a) o quien haga sus veces en la Coordinación Zonal	Registrar y custodiar garantías	Registra y custodia las garantías suscritas. Ver lineamiento específico No. 3.	Plantilla 1: Base de datos para el control de garantías vigentes; Expediente de custodia de garantías.
6.	Tesorero(a) o quien haga sus veces en la Coordinación Zonal	Solicitar registro contable de ingreso de garantías	Solicita el registro contable de ingreso de garantías. Ver	Correo electrónico institucional enviado;

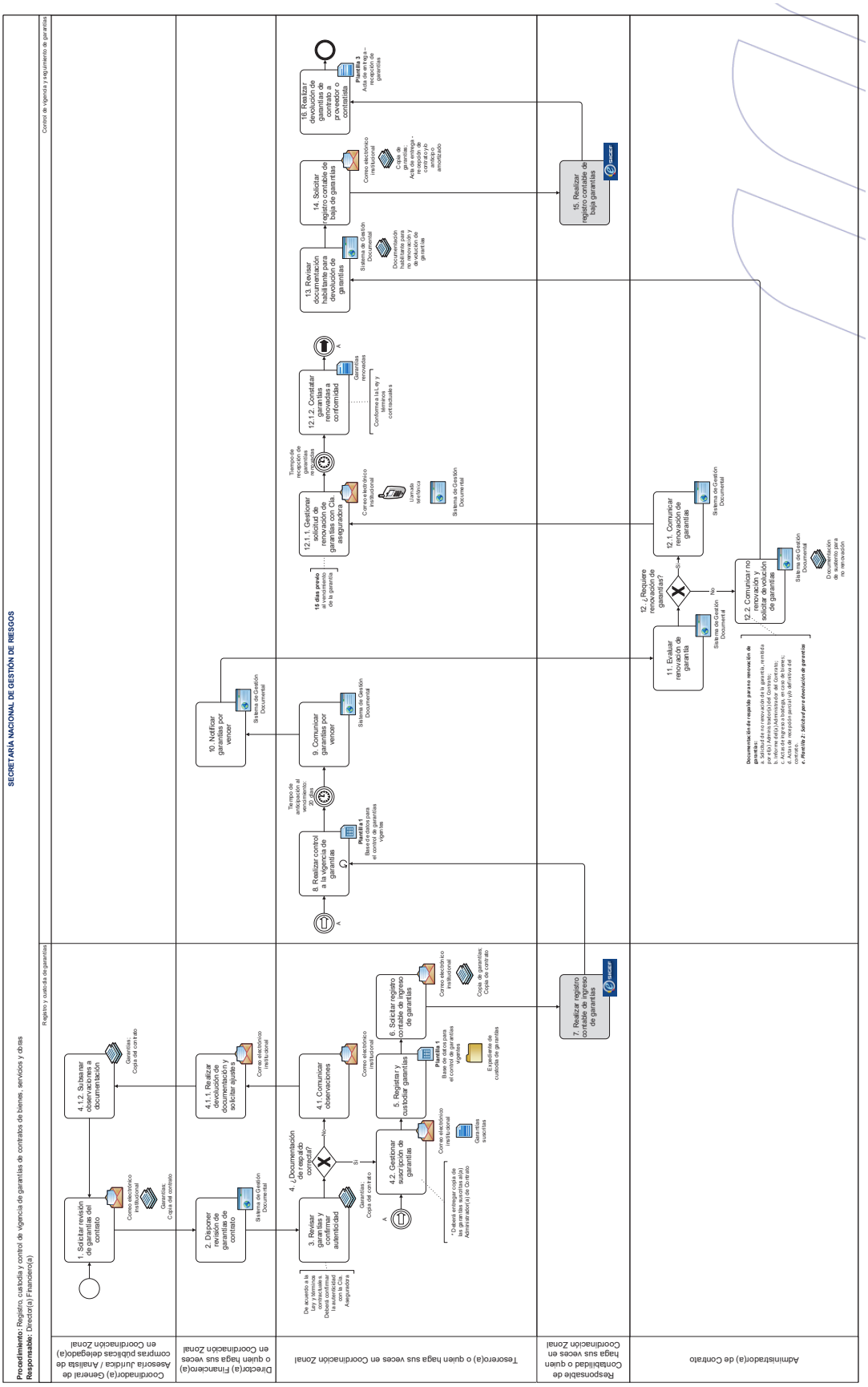
No.	Rol	Actividad	Descripción	Documento y/o Registro
			lineamiento específico No. 4.	Copia de garantías; Copia de contrato.
7.	Responsable de Contabilidad o quien haga sus veces en la Coordinación Zonal	Realizar registro contable de ingreso de garantías	Realiza registro contable de ingreso de garantías en el sistema financiero. Ver lineamiento específico No. 4.	Copia de garantías; Copia del contrato; Sistema Integrado de gestión financiera eSIGEF.
8.	Tesorero(a) o quien haga sus veces en la Coordinación Zonal	Realizar control a la vigencia de garantías	Realiza el control a la vigencia de las garantías de los contratos. Ver lineamiento específico No. 5.	Plantilla 1: Base de datos para el control de garantías vigentes
9.	Tesorero(a) o quien haga sus veces en la Coordinación Zonal	Comunicar garantías por vencer	Comunica las garantías que están por vencer. Ver lineamiento específico No. 5 y No. 6.	Memorando reasignado mediante Sistema de Gestión Documental
10.	Director(a) Financiero(a) o quien haga sus veces en Coordinación Zonal	Notificar garantías por vencer	Notifica garantías por vencer. Ver lineamiento específico No. 6.	Memorando enviado mediante Sistema de Gestión Documental
11.	Administrador(a) de Contrato	Evaluar renovación de garantías	Evalúa la necesidad de renovación de garantías del contrato. Ver lineamiento específico No. 6.	Memorando recibido mediante Sistema de Gestión Documental
12.	Administrador(a) de Contrato	¿Requiere renovación de garantías?	Determina si requiere la renovación de las garantías del	No aplica

No.	Rol	Actividad	Descripción	Documento y/o Registro
			contrato. Si requiere la renovación continúa en la actividad No. 12.1., caso contrario continúa en la actividad No. 12.2.	
12.1.	Administrador(a) de Contrato	Comunicar renovación de garantías	Comunica la renovación de las garantías del contrato.	Memorando enviado mediante Sistema de Gestión Documental
12.1.1.	Tesorero(a) o quien haga sus veces en la Coordinación Zonal	Gestionar solicitud de renovación de garantías con Cía. aseguradora	Gestiona la solicitud de renovación de garantías con la compañía aseguradora. Ver lineamiento específico No. 7.	Correo electrónico institucional; Llamada telefónica; Oficio enviado mediante Sistema de Gestión Documental.
12.1.2.	Tesorero(a) o quien haga sus veces en la Coordinación Zonal	Constatar garantías renovadas a conformidad	Constata las garantías renovadas a conformidad. Regresa a la actividad No.8.	Garantías renovadas
12.2.	Administrador(a) de Contrato	Comunicar no renovación y solicitar devolución de garantías	Comunica la no renovación y solicita la devolución de las garantías. Ver lineamiento general No. 5 y lineamiento específico No. 6	Memorando enviado mediante Sistema de Gestión Documental; Informe del(a) Administrador del Contrato;

No.	Rol	Actividad	Descripción	Documento y/o Registro
				Actas de ingreso a bodega, en caso de bienes; Actas de recepción parcial y/o definitiva del contrato; Plantilla 2: Solicitud para devolución de garantías.
13.	Tesorero(a) o quien haga sus veces en la Coordinación Zonal	Revisar documentación habilitante para devolución de garantías	Revisa la documentación habilitante para la devolución de las garantías del contrato. Ver lineamiento general No. 5 y No. 6; y, lineamiento específico No.8.	Oficio recibido mediante Sistema de Gestión Documental Informe del(a) Administrador del Contrato; Actas de ingreso a bodega, en caso de bienes; Actas de recepción parcial y/o definitiva del contrato; Plantilla 2: Solicitud para devolución de garantías.
14.	Tesorero(a) o quien haga sus veces en la Coordinación Zonal	Solicitar registro contable de baja de garantías	Solicita el registro contable de baja de garantías del contrato. Ver lineamiento específico No.9	Correo Institucional enviado; Copias de las garantías;

No.	Rol	Actividad	Descripción	Documento y/o Registro
				Acta de entrega - recepción de contrato y/o anticipo amortizado.
15.	Responsable de Contabilidad o quien haga sus veces en la Coordinación Zonal	Realizar registro contable de baja garantías	Realiza el registro contable de baja de garantías. Ver lineamiento específico No.9	Sistema Integrado de gestión financiera eSIGEF
16.	Tesorero(a) o quien haga sus veces en la Coordinación Zonal	Realizar devolución de garantías de contrato a proveedor o contratista	Realiza la devolución de las garantías del contrato al proveedor o contratista. Ver lineamiento general No. 6 y lineamiento específico No. 10.	Plantilla 3: Acta de entrega - recepción de garantías

5. DIAGRAMA DE FLUJO



6. ANEXOS

Plantilla:

- Plantilla 1: Base de datos para el control de garantías vigentes
- Plantilla 2: Solicitud para devolución de garantías
- Plantilla 3: Acta de entrega - recepción de garantías

Secretaría Nacional de Gestión de Riesgos

PLANTILLA No. 1
BASE DE DATOS PARA EL CONTROL DE GARANTÍAS VIGENTES

ORDEN	RUC	CONTRATISTA	Nº CONTRATO	DESCRIPCION	ASEGURADORA	No. DE POLIZA	TIPO DE POLIZA	SUMA ASEGURADA	FECHA DE VENCIMIENTO	ESTADO	OBSERVACIONES
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											
17											
18											
19											
20											
21											
22											
23											
24											
25											
26											
27											
28											
29											
30											

Plantilla No. 2: Solicitud para devolución de garantías

Samborondón, XX de XXXX de 20XX

Ing.
XXXX XXXX XX
Tesorera
Secretaría Nacional de Gestión de Riesgos

De mi consideración:

Por medio de la presente y en mi calidad de Administrador del Contrato/Orden de Compra No. 000-0000 cuyo objeto es **"----------",** informo a usted que con fecha dd-mm-aa se suscribió el acta de recepción definitiva o única, cumpliendo a entera satisfacción lo establecido en el contrato/orden de compra.

Por lo que acorde al artículo 263 del RLOSNCP solicito a usted proceda con la devolución de la Póliza No. 000000 por FIEL CUMPLIMIENTO DE CONTRATO por el valor de USD0,000.00 al contratista/proveedor.

Adicionalmente, solicito que la póliza del Buen Uso del Anticipo No.0000 por el valor de USD0,000.00 se devuelva, cuando este haya sido devengado en su totalidad.

La presente solicitud se realiza de acuerdo a lo indicado en el **REGLAMENTO GENERAL A LA LEY ORGÁNICA DEL SISTEMA NACIONAL DE CONTRATACIÓN PÚBLICA**:

"Artículo 263.- Devolución de garantías. - *Las garantías serán devueltas cuando se han cumplido todas las obligaciones que avalan.*

- *La garantía original de fiel cumplimiento del contrato se devolverá cuando se haya suscrito el acta de entrega recepción definitiva o única.*
- *La garantía original de buen uso del anticipo se devolverá cuando éste haya sido amortizado en su totalidad, conforme detalla el artículo 265".*
  (Art. 265.1 .- Anticipo devengado)

Para sustento se adjunta **ACTA DE ENTREGA RECEPCIÓN DEFINITIVA O ÚNICA**.

Particular que comunico para los fines pertinentes.

Atentamente,

Nombre y Apellido
C.I.
Administrador del Contrato No. 000-000

Plantilla No. 3: Acta de Entrega y Recepción de Garantías

Samborondón, XX de XXXX de 20XX

Ing.
XXXX XXXX XX
Tesorera
Secretaría Nacional de Gestión de Riesgos

De mi consideración:

Por medio de la presente y en mi calidad de Administrador del Contrato/Orden de Compra No. 000-0000 cuyo objeto es **"----------",** informo a usted que con fecha dd-mm-aa se suscribió el acta de recepción definitiva o única, cumpliendo a entera satisfacción lo establecido en el contrato/orden de compra.

Por lo que acorde al artículo 263 del RLOSNCP solicito a usted proceda con la devolución de la Póliza No. 000000 por FIEL CUMPLIMIENTO DE CONTRATO por el valor de USD0,000.00 al contratista/proveedor.

Adicionalmente, solicito que la póliza del Buen Uso del Anticipo No.0000 por el valor de USD0,000.00 se devuelva, cuando este haya sido devengado en su totalidad.

La presente solicitud se realiza de acuerdo a lo indicado en el **REGLAMENTO GENERAL A LA LEY ORGÁNICA DEL SISTEMA NACIONAL DE CONTRATACIÓN PÚBLICA**:

"Artículo 263.- Devolución de garantías. - *Las garantías serán devueltas cuando se han cumplido todas las obligaciones que avalan.*

- *La garantía original de fiel cumplimiento del contrato se devolverá cuando se haya suscrito el acta de entrega recepción definitiva o única.*
- *La garantía original de buen uso del anticipo se devolverá cuando éste haya sido amortizado en su totalidad, conforme detalla el artículo 265".*
  (Art. 265.1 .- Anticipo devengado)

Para sustento se adjunta **ACTA DE ENTREGA RECEPCIÓN DEFINITIVA O ÚNICA**.

Particular que comunico para los fines pertinentes.

