SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

Lima, 19 de febrero de 2021

Resolución S.B.S.
Nº 504-2021

La Superintendenta de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones

CONSIDERANDO:

Que, el Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, aprobado mediante la Resolución SBS N° 272-2017, incorpora disposiciones que tienen por finalidad que las empresas supervisadas cuenten con una gestión de riesgos y gobierno corporativo adecuados;

Que, mediante el Reglamento para la Gestión del Riesgo Operacional, aprobado mediante la Resolución SBS N° 2116-2009, se incluyen disposiciones que las empresas deben cumplir en la gestión efectiva del riesgo operacional;

Que, esta Superintendencia emitió la Circular G-140-2009 con la finalidad de establecer criterios mínimos para una adecuada gestión de la seguridad de la información;

Que, resulta necesario actualizar la normativa sobre gestión de seguridad de la información vía la aprobación de un reglamento, complementario al Reglamento para la Gestión del Riesgo Operacional, tomando en cuenta los estándares y buenas prácticas internacionales sobre seguridad de la información, entre los que se encuentran los publicados por el National Institute of Standards and Technology y la familia de estándares ISO/IEC;

Que, la creciente interconectividad y mayor adopción de canales digitales para la provisión de los servicios, así como la virtualización de algunos productos, del sistema financiero, de seguros y privado de pensiones, hace necesario que las empresas de dichos sistemas supervisados fortalezcan sus capacidades de ciberseguridad y procesos de autenticación;

Que, asimismo, es necesario modificar el Reglamento de Tarjetas de Crédito y Débito, aprobado por la Resolución SBS Nº 6523-2013 y normas sus modificatorias; el Reglamento de Operaciones con Dinero Electrónico aprobado por Resolución SBS N° 6283-2013 y sus normas modificatorias; el Reglamento de Auditoría Interna, aprobado por la Resolución SBS Nº 11699-2008 y sus normas modificatorias; así como el Reglamento de Auditoría Externa, aprobado por la Resolución SBS Nº 17026-2010 y sus normas modificatorias;

Que, para recoger las opiniones del público, se dispuso la prepublicación del proyecto de resolución sobre la materia en el portal electrónico de la Superintendencia, al amparo de lo dispuesto en el Decreto Supremo Nº 001-2009-JUS;

Con el visto bueno de las Superintendencias Adjuntas de Banca y Microfinanzas, de Administradoras Privadas de Fondos de Pensiones, de Seguros, de Riesgos, de Conducta de Mercado e Inclusión Financiera y de Asesoría Jurídica; y,

En uso de las atribuciones conferidas por los numerales 7 y 9 del artículo 349 de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, Ley N° 26702 y sus modificatorias, y el inciso d) del artículo 57 de la Ley del Sistema Privado de Administración de Fondos de Pensiones, cuyo Texto Único Ordenado es aprobado por Decreto Supremo N° 054-97-EF;

RESUELVE:

Artículo Primero.- Aprobar el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, según se indica a continuación**:**

REGLAMENTO PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Alcance

1.1. El presente Reglamento es de aplicación a las empresas señaladas en los artículos 16 y 17 de la Ley General, así como a las Administradoras Privadas de Fondos de Pensiones (AFP), en adelante empresas, al igual que las referidas en los párrafos 1.2 y 1.3.

1.2. También es de aplicación al Banco de la Nación, al Banco Agropecuario, a la Corporación Financiera de Desarrollo (COFIDE), al Fondo MIVIVIENDA S.A., y a las Derramas y Cajas de Beneficios bajo control de la Superintendencia, en tanto no se contrapongan con las normativas específicas que regulen el accionar de dichas instituciones.

1.3. Es de aplicación a las empresas corredoras de seguros de acuerdo con lo dispuesto en la Cuarta Disposición Complementaria Final del presente Reglamento.

Artículo 2. Definiciones

Para efectos de la aplicación del presente Reglamento deben considerarse las siguientes definiciones:

a) **Activo de información**: Información o soporte en que ella reside, que es gestionado de acuerdo con las necesidades de negocios y los requerimientos legales, de manera que puede ser entendida, compartida y usada. Es de valor para la empresa y tiene un ciclo de vida.

b) **Amenaza**: Evento que puede afectar adversamente la operación de las empresas y sus activos de información, mediante el aprovechamiento de una vulnerabilidad.

c) **Autenticación:** Para fines de esta norma, es el proceso que permite verificar que una entidad es quien dice ser, para lo cual hace uso de las credenciales que se le asignan. La autenticación puede usar uno, dos o más factores de autenticación independientes, de modo que el uso sin autorización de uno de ellos no compromete la fiabilidad o el acceso a los otros factores.

d) **Canal digital**: Medio empleado por las empresas para proveer servicios cuyo almacenamiento, procesamiento y transmisión se realiza mediante la representación de datos en bits.

e) **Ciberseguridad**: Protección de los activos de información mediante la prevención, detección, respuesta y recuperación ante incidentes que afecten su disponibilidad, confidencialidad o integridad en el ciberespacio; el que consiste a su vez en un sistema complejo que no tiene existencia física, en el que interactúan personas, dispositivos y sistemas informáticos.
f) **Credencial**: Conjunto de datos que es generado y asignado a una entidad o un usuario para fines de autenticación.
g) **Directorio**: Directorio u órgano equivalente.
h) **Entidad**: Usuario, dispositivo o sistema informático que tiene una identidad en un sistema, lo cual la hace separada y distinta de cualquier otra en dicho sistema.
i) **Evento**: Un suceso o serie de sucesos que puede ser interno o externo a la empresa, originado por la misma causa, que ocurre durante el mismo periodo de tiempo, según lo definido en el Reglamento de Gobierno Corporativo y Gestión Integral de Riesgos.
j) **Factores de autenticación de usuario**: Aquellos factores empleados para verificar la identidad de un usuario, que pueden corresponder a las siguientes categorías:
   - Algo que solo el usuario conoce.
   - Algo que solo el usuario posee.
   - Algo que el usuario es, que incluye las características biométricas.
k) **Identidad:** Una colección de atributos que definen de forma exclusiva a una entidad.
l) **Incidente:** Evento que se ha determinado que tiene un impacto adverso sobre la organización y que requiere de acciones de respuesta y recuperación.
m) **Información**: Datos que pueden ser procesados, distribuidos, almacenados y representados en cualquier medio electrónico, digital, óptico, magnético, impreso u otros, que son el elemento fundamental de los activos de información.
n) **Interfaz de programación de aplicaciones**: Colección de métodos de invocación y parámetros asociados que puede utilizar un software para solicitar acciones de otro software, lo que define los términos en que estos intercambian datos. También conocido como API, por sus siglas en inglés.
o) **Servicios en nube**: Servicio de procesamiento de datos provisto mediante una infraestructura tecnológica que permite el acceso de red a conveniencia y bajo demanda, a un conjunto compartido de recursos informáticos configurables que se pueden habilitar y suministrar rápidamente, con mínimo esfuerzo de gestión o interacción con los proveedores de servicios.
p) **Reglamento:** Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad.
q) **Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos:** Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, aprobado por la Resolución SBS Nº 272-2017 y sus normas modificatorias.
r) **Reglamento para la Gestión de Riesgo Operacional**: Reglamento para la Gestión de Riesgo Operacional, aprobado por la Resolución SBS Nº 2116-2009 y sus normas modificatorias.
s) **Superintendencia:** Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones.
t) **Procesamiento de datos:** El conjunto de procesos que consiste en la recolección, registro, organización, estructuración, almacenamiento, adaptación, recuperación, consulta, uso, transferencia, difusión, borrado o destrucción de datos.
u) **Usuario:** persona natural o jurídica que utiliza o puede utilizar los productos ofrecidos por las empresas.
v) **Vulnerabilidad**: Debilidad que expone a los activos de información ante amenazas que pueden originar incidentes con afectación a los mismos activos de información, y a otros de los que forma parte o con los que interactúa.