Atentamente,

Nombre y Apellido
C.I.
Administrador del Contrato No. 000-000

SUPERINTENDENCIA DE BANCOS

RESOLUCIÓN Nro. SB-2025-02323

ROBERTO JOSÉ ROMERO VON BUCHWALD
SUPERINTENDENTE DE BANCOS

CONSIDERANDO:

Que el artículo 82 de la Constitución de la República del Ecuador, señala: *"El derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes.";*

Que el artículo 84 de la Carta Magna, establece: *"La Asamblea Nacional y todo órgano con potestad normativa tendrá la obligación de adecuar, formal y materialmente, las leyes y demás normas jurídicas a los derechos previstos en la Constitución y los tratados internacionales, y los que sean necesarios para garantizar la dignidad del ser humano o de las comunidades, pueblos y nacionalidades. En ningún caso, la reforma de la Constitución, las leyes, otras normas jurídicas ni los actos del poder público atentarán contra los derechos que reconoce la Constitución.";*

Que el numeral 6 del artículo 132 ibidem, dispone: *"(…) 6. Otorgar a los organismos públicos de control y regulación la facultad de expedir normas de carácter general en las materias propias de su competencia, sin que puedan alterar o innovar las disposiciones legales.";*

Que el artículo 213 de la Constitución de la República del Ecuador, señala que, *"Las superintendencias son organismos técnicos de vigilancia, auditoría, intervención y control de las actividades económicas, sociales y ambientales, y de los servicios que prestan las entidades públicas y privadas, con el propósito de que estas actividades y servicios se sujeten al ordenamiento jurídico y atiendan al interés general. Las superintendencias actuarán de oficio o por requerimiento ciudadano. Las facultades específicas de las superintendencias y las áreas que requieran del control, auditoría y vigilancia de cada una de ellas se determinarán de acuerdo con la ley. (…)";*

Que artículo 309 de la Carta Magna, señala que: *"El sistema financiero nacional se compone de los sectores público, privado, y del popular y solidario, que intermedian recursos del público. Cada uno de estos sectores contará con normas y entidades de control específicas y diferenciadas, que se encargarán de preservar su seguridad, estabilidad, transparencia y solidez. Estas entidades serán autónomas. Los directivos de las entidades de control serán responsables administrativa, civil y penalmente por sus decisiones.";*

Que el artículo 14 numeral 2 del Código Orgánico Monetario Financiero, señala: *"Corresponde a la Junta de Política y Regulación Financiera lo siguiente: (…) 2. Emitir las regulaciones que permitan mantener la integralidad, solidez, sostenibilidad y estabilidad de los sistemas financiero nacional, de valores, seguros y servicios de atención integral de salud prepagada en atención a lo previsto en el artículo 309 de la Constitución de la República del Ecuador. (…)";*

Que El artículo 14. 1 numeral 27 ibidem, establece: ***"****Para el desempeño de sus funciones, la Junta de Política y Regulación Financiera tiene que cumplir los siguientes deberes y ejercer las siguientes facultades: (…) 27. Ejercer las demás funciones, deberes y facultades que le asigne este Código y la ley. (…)";*

Que El artículo 60 del Código Orgánico Monetario y Financiero, dispone que la finalidad de la Superintendencia de Bancos es la siguiente: ***"****La Superintendencia de Bancos efectuará la vigilancia, auditoría, intervención, control y supervisión de las actividades financieras que ejercen las entidades públicas y privadas del sistema financiero nacional, con el propósito de que estas actividades atiendan al interés general, se sujeten al ordenamiento jurídico, y de evitar, prevenir y desincentivar prácticas fraudulentas y prohibidas con el fin de proteger los derechos de los usuarios y/o clientes del sistema financiero nacional.";*

Que el numeral 7 del artículo 62 del Código Orgánico Monetario y Financiero, establece que, *"(…) 7. Velar por la estabilidad, solidez y correcto funcionamiento de las entidades sujetas a su control y, en general, vigilar que cumplan las normas que rigen su funcionamiento, las actividades financieras que presten, mediante la supervisión permanente preventiva extra situ y visitas de inspección in situ, sin restricción alguna, de acuerdo a las mejores prácticas, que permitan determinar la situación económica y financiera de las entidades, el manejo de sus negocios, evaluar la calidad y control de la gestión de riesgo y verificar la veracidad de la información que generan; (…)";*

Que el último inciso del artículo 62 ibidem, señala que, *"La superintendencia, para el cumplimiento de estas funciones, podrá expedir todos los actos y contratos que fueren necesarios. Asimismo, podrá expedir las normas en las materias propias de su competencia, sin que puedan alterar o innovar las disposiciones legales ni las regulaciones que expida la Junta de Política y Regulación Monetaria y Financiera.";*

Que el artículo 99 ut supra, determina: ***"****Son medios de pago los cheques, billeteras electrónicas y los medios de pago electrónicos que comprenden las transferencias para pago o cobro, las tarjetas de crédito, débito, prepago, recargables o no, encaje y seguro de depósito; las billeteras electrónicas con la categoría de banca enteramente digital que cumplan con el fondo y reservas de liquidez, encaje y seguro de depósito, que cumplan con el fondo y reservas de liquidez, y, otros medios de pago centrados en la tecnología, previa licencia de la Superintendencia de Bancos y en los términos de que determine y regule la Junta de Política y Regulación Monetaria.";*

Que el numeral 4 y 5 artículo 162 ibidem, define: *"El sector financiero privado está compuesto por las siguientes entidades:*

(…)

4. De servicios financieros tecnológicos: son las entidades que desarrollan actividades financieras centradas en la tecnología digital y electrónica o que realicen actividades que representen riesgo financiero según lo determinado por la Junta de Política y Regulación Financiera; salvo que tengan relación con el sistema de pagos, cuya regulación le corresponde a la Junta de Política y Regulación Monetaria y su control le corresponde a el Banco Central.

5. Sociedades especializadas de depósitos y pagos electrónicos: son entidades cuyo objeto único es la recepción de recursos con fines exclusivos de facilitar pagos y traspasos de recursos mediante los medios de pago electrónicos autorizados; y, enviar y recibir giros financieros de conformidad con la regulación que emita la Junta de Política y Regulación Monetaria. Los requisitos para su constitución serán regulados por la Junta de Política y Regulación Financiera controlados por el Banco Central del Ecuador, quienes serán los encargados de emitir la información correspondiente en caso de requerir

intervención de supervisión o sanción por parte de la Superintendencia de Compañías, Valores y Seguros con la Superintendencia de Bancos, Superintendencia de Economía Popular y Solidaria, según corresponda y que serán los encargados de proceder conforme lo disponga la Ley. A las sociedades especializadas de depósitos y pagos electrónicos se les aplicarán todas las disposiciones correspondientes a las de servicios financieros tecnológicos.";

Que el artículo 439. 1 del Código Orgánico Monetario y Financiero, dispone: *"Son entidades de servicios financieros tecnológicos las empresas que desarrollan actividades financieras centradas en la tecnología, entre las que se encuentran las siguientes:*

1. Concesión digital de créditos: Son empresas que ofrecen productos de crédito a través de plataformas electrónicas, sin que esto implique captación de recursos del público con finalidad de intermediación.
2. Neobancos: Son aquellas entidades financieras dedicadas a ofrecer servicios de intermediación bancaria de forma digital conforme a los nuevos avances tecnológicos. Deberán cumplir con todas las regulaciones y disposiciones correspondientes a la actividad bancaria tradicional.
3. Finanzas personales y asesoría financiera: Administración de finanzas personales, comparadores y distribuidores de productos financieros, asesores automatizados y planeación financiera, siempre que su operación esté apoyada en la tecnología.
4. Otros que sean determinados por la Junta de Política y Regulación Financiera.";

Que el artículo 439. 2 ut supra, establece: *"Los servicios financieros tecnológicos serán prestados por personas jurídicas constituidas como sociedades anónimas cuya vida jurídica se regirá por las disposiciones de la Ley de Compañías. Su objeto social será específico y exclusivo para la realización de Actividades Fintech y no podrá contener actividades distintas.";*

Que el artículo 439. 4 del Código Orgánico Monetario y Financiero, dispone: *"Las compañías, para prestar los servicios financieros tecnológicos, deberán calificarse ante la Superintendencia de Bancos, la Superintendencia de Economía Popular y Solidaria o el Banco Central, según corresponda.*

Dichos organismos de control establecerán los requerimientos para su calificación, supervisión y control. En los mismos deberán observar criterios diferenciados según los riesgos financieros y tecnológicos que cada empresa genere.

Los criterios diferenciados según los riesgos serán elaborados por expertos en economía y seguridad de la información determinados por el órgano regulador competente.";

Que el artículo 439.6 ut supra, establece: *"El control societario de estas compañías está a cargo de la Superintendencia de Compañías, Valores y Seguros. La supervisión y control de aquellas compañías que desarrollen actividades financieras de alto riesgo le corresponderá a la Superintendencia de Bancos, a la Superintendencia de Economía Popular y Solidaria o al Banco Central del Ecuador, según sus competencias. La determinación de qué actividades financieras basadas en tecnología representan un alto riesgo le corresponderá a la Junta de Política y Regulación Financiera.";*

Que el artículo 5 de la Ley para el Desarrollo Servicios Financieros Tecnológicos, define: *"Para efectos de esta Ley se entenderá que las Actividades Fintech implican el desarrollo, prestación, uso u oferta de:*

i) Infraestructuras tecnologías para canalizar medios de pago;
ii) Servicios financieros tecnológicos;
iii) Sociedades especializadas de depósitos y pagos electrónicos;
iv) Servicios tecnológicos del mercado de valores; y,
v) Servicios tecnológicos de seguros.";

Que el artículo 7 ut supra, establece: *"Para ejercer Actividades Fintech en Ecuador, las compañías deberán cumplir con los siguientes requisitos:*

7.1. Estar debidamente constituidas como sociedades nacionales, o estar autorizadas como sucursales de compañías extranjeras en Ecuador. Adicionalmente se requerirá autorización para la prestación de cualquiera de las Actividades Fintech establecidas en esta Ley, por la Superintendencia de Bancos, la Superintendencia de Economía Popular y Solidaria, la Superintendencia de Compañías, Valores y Seguros o el Banco Central del Ecuador, según corresponda.
7.2. El objeto social de las antedichas compañías nacionales, o sucursales de compañías extranjeras, será específico y exclusivo para la realización de Actividades Fintech y no podrá contener actividades distintas.";

Que el artículo 8 de la Ley para el Desarrollo Servicios Financieros Tecnológicos, define: *"Las compañías fintech estarán reguladas por la Junta de Política y Regulación Monetaria y Junta de Política y Regulación Financiera, según corresponda; y, supervisadas y controladas por el Banco Central del Ecuador, la Superintendencia de Compañías, Valores y Seguros, la Superintendencia de Bancos o la Superintendencia de Economía Popular y Solidaria, en el ámbito de sus competencias y según la regulación que se emita para el efecto.";*

Que el artículo 4 del Reglamento a la Ley para el Desarrollo Servicios Financieros Tecnológicos**,** establece: *"La calificación, supervisión y control de las compañías que desarrollen Actividades Fintech le corresponderá al Banco Central del Ecuador, a la Superintendencia de Compañías. Valores y Seguros, o a la Superintendencia de Bancos, en el ámbito de sus competencias y según la regulación que se emita para el efecto. Dichas entidades deberán crear direcciones o intendencias dedicadas a la supervisión y control de las compañías que desarrollen Actividades Fintech. Así mismo, deberán, oportunamente, capacitar al personal que estará dedicado a las tareas de supervisión y control de Actividades Fintech.*

La creación de direcciones o intendencias estarán sujetas a la disponibilidad presupuestaria, previo dictamen favorable del ente rector de las finanzas públicas.";

Que el artículo 8 del Reglamento ut supra, dispone: ***"****Los entes de regulación, deberán emitir la regulación respectiva en materia de la seguridad de la información y ciberseguridad.".*

Que el artículo 8 de la Resolución Nro. JPRF-F-2023-076 de 11 de septiembre de 2023 de las Entidades de Concesión Digital de Créditos, dispone: "*La supervisión y control de estas entidades le corresponderá a la Superintendencia de Bancos con un enfoque de gestión de riesgos.";*

Que el artículo 26 de la Resolución ibidem, establece: *"Las entidades establecerán una Unidad de Riesgos que deberá contar de manera permanente con los recursos humanos, materiales y*

tecnológicos necesarios y suficientes para ejecutar sus funciones. La Unidad estará compuesta por personal capacitado que demuestre un sólido conocimiento y experiencia en el manejo y control de riesgos, y que sea capaz de comprender las metodologías y procedimientos de la entidad para identificar, medir, controlar/mitigar y supervisar los riesgos presentes y futuros.

El número de funcionarios de la Unidad de Riesgos deberá guardar proporción con la naturaleza, complejidad y volumen de los negocios, operaciones y actividades desarrolladas por la entidad.";

Que el artículo 29 de la Resolución Nro. JPRF-F-2023-076 de 11 de septiembre de 2023 de las Entidades de Concesión Digital de Créditos, dispone: "*El riesgo operativo se refiere a la probabilidad de pérdidas derivadas de fallos en procesos, personas, tecnología de la información o eventos externos; incluye además el riesgo legal, que se relaciona con pérdidas por no cumplir adecuadamente con disposiciones legales, normativas o decisiones administrativas. Esta inobservancia puede deberse a errores, negligencia o mala interpretación; también se puede originar por una redacción deficiente en contratos o la incorrecta especificación de derechos entre partes; sin embargo, no abarca riesgos sistémicos, estratégicos ni de reputación.";*

Que el artículo 30 de la Resolución ut supra, define: "*Las entidades deben establecer políticas y metodologías claras para la gestión del riesgo operativo, las cuales deberán observar los procesos de identificación, medición, control, y monitoreo del riesgo operativo en todas sus operaciones y negocios; para ello, es esencial realizar evaluaciones continuas del riesgo operativo, incluidos los proyectos actuales y nuevos productos.";*

Que el artículo 31 de la Resolución ibidem, establece: "*Las entidades tienen la obligación de identificar riesgos operativos basándose en diferentes categorías como línea de negocio, tipo de evento y factor de riesgo. Para ello, deben aplicar una metodología adecuadamente documentada y aprobada, utilizando herramientas como autoevaluaciones, mapas de riesgos, indicadores y tablas de control, entre otras.*

Para los eventos de riesgo operativo se considerarán al menos:

a. Fraude interno;
b. Fraude externo;
c. Prácticas laborales y seguridad del ambiente de trabajo;
d. Prácticas relacionadas con los clientes, los productos y el negocio;
e. Daños a los activos físicos;
f. Interrupción del negocio por fallas en la tecnología de la información; y,
g. Deficiencias en el diseño y/o la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros.";

Que el artículo 32 de la Resolución Nro. JPRF-F-2023-076 de 11 de septiembre de 2023 de las Entidades de Concesión Digital de Créditos, define: "*La cuantificación de riesgos operativos se determinará sobre la base de su probabilidad de ocurrencia e impacto de los posibles eventos de riesgo operativo. Esta información proporciona a la Junta General de Accionistas o al Directorio y al representante legal una perspectiva precisa de la exposición de la entidad al riesgo operativo, facilitando la toma de decisiones informadas para su gestión.";*

Que el artículo 33 de la Resolución ut supra, dispone: "*Las entidades deben establecer y revisar periódicamente planes de mitigación, que podrían involucrar ajustes en estrategias, políticas, procesos y procedimientos. Esto también podría requerir la implementación o revisión de límites de riesgo, controles, planes de continuidad de negocio, términos de seguros y servicios de terceros, entre otros. Estos controles deben integrarse plenamente en las operaciones diarias de la entidad, garantizando respuestas rápidas a posibles incidencias de riesgo operativo. Además, las entidades deben establecer mecanismos adicionales para enfrentar las fuentes de riesgos no específicamente mencionados en esta norma, pero que estén relacionados con factores del riesgo operativo.";*

Que el artículo 34 de la Resolución ibidem, establece: "*Las entidades tienen la obligación de monitorear continuamente los riesgos operativos asociados a sus procesos y nivel de exposición. Para asegurar una gestión eficaz, deben contar con un sistema organizado de reportes que proporcione información relevante y oportuna para la toma de decisiones.";*

Que el artículo 42 de la Resolución Nro. JPRF-F-2023-076 de 11 de septiembre de 2023 de las Entidades de Concesión Digital de Créditos, define: "*Las entidades deben gestionar proactivamente el riesgo legal, identificando, midiendo, controlando, mitigando y monitoreando potenciales eventos que conlleven a pérdidas. Las entidades deben desarrollar planes acordes al ordenamiento jurídico ecuatoriano.";*

Que la disposición general segunda de la Resolución ut supra, establece: "*Las entidades de concesión digital de créditos aplicarán lo establecido en la norma que determina la relación entre el patrimonio técnico total y los activos y contingentes ponderados por riesgo para las entidades del sistema financiero público y privado, una vez que la Superintendencia de Bancos emita la norma que disponga el régimen contable respectivo. (…)";*

Que el artículo 60 de la Resolución Nro. JPRF-F-2025-0155 de 20 de mayo de 2025 de las Entidades de Administración de Finanzas Personales y/o Asesoría Financiera, establece: "*La supervisión y control de las entidades de administración de finanzas personales estará a cargo de la Superintendencia de Bancos. La Superintendencia de Bancos establecerá los estándares de gobierno corporativo y de gestión de riesgos que deberán observar dichas entidades, incluyendo lineamientos específicos sobre ciberseguridad y seguridad de la información.";*

Que el artículo 63 de la Resolución ibidem, define: "*Las entidades que presten servicios de administración de finanzas personales deberán implementar un sistema de gestión de riesgos para la identificación, medición, control y monitoreo de forma continua de los riesgos a los que están expuestas en el desarrollo de sus actividades y sobre las recomendaciones que realicen a los usuarios.*

Este sistema cubrirá, como mínimo, los riesgos operativos con énfasis en la seguridad de la información, y de lavado de activos y financiamiento de delitos, como el terrorismo, sin perjuicio de otros que determine la Superintendencia de Bancos.

Para la gestión de riesgos se contará con personal idóneo, con experiencia o formación en finanzas, economía, administración de riesgos o áreas afines, y con manejo de los recursos tecnológicos suficientes para el cumplimiento de sus funciones.";

Que el artículo 65 de la Resolución ut supra, establece: "*Las entidades administradoras de finanzas personales deben contar con un comité de gestión de riesgos, que será responsable de aprobar las políticas, procedimientos y manuales de riesgos, así como de evaluar periódicamente la efectividad de los controles implementados.*

La Superintendencia de Bancos, en función del tamaño, volumen de operaciones y naturaleza jurídica de la entidad, podrá establecer requisitos diferenciados para la conformación del Comité de Gestión de Riesgos, así como los plazos para sus sesiones y demás competencias.";

Que el artículo 66 de la Resolución Nro. JPRF-F-2025-0155 de 20 de mayo de 2025 de las Entidades de Administración de Finanzas Personales y/o Asesoría Financiera, define: "*Las entidades de administración de finanzas personales identificarán y clasificarán los eventos de riesgo operativo con base en factores de procesos, personas, tecnología e incidentes externos, documentando sus procedimientos para la prevención y tratamiento de estos eventos.*

Estas entidades deberán gestionar su riesgo operativo a través de una matriz que mida la probabilidad e impacto de la ocurrencia de un evento de riesgo, determinando los recursos que quedarían expuestos ante su materialización. El valor estimado por la ocurrencia de eventos relacionados con la administración de portafolios de inversión conforme a instrucciones del usuario y los derivados de la administración de presupuesto personal deberá encontrarse asegurada por una póliza de seguro de responsabilidad civil.

Las entidades deberán contar con sistemas de alerta temprana y manuales de procedimientos que incluyan los controles internos, planes de contingencia y mecanismos de reporte de incidentes.

Todas las operaciones, particularmente las que se realicen de manera automatizada o a través de algoritmos, deberán tener trazabilidad y registro que permitan una auditoría posterior.

Las entidades de administración de finanzas personales deberán gestionar el riesgo legal y operativo relacionado con sus intermediarios financieros y sus custodios de valores.";

Que el artículo 67 de la Resolución ut supra, establece: "*Las entidades de administración de finanzas personales implementarán políticas y procedimientos alineados con estándares internacionales de seguridad de la información, protegiendo la confidencialidad, integridad y disponibilidad de los datos de los usuarios y de la propia entidad.*

Se designará a un responsable de la seguridad de la información, encargado de monitorear y evaluar de forma continua la eficacia de los controles de ciberseguridad.

En caso de incidentes de seguridad que afecten la operatividad de los servicios o la protección de los datos personales, se deberá notificar de forma inmediata a la Superintendencia de Bancos y adoptar las medidas de mitigación que correspondan.";

Que el artículo 68 de la Resolución ibidem, dispone: "*Las entidades de administración de finanzas personales deberán contar con un plan de continuidad del negocio que incluya estrategias de recuperación, puntos de restauración de datos y asignación de responsables para el caso de incidentes que interrumpan sus actividades. En el marco del plan de continuidad se realizarán pruebas*

periódicas de su efectividad con una periodicidad mínima de un (1) año; y sus resultados serán remitidos a la Superintendencia de Bancos.

Dicho plan se actualizará al menos una vez al año o cuando se produzcan cambios relevantes en la estructura, tecnología o personal de la entidad.";

Que el artículo 69 de la Resolución Nro. JPRF-F-2025-0155 de 20 de mayo de 2025 de las Entidades de Administración de Finanzas Personales y/o Asesoría Financiera, define: "*Las entidades administradoras de finanzas personales estarán sujetas a las disposiciones establecidas en el presente capítulo en materia de prevención del riesgo de lavado de activos y financiamiento de delitos, debiendo implementar los mecanismos y procedimientos necesarios para asegurar el cumplimiento integral de esta normativa.*

Estas entidades estarán sujetas al cumplimiento de la debida diligencia, conforme a la normativa vigente en materia de prevención de lavado de activos y financiamiento de otros delitos.";

Que a través de la Resolución Nro. JPRF-F-2025-0155 de 20 de mayo de 2025, la Junta de Política y Regulación Financiera incorporó la Sección III "De las entidades que prestan servicios de administración de finanzas personales y/o asesoría financiera" a continuación de la Sección II "Entidades de Concesión Digital de Crédito", Capítulo LXII "Norma que regula las entidades de Servicios Financieros Tecnológicos", Título II "Sistema Financiero Nacional", Libro I "Sistema Monetario y Financiero" de la Codificación de Resoluciones Monetarias, Financieras, de Valores y Seguros;

Que con Memorando Nro. SB- INJ-2025-0574-M de 29 de mayo de 2025, la Intendencia Nacional Jurídica pone en conocimiento del Intendente General la Resolución Nro. JPRF-F-2025-0155 de 20 de mayo de 2025, mediante la cual se dispone a la Superintendencia de Bancos emitir la norma de control para las entidades de administración de finanzas personales y/o asesoría financiera en un término de noventa (90) días, por lo que solicitó a la Intendencia General se socialicé a las áreas pertinentes el contenido de la Resolución Nro. JPRF-F-2025-0155 de 20 de mayo de 2025, a fin de que se puedan desarrollar las actividades a cumplir en la mencionada norma, resaltando que la fecha tentativa para culminar dichas actividades es el 25 de septiembre de 2025, de acuerdo con el término señalado por la Junta de Política y Regulación Financiera;

Que a través de Memorando Nro. SB-IG-2025-0216-M de 09 de junio de 2025, la Intendencia General instruye a la Intendencia Nacional de Control del Sector Financiero Privado, Intendencia Nacional de Riesgos y Estudios, Intendencia Nacional Jurídica, el cumplimiento de la Resolución Nro. JPRF-F-2025-0155 de 20 de mayo de 2025, en los plazos establecidos y de acuerdo con sus competencias y responsabilidades y, dispone a la Dirección Nacional de Desarrollo y Monitoreo la coordinación y acompañamiento a cada una de las áreas intervinientes a fin de cumplir con las actividades y los términos legales establecidos por la Junta Política y Regulación Financiera. Así también, como de consolidar y remitir a la Intendencia General reportes de avances mensuales que elaborarán las áreas responsables del cumplimiento de las actividades establecidas;

Que del 03 al 09 de septiembre de 2025, se llevaron a cabo las mesas de trabajo con la presencia de delegados de la Intendencia Nacional de Control del Sector Financiero Privado, Intendencia Nacional de Riesgos y Estudios, Coordinación General de Tecnologías de la Información y Comunicación,

Dirección de Trámites Legales, Dirección de Normativa, y la Dirección de Desarrollo y Monitoreo, para la construcción de las propuestas de norma que conllevan el cumplimiento de la Resolución Nro. JPRF-F-2025-0155 de 20 de mayo de 2025;

Que a través de Memorando Nro. SB-INRE-2025-0547-M de 17 de septiembre de 2025, la Intendencia Nacional de Riesgos y Estudios, emite el informe técnico con la propuesta de creación del "Capítulo XI "Norma de control para la gestión integral y administración de riesgos de las entidades de servicios financieros tecnológicos" concluyendo en la necesidad de dotar a este sector emergente de un marco normativo de supervisión y control, que permita gestionar de manera proporcional y efectiva los riesgos operativos, tecnológicos, legales y de ciberseguridad derivados de la innovación tecnológica;

Que mediante Memorando Nro. SB-INJ-2025-1051-M de 19 de septiembre de 2025, la Intendencia Nacional Jurídica, emite el informe jurídico con criterio favorable para la creación del Capítulo XI "Norma de control para la gestión integral y administración de riesgos de las entidades de servicios financieros tecnológicos" del Título IX "De la gestión y administración de riesgos", del Libro I "Normas de control para las entidades de los sectores financiero público y privado" de la Codificación de las Normas de la Superintendencia de Bancos;

Que con Memorando Nro. SB-IG-2025-0329-M de 25 de septiembre de 2025, el Intendente General, remite al Superintendente de Bancos, la propuesta de reforma del Capítulo V de la "Norma de calificación, supervisión y control para las entidades de servicios financieros tecnológicos; y, de la emisión de la licencia para el ejercicio de las actividades Fintech de las sociedades especializadas de depósitos y pagos electrónicos", del Título II "De la constitución y emisión de la autorización para el ejercicio de las actividades financieras y permisos de funcionamiento de las entidades de los sectores financieros público y privado"; y la creación del Capítulo I "Norma para la supervisión y control de las entidades de servicios financieros tecnológicos; y, de las actividades Fintech de las sociedades especializadas de depósitos y pagos electrónicos" dentro del Título XXI "De la supervisión y control de las entidades de servicios financieros tecnológicos", del Libro I "Normas de control para las entidades de los sectores financieros público y privado" de la Codificación de las Normas de la Superintendencia de Bancos;

Que mediante acción de personal Nro. 0046 de 28 de enero de 2025, se me designó Superintendente de Bancos; y, por ende, máxima autoridad de este Organismo de Control; y,

En ejercicio de las atribuciones constitucionales y legales conferidas en el Código Orgánico Monetario y Financiero; y la Codificación de Resoluciones Monetarias, Financieras, de Valores y Seguros,

RESUELVE:

ARTÍCULO UNO.- Crear el Capítulo XI "Norma de control para la gestión integral y administración de riesgos de las entidades de servicios financieros tecnológicos", dentro del Título IX **"**De la gestión y administración de riesgos", Libro I "Normas de control para las entidades de los sectores financieros público y privado" de la Codificación de las Normas de la Superintendencia de Bancos, con el siguiente texto:

"CAPÍTULO XI.- NORMA DE CONTROL PARA LA GESTIÓN INTEGRAL Y ADMINISTRACIÓN DE RIESGOS DE LAS ENTIDADES DE SERVICIOS FINANCIEROS TECNOLÓGICOS

SECCIÓN I.- DISPOSICIONES GENERALES

ARTÍCULO 1.- Objeto. *La presente norma tiene por objeto establecer los lineamientos para la gestión integral de riesgos aplicables a las entidades de servicios financieros tecnológicos, con el fin de salvaguardar la estabilidad financiera, la continuidad operativa y la protección al usuario.*

ARTÍCULO 2.- Ámbito de aplicación. *La presente norma será de cumplimiento obligatorio para las entidades de servicios financieros tecnológicos controladas por la Superintendencia de Bancos.*

Sin perjuicio de lo anterior, en lo relativo a sistemas y servicios de pago, las entidades observarán la normativa del Banco Central del Ecuador; y, en materia de protección de datos personales, cumplirán la Ley Orgánica de Protección de Datos Personales y las directrices de la autoridad competente.