Artículo 3. Sistema de gestión de seguridad de la información y Ciberseguridad (SGSI-C)

3.1. El sistema de gestión de seguridad de la información y ciberseguridad (SGSI-C) es el conjunto de políticas, procesos, procedimientos, roles y responsabilidades, diseñados para identificar y proteger los activos de información, detectar eventos de seguridad, así como prever la respuesta y recuperación ante incidentes de ciberseguridad.

3.2. El sistema de gestión de seguridad de la información y ciberseguridad (SGSI-C) implica, cuando menos, los siguientes objetivos:

a) Confidencialidad: La información sólo es disponible para entidades o procesos autorizados, incluyendo las medidas para proteger la información personal y la información propietaria;
b) Disponibilidad: Asegurar acceso y uso oportuno a la información; e,
c) Integridad: Asegurar el no repudio de la información y su autenticidad, y evitar su modificación o destrucción indebida.

Artículo 4. Proporcionalidad del sistema de gestión de seguridad de la información y ciberseguridad (SGSI-C)

4.1. El sistema de gestión de seguridad de la información y ciberseguridad (SGSI-C) de la empresa debe ser proporcional al tamaño, la naturaleza y la complejidad de sus operaciones.

4.2. Las disposiciones descritas en el Capítulo II, Subcapítulos I, II, III y IV del presente Reglamento son de aplicación obligatoria a las siguientes empresas (Régimen General):

a) Empresa Bancaria;
b) Empresa Financiera;
c) Caja Municipal de Ahorro y Crédito - CMAC;
d) Caja Municipal de Crédito Popular - CMCP;
e) Caja Rural de Ahorro y Crédito - CRAC;
f) Empresa de Seguros y/o Reaseguros, conforme a lo dispuesto en el párrafo 4.4;
g) Empresa de Transporte, Custodia y Administración de Numerario;
h) Administradora Privada de Fondos de Pensiones;
i) Empresa Emisora de Tarjetas de Crédito y/o de Débito;
j) Empresa Emisora de Dinero Electrónico; y
k) El Banco de la Nación.

4.3. Las disposiciones descritas en el Capítulo II, Subcapítulo V del presente Reglamento son de aplicación obligatoria a las siguientes empresas (Régimen Simplificado)[1]:

a) Banco de Inversión;
b) Empresa de Seguros y/o Reaseguros, no contempladas en el párrafo 4.4;
c) Entidad de Desarrollo a la Pequeña y Micro Empresa – EDPYME;
d) Empresa de Transferencia de Fondos;
e) Derrama y Caja de Beneficios bajo control de la Superintendencia;
f) La Corporación Financiera de Desarrollo –COFIDE;
g) El Fondo MIVIVIENDA S.A.;
h) Empresas afianzadoras y de garantías; y
i) El Banco Agropecuario.

[1] Párrafo modificado por la Resolución SBS Nº 1515-2021 del 24/05/2021.

4.4. Las empresas de Seguros y/o Reaseguros cuyo volumen promedio de activos de los últimos tres (3) años sea mayor o igual a 450 millones de soles están comprendidas en el Régimen General del presente Reglamento.

4.5. Las empresas señaladas en el Artículo 1, no listadas en los párrafos 4.2 o 4.3 anteriores del presente Reglamento, podrán establecer un sistema de gestión de seguridad de la información y ciberseguridad (SGSI-C) conforme a las disposiciones de este Reglamento.

4.6. En caso las empresas del Sistema Financiero y las empresas emisoras de dinero electrónico listadas en el párrafo 4.2 encuentren limitaciones materiales para cumplir con el Régimen General pueden solicitar autorización para la aplicación del Régimen Simplificado del presente Reglamento, para lo cual deben presentar un informe que sustente la razonabilidad de la solicitud, en términos del tamaño, la naturaleza y la complejidad de sus operaciones, la cual será respondida por la Superintendencia en el plazo de sesenta (60) días hábiles[2].

4.7. Las disposiciones descritas en el Capítulo II, Subcapítulo VI (Régimen Reforzado) del presente Reglamento son de aplicación obligatoria a las empresas sujetas a un requerimiento de patrimonio efectivo por riesgo de concentración de mercado, de acuerdo con lo señalado en el Reglamento para el requerimiento de patrimonio efectivo adicional, aprobado por la Resolución SBS Nº 8425-2011 y sus normas modificatorias.

Artículo 5. Responsabilidades del directorio
El directorio es responsable de aprobar y facilitar las acciones requeridas para contar con un SGSI-C apropiado a las necesidades de la empresa y su perfil de riesgo, entre ellas:

a) Aprobar políticas y lineamientos para la implementación del SGSI-C y su mejora continua.
b) Asignar los recursos técnicos, de personal, financieros requeridos para su implementación y adecuado funcionamiento.
c) Aprobar la organización, roles y responsabilidades para el SGSI-C, incluyendo los lineamientos de difusión y capacitación que contribuyan a un mejor conocimiento de los riesgos involucrados.

Artículo 6. Responsabilidades de la gerencia
6.1 La gerencia general es responsable de tomar las medidas necesarias para implementar el SGSI-C de acuerdo a las disposiciones del directorio y lo dispuesto en este Reglamento.

6.2 Los gerentes de las unidades de negocios y de apoyo son responsables de apoyar el buen funcionamiento del SGSI-C y gestionar los riesgos asociados a la seguridad de la información y Ciberseguridad en el marco de sus funciones.

Artículo 7. Funciones del comité de riesgos
7.1 Adicionalmente a las funciones que se han dispuesto que el Comité de Riesgos de las empresas asuman por parte de la normativa de la Superintendencia, se encuentran las siguientes vinculadas a la seguridad de la información y ciberseguridad:
   a) Aprobar el plan estratégico del SGSI-C y recomendar acciones a seguir.
   b) Aprobar el plan de capacitación a fin de garantizar que el personal, la plana gerencial y el directorio cuenten con competencias necesarias en seguridad de la información y Ciberseguridad.

[2] Párrafo modificado por la Resolución SBS Nº 1515-2021 del 24/05/2021.

c) Fomentar la cultura de riesgo y conciencia de la necesidad de medidas apropiadas para su prevención.

7.2. Para el cumplimiento de las funciones indicadas en el párrafo 7.1, la empresa puede constituir un Comité Especializado en Seguridad de la Información y Ciberseguridad (CSIC). Para las empresas comprendidas en el régimen simplificado, que no cuenten con un Comité de Riesgos o un CSIC, las funciones antes indicadas son asignadas a la Gerencia General.

Artículo 8. Función de Seguridad de Información y Ciberseguridad

8.1. Son responsabilidades de la función de seguridad de la información y ciberseguridad:

a) Proponer el Plan estratégico del SGSI-C y desarrollar los planes operativos.
b) Implementar y manejar las operaciones diarias necesarias para el funcionamiento efectivo del SGSI-C.
c) Implementar procesos de autenticación para controlar el acceso a la información y sistema que utilice la empresa, y a los servicios que provea.
d) Informar al Comité de Riesgos periódicamente sobre los riesgos que enfrenta la empresa en materia de seguridad de información y ciberseguridad.
e) Informar sobre los incidentes de seguridad de la información al Comité de Riesgos o CSIC, según los lineamientos que este establezca, y a las entidades gubernamentales que lo requieran de acuerdo con la normativa vigente.
f) Evaluar las amenazas de seguridad en las estrategias de continuidad del negocio que la empresa defina y proponer medidas de mitigación de riesgos, así como informar al Comité de Riesgos o CSIC.
g) En general realizar lo necesario para dar debido cumplimiento a lo dispuesto en el presente Reglamento.

8.2. Las empresas deben implementar la función de seguridad de la información y ciberseguridad. Además deben contar con un equipo de trabajo multidisciplinario de manejo de incidentes de ciberseguridad, el cual debe estar capacitado para implementar el plan y los procedimientos para gestionarlos, conformado por representantes de las áreas que permitan prever en ellos los aspectos legales, técnicos y organizacionales, de forma consistente con los requerimientos del programa de ciberseguridad establecidos en este Reglamento.

8.3. Las empresas comprendidas en el régimen simplificado, deben contar con una función de seguridad de la información y ciberseguridad, que cumpla por lo menos con los literales a), e), f) y g) del párrafo 8.1 del presente artículo.

Artículo 9. Información a la Superintendencia

Como parte de los informes periódicos sobre gestión del riesgo operacional requeridos por el Reglamento para la Gestión del Riesgo Operacional, las empresas deben incluir información sobre la gestión de la seguridad de la información y ciberseguridad.

CAPÍTULO II
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD (SGSI-C)

SUBCAPÍTULO I
RÉGIMEN GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD (SGSI-C)

Artículo 10. Objetivos y requerimientos del SGSI-C
Son objetivos del SGSI-C los siguientes:

1. Identificar los activos de información, analizar las amenazas y vulnerabilidades asociadas a estos, y formular programas y medidas que busquen reducir la posibilidad de incidentes en los siguientes aspectos:

   a) El diseño e implementación de nuevos productos y procesos, proyectos y cambios operativos.
   b) Las obligaciones de seguridad de la información que se derivan de disposiciones normativas, normas internas y de acuerdos contractuales.
   c) Las relaciones con terceros, en el sentido más amplio, incluyendo proveedores de servicios y empresas con las que se tiene relaciones de subcontratación.
   d) Cualquier otra actividad que, a criterio de la empresa, exponga sus activos de información por causa interna o externa.

2. Revisar periódicamente el alcance y la efectividad de los controles mínimos indicados en el artículo 12 de este Reglamento y contar con capacidades de detección, respuesta y recuperación ante incidentes de seguridad de la información.

3. Establecer la relación existente con los planes de emergencia, crisis y de continuidad establecidos según lo previsto en la normativa correspondiente.

Artículo 11. Alcance del SGSI-C
El alcance del SGSI-C debe incluir las funciones y unidades organizacionales, las ubicaciones físicas existentes, la infraestructura tecnológica y de comunicaciones, así como el perímetro de control asociado a las relaciones con terceros, que estén bajo responsabilidad de la empresa, conforme a las disposiciones establecidas sobre subcontratación en el Reglamento de Gobierno Corporativo y Gestión Integral de Riesgos.

Artículo 12. Medidas mínimas de seguridad de la información a adoptar por las empresas
Las empresas deben adoptar las siguientes medidas mínimas de seguridad de información:

1. Seguridad de los recursos humanos:
   a) Implementar protocolos de seguridad de la información aplicables en el reclutamiento e incorporación del personal, ante cambio de puesto y terminación del vínculo laboral.
   b) Procesos disciplinarios en caso de incumplimiento de las políticas de seguridad de la información.
2. Controles de acceso físico y lógico:
   a) Prevenir el acceso no autorizado a la información, así como a los sistemas, equipos e instalaciones mediante los cuales es procesada, transmitida o almacenada, sea de manera presencial o remota.
   b) Implementar procedimientos de administración de accesos, lo que debe incluir a las cuentas de accesos con privilegios administrativos; asegurando una segregación de funciones para reducir el riesgo de error o fraude, siguiendo los principios de mínimo privilegio y necesidad de conocer.

c) Implementar procesos de autenticación para controlar el acceso a los activos de información; en particular, para el acceso a los servicios provistos a usuarios por canales digitales, los procesos de autenticación deben cumplir los requisitos establecidos en el Subcapítulo III del Capítulo II del presente Reglamento.

3. Seguridad en las operaciones:
   a) Asegurar y prever el funcionamiento continuo de las instalaciones de procesamiento, almacenamiento y transmisión de información.
   b) Mantener la operación de los sistemas informáticos acorde a procedimientos previamente establecidos.
   c) Controlar los cambios en el ambiente operativo de sistemas, y mantener segregados los ambientes de desarrollo, pruebas y producción.
   d) Implementar controles que aseguren la integridad de las transacciones que son ejecutadas en los servicios y sistemas informáticos.
   e) Restringir la instalación de software en los sistemas operativos y prevenir la explotación de las vulnerabilidades de seguridad de la información.
   f) Contar con protocolos de respuesta y recuperación ante incidentes de malware; generar y probar copias de respaldo de información, software y elementos que faciliten su restablecimiento.
   g) Definir, implementar y mantener líneas base de configuración segura para el uso de dispositivos e implementación de sistemas informáticos.
   h) Contar con una estrategia de copias de respaldo y procedimientos de restauración de información ante posibles incidentes, de origen interno o externo, que comprometa la disponibilidad de la información para las operaciones y del ambiente productivo del centro de procesamiento de datos.