ARTÍCULO 3.- Principios. *La gestión integral de riesgos de las entidades de servicios financieros tecnológicos se regirá por los siguientes principios:*

1. ***Proporcionalidad.*** *Las políticas, procesos, procedimientos y metodologías deberán adecuarse al tamaño, complejidad y volumen de operaciones de la entidad partiendo de una línea base que esta normativa establezca;*

2. ***Integralidad.*** *La gestión de riesgos abarcará todos los procesos, actividades y operaciones de la entidad, incluidas aquellas tercerizadas;*

3. ***Transparencia.*** *La información sobre riesgos y controles deberá estar debidamente documentada y disponible para la Superintendencia de Bancos;*

4. ***Innovación responsable.*** *Los servicios financieros tecnológicos deberán gestionarse con enfoque prudencial, mitigando riesgos inherentes a la digitalización; y,*

5. ***Protección al usuario.*** *Todas las decisiones en materia de gestión integral y administración de riesgos deberán priorizar la seguridad, confianza y continuidad de los servicios a los usuarios.*

ARTÍCULO 4. - Definiciones. *Para efectos de esta norma, se entenderá por:*

1. ***Actividad.*** *Es el conjunto de tareas que ejecutan las entidades controladas.*

2. ***Administración de la continuidad del negocio.*** *Es un proceso permanente que garantiza la continuidad de las operaciones de las entidades de servicios financieros tecnológicos, a través del mantenimiento efectivo de un sistema de gestión de continuidad del negocio.*

3. ***Apetito al riesgo.*** *Es el nivel de exposición al riesgo operativo, definido por la entidad de servicios financieros tecnológicos, que está dispuesta a asumir o aceptar, en el desarrollo de sus operaciones con la finalidad de alcanzar sus objetivos estratégicos.*

4. ***Canales electrónicos.*** *Se refiere a todas las vías o formas a través de las cuales los usuarios pueden efectuar transacciones con las entidades de servicios financieros tecnológicos,*

mediante el uso de elementos o dispositivos electrónicos o tecnológicos, utilizando o no tarjetas, conforme a los tipos de canales (tabla 107) definidos en el manual de tablas de la normativa vigente de la Superintendencia de Bancos.

5. ***Causa raíz.*** *Es la causa principal que genera un incidente o problema; su identificación permite aplicar soluciones adecuadas, prevenir y resolver sistemáticamente la ocurrencia de un incidente o problema, con el objetivo de evitar futuras ocurrencias.*
6. ***Ciberseguridad.*** *Conjunto de medidas de protección de la infraestructura tecnológica y de la información, a través del tratamiento de las amenazas que ponen en riesgo la información procesada por los diferentes componentes tecnológicos interconectados.*
7. ***Cliente/Usuario.*** *Es la persona natural o jurídica que contrata los servicios prestados por las entidades de servicios financieros tecnológicos.*
8. ***Confidencialidad.*** *Es un principio y una práctica que se refiere a la protección y resguardo de la información sensible o privada para evitar su acceso o divulgación no autorizada.*
9. ***Cumplimiento.*** *Se refiere a la observancia y aplicación de las leyes, reglamentos y demás normativa, así como los acuerdos contractuales en los procesos, actividades y operaciones a los que las entidades de servicios financieros tecnológicos están sujetas.*
10. ***Datos.*** *Es cualquier forma de registro sea este electrónico, óptico, magnético, impreso o en otros medios, susceptible de ser capturado, almacenado, procesado y distribuido.*
11. ***Datos personales crediticios.*** *Datos que integran el comportamiento económico de personas naturales, para analizar su capacidad financiera.*
12. ***Datos personales sensibles.*** *Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.*
13. ***Disponibilidad.*** *Es el atributo de que los usuarios autorizados tienen acceso a la información cada vez que lo requieran a través de los medios que satisfagan sus necesidades.*
14. ***Evento de riesgo operativo.*** *Es el hecho que deriva en pérdidas para las entidades de servicios financieros tecnológicos, originado por fallas o insuficiencias en los factores de riesgo operativo.*
15. ***Factor de riesgo operativo.*** *Es la causa primaria o el origen de un evento de riesgo operativo. Los factores son: procesos, personas, tecnología de la información y eventos externos.*
16. ***Indicadores Claves de Riesgo.*** *Es una métrica que permite monitorear la exposición a un determinado riesgo, y ayudan a tomar acciones oportunas en el caso de desviaciones.*
17. ***Incidente.*** *Es una interrupción no planificada de un servicio o la reducción de su calidad, que afecta el normal funcionamiento de sus servicios.*
18. ***Infraestructura tecnológica.*** *Conjunto de elementos tecnológicos agrupados y organizados cuya función es soportar las operaciones de una entidad.*
19. ***Integridad.*** *Es el atributo de mantener la totalidad y exactitud de la información y de los métodos de procesamiento.*
20. ***Línea de negocio.*** *Es una especialización del negocio que agrupa procesos encaminados a generar productos y servicios especializados para atender un segmento del mercado objetivo, definido en la planificación estratégica de la entidad de servicios financieros tecnológicos.*
21. ***Perfil de Riesgo Operativo.*** *Es el nivel del riesgo de la entidad de servicios financieros tecnológicos que refleja la naturaleza y magnitud de los riesgos operativos a los que está expuesto.*

22. ***Plan de continuidad del negocio.*** *Es el conjunto de procedimientos que orientan a las entidades a mantener su operatividad en el caso de que ocurran interrupciones que afecten sus servicios.*
23. ***Problema.*** *Consecuencia de uno o varios incidentes críticos o un incidente que se repite muchas veces y por ello se debe encontrar su causa raíz.*
24. ***Proceso crítico.*** *Es el conjunto de actividades indispensables para la continuidad del negocio y las operaciones de la entidad de servicios financieros tecnológicos, y cuya falta de identificación o aplicación deficiente puede generarle un impacto negativo.*
25. ***Protección de datos.*** *Son las medidas técnicas, organizativas, legales y de cualquier otra índole, que sean necesarias, para que el tratamiento de los datos sea utilizado exclusivamente para el propósito con el que fueron solicitados y/o autorizados, de conformidad con la ley vigente para el efecto.*
26. ***Proveedor crítico.*** *Tercero cuya falla pueda generar un incidente o impedir el cumplimiento de los tiempos y puntos de recuperación objetivo RTO/RPO aprobados.*
27. ***Punto de recuperación objetivo (RPO).*** *Es la cantidad máxima aceptable de pérdida de los datos medidos en el tiempo.*
28. ***Resiliencia Operativa.*** *Capacidad de una entidad de servicios financieros tecnológicos para seguir entregando los servicios críticos durante eventos disruptivos; esta capacidad le permite a la entidad identificar y protegerse de amenazas y potenciales fallas, respondiendo y adaptándose a ellas; así como, recuperarse y aprender de los eventos disruptivos con la finalidad de minimizar su impacto hacia el futuro en la entrega de los servicios críticos.*
29. ***Seguridad de la información.*** *Son los mecanismos adoptados por la entidad que le permiten preservar la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella, incluye los aspectos relacionados con ciberseguridad.*
30. ***Servicios en la nube.*** *Es la provisión de servicios informáticos accesibles a través de la internet, estos pueden ser de infraestructura, plataforma y/o software.*
31. ***Servicio crítico.*** *Proceso o funcionalidad cuya indisponibilidad impide la ejecución de transacciones, el acceso a cuentas, la sincronización de datos financieros, la emisión de órdenes o la continuidad del negocio dentro de los tiempos y puntos de recuperación objetivo (RTO/RPO) aprobados.*
32. ***Tecnología de la información.*** *Es el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes y comunicaciones, entre otros.*
33. ***Tecnología Regulatoria (RegTech).*** *Es el uso de tecnologías innovadoras, como la automatización, inteligencia artificial y análisis de datos, para mejorar la eficiencia, precisión y trazabilidad del cumplimiento normativo en las entidades.*
34. ***Tiempo de recuperación objetivo (RTO).*** *Es el período de tiempo transcurrido después de un incidente, para reanudar una actividad o recuperar los recursos antes de que la entidad controlada genere pérdidas significativas.*
35. ***Tolerancia al riesgo.*** *Es el grado de desviación del riesgo operativo respecto del nivel de apetito de riesgo definido por el órgano de gobierno que la entidad de servicios financieros tecnológicos puede soportar.*
36. ***Transacciones. -*** *Son movimientos que realizan los clientes y/o usuarios a través de los canales que brindan las entidades; y pueden ser monetarias y no monetarias.*
37. ***Transacciones monetarias. -*** *Son las que implican movimiento de dinero y son realizadas por los clientes a través de canales presenciales o canales electrónicos, tales como: transferencias, depósitos, retiros, operaciones de crédito, pagos, recargas de telefonía móvil, entre otras.*

38. Transacciones no monetarias. - *Son las que no implican movimiento de dinero y son realizadas por los clientes a través de canales presenciales o canales electrónicos, tales como: consultas, cambios de clave, personalización de condiciones.*

ARTÍCULO 5.- Riesgos sujetos a normativa específica. *Los riesgos de crédito, liquidez, mercado y de prevención y administración del riesgo de lavado de activos y financiación de delitos, se regularán en lo que aplique conforme a las normas específicas emitidas por la Superintendencia de Bancos para los sectores financiero público y privado, sin perjuicio de lo dispuesto en relación con estos riesgos en la norma emitida por la Junta de Política y Regulación Financiera y Monetaria para las entidades de servicios financieros tecnológicos.*

Por su parte, los riesgos operativos, tecnológicos, de seguridad de la información, ciberseguridad, continuidad del negocio, servicios provistos por terceros, legales y demás riesgos no financieros inherentes a la naturaleza de las entidades de servicios financieros tecnológicos, se regirán conforme lo establecido en la presente norma.

SECCIÓN II.- ADMINISTRACIÓN DE RIESGOS

ARTÍCULO 6.- Modelo de gestión de riesgos. *En el marco de la administración integral de riesgos, y alineado al apetito y tolerancia del riesgo definidos por la organización; la entidad controlada debe definir políticas, procesos, procedimientos y metodologías para la administración del riesgo; y, definirán y adoptarán un modelo basado en el esquema de tres líneas de defensa considerando su objeto social, tamaño, naturaleza, complejidad de sus operaciones y demás características propias.*

Las líneas de defensa de las entidades controladas deben cumplir y sin limitarse con las siguientes funciones:

1. Primera línea

a) *Identificar y evaluar la materialidad de los riesgos inherentes a su gestión de negocio y operativa mediante el uso de herramientas de gestión de riesgos;*
b) *Establecer controles apropiados para mitigar los riesgos inherentes y evaluar el diseño y la efectividad de estos controles;*
c) *Reportar los perfiles de riesgo de la gestión de negocio y operativa; y,*
d) *Informar sobre los riesgos residuales no mitigados por los controles, incluidos los eventos de pérdida, deficiencias de control, deficiencias de procesos y sus incumplimientos.*

2. Segunda línea

a) *Desarrollar una visión independiente con respecto a las unidades de negocio, identificar riesgos, proponer controles clave y monitorear permanentemente el apetito y la tolerancia al riesgo;*
b) *Evaluar periódicamente en la gestión de negocio y operativa la implementación de las metodologías o herramientas de gestión del riesgo, manteniendo evidencias de la evaluación realizada;*
c) *Desarrollar y mantener políticas, estándares y directrices de gestión y medición de riesgos;*
d) *Monitorear y reportar los perfiles de riesgo; y,*

e) *Diseñar y brindar capacitación y concientización sobre los riesgos.*

3. Tercera línea

a) *Revisar el diseño y la implementación de los sistemas de gestión de riesgos y los procesos asociados de la primera y segunda línea de defensa;*
b) *Revisar los procesos para garantizar que sean independientes y se implementen de manera coherente con las políticas establecidas; y,*
c) *Asegurar que los sistemas de cuantificación utilizados para evaluar los riesgos reflejen el perfil de riesgo de la entidad.*

ARTÍCULO 7.- Comité de Administración Integral de Riesgos. *Las entidades de servicios financieros tecnológicos deberán contar con un Comité de Administración Integral de Riesgos, cuya conformación, atribuciones y funcionamiento observarán el principio de proporcionalidad, en función del tamaño, complejidad y volumen de operaciones de cada entidad.*

El Comité estará conformado, como mínimo por: un miembro de la Junta General de Accionistas, Directorio u órgano de gobierno que haga sus veces, quien lo presidirá; el representante legal de la entidad; y, el jefe de la Unidad de Riesgos o el responsable de riesgos.