4. Seguridad en las comunicaciones:
   a) Implementar y mantener la seguridad de redes de comunicaciones acorde a la información que por ella se trasmite y las amenazas a las que se encuentra expuesta.
   b) Asegurar que las redes de comunicaciones y servicios de red son gestionados y controlados para proteger la información.
   c) Segregar los servicios de información disponibles, usuarios y sistemas en las redes de la empresa.
   d) Implementar protocolos seguros y controles de seguridad para la transferencia de información, dentro de la organización y con partes externas.
   e) Asegurar que el acceso remoto, el uso de equipos personales en la red de la empresa, dispositivos móviles y la interconexión entre redes propias y de terceros cuente con controles acorde a las amenazas de seguridad existentes.

5. Adquisición, desarrollo y mantenimiento de sistemas:
   a) Implementar y mantener la seguridad en los servicios y sistemas informáticos acorde a la información que se procese y amenazas a las que se encuentren expuestos.
   b) Asegurar que se incluyan prácticas de seguridad de la información en la planificación, desarrollo, implementación, operación, soporte y desactivación en las aplicaciones y sistemas informáticos.
   c) Limitar el acceso a la modificación de librerías de programas fuente y mantener un estricto control de cambios.
   d) Cuando la plataforma operativa sea cambiada, las aplicaciones críticas deben ser revisadas y probadas para evitar efectos adversos en la seguridad de estas.

e) Asegurar que se efectúen pruebas técnicas, funcionales y de seguridad de la información en los sistemas informáticos antes del pase a producción.
f) Implementar y verificar el cumplimiento de procedimientos que incluyan prácticas de desarrollo seguro de servicios y sistemas informáticos.

6. Gestión de incidentes de ciberseguridad:
   a) Implementar procedimientos para la gestión de incidentes de ciberseguridad, de acuerdo a lo señalado en el párrafo 8.2 del artículo 8 del presente Reglamento; así también, intercambiar información cuando corresponda, conforme al artículo 16 del presente Reglamento.
   b) Implementar una metodología para clasificar los incidentes de ciberseguridad y prever protocolos de respuesta y recuperación.
   c) Contar con un servicio de operaciones de seguridad de la información, que incluya capacidades para la detección y respuesta, el monitoreo de comunicaciones en la red interna y el grado de funcionamiento de la infraestructura tecnológica.
   d) Contar con acceso a la información de inteligencia de amenazas, vulnerabilidades e incidentes, así como también a bases de conocimiento de técnicas y tácticas utilizadas por los agentes de amenazas.
   e) Implementar mecanismos de reporte interno de incidentes de ciberseguridad, de acuerdo con lo señalado en el artículo 8 del presente Reglamento, y a la Superintendencia conforme al artículo 15 del presente Reglamento.
   f) Identificar las posibles mejoras para su incorporación a la gestión de incidentes de ciberseguridad, luego de la ocurrencia de estos.
   g) Preservar las evidencias que faciliten las investigaciones forenses luego de la ocurrencia de incidentes de seguridad de la información.

7. Seguridad física y ambiental
   a) Implementar controles para evitar el acceso físico no autorizado, daños o interferencias a la información o instalaciones de procesamiento de la empresa.
   b) Adoptar medidas para evitar pérdida, daño, robo o compromiso de los activos de información y la interrupción de las operaciones, mediante la protección del equipamiento y dispositivos tomando en cuenta el entorno donde son utilizados.

8. Criptografía
   a) Utilizar criptografía para asegurar la confidencialidad, autenticidad e integridad de la información, tanto cuando los datos asociados están en almacenamiento y en transmisión.
   b) Implementar los procedimientos necesarios para administrar el ciclo de vida de las llaves criptográficas a utilizar.

9. Gestión de activos de información
   a) Identificar los activos de información mediante un inventario, asignar su custodia, establecer lineamientos de uso aceptable de ellos y la devolución al término del acuerdo por el que se proporcionó.
   b) Asegurar que el nivel de protección y tratamiento de la información se realice acorde a su clasificación en términos de los requisitos legales, valor, criticidad y sensibilidad a la divulgación o modificación no autorizada.
   c) Establecer medidas para evitar la divulgación, modificación, eliminación o destrucción no autorizadas de información, en el uso de dispositivos removibles.

Artículo 13. Actividades planificadas
En el marco del Plan estratégico del SGSI-C, la empresa debe mantener planes operativos, por lo menos para los siguientes fines:

a) Identificar los activos de información, clasificarlos, analizar las amenazas y vulnerabilidades asociadas a estos, y tomar medidas de tratamiento correspondientes.
b) Someter el SGSI-C a evaluaciones, revisiones y pruebas periódicas para determinar su efectividad, mediante servicios internos y externos, y en función al nivel de complejidad y amenazas sobre los activos de información asociados. En función a los resultados que obtenga, debe incorporar las mejoras o adoptar los correctivos.
c) Atender las necesidades de capacitación y difusión, según corresponda a los roles y funciones en la organización, en materia de seguridad de la información y ciberseguridad para asegurar la efectividad del SGSI-C.
d) Desarrollar el programa de ciberseguridad, conforme al Subcapítulo II del Capítulo II del presente Reglamento.
e) Revisar periódicamente, y actualizar cuando corresponda, las políticas de seguridad de la información que se establezcan para implementar los requerimientos establecidos en el artículo 12 del presente Reglamento.

SUBCAPÍTULO II
CIBERSEGURIDAD

Artículo 14. Programa de ciberseguridad
14.1 Toda empresa que cuente con presencia en el ciberespacio debe mantener, con carácter permanente, un programa de ciberseguridad (PG-C) aplicable a las operaciones, procesos y otros activos de información asociados.

14.2 El PG-C debe prever un diagnóstico y un plan de mejora sobre sus capacidades de ciberseguridad, para lo cual debe seleccionar un marco de referencia internacional sobre la materia, que le permita cuando menos lo siguiente:
a) Identificación de los activos de información.
b) Protección frente a las amenazas a los activos de información.
c) Detección de incidentes de ciberseguridad.
d) Respuesta con medidas que reduzcan el impacto de los incidentes.
e) Recuperación de las capacidades o servicios tecnológicos que pudieran ser afectados.

Artículo 15. Reporte de incidentes de ciberseguridad significativos
15.1 La empresa debe reportar a la Superintendencia, en cuanto advierta la ocurrencia de un incidente de ciberseguridad que presente un impacto adverso significativo verificado o presumible de:

a) Pérdida o hurto de información de la empresa o de clientes.
b) Fraude interno o externo.
c) Impacto negativo en la imagen y reputación de la empresa.
d) Interrupción de operaciones.

15.2 La empresa debe efectuar un análisis forense para determinar las causas del incidente y tomar las medidas para su gestión. El informe resultante de dicho análisis debe estar a disposición de la Superintendencia, el que debe tener un contenido ejecutivo y también con el detalle técnico correspondiente.

15.3 La Superintendencia, mediante norma de carácter general, establece el contenido mínimo, formato y protocolos adicionales a utilizar en dicho reporte.

Artículo 16. Intercambio de información de ciberseguridad

16.1 La empresa debe hacer los arreglos necesarios para contar con información que le permita tomar acción oportuna frente a las amenazas de ciberseguridad y para el tratamiento de las vulnerabilidades.

16.2 Al intercambiar información relativa a ciberseguridad, la empresa puede suscribir acuerdos con otras empresas del sector o con terceros que resulten relevantes, de forma bipartita, colectiva o gremial, para lo cual definirán los criterios pertinentes.

16.3 Mediante norma de carácter general, la Superintendencia puede establecer requerimientos específicos para que se incorporen en el intercambio de información de ciberseguridad.

SUBCAPÍTULO III
AUTENTICACIÓN

Artículo 17. Implementación de los procesos autenticación

17.1 La empresa debe implementar procesos de autenticación, conforme a la definición establecida en este Reglamento, para controlar el acceso a los servicios que provea a sus usuarios por canales digitales, previo a lo cual debe evaluar formalmente y tomar medidas sobre:

a) El o los factores de autenticación que serán requeridos.
b) Estándares criptográficos vigentes, basados en software o en hardware, y sus prestaciones de confidencialidad o integridad esperadas.
c) Plazos y condiciones en las que será obligatorio requerir al usuario volver a autenticarse, lo que incluye y no se limita a casos por periodo de inactividad o sesiones de uso prolongado de sistemas.
d) Línea base de controles de seguridad de la información requerida para prevenir las amenazas a que esté expuesto el proceso de autenticación, lo que incluye, y no se restringe, al número límite de intentos fallidos de autenticación, la prevención de ataques de interceptación y manipulación de mensajes.
e) Lineamientos para la retención de registros de auditoría para la detección de amenazas conocidas y eventos de seguridad de la información.

17.2 Los procesos de autenticación deben ser reevaluados siempre que la tecnología utilizada para su implementación deje de contar con el soporte del fabricante, o tras el descubrimiento de nuevas vulnerabilidades que pueden exponerlos.

17.3 La empresa debe mantener y proteger los registros detallados de lo actuado en cada enrolamiento de usuario, intento de autenticación y cada operación que requiera de autenticación previa.

17.4 La empresa debe contar con herramientas y procedimientos para implementar el monitoreo de transacciones que permita tomar medidas de reducción de la posibilidad de operaciones fraudulentas, que incorpore los escenarios de fraude ya conocidos, y el robo o compromiso de los elementos utilizados para la autenticación.

Artículo 18. Enrolamiento del usuario en servicios provistos por canal digital

18.1 El enrolamiento de un usuario en un canal digital requiere por lo menos:

a) Verificar la identidad del usuario y tomar las medidas necesarias para reducir la posibilidad de suplantación de identidad, lo que incluye el uso de dos factores independientes de categorías diferentes, según el literal j) del artículo 2 de este Reglamento.
b) Generar las credenciales y asignarlas al usuario.

18.2 La empresa debe gestionar el ciclo de vida de las credenciales que genere y asigne a sus usuarios, para lo cual debe prever los procedimientos para su activación, suspensión, reemplazo, renovación y revocación; así también, cuando corresponda, asegurar su confidencialidad e integridad.

Artículo 19. Autenticación reforzada para operaciones por canal digital

Se requiere de autenticación reforzada para aquellas acciones que puedan originar operaciones fraudulentas u otro abuso del servicio en perjuicio del cliente, como las operaciones a través de un canal digital que impliquen pagos o transferencia de fondos a terceros, registro de un beneficiario de confianza, modificación en los productos de seguro ahorro/inversión contratados, la contratación de un producto o servicio, modificación de límites y condiciones, para lo cual se requiere:

a) Utilizar una combinación de factores de autenticación, según el literal j) del artículo 2 del presente Reglamento que, por lo menos, correspondan a dos categorías distintas y que sean independientes uno del otro.
b) Generar un código de autenticación mediante métodos criptográficos, a partir de los datos específicos de cada operación, el cual debe utilizarse por única vez.
c) Cuando la operación sea exitosa, notificar los datos de la operación al usuario.

Artículo 20. Exenciones de autenticación reforzada para operaciones por canal digital

20.1 Están exentas del requisito de autenticación reforzada indicado en el artículo 19 del presente Reglamento, las siguientes operaciones realizadas por canal digital:

a) Las operaciones de pago, pagos periódicos o transferencia hacia un beneficiario registrado previamente por el usuario como beneficiario de confianza, como destinatario usual de dichas operaciones.
b) Las operaciones de pago, pagos periódicos o transferencias a cuentas en las que el cliente y el beneficiario sean la misma persona, sea natural o jurídica, y siempre que dichas cuentas se mantengan en la misma empresa.

20.2 Las operaciones de pago que presenten un nivel de riesgo de fraude bajo, como resultado de un análisis del riesgo en línea por operación, están exentas de la autenticación reforzada, siempre que la empresa cumpla con:

i. Implementar alguno de los estándares de la industria de pagos, EMV 3DS y tokenización de pagos EMV, en sus versiones más recientes.
ii. Definir el monto de umbral por operación por debajo del cual aplicará la exención por el citado análisis de riesgos.

iii. Medir periódicamente el ratio de fraude de las operaciones de pago por canal y tipo de operación.
iv. Actualizar periódicamente las reglas aplicables en el análisis de riesgo en función al indicador de riesgo de fraude.
v. Utilizar los datos que estén disponibles por cada tipo de operación, que incluye, pero no se limita a, los asociados al comportamiento del usuario, al medio utilizado y los que de este se pueda obtener para fines del análisis de riesgo.

20.3 Las operaciones no reconocidas por los clientes que hayan sido efectuadas en aplicación de la exención señalada en el párrafo 20.2 del presente artículo, o que fueron realizadas luego de que el usuario reportara el robo o pérdida de sus credenciales, son responsabilidad de la empresa, para lo cual deben implementar mecanismos que ante el repudio de la operación por parte del usuario garanticen su aplicación inmediata.