En los casos en que la entidad no cuente con Junta General de Accionistas ni con Directorio, el Comité será presidido por un representante de los socios o accionistas según corresponda.

El Comité se reunirá ordinariamente al menos una vez al mes y, de manera extraordinaria, cuando así lo requiera la naturaleza de los riesgos identificados. El quórum de las reuniones se cumplirá con la mayoría simple de sus miembros, y las decisiones se adoptarán por mayoría de votos; en caso de empate, el presidente tendrá voto dirimente.

La Superintendencia de Bancos, en función del tamaño, volumen de operaciones y naturaleza jurídica de la entidad, podrá exigir requisitos diferenciados para la conformación y periodicidad de sesiones.

ARTÍCULO 8.- Funciones del Comité de Administración Integral de Riesgos. *Las funciones principales que debe cumplir el Comité de Administración Integral de Riesgos, son las siguientes:*

1. *Aprobar y mantener actualizados los manuales, políticas, procedimientos, metodologías, algoritmos y/o modelos automatizados para la gestión de riesgos; así como, el plan de continuidad del negocio, cuando exista delegación expresa del órgano de gobierno de la entidad;*

2. *Evaluar periódicamente la efectividad de los controles internos y externos implementados, proponiendo y adoptando acciones correctivas cuando se identifiquen deficiencias;*

3. *Supervisar la adecuada administración de riesgos, incluidos los riesgos operativos y tecnológicos, aquellos vinculados a la ciberseguridad, seguridad de la información y uso de algoritmos, de ser el caso;*

4. *Informar oportunamente al Directorio, a la Junta General de Accionistas o, en su defecto, al órgano de gobierno que haga sus veces, sobre la evolución de los niveles de exposición a riesgos y la probabilidad de afectación ante cambios en el entorno económico, tecnológico o regulatorio;*

5. *Mantener registros documentales que respalden el cumplimiento de sus funciones, asegurando que los informes presentados al órgano de gobierno cuenten con la aprobación y legalización correspondiente y estén disponibles para la supervisión de la Superintendencia de Bancos;*

6. *Revisar los incidentes operativos y tecnológicos reportados por la Unidad o Responsable de Riesgos, verificando la implementación de medidas correctivas;*

7. *Poner en conocimiento del órgano de gobierno de la entidad y de la Superintendencia de Bancos los incidentes, indicando las causas, impactos y acciones de mitigación adoptadas;*

8. *Supervisar a los proveedores externos, verificando el cumplimiento de cláusulas de seguridad, continuidad y auditoría, así como el monitoreo periódico de su desempeño;*

9. *Revisar los resultados del monitoreo a los algoritmos y/o modelos automatizados utilizados por la entidad, asegurando su trazabilidad, explicabilidad y actualización, y verificar la existencia a través del responsable del algoritmo de ser el caso;*

10. *Aprobar los planes de acción para la mitigación de riesgos, verificando su adecuada implementación y seguimiento hasta su cierre;*

11. *Promover la cultura de gestión de riesgos en toda la organización, a través de programas de capacitación y sensibilización del personal;*

12. *Validar los planes de comunicación y atención al usuario en caso de incidentes, asegurando protocolos claros de transparencia y mecanismos efectivos de respuesta a consultas, quejas y reclamos;*

13. *Supervisar el diseño, implementación y actualización de sistemas de indicadores de alerta temprana, que permitan identificar, medir y reportar oportunamente riesgos emergentes, incidentes potenciales y desviaciones significativas respecto de los parámetros normales de operación; y,*

14. *Cumplir con las demás funciones que determine el órgano de gobierno de la entidad o que establezca la Superintendencia de Bancos.*

La Superintendencia de Bancos, en función del tamaño, volumen de operaciones, naturaleza jurídica y tipo de la entidad de servicios financieros tecnológicos, con base en los correspondientes informes técnicos y/o jurídicos podrá establecer requisitos diferenciados para las competencias del Comité de Administración Integral de Riesgos, a fin de asegurar la proporcionalidad en su aplicación.

ARTÍCULO 9.- Unidad de Riesgos. *Las entidades de servicios financieros tecnológicos deberán contar con una Unidad de Riesgos responsable de la implementación y ejecución del sistema de gestión de riesgos, con independencia funcional de las áreas de negocio.*

En aplicación del principio de proporcionalidad, cuando la dimensión, volumen de operaciones, naturaleza y tipo de entidad de servicios financieros no justifique la creación de una Unidad de Riesgos independiente, la Superintendencia de Bancos, con base en los correspondientes informes técnicos y/o jurídicos, podrá en su lugar disponer la designación de un responsable de Riesgos con competencias técnicas verificables, quien reportará directamente al representante legal.

El responsable de Riesgos deberá contar con conocimientos, experiencia y un perfil profesional adecuado en materia de administración de riesgos financieros, operativos y tecnológicos, acreditando formación académica o experiencia equivalente que garantice el cumplimiento de sus funciones.

ARTÍCULO 10.- Funciones de la unidad o responsable de riesgos. *Las funciones principales que debe cumplir la unidad o responsable de riesgos, son las siguientes:*

1. *Elaborar y proponer al Comité de Administración Integral de Riesgos los manuales, políticas, procedimientos y metodologías de gestión de riesgos, así como los planes de continuidad del negocio, para su revisión y aprobación;*

2. *Implementar y monitorear la efectividad de los controles internos y externos, elaborando reportes periódicos al Comité con recomendaciones de acciones correctivas cuando se identifiquen deficiencias;*

3. *Gestionar y mantener actualizada la matriz de riesgos, identificando y evaluando los riesgos operativos y tecnológicos, incluidos aquellos vinculados a la ciberseguridad, seguridad de la información y uso de algoritmos de ser el caso, y reportando al Comité los hallazgos;*

4. *Preparar informes técnicos para el Comité y el órgano de gobierno sobre la evolución de los niveles de exposición a riesgos y los posibles impactos derivados de cambios en el entorno económico, tecnológico o regulatorio;*

5. *Mantener registros actualizados y sistematizados sobre los procesos de gestión de riesgos, asegurando que estén disponibles para el Comité y para la Superintendencia de Bancos en procesos de supervisión;*

6. *Registrar y analizar los incidentes operativos y tecnológicos, proponiendo planes de acción de mitigación y remitiendo al Comité los resultados de la implementación de medidas correctivas;*

7. *Elaborar reportes sobre incidentes que incluyan causas, impactos y acciones adoptadas, y ponerlos a conocimiento oportuno del Comité, del órgano de gobierno de la entidad y de la Superintendencia de Bancos;*

8. *Evaluar periódicamente a los proveedores externos respecto del cumplimiento de cláusulas contractuales de seguridad, continuidad y auditoría, informando al Comité sobre los resultados obtenidos;*

9. *Verificar la trazabilidad, explicabilidad y actualización de algoritmos y/o modelos automatizados, generando informes técnicos que permitan al Comité adoptar decisiones sobre ajustes o validaciones necesarias;*

10. *Elaborar y ejecutar planes de acción para la mitigación de riesgos, de acuerdo con las decisiones adoptadas por el Comité, y reportar su avance hasta el cierre definitivo;*

11. *Desarrollar e implementar programas de capacitación y sensibilización interna, que fortalezcan la cultura de riesgos, y presentar al Comité informes sobre su cumplimiento y efectividad;*

12. *Diseñar protocolos de comunicación y atención al usuario en caso de incidentes, remitiéndolos al Comité para su validación y asegurando su ejecución cuando corresponda;*

13. *Desarrollar, mantener y reportar sistemas de indicadores de alerta temprana, informando periódicamente al Comité sobre riesgos emergentes, incidentes potenciales y desviaciones respecto de los parámetros normales de operación; y,*

14. *Ejecutar las demás funciones que disponga el Comité de Administración Integral de Riesgos o la Superintendencia de Bancos, en el marco de la normativa vigente.*

La Superintendencia de Bancos, en función del tamaño, volumen de operaciones, naturaleza jurídica y tipo de entidad de servicios financieros tecnológicos, podrá establecer funciones diferenciadas para la unidad o responsable de riesgos, a fin de asegurar la proporcionalidad en su aplicación.

SECCIÓN III.- ADMINISTRACIÓN DEL RIESGO OPERATIVO

ARTÍCULO 11.- Identificación de riesgos operativos. *Las entidades de servicios financieros tecnológicos deberán identificar los riesgos operativos considerando sus líneas de negocio, los tipos de eventos, los factores de riesgo operativo y las fallas o insuficiencias detectadas en sus procesos. Para el efecto, deberán contar con una metodología debidamente documentada y aprobada por el Comité de Administración Integral de Riesgos, que incorpore el uso de herramientas acordes a la naturaleza, complejidad y tamaño de la entidad, tales como autoevaluaciones, mapas de riesgos, indicadores clave de riesgo (KRI), tablas de control (scorecards), bases de datos de incidentes u otras técnicas equivalentes.*

Los tipos de eventos de riesgo operativo que, como mínimo, deberán considerarse son los siguientes:

1. *Fraude interno;*
2. *Fraude externo;*
3. *Prácticas laborales y seguridad del ambiente de trabajo;*
4. *Prácticas relacionadas con los clientes, productos y el negocio;*
5. *Daños a los activos físicos;*
6. *Interrupción del negocio por fallas en la tecnología de la información; y,*
7. *Deficiencias en el diseño y/o la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros.*

Para mayor detalle, las entidades de servicios financieros tecnológicos deberán observar lo dispuesto en el anexo 1 eventos de riesgo operativo de acuerdo con Basilea, que forma parte integrante de esta norma.

ARTÍCULO 12.- Medición y cuantificación del riesgo operativo. *Una vez identificados los riesgos operativos y las fallas o insuficiencias en relación con los eventos de riesgo, las entidades de servicios financieros tecnológicos deberán medirlos determinando su probabilidad de ocurrencia y su impacto potencial, de manera que el Comité de Administración Integral de Riesgos y el órgano de gobierno de la entidad cuenten con una visión clara de la exposición, con el fin de apoyar la toma de decisiones y acciones oportunas.*

Con base en los resultados de la medición, el órgano de gobierno estará en capacidad de decidir si mitiga, transfiere, asume o evita los riesgos identificados, aplicando las medidas que resulten más adecuadas para reducir sus efectos en la operación y en la protección de los usuarios.

Las entidades de servicios financieros tecnológicos deberán implementar mecanismos de cuantificación periódica sobre los eventos de pérdida producidos por riesgos operativos, que permitan evaluar su materialidad y actualizar la declaración institucional de apetito y tolerancia al riesgo operativo, en concordancia con lo aprobado por el Comité de Administración Integral de Riesgos.

La medición y cuantificación del riesgo operativo se realizará en función del tamaño, naturaleza, complejidad y volumen de operaciones de cada entidad, conforme a los lineamientos que para el efecto establezca la Superintendencia de Bancos.

ARTÍCULO 13.- Control y mitigación del riesgo operativo. *La administración del riesgo operativo en las entidades de servicios financieros tecnológicos deberá sustentarse en la existencia de planes de mitigación formalmente establecidos, aprobados por el Comité de Administración Integral de Riesgos y revisados de manera periódica. Dichos planes deberán contemplar, al menos:*

1. *Revisión y actualización de las estrategias, políticas, procesos y procedimientos de gestión de riesgos;*
2. *Implementación o modificación de límites de exposición al riesgo operativo;*
3. *Adopción, implementación y actualización de controles internos y tecnológicos;*
4. *Formulación, prueba y actualización del plan de continuidad del negocio;*
5. *Revisión periódica de los términos y coberturas de pólizas de seguros contratadas, de existir;*
6. *Evaluación y gestión de riesgos derivados de servicios provistos por terceros;*
7. *Evaluación de coberturas de seguros relacionadas con riesgo operativo y tecnológico (incluidos ciber riesgos y fraude), definiendo, de ser pertinente, límites mínimos acordes al tamaño y materialidad de los riesgos de la entidad; y,*
8. *Otros mecanismos de control y mitigación que resulten pertinentes en función del tamaño, naturaleza y complejidad de las operaciones de la entidad.*

Los controles deberán integrarse a las actividades regulares de la entidad, de forma que permitan generar respuestas oportunas y efectivas frente a los eventos de riesgo operativo y las fallas o insuficiencias que los ocasionen.

Las entidades de servicios financieros tecnológicos deberán implementar mecanismos efectivos adicionales de mitigación para los riesgos vinculados a los factores de riesgo operativo, sin perjuicio de los establecidos en la presente norma.

ARTÍCULO 14.- Monitoreo y reporte de riesgo operativo. *Las entidades de servicios financieros tecnológicos deberán realizar un monitoreo permanente de los riesgos asociados a sus procesos, su nivel de exposición y la efectividad de los controles implementados. Para ello, deberán contar con un esquema organizado de reportes e informes que proporcione información suficiente, pertinente y oportuna para la toma de decisiones del Comité de Administración Integral de Riesgos, del órgano de gobierno y de la Superintendencia de Bancos, cuyo alcance y nivel de detalle se ajustará al tamaño, naturaleza, complejidad y volumen de operaciones de la entidad.*

Los reportes e informes deberán incluir, como mínimo:

1. *Indicadores clave de riesgo operativo (KRI) que permitan evaluar la eficiencia y eficacia de las políticas, procesos, procedimientos y metodologías aplicadas;*
2. *Grado de cumplimiento de los planes de mitigación, con detalle de avances, desviaciones y acciones correctivas; y,*
3. *Matriz y mapas de riesgos operativos, que incorporen al menos: línea de negocio, proceso, tipo de riesgo, evento de riesgo operativo, factor de riesgo, fallas o insuficiencias, impacto y probabilidad inicial, controles existentes, planes de mitigación, impacto y probabilidad final, y riesgo residual.*

Las entidades de servicios financieros tecnológicos deberán presentar al Comité de Administración Integral de Riesgos informes periódicos con una periodicidad mínima trimestral, que incluyan:

1. *Los niveles de exposición al riesgo operativo y su evolución;*
2. *Los resultados de los indicadores clave de riesgo;*
3. *La eficacia de las políticas, procesos, procedimientos y metodologías aplicadas;*
4. *El grado de cumplimiento de los planes de mitigación; y,*
5. *Conclusiones y recomendaciones para fortalecer la administración del riesgo operativo.*

La forma, alcance y nivel de detalle de los informes se ajustará al tamaño, naturaleza, complejidad y volumen de operaciones de cada entidad que serán establecidos en base a los lineamientos dictados por este organismo de control.