Artículo 21. Uso de API para la provisión de servicios en línea

21.1 El uso de interfaces de programación de aplicaciones, para proveer servicios para realizar operaciones, a través de servicios de terceros, requiere que se implementen las siguientes medidas:
a) Análisis de riesgos asociados e implementar las medidas de mitigación.
b) La autenticación mutua de los sistemas y la de los usuarios.
c) La autorización de las operaciones por parte de los usuarios.
d) El cifrado de datos en almacenamiento o transmisión.
e) Prácticas de desarrollo seguro de API y revisión de prácticas de codificación segura.
f) Análisis de vulnerabilidades y pruebas de penetración.
g) La seguridad de la infraestructura tecnológica que lo soporta.
h) Los mecanismos de tolerancia ante fallos y de contingencia.
i) Control de accesos en el entorno de datos, sistemas e infraestructura.
j) Monitoreo de eventos de seguridad de la información y gestión de estos cuando se constituyan en incidentes.

21.2 La empresa debe tomar como referencia estándares y marcos de referencia internacionales, y cuando sea factible adoptarlos en el marco de acuerdos gremiales o sectoriales, para la implementación del intercambio y encriptación de datos, así como la autenticación y la autorización de operaciones, sin que ello sea una lista restrictiva.

21.3 Las especificaciones técnicas de las API utilizadas deben encontrarse documentadas de forma que facilite su auditoría y la implementación necesaria para su uso.

21.4 Las empresas deben implementar las medidas necesarias para garantizar que el tercero autorizado por el usuario, acceda únicamente a la información indicada por este último.

SUBCAPÍTULO IV
PROVISIÓN DE SERVICIOS POR TERCEROS

Artículo 22. Servicios provistos por terceros

En el caso de servicios provistos por terceros en aspectos referidos a gestión de tecnología de la información, a gestión de seguridad de la información o a procesamiento de datos, la empresa, además de cumplir con los requerimientos establecidos en el Reglamento de Gobierno Corporativo y Gestión Integral de Riesgos y el Reglamento para la Gestión de Riesgo Operacional debe:

a) Evaluar las amenazas y vulnerabilidades de seguridad de la información en la provisión de bienes y servicios e implementar medidas de tratamiento.
b) Asegurar que el arreglo contractual con el proveedor y su implementación le permiten cumplir con las obligaciones establecidas en el presente Reglamento.
c) Establecer los roles y responsabilidades que el proveedor asume contractualmente sobre la seguridad de la información y asegurar que la empresa efectúe las implementaciones complementarias correspondientes para la atención de los requerimientos del presente Reglamento.

Artículo 23. Uso de servicios en nube

Para hacer uso de los servicios en nube, la empresa debe implementar políticas y procedimientos de seguridad de la información que sean de aplicación específica, que tome en cuenta un marco de buenas prácticas internacionales para el uso de estos servicios, y que además de los requerimientos del artículo 22 del Reglamento, incluya los siguientes aspectos:

a) Requerimientos de seguridad de la información que los servicios de nube deben cumplir y procedimientos para asegurar la implementación antes de su uso.
b) Lineamientos para segregación de redes que permita el aislamiento de la información de la empresa respecto a la de terceros en el entorno compartido del servicio en nube.
c) Evaluación de la disponibilidad de registro de eventos (log) que el proveedor de servicio en nube ofrece y atención de la necesidad de registros adicionales para el monitoreo de seguridad de la información.
d) Previsión de plan de capacitación para los niveles gerenciales, administradores de estos servicios, personal a cargo de su implementación y quienes hacen uso de ellos, sobre aquello necesario para el manejo de la seguridad de la información en estos.

Artículo 24. Servicios significativos de procesamiento de datos

24.1 La contratación de un servicio significativo provisto por terceros para el procesamiento de datos, incluido los servicios en nube, debe ser considerado como un cambio importante en el ambiente informático, siendo aplicable la definición de servicio significativo establecida en el Reglamento de Gobierno Corporativo y Gestión Integral de Riesgos y la normativa vigente asociada a nuevos productos y cambios importantes.

24.2 La empresa debe cumplir los siguientes aspectos referidos a la contratación de un servicio significativo provisto por terceros para el procesamiento de datos, que incluye servicios en nube, de manera complementaria a lo establecido en los artículos 22 y 23 del presente Reglamento, según corresponda:

a) Asegurar el acceso adecuado a la información, en tiempos razonables y a solo requerimiento, por parte de la Superintendencia, Auditoría Interna y la Sociedad de Auditoría Externa, en condiciones normales de operación y en regímenes especiales.
b) Gestionar los incidentes de seguridad de la información, conforme al numeral 6 del artículo 12 y de desarrollar las actividades planificadas previstas en el artículo 13 del presente Reglamento, en lo aplicable al servicio significativo de procesamiento de datos del que se trate.
c) Contar con una estrategia de salida de los servicios a cargo del proveedor que permita retomar operaciones por cuenta propia o mediante otro proveedor. Dicha estrategia debe prever, entre

otros aspectos, las acciones necesarias para la migración de la información a los recursos de la empresa o de otro proveedor.[3]

d) Mantener un inventario de los servicios que el proveedor, a su vez, contrata con terceros (contratación en cadena) y que se encuentren relacionados a los servicios contratados por la empresa.
e) Asegurar que la información de carácter confidencial en custodia del proveedor sea eliminada definitivamente ante la resolución del acuerdo contractual.
f) Verificar anualmente que el proveedor de servicios de procesamiento de datos cuenta con controles de seguridad de la información, conforme a la normativa vigente sobre seguridad de la información, en lo aplicable al servicio provisto. Ello puede ser sustentado mediante informes independientes y reportes de auditoría que incluyen en su alcance la verificación de dichos controles.
g) Cuando se trate de servicios en nube, para cumplir con lo requerido en el literal previo, la empresa debe evidenciar anualmente que el proveedor mantiene vigente las certificaciones ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018, y que cuenta con un reporte SOC 2 tipo 2 u otros equivalentes, relevantes al servicio provisto y a la zona o región desde donde se provee el servicio.

24.3 La empresa debe informar a esta Superintendencia sobre el servicio contratado, el proveedor involucrado, los niveles de servicio acordados, infraestructura tecnológica utilizada, así como los procedimientos y responsables para dar cumplimiento a los literales del a) al f), y según corresponda g) del párrafo anterior; como máximo treinta (30) días calendario después de iniciar la provisión del procesamiento de datos[4].

Artículo 25. Autorización para la contratación de servicio significativo de procesamiento de datos provisto por terceros desde el exterior[5]

25.1 La empresa debe solicitar autorización de la Superintendencia, previo a la contratación de un servicio significativo de procesamiento de datos provisto por terceros desde el exterior, en caso dicho servicio presente limitaciones para cumplir con los requerimientos establecidos en el párrafo 24.2 del artículo 24 del presente Reglamento, la cual será respondida por la Superintendencia en el plazo de sesenta (60) días hábiles. Para solicitar dicha autorización las empresas deben presentar junto con su solicitud, un informe con los sustentos legales de las limitaciones identificadas y una propuesta de plan de implementación de las medidas compensatorias.

25.2 La autorización que conceda esta Superintendencia es específica al proveedor del servicio y, al país y ciudad desde el que se recibe, así como a las condiciones generales que fueron objeto de la autorización, por lo que de existir modificaciones en ellas y, de mantenerse la limitación citada en el párrafo previo, se requiere de un nuevo procedimiento de autorización ante la Superintendencia.

SUBCAPÍTULO V
RÉGIMEN SIMPLIFICADO DEL SGSI-C

[3] Inciso modificado por la Resolución SBS Nº 1515-2021 del 24/05/2021.
[4] Párrafo modificado por la Resolución SBS Nº 1515-2021 del 24/05/2021.
[5] Artículo vigente a partir del 24.02.2021

Artículo 26. Sistema simplificado de gestión de seguridad de la información

26.1 El régimen simplificado de gestión de seguridad de la información requiere la planificación y ejecución de las siguientes actividades mínimas, cuya periodicidad por lo menos debe ser anual:

a) Identificar con las unidades de negocio y de apoyo, cuál es la información de mayor importancia, por las obligaciones normativas o contractuales existentes, y por la necesidad de operar.
b) Identificar los dispositivos que se conectan a la red interna y todo software que se encuentre instalado en la infraestructura tecnológica, y asegurar que se encuentren acorde a una configuración segura previamente establecida.
c) Identificar las cuentas de usuario con permisos de acceso habilitados y en particular las que poseen privilegios administrativos con posibilidad de adicionar software a la infraestructura, y mantener el principio de mínimos privilegios otorgados.
d) Implementar y mantener una línea base de seguridad en sistemas operativos y aplicaciones utilizadas, incluidos los correspondientes a dispositivos móviles, estaciones de trabajo, servidores y dispositivos de comunicaciones. Identificar y evaluar la habilitación de las funciones de seguridad integradas en los sistemas operativos.
e) Priorizar y gestionar las vulnerabilidades de seguridad identificadas, para cuya identificación oportuna debe contar con los servicios de información necesarios.
f) Desarrollar una campaña de orientación para la adopción de prácticas seguras dirigida a los empleados, plana gerencial y de dirección.

26.2 En caso la empresa provea alguna de las operaciones indicadas en el artículo 19 del presente Reglamento por canal digital, en lo que corresponda a su implementación, debe cumplir con las disposiciones establecidas en el Subcapítulo III del Capítulo II del presente Reglamento.

26.3 En caso utilice servicios significativos provistos por terceros, en lo que corresponda a su implementación, la empresa debe cumplir con las disposiciones establecidas en el Subcapítulo IV del Capítulo II del presente Reglamento.

26.4 La empresa debe mantener un programa de ciberseguridad, conforme al Subcapítulo II del Capítulo II del presente Reglamento, con un alcance que por lo menos incluya los servicios indicados en los párrafos 26.2 y 26.3 del artículo 26 del presente Reglamento.

SUBCAPÍTULO VI
RÉGIMEN REFORZADO DEL SGSI-C

Artículo 27. Requerimientos adicionales para empresa con concentración de mercado

27.1 El directorio debe designar a un director como responsable de velar por la efectividad del sistema de gestión de seguridad de la información, lo que incluye el desarrollo del plan estratégico del SGSI-C.

27.2 La empresa debe someter periódicamente a una evaluación independiente del alcance y la efectividad del SGSI-C; dicha evaluación podrá ser realizada por la unidad de auditoría interna u otro equipo que cumpla el requisito de independencia, siempre que posea experiencia previa y certificaciones internacionales que demuestren la preparación técnica necesaria.

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera.- La empresa puede contar con un marco para la gestión de los riesgos asociados a la seguridad de la información, que debe ser integrado en lo que corresponda en la gestión del riesgo operacional, conforme a los lineamientos establecidos en el artículo 22° del Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos.

Segunda.- Los informes a los que se refieren los literales g) y h) del artículo 12°, y el artículo 27° del Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos deben incluir la evaluación de los riesgos asociados a la seguridad de la información.

Tercera- En caso de eventos que afecten la continuidad operativa y que tengan como causa probable un incidente de seguridad de la información, es aplicable lo señalado en el artículo 15 del Reglamento para la Gestión de la Continuidad del Negocio, aprobado por la Resolución SBS Nº 877-2020, sobre reporte de eventos de interrupción significativa.

Cuarta.- La aplicación del presente Reglamento se extiende a las empresas corredoras de seguros del segmento 1, según segmentación establecida en el artículo 36 del Reglamento para la Supervisión y Control de los Corredores y Auxiliares de Seguros aprobado por la Resolución SBS N° 809-2019, a dichas empresas les es exigible el párrafo 26.1 del artículo 26, Subcapítulo V, Capítulo II, del presente Reglamento.

Artículo Segundo.- Modificar el Reglamento de Auditoría Interna, aprobado por la Resolución SBS N° 11699-2008 y sus modificatorias, conforme a lo siguiente:

En el Anexo "Actividades Programadas", sustituir el numeral 3 de la Sección I, el numeral 1 de la Sección II, el numeral 1 de la Sección III, el numeral 2 de la Sección IV, el numeral 3 de la Sección V y el numeral 1 de la Sección VI, conforme a los siguientes textos:

> "I. ***EMPRESAS SEÑALADAS EN LOS LITERALES A, B Y C DEL ARTÍCULO 16° DE LA LEY GENERAL (EXCEPTO LAS EMPRESAS AFIANZADORAS Y DE GARANTÍAS), BANCO DE LA NACIÓN, BANCO AGROPECUARIO, FONDO MIVIVIENDA Y CORPORACIÓN FINANCIERA DE DESARROLLO (COFIDE)***
> *(….)*
> *3) Evaluación de la gestión del riesgo operacional y del cumplimiento de los procedimientos utilizados para la administración de los riesgos de operación; así como, de las disposiciones de la normativa vigente sobre gestión de continuidad del negocio y de seguridad de la información y ciberseguridad;*
> *(….)"*
>
> "II. ***EMPRESAS DE SEGUROS Y/O DE REASEGUROS:***
> *1) Evaluación de la gestión de los riesgos distintos a los riegos técnicos de seguros, que incluyen riesgo operacional, de mercado, de crédito, entre otros, y de las disposiciones de la normativa vigente sobre gestión de continuidad del negocio y de seguridad de la información y ciberseguridad;*
> *(...)"*
>
> *"III.* ***EMPRESAS DE SERVICIOS COMPLEMENTARIOS Y CONEXOS***
> *1) Evaluación de la gestión del riesgo operacional y del cumplimiento de los procedimientos utilizados para la administración de los riesgos de operación; así como, de las*

disposiciones de la normativa vigente sobre gestión de continuidad del negocio y de seguridad de la información y ciberseguridad.