ARTÍCULO 15.- Registro y base de datos de incidentes de riesgo operativo. *Las entidades de servicios financieros tecnológicos deberán conformar y mantener una base de datos centralizada que permita registrar, ordenar, clasificar y disponer de información sobre los riesgos y eventos de riesgo operativo, incluidos los de orden legal, de seguridad de la información, ciberseguridad, servicios provistos por terceros, uso de algoritmos y/o modelos automatizados y continuidad del negocio.*

La base de datos deberá contener, como mínimo:

1. *Descripción del evento de riesgo operativo;*
2. *Línea de negocio, proceso o servicio afectado;*
3. *Factor de riesgo operativo que lo originó;*
4. *Efecto cuantitativo de la pérdida producida o estimada;*
5. *Frecuencia y probabilidad de ocurrencia; y,*
6. *Acciones de mitigación adoptadas.*

La administración y actualización de la base de datos será responsabilidad de la Unidad o Responsable de Riesgos.

Las entidades considerando su tamaño, volumen o complejidad podrán implementar mecanismos simplificados de registro, siempre que aseguren la trazabilidad de la información, la identificación de eventos y la comunicación oportuna al Comité de Administración Integral de Riesgos, al órgano de gobierno y a la Superintendencia de Bancos.

ARTÍCULO 16.- Auditoria del sistema de gestión del riesgo operativo. *La función de auditoría interna será responsable de evaluar objetiva e independientemente el cumplimiento de los lineamientos establecidos en esta norma, verificando que las actividades de la primera y segunda línea de defensa se ejecuten de acuerdo con las políticas aprobadas y los estándares de gestión de riesgos.*

En el marco de esta evaluación, la auditoría interna deberá, como mínimo:

1. *Verificar la efectividad de los controles implementados para mitigar los riesgos operativos en cada uno de sus factores;*

2. *Revisar periódicamente el funcionamiento del sistema de gestión de continuidad del negocio; y,*

3. *Revisar la efectividad de las medidas de seguridad de la información y ciberseguridad aplicadas en los servicios y canales electrónicos.*

SUBSECCIÓN I.- FACTORES DEL RIESGO OPERATIVO

ARTÍCULO 17.- Administración del riesgo operativo por factores. *Con el propósito de minimizar la probabilidad de incurrir en pérdidas atribuibles al riesgo operativo, las entidades de servicios financieros tecnológicos deberán administrar este riesgo considerando, al menos, los siguientes factores:*

1. *Procesos;*
2. *Personas;*
3. *Tecnología de la información; y,*
4. *Eventos externos.*

El alcance y nivel de detalle en la administración de cada factor se ajustará al tamaño, naturaleza, complejidad y volumen de operaciones de la entidad.

ARTÍCULO 18.- Factor procesos. *Las entidades de servicios financieros tecnológicos deberán gestionar sus procesos bajo un enfoque eficiente y eficaz de gestión por procesos, tomando como referencia estándares internacionales como ISO 9001 e ISO 31000, de conformidad con su estrategia institucional y las políticas aprobadas por el Comité de Administración Integral de Riesgos.*

Para el efecto, deberán observar, al menos, lo siguiente:

1. *Definición del mapa de procesos, agrupados en:*

a) ***Procesos estratégicos o gobernantes****: proporcionan directrices y políticas institucionales (planificación estratégica, estructura organizacional, administración integral de riesgos, continuidad del negocio, seguridad de la información, entre otros).*

b) ***Procesos productivos u operativos:*** *permiten ejecutar efectivamente los productos o servicios ofrecidos a los usuarios.*

c) ***Procesos habilitantes o de apoyo:*** *respaldan la ejecución de los procesos estratégicos y productivos.*

2. *Asignación de procesos a líneas de negocio, garantizando que cada proceso productivo corresponda a una línea de negocio definida. En caso de que un proceso intervenga en más de una línea, deberá aplicarse una metodología formal que asegure consistencia y trazabilidad.*

3. *Metodología formal para el diseño, control, actualización, seguimiento y medición de los procesos, que deberá contemplar al menos:*

a) *Descripción y diagramación en secuencia lógica y ordenada de las actividades, tareas y controles;*
b) *Determinación de responsables del proceso y de la implementación de controles y planes de acción;*
c) *Identificación de clientes internos y externos;*
d) *Productos y servicios generados;*
e) *Difusión y comunicación de los procesos, garantizando su correcta aplicación; y,*
f) *Actualización y mejora continua mediante revisiones periódicas: al menos una vez al año para procesos críticos o productivos, y al menos una vez cada dos años para los demás.*

4. *Inventarios actualizados de procesos, que incluyan como mínimo: categoría (estratégico, productivo, de apoyo), línea de negocio, nombre del proceso, criticidad, procedimientos asociados, responsables, productos o servicios entregados, fecha de aprobación y última actualización.*

5. *Separación de funciones, evitando concentraciones de carácter incompatible que permitan la ocurrencia u ocultamiento de fraudes, errores u otros eventos de riesgo operativo.*

6. *Definición de indicadores clave de desempeño y de riesgo (KPI/KRI) para los procesos, que permitan medir su eficacia, eficiencia y niveles de exposición al riesgo operativo.*

ARTÍCULO 19.- Factor personas. *Las entidades de servicios financieros tecnológicos deberán administrar el capital humano de manera que les permita gestionar adecuadamente los riesgos asociados a este factor, garantizando la idoneidad, continuidad y seguridad en la prestación de los servicios.*

Para el efecto, deberán observar, como mínimo, lo siguiente:

1. ***Políticas y procedimientos de gestión de personal.*** *Definir formalmente políticas, procesos y procedimientos para la incorporación, permanencia y desvinculación del personal, en cumplimiento de la normativa laboral aplicable y en concordancia con la estrategia de la entidad. Dichas políticas deberán asegurar la adecuada planificación y administración del capital humano.*

   a) ***Incorporación.*** *Incluir procesos de reclutamiento, selección, contratación e inducción que garanticen la idoneidad del personal en función de las competencias requeridas, tanto técnicas como éticas.*

   b) ***Permanencia.*** *Establecer programas de capacitación continua, sistemas de evaluación del desempeño y mecanismos de identificación de puestos críticos y personal clave, asegurando planes de reemplazo en caso de ausencias temporales o definitivas.*

   c) ***Desvinculación.*** *Implementar procedimientos formales para la terminación de la relación laboral, que incluyan aspectos jurídicos y la adecuada transferencia de responsabilidades, protegiendo la continuidad del negocio.*

2. ***Confidencialidad y seguridad de la información.*** *Mantener actualizados los acuerdos de confidencialidad relacionados con las funciones que desempeñe el personal y los riesgos asociados, incluyendo la obligación de resguardar información sensible aún después del cambio de funciones o de la desvinculación.*

3. ***Archivo digital centralizado.*** *Contar con un registro digital actualizado del capital humano, que incluya, al menos, información sobre formación académica, experiencia, procesos de selección, historial de capacitación, evaluaciones de desempeño y desvinculación.*

El alcance y nivel de detalle de estas obligaciones se ajustará al tamaño, naturaleza, complejidad y volumen de operaciones de la entidad.

ARTÍCULO 20.- Factor tecnología de la información. *Las entidades de servicios financieros tecnológicos deberán administrar los riesgos asociados a la tecnología de la información, de manera que se garantice la captura, procesamiento, almacenamiento y transmisión de la información de forma oportuna, confiable y segura; la continuidad de las operaciones; y la disponibilidad de la información para la toma de decisiones, incluso cuando los servicios sean provistos por terceros.*

Para el efecto, deberán observar, como mínimo, lo siguiente:

1. ***Gobernanza de la tecnología.*** *Contar con políticas, procesos y procedimientos de gestión tecnológica aprobados por el Comité de Administración Integral de Riesgos, alineados a los objetivos institucionales. Las entidades según su estructura, volumen o complejidad podrán establecer un comité de tecnología o designar un responsable de tecnología y seguridad de la información; que lidere la gestión estratégica de los sistemas tecnológicos y de la seguridad de la información.*

   El comité, de existir, de tecnología estará integrado como mínimo por: un miembro de la Junta General de Accionistas, Directorio u órgano de gobierno que haga sus veces, quien lo presidirá,

el representante legal de la entidad, el jefe de la unidad de riesgos o el responsable de riesgos, el responsable del área de tecnología y seguridad de la información. El presidente del Comité tendrá voto dirimente.

En los casos en que la entidad no cuente con Junta General de Accionistas ni con Directorio, el Comité será presidido por un representante de los socios o accionistas según corresponda.

El Comité se reunirá ordinariamente al menos una vez al mes y, de manera extraordinaria, cuando así lo requiera la naturaleza de los riesgos identificados. El quórum se conformará con la mayoría simple de sus miembros, y las decisiones se adoptarán por mayoría de votos.

Cuando la entidad no cuente con un Comité de Tecnología independiente, el responsable de tecnología y seguridad de la información deberá integrarse al Comité de Administración Integral de Riesgos, con voz y voto, a fin de garantizar el tratamiento formal de los temas relacionados con tecnología, seguridad de la información y ciberseguridad.

La Superintendencia de Bancos, en función del tamaño, volumen de operaciones y naturaleza jurídica de la entidad, podrá establecer requisitos diferenciados para la conformación y periodicidad de sesiones.

2. *Planificación y gestión tecnológica: Disponer de un plan estratégico y un plan operativo anual de tecnología de la información, alineados con la estrategia institucional, que incluya actividades, responsables, cronogramas y presupuesto, para asegurar el cumplimiento de los objetivos tecnológicos.*

3. *Seguridad de la información y ciberseguridad: Implementar políticas y controles alineados con estándares internacionales que aseguren la confidencialidad, integridad y disponibilidad de la información, incluyendo:*

- ***a)*** *Mecanismos de prevención, detección y respuesta ante incidentes cibernéticos;*
- ***b)*** *Procedimientos de gestión de accesos y privilegios;*
- ***c)*** *Protocolos de respaldo, recuperación y continuidad de servicios críticos; y,*
- ***d)*** *Notificación a la Superintendencia de Bancos de incidentes que afecten la seguridad o continuidad de los servicios.*

4. *Gestión de incidentes tecnológicos: Contar con procedimientos documentados para la identificación, análisis de causa raíz, mitigación y seguimiento de incidentes y problemas tecnológicos, con registros disponibles para revisión del Comité de Administración Integral de Riesgos y la Superintendencia de Bancos.*

5. *Proveedores y servicios tecnológicos externos: Cuando se contraten servicios tecnológicos críticos, las entidades de servicios financieros tecnológicos deberán establecer mecanismos de supervisión, asegurando que los contratos incluyan cláusulas de seguridad, continuidad, confidencialidad y derecho de auditoría, en concordancia con la presente norma.*

6. *Control de cambios y desarrollo de software: Adoptar metodologías que aseguren que los cambios a aplicaciones e infraestructura estén debidamente autorizados, probados,*

documentados y registrados, considerando medidas de seguridad de la información y pruebas de calidad antes de su paso a producción.

7. *Infraestructura tecnológica crítica: Asegurar que la infraestructura que soporta las operaciones críticas cuente con los mecanismos de redundancia, monitoreo y seguridad necesarios para evitar interrupciones del negocio, conforme al tamaño y complejidad de la entidad.*

8. *Monitoreo en tiempo real: Utilizar soluciones de monitoreo continuo y herramientas de tecnología regulatoria (RegTech) para detectar vulnerabilidades, anomalías y posibles brechas de seguridad y para automatizar la verificación del cumplimiento normativo (gestión de requisitos, control documental y alertas regulatorias), garantizando respuestas oportunas y manteniendo evidencia trazable.*

ARTÍCULO 21.- Factor eventos externos. *En la administración del riesgo operativo, las entidades de servicios financieros tecnológicos deberán considerar la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos a su control, tales como fallas en los servicios públicos, desastres naturales, ataques cibernéticos, interrupciones en proveedores críticos de servicios tecnológicos, eventos de conmoción social, atentados u otros actos delictivos que pudieran alterar el desarrollo normal de sus actividades, cuyo análisis y nivel de detalle se ajustará al tamaño, naturaleza, complejidad y volumen de operaciones de la entidad.*

La gestión de los riesgos relacionados con eventos externos deberá formar parte integral de la administración de la continuidad del negocio, manteniendo procedimientos actualizados y probados que permitan garantizar la capacidad de la entidad para operar de manera continua y minimizar las pérdidas en caso de una interrupción, de acuerdo con metodologías que podrán ser simplificadas en el caso de entidades de servicios financieros tecnológicos de menor tamaño o complejidad, siempre que aseguren la identificación, tratamiento y reporte oportuno de dichos riesgos.

SUBSECCIÓN II.- GESTIÓN DE INCIDENTES Y PROBLEMAS

ARTÍCULO 22.- Gestión de incidentes y problemas. *Las entidades de servicios financieros tecnológicos deben desarrollar e implementar planes de respuesta y recuperación para gestionar los incidentes y problemas que puedan afectar el normal funcionamiento de sus servicios, especialmente de sus servicios críticos en línea con el apetito y la tolerancia al riesgo definida por la entidad, de manera que contribuya a la resiliencia operativa de la entidad. Para ello deben implementar como mínimo lo siguiente, pero sin limitarse a:*

1. *Procedimientos que garanticen que los productos y servicios críticos sean recuperados de manera prioritaria en casos de indisponibilidad, degradación e intermitencia, en un tiempo no mayor a tres (03) horas dentro de las siguientes veinte y cuatro (24) horas consecutivas.*

2. *Asignar un responsable de la gestión de incidentes, encargado de su registro, trazabilidad y cierre, manteniendo evidencia documentada de las acciones adoptadas. En el caso de entidades que por el tamaño, complejidad o volumen de operaciones no cuenten con responsable de la gestión de incidentes, esta función podrá ser asumida por el responsable de Riesgos.*

3. *La gestión de incidentes debe abarcar el ciclo de vida del incidente, que incluya entre otros: registro, priorización en función de la gravedad, análisis, escalamiento, solución, monitoreo, lecciones aprendidas y reporte a las partes interesadas tanto internas como externas.*

4. *Incorporar en la gestión de problemas el análisis de causa raíz, planes de acción efectivos y la correlación de incidentes recurrentes, asegurando independencia del personal que administra las plataformas afectadas.*

5. *Mantener una base de conocimiento actualizada sobre incidentes y problemas, que incluya recursos internos y externos, y permita retroalimentar la mejora continua de los controles.*

6. *Realizar pruebas controladas de los planes de gestión de incidentes y problemas, a fin de evaluar su efectividad y garantizar la resiliencia operativa de la entidad.*

7. *Activar los planes de contingencia y continuidad del negocio cuando los incidentes tengan un impacto material en los servicios críticos.*

8. *Las entidades de servicios financieros tecnológicos deben comunicar a la Superintendencia de Bancos los incidentes que afecten a sus servicios críticos y remitir un informe formal del incidente máximo en cinco (5) días plazo siguientes al incidente, y en veinte (20) días plazo el informe de causa raíz del problema.*

9. *Remitir, mediante oficio hasta máximo el 31 de enero de cada año en curso, el "Plan anual de mantenimientos programados / Pruebas Centro de Datos Alterno". El "Plan anual de mantenimientos programados" debe incluir al menos la siguiente información:*

- ***a)*** *Fecha y hora del inicio del mantenimiento / Pruebas Centro de Datos Alterno (dd/mm/aaaa hh:mm:ss);*
- ***b)*** *Objetivo del mantenimiento / Prueba DCA c) Canales de atención al usuario afectados*
- ***c)*** *Infraestructura tecnológica que interviene;*
- ***d)*** *Detalle de las actividades a desarrollarse que incluya la línea de tiempo; y,*
- ***e)*** *Fecha final y hora del mantenimiento / Prueba DCA (dd/mm/aaaa hh:mm:ss)*

10. *En caso de existir modificaciones al "Plan anual de mantenimientos programados/ Pruebas centro de datos alterno" se deberá notificar a la Superintendencia de Bancos y al canal de reporte con al menos, 5 días de antelación, conforme señala el artículo 201 del Código Orgánico Monetario y Financiero.*

11. *En caso de presentar incidentes en la ejecución de los mantenimientos programados o pruebas en el DCA, se debe aplicar lo dispuesto para el caso de incidentes.*

12. *Con relación a los incidentes, notificar al canal de reporte, correspondiente a la Dirección de Evaluación de Riesgos, lo siguiente:*

- ***a)*** *Los incidentes o eventos que ocasionen indisponibilidad o intermitencia mayor a treinta (30) minutos en los canales de atención al usuario a través de los cuales se ofrece productos y servicios.*

b) *Los incidentes o eventos que ocasionen indisponibilidad o intermitencia mayor a treinta (30) minutos en los canales de atención al usuario a través de los cuales se ofrece productos y servicios que fueren ocasionados por un tercero.*

c) *Las notificaciones deberán ser remitidas en el lapso máximo de cinco (5) minutos posteriores al tiempo límite de indisponibilidad o intermitencia de treinta (30) minutos.*

d) *La notificación deberá contener la siguiente información:*

- *Fecha y hora del inicio del incidente (dd/mm/aaaa hh:mm:ss)*
- *Nivel de criticidad*
- *Canales de atención al usuario afectados*
- *Descripción de la indisponibilidad o afectación*
- *Componentes tecnológicos afectados*
- *Acciones adoptadas por la entidad para recuperación del servicio, planes de contingencia implementados*

e) *Reportes, cada treinta (30) minutos, de los avances del incidente hasta que se restablezcan totalmente todos los canales de atención al usuario a través de los cuales se ofrece productos y servicios, especificando la fecha y hora de fin del incidente.*

f) *Durante o luego de ocurrido un incidente la entidad no deberá establecer como ventanas de mantenimiento programadas los tiempos de interrupción de los canales de atención al usuario a través de los cuales se ofrece productos y servicios.*

13. *Remitir mediante oficio el informe del incidente en los cinco (5) días plazo una vez superado el incidente. Este deberá contener el ciclo de vida del incidente con al menos lo siguiente: Registro del incidente, priorización en función de la gravedad, análisis, escalamiento, solución, monitoreo, lecciones aprendidas, reporte a las partes interesadas tanto internas como externas y planes de contingencia implementados; y, en el plazo de veinte (20) días el informe de causa raíz del problema una vez cerrado el incidente.*

14. *Remitir al ente de control un informe trimestral hasta el quince (15) del mes posterior con el detalle de todos los incidentes o eventos que generaron indisponibilidad o intermitencias, menores o iguales a treinta (30) minutos, en los canales de atención al usuario que considere los aspectos del numeral 12 literal d) y numeral 13.*

15. *En cualquiera de los casos en los que se presenten indisponibilidades en los canales de atención al usuario las entidades controladas deben comunicar de manera oportuna a los usuarios.*

16. *Remitir al ente de control el nombre, cargo, correo electrónico y teléfono de contacto de la persona responsable en la entidad de la gestión de incidentes que pueda proporcionar la información técnica del avance de la resolución de estos, en el plazo de cinco (5) días a partir de su calificación, se deberá actualizar esta información en caso de que haya cambios del delegado en la entidad.*

Las entidades de servicios financieros tecnológicos deberán notificar los incidentes conforme lo previsto en esta norma al canal de reporte sb_monitoreo@superbancos.gob.ec, asegurando que la información sea suficiente, oportuna y confiable para la toma de decisiones y la supervisión de la Superintendencia de Bancos.

SUBSECCIÓN III.- GESTIÓN DE LA CONTINUIDAD DE NEGOCIO

ARTÍCULO 23.- Sistema de gestión de continuidad del negocio. *Las entidades de servicios financieros tecnológicos deberán establecer, implementar, mantener y mejorar un sistema de gestión de la continuidad del negocio, con el fin de garantizar su capacidad de operar de forma continua y limitar las pérdidas en caso de una interrupción grave. Este sistema deberá alinearse a estándares internacionales reconocidos, como la norma ISO 22301 o la que la sustituya, y considerar tanto eventos internos como externos que pudieran afectar la prestación de servicios críticos.*

El sistema de continuidad del negocio deberá contemplar, como mínimo:

1. ***Gobernanza y responsabilidad.*** *La entidad deberá designar un responsable de continuidad del negocio, acorde a su tamaño y complejidad, que dirija el establecimiento, implementación y mantenimiento del sistema. Con base en el tamaño, complejidad y volumen de operaciones, la Superintendencia de Bancos podrá requerir la conformación de un comité especializado en continuidad del negocio, encargado de evaluar y supervisar el sistema y proponer su aprobación al órgano de gobierno;*

2. ***Marco de referencia.*** *El sistema deberá incluir políticas, estrategias, objetivos, metodologías y planes de continuidad revisados periódicamente y aprobados por el órgano de gobierno, en concordancia con el sistema de gestión de riesgos;*

3. ***Análisis de impacto al negocio (BIA).*** *Identificación de procesos críticos, dependencias internas y externas, recursos de soporte y tiempos y puntos de recuperación objetivo (RTO/RPO), revisados al menos una vez al año o cuando existan cambios significativos en la organización o su entorno;*

4. ***Estrategias de continuidad.*** *Definición y selección de alternativas que permitan mantener la operatividad de los procesos críticos dentro de los tiempos objetivo de recuperación, considerando seguridad del personal, infraestructura alterna, proveedores y aplicativos relacionados; y,*

5. ***Pruebas y mejora continua.*** *Realización periódica de pruebas del plan de continuidad y planes de contingencia, incluyendo la participación de proveedores críticos y validación de sitios alternos, cuyos resultados deberán documentarse e incorporarse al proceso de mejora continua con responsables y plazos.*

El alcance y nivel de detalle del sistema de gestión de continuidad del negocio se ajustará al tamaño, naturaleza, complejidad y volumen de operaciones de cada entidad.

ARTÍCULO 24.- Plan de continuidad del negocio. *Las entidades de servicios financieros tecnológicos deberán contar con un plan de continuidad del negocio que operacionalice el sistema de gestión de continuidad del negocio y que, como mínimo, considere:*

1. *Escenarios de riesgo y procesos críticos cubiertos por el plan;*

2. *Tiempos y puntos de recuperación objetivo (RTO/RPO) de cada proceso crítico;*

3. *Estrategias de continuidad para cada proceso crítico, detallando personal responsable, infraestructura y ubicaciones alternas, proveedores y aplicativos necesarios;*

4. *Procedimientos operativos para la reanudación urgente de procesos críticos, incluidos protocolos de traslado a sitios alternos que no estén expuestos a los mismos riesgos que la sede principal;*

5. *Protocolos de comunicación interna y externa, incluyendo comunicación con empleados, proveedores, usuarios y autoridades competentes;*

6. *Procedimientos de emergencia para preservar la seguridad del personal;*

7. *Plan de recuperación tecnológica y de desastres, que contemple restauración en ubicaciones remotas seguras;*

8. *Roles y responsabilidades de los encargados de la ejecución del plan;*

9. *Criterios claros de activación e invocación del plan; y,*

10. *En caso de entidades de servicios financieros tecnológicos dependientes de matrices en el exterior, el plan local deberá estar alineado y coordinado con el plan de continuidad de la casa matriz, garantizando la resiliencia de las operaciones en Ecuador.*

El plan deberá ser revisado, probado y actualizado al menos con periodicidad anual, y mantenerse a disposición de la Superintendencia de Bancos.

SUBSECCIÓN IV.- RIESGO LEGAL

ARTÍCULO 25.- Riesgo legal. *Las entidades de servicios financieros tecnológicos deberán identificar, medir, controlar, mitigar y monitorear los riesgos legales que pudieran afectar sus operaciones y derivar en pérdidas financieras, reputacionales o sanciones regulatorias. Estos riesgos pueden originarse, entre otros, en actos societarios, estipulaciones contractuales, incumplimiento normativo, relaciones con proveedores, uso de tecnologías y/o algoritmos, así como en operaciones vinculadas al giro del negocio.*

En función de su tamaño, naturaleza y complejidad de operaciones, las entidades de servicios financieros tecnológicos deberán contar con mecanismos adecuados de asesoría jurídica, interna o externa, que permitan gestionar los riesgos legales de manera eficaz, también contemplará cumplimiento de Ley Orgánica de Protección de Datos Personales.

Como parte de su gestión, las entidades de servicios financieros tecnológicos deberán mantener matrices de riesgo legal actualizadas, que identifiquen los principales escenarios de exposición, medidas de mitigación y responsables de su control.

SUBSECCIÓN V.- SERVICIOS PROVISTOS POR TERCEROS

ARTÍCULO 26.- Administración de proveedores de servicios terceros. *Las entidades de servicios financieros tecnológicos deberán implementar un proceso integral para la gestión de proveedores externos que soporten sus operaciones, en especial aquellos vinculados con procesos críticos o con servicios tecnológicos. Este proceso deberá abarcar la evaluación previa a la contratación, la suscripción de contratos, el monitoreo del servicio y su eventual renovación o terminación, con el fin de garantizar la continuidad, seguridad y calidad de los servicios prestados.*

Para el efecto, las entidades de servicios financieros tecnológicos deberán observar, como mínimo, lo siguiente:

1. ***Evaluación previa****. Antes de la contratación, la entidad deberá realizar una evaluación proporcional a la criticidad del servicio, que considere la experiencia del proveedor, su capacidad técnica, financiera y operativa, así como los riesgos asociados en materia de seguridad de la información, ciberseguridad, continuidad del negocio y cumplimiento normativo;*

2. ***Contratos****. Los contratos deberán contener cláusulas claras sobre: niveles de servicio, medidas de seguridad de la información y protección de datos personales, continuidad del negocio, derechos de auditoría por parte de la entidad y de la Superintendencia de Bancos, y mecanismos de sanción o terminación en caso de incumplimiento;*

3. ***Monitoreo y control****. La entidad deberá establecer procedimientos para monitorear periódicamente el cumplimiento de los niveles de servicio y demás obligaciones contractuales, utilizando mecanismos propios de validación cuando sea posible, y no únicamente la información reportada por el proveedor;*

4. ***Dependencia de proveedores críticos****. Cuando la entidad dependa de un único proveedor para un servicio crítico, deberá asegurarse de que este cuente con planes de contingencia y continuidad de negocio probados y actualizados, y documentar las medidas de mitigación de riesgos;*

5. ***Servicios en la nube y tecnológicos.*** *En caso de contratar servicios de infraestructura, plataforma o software en la nube, la entidad deberá elaborar informes técnicos, legales y de seguridad de la información que identifiquen y mitiguen los riesgos asociados. La Superintendencia de Bancos podrá establecer lineamientos específicos sobre estándares mínimos aplicables a estos servicios; y,*

6. ***Notificación al órgano de control****. Las entidades de servicios financieros tecnológicos deberán notificar a la Superintendencia de Bancos sobre la contratación de proveedores que soporten*

procesos críticos, proporcionando la documentación que respalde la gestión de riesgos realizada.

El alcance y nivel de detalle de estas obligaciones se ajustará al tamaño, naturaleza, complejidad y volumen de operaciones de la entidad.

SUBSECCIÓN VI. - SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

ARTÍCULO 27.- Sistema de gestión de seguridad de la información. *Las entidades de servicios financieros tecnológicos deberán establecer, implementar, mantener y mejorar de forma continua un* ***Sistema de Gestión de Seguridad de la Información****, alineado a estándares internacionales (ISO 27001, ISO 27017, ISO 27018, NIST Cybersecurity Framework, o los que los sustituyan), que permita:*

1. *Proteger la confidencialidad, integridad y disponibilidad de la información;*
2. *Prevenir accesos, usos, revelaciones, modificaciones, daños o pérdidas no autorizadas; y,*
3. *Procurar la resiliencia tecnológica y operativa de sus procesos y servicios.*

ARTÍCULO 28.- Funciones y responsables. *Las entidades de servicios financieros tecnológicos deberán:*

1. *Definir formalmente las funciones y responsabilidades relacionadas con la seguridad de la información, incluyendo la gestión de ciberseguridad;*

2. *Designar un* ***responsable de seguridad de la información****, con conocimientos y experiencia suficientes en la materia, acorde al tamaño y complejidad de la entidad;*

3. *En entidades de servicios financieros tecnológicos de mayor complejidad, contar con una unidad especializada de seguridad de la información, la cual sea independiente de las unidades de negocio, riesgos, tecnología y auditoría, en caso de existirlas; y,*

4. *Diseñar e implementar programas de capacitación periódica en seguridad de la información y ciberseguridad, con alcance a todo el personal y refuerzos para funciones críticas*

ARTÍCULO 29.- Requisitos del sistema de gestión de seguridad de la información. *Las entidades de servicios financieros tecnológicos deberán contar con un Sistema de Gestión de Seguridad de la Información que contemple, sin limitarse, a lo siguiente:*

1. ***Políticas y procedimientos documentados*** *de seguridad de la información y ciberseguridad, revisados y actualizados al menos una vez al año o cuando existan cambios significativos;*

2. ***Controles de acceso físico y lógico,*** *que incluyan autenticación robusta, segregación de funciones y gestión de usuarios privilegiados;*

3. ***Inventario y clasificación de activos de información****, considerando su criticidad, valor, requisitos legales y de protección de datos personales;*

4. ***Gestión de incidentes de seguridad de la información y ciberseguridad**, que incluya mecanismos de detección, registro, análisis de causa raíz, respuesta, recuperación y notificación a la Superintendencia de Bancos conforme la normativa vigente;*

5. ***Evaluaciones periódicas de riesgos de seguridad de la información y ciberseguridad**, alineadas a la metodología de gestión de riesgos de la entidad, que permitan identificar, medir, controlar y monitorear amenazas y vulnerabilidades;*

6. ***Capacitación y concienciación del personal**, orientada a la prevención de riesgos de seguridad de la información, ciberseguridad y protección de datos;*

7. ***Controles de movilidad y acceso remoto,** implementar, según la naturaleza, complejidad y volumen de operaciones de la entidad, controles de seguridad para el uso de dispositivos móviles y el acceso remoto (incluyendo, de ser el caso, redes privadas virtuales - VPN y esquemas de confianza cero - Zero Trust), así como la gestión de parches de software y firmware, la protección de redes mediante firewalls y sistemas de detección y prevención de intrusos (IDS/IPS), la gestión de identidades y accesos (IAM), la gestión de privilegios (PAM), y mecanismos de control de identidad para prevenir la suplantación de terceros;*

8. ***Condiciones ambientales y emplazamiento seguro,** gestionar condiciones ambientales y localización segura de equipos críticos;*

9. ***Gestión de amenazas cibernéticas,** definir procedimientos para phishing, malware, ransomware e inyección de código, con campañas simuladas y métricas de mejora; y,*

10. ***Auditorías internas y externas** que verifiquen la efectividad del **Sistema de Gestión de Seguridad de la Información** y el cumplimiento de la normativa aplicable. Las entidades en función de su tamaño podrán realizar estas auditorías de manera proporcional a su naturaleza y complejidad.*

SUBSECCIÓN VII.- SEGURIDADES EN CANALES ELECTRÓNICOS

***ARTÍCULO 30.- Seguridad en canales electrónicos.** Las entidades de servicios financieros tecnológicos deberán establecer políticas, procesos y controles para garantizar la seguridad en las transacciones realizadas a través de canales electrónicos, de ser el caso, asegurando la confidencialidad, integridad y disponibilidad de la información, así como la protección de los recursos de sus usuarios.*

En función del tamaño, complejidad y volumen de operaciones, las entidades de servicios financieros tecnológicos deberán, como mínimo:

1. *Implementar **mecanismos de autenticación fuerte** en el acceso y ejecución de transacciones electrónicas;*

2. *Asegurar la **transmisión y almacenamiento cifrado de datos sensibles**, conforme a estándares internacionales vigentes;*

3. *Contar con **sistemas de monitoreo y detección de fraudes** que permitan identificar y alertar sobre transacciones inusuales o no autorizadas, estableciendo procedimientos para su bloqueo y resolución;*

4. *Mantener **registros históricos suficientes** de las transacciones electrónicas, para fines de auditoría, control interno y atención de reclamos; y,*

5. *Desarrollar e implementar programas de información y capacitación periódica dirigidos a los usuarios sobre los riesgos asociados al uso de canales electrónicos y las medidas de seguridad disponibles.*

Cuando las entidades operen canales electrónicos tradicionales (cajeros automáticos, puntos de venta, corresponsales no bancarios u otros), deberán sujetarse a las disposiciones específicas emitidas por la Superintendencia de Bancos.

DISPOSICIONES GENERALES

PRIMERA.- *La Superintendencia de Bancos con base en los resultados de sus evaluaciones in situ y/o extra situ, podrá disponer a las entidades de servicios financieros tecnológicos la implementación de controles adicionales o complementarios, para lo cual se podrá considerar lo detallado en la "Norma de control para la gestión del riesgo operativo", así como en las mejores prácticas internacionales.*

SEGUNDA.- *La Superintendencia de Bancos podrá disponer a las entidades controladas la contratación de empresas auditoras externas debidamente calificadas para llevar a cabo procesos de evaluación especializada relacionados con el cumplimiento de lo detallado en la presente norma.*

TERCERA.- *Los casos de duda en la aplicación de la presente norma serán resueltos por la Superintendencia de Bancos."*

DISPOSICIÓN FINAL.- La presente Resolución entrará en vigor a partir de su expedición, sin perjuicio de su publicación en el Registro Oficial.

COMUNÍQUESE Y PUBLÍQUESE EN EL REGISTRO OFICIAL.- Dada en la Superintendencia de Bancos, en Quito, Distrito Metropolitano, el 25 de septiembre de 2025.

Firmado electrónicamente por:
ROBERTO JOSE ROMERO VON BUCHWALD
Validar únicamente con FirmaEC

Eco. Roberto José Romero von Buchwald
SUPERINTENDENTE DE BANCOS

LO CERTIFICO.- En Quito, Distrito Metropolitano, el 25 de septiembre de 2025.

Firmado electrónicamente por:
DELIA MARIA PENAFIEL GUZMAN
Validar únicamente con FirmaEC

Mgt. Delia María Peñafiel Guzmán
SECRETARIO GENERAL

ANEXO 1. EVENTOS DE RIESGO OPERATIVO DE ACUERDO CON BASILEA

Categoría de Tipo de Eventos (nivel 1)	Definición	Categoría (nivel 2)	Ejemplos de actividades (Nivel 3)
Fraude interno	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar regulaciones, leyes o políticas empresariales (excluidos los eventos de diversidad / discriminación) en las que se encuentra implicada, al menos, una parte interna a la empresa	Actividades no autorizadas	i) Operaciones no reveladas intencionalmente; ii) Operaciones no autorizadas con pérdidas monetarias; y iii) Valoración errónea intencional de posiciones
		Hurto y fraude	i) Fraude/fraude crediticio/ depósitos sin valor Hurto/extorsión/malversación / robo; ii) Apropiación indebida de activos; iii) Destrucción dolosa de activos; iv) Falsificación; v) Utilización de cheques sin fondos; vi) Contrabando; vii) Apropiación de cuentas, de identidad, etc.; viii) Incumplimiento/evasión intencional de impuestos; ix) Soborno/cohecho; y x) Abuso de información privilegiada
Fraude externo	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte un tercero	Hurto y fraude	i) Hurto/robo; ii) Falsificación; y, iii) Utilización de cheques sin fondos
		Seguridad de los sistemas	i) Daños por ataques informáticos; y, ii) Robo de información con pérdidas monetarias
Relaciones laborales y seguridad en el puesto de	Pérdidas derivadas de actuaciones incompatibles con la	Relaciones laborales	i) Cuestiones relativas a remuneración, prestaciones sociales, extinción de contratos; y, ii) Organización laboral

trabajo	legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamaciones por daños personales, o sobre casos relacionados con la discriminación	Higiene y seguridad en el trabajo	i) Imposibilidad en general (resbalones, caídas, etc.); ii) Casos relacionados con las normas de higiene y seguridad en el trabajo; y, iii) Indemnización a los trabajadores
		Diversidad y discriminación	Todo tipo de discriminación
Incidencias en el negocio y fallos en los sistemas	Pérdidas derivadas de interrupción en los negocios o por fallas en los sistemas	Sistemas	i) Hardware; ii) Software; iii) Telecomunicaciones; y; iv)Interrupción / incidencias en el suministro

Categoría de Tipo de Eventos (nivel 1)	**Definición**	**Categoría (nivel 2)**	**Ejemplos de actividades (Nivel 3)**
Daños a activos materiales	Pérdidas derivadas por daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros eventos	Desastres otros acontecimientos	i) Pérdidas por desastres naturales; ii) Pérdidas humanas por causas externas (terrorismo, vandalismo)
Clientes, productos y prácticas empresariales	Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación profesional frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto	Adecuación, divulgación de información y confianza	i) Abusos de confianza / incumplimiento de pautas; ii) Apropiamiento / divulgación de información; iii) Violación de la privacidad de clientes minoristas; iv) Quebrantamiento de privacidad; v) Ventas agresivas; vi) Pérdidas de cuentas; vii) Mal uso de información confidencial; y ii) Responsabilidad del prestamista
		Prácticas empresariales o de mercado impropias	i) Prácticas anticompetencia; ii) Prácticas impropias comerciales y de mercado; iii) Manipulación del mercado; iv) Comercialización de información privilegiada a favor de la empresa; v) Actividades no autorizadas; y, vi) Lavado de dinero
		Productos defectuosos	i) Defectos del producto; y, ii) Error de modelo

		Selección, patrocinio y riesgos	i) Fallida investigación a clientes según los protocolos; y, ii) Superación de los límites de exposición frente a clientes
		Actividades de asesoramiento	Litigios sobre resultados de las actividades de asesoramiento
Ejecución, entrega y gestión de procesos	Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores	Recepción, ejecución y mantenimiento de operaciones	i) Comunicación defectuosa; ii) Errores de introducción de datos, mantenimiento o descarga; iii) Incumplimiento de plazos o de responsabilidades; iv) Ejecución errónea de modelos / sistemas; v) Error contable / atribución a entidades erróneas; vi) Errores en otras tareas; vii) Fallo en la entrega; viii) Fallo en la gestión del colateral; y ix) Mantenimiento de datos de referencia

Categoría de Tipo de Eventos (nivel 1)	Definición	Categoría (nivel 2)	Ejemplos de actividades (Nivel 3)
		Seguimiento y monitoreo	i) Incumplimiento en la obligación reportar; y, ii) Inexactitud de informes externos (incurriendo en pérdidas)
		Aceptación de clientes y documentación	i) Extravío de autorizaciones / rechazos de clientes; y, ii) Documentos jurídicos inexistentes / incompletos
		Gestión de cuentas de clientes	i) Acceso no autorizado a cuentas; ii) Registros incorrectos de clientes (incurriendo en pérdidas); y, iii) Pérdida o daño de activos de clientes por negligencia
		Contrapartes comerciales	i) Fallos con contrapartes no-clientes; y ii) Otros litigios con contrapartes distintas de clientes
		Distribuidores y proveedores	i) Subcontratación; y, ii) Litigios con distribuidores

Mgs. Jaqueline Vargas Camacho
DIRECTORA (E)

Quito:
Calle Mañosca 201 y Av. 10 de Agosto
Atención ciudadana
Telf.: 3941-800
Ext.: 3134

www.registroficial.gob.ec

NGA/FMA

El Pleno de la Corte Constitucional mediante Resolución Administrativa No. 010-AD-CC-2019, resolvió la gratuidad de la publicación virtual del Registro Oficial y sus productos, así como la eliminación de su publicación en sustrato papel, como un derecho de acceso gratuito de la información a la ciudadanía ecuatoriana.

"Al servicio del país desde el 1º de julio de 1895"