(...)"

*"IV. **EMPRESAS AFIANZADORAS Y DE GARANTÍAS***

(…)

2) Evaluación de la gestión del riesgo operacional y del cumplimiento de los procedimientos utilizados para la administración de los riesgos de operación; así como, de las disposiciones de la normativa vigente sobre seguridad de la información y Ciberseguridad.

(...)"

*"V. **DERRAMAS Y CAJAS DE PENSIONES***

3) Evaluación de la gestión del riesgo operacional y del cumplimiento de los procedimientos utilizados para la administración de los riesgos de operación; así como, de las disposiciones de la normativa vigente sobre gestión de continuidad del negocio y de seguridad de la información y Ciberseguridad;

(...)"

*"VI. **ADMINISTRADORAS PRIVADAS DE FONDOS DE PENSIONES (AFP):***

1) Evaluación de la gestión del riesgo operacional y de las disposiciones de la normativa vigente sobre gestión de continuidad del negocio y de seguridad de la información;

(...)"

Artículo Tercero.- Modificar el literal b) del segundo párrafo del artículo 20° Informe sobre el sistema de control interno del Reglamento de Auditoría Externa, aprobado por Resolución SBS N° 17026-2010 y sus modificatorias, de acuerdo a lo siguiente al siguiente texto:

*"**Artículo 20°.- Informe sobre el sistema de control interno***

(…)

b) Evaluación de los sistemas de información de la empresa en el ámbito de la auditoría externa, que incluye, entre otros, el flujo de información en los niveles internos de la empresa para su adecuada gestión, y la revisión selectiva de la validez de los datos contenidos en la información complementaria a los estados financieros (anexos y reportes) que presentan las empresas a esta Superintendencia, según las normas vigentes sobre la materia; donde deben precisarse los sistemas que fueron parte del alcance de dicha evaluación; y,

(…)"

Artículo Cuarto.- Modificar el procedimiento N° 123 relativo a la "Autorización del Procesamiento Principal en el Exterior" por "Autorización para la contratación del servicio significativo de Procesamiento de Datos provisto por terceros desde el Exterior" e incorporar el procedimiento N°198 relativo a "Autorización para aplicar el Régimen Simplificado del Sistema de Gestión de la Seguridad de la Información y la Ciberseguridad" en el Texto Único de Procedimientos Administrativos de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones, aprobado mediante Resolución Nº 1678-2018, cuyo texto se anexa a la presente la presente resolución y se publica en el Portal Web institucional (www.sbs.gob.pe).

Artículo Quinto.- Modificar el Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, aprobado mediante Resolución SBS N° 272-2017 y sus modificatorias, de acuerdo a lo siguiente:

1. Incorporar en el Artículo 2 del Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, aprobado mediante Resolución SBS N° 272-2017 el siguiente texto:

"*rr) Proveedor: tercero contratado para brindar bienes y/o servicios a una empresa, incluso bajo la modalidad de subcontratación. Las empresas que forman parte del mismo grupo económico que la empresa contratante también son consideradas como terceros."*

d) Modificar en el Artículo 2 Definiciones y/o referencias, el literal jj) Subcontratación, de acuerdo a lo siguiente:

"jj) Subcontratación: Modalidad mediante la cual una empresa contrata a un proveedor para que este entregue bienes y/o servicios que podrían ser desarrollados por ella."

3. Sustituir el Capítulo IV, así como su referencia en el Índice de dicho Reglamento por "Bienes y/o Servicios Provistos por Terceros", con el siguiente texto:

"CAPÍTULO IV
BIENES Y/O SERVICIOS PROVISTOS POR TERCEROS

Artículo 35.- Aspectos generales

35.1. Los bienes y/o servicios provistos por terceros son aquellos entregados a la empresa por parte de un proveedor.

35.2. En caso se trate de un bien y/o servicio que pudiera ser desarrollado por la empresa pero decide solicitarlo a través de un tercero, se configura la modalidad de subcontratación.

35.3. Los bienes y/o servicios significativos provistos por terceros son aquellos que, en caso de falla o suspensión, pueden poner en riesgo importante a la empresa al afectar sus ingresos, solvencia, continuidad operativa o reputación. En caso de que algún bien y/o servicio significativo sea provisto por un tercero bajo la modalidad de subcontratación, la subcontratación se considera significativa.

35.4. Un proveedor es considerado significativo cuando provee servicios significativos, se encuentre o no, bajo la modalidad de subcontratación.

Artículo 36.- Bienes y/o servicios provistos por terceros
36.1 Los riesgos asociados a la entrega de bien y/o servicios provistos por terceros deben ser gestionados como parte del marco de gestión integral de riesgos de la empresa.

36.2 La empresa es responsable de los resultados de los bienes y/o servicios provistos por terceros bajo la modalidad de subcontratación.

36.3 La empresa debe realizar una evaluación de los riesgos asociados a los servicios significativos provistos por terceros, ya sea que se encuentren o no bajo la modalidad de subcontratación. Dicha evaluación debe ser presentada al directorio para su aprobación.

36.4 En el caso de subcontratación significativa se debe contar con cláusulas que faciliten una adecuada revisión de la respectiva prestación por parte de las empresas, de la unidad de auditoría

interna, de la sociedad de auditoría externa, así como por parte de la Superintendencia o las personas que esta designe, en los contratos suscritos con los proveedores.

36.5 La subcontratación de las funciones de la gestión de riesgos es considerada como significativa para fines de este Reglamento.

36.6 Esta Superintendencia puede definir requisitos adicionales para algunos bienes y/o servicios específicos provistos por terceros.

Artículo 37°.- Autorización para la contratación de bienes y/o servicios significativos provistos por terceros
La contratación de los siguientes bienes y/o servicios significativos requiere autorización previa de esta Superintendencia y debe sujetarse a lo establecido en las normas reglamentarias específicas:

a) La subcontratación significativa de auditoría interna, de acuerdo con lo establecido en el Reglamento de Auditoría Interna o norma que lo sustituya;
b) Otros que indique la Superintendencia mediante norma general."

Artículo Sexto.- Modificar Reglamento de Riesgo Operacional, aprobado por Resolución SBS Nº 2116-2009, según se indica a continuación:

1. Sustituir el literal i del artículo 2 y el artículo 14, de acuerdo con el siguiente texto:

"**Artículo 2.- Definiciones**
(…)
i. Subcontratación: Modalidad mediante la cual una empresa contrata a un proveedor para que este entregue bienes y/o servicios que podrían ser desarrollados por ella.
(…)

2. Sustituir el artículo 14 de acuerdo con el siguiente texto:

*"**Artículo 14.- Bienes y/o servicios provistos por terceros***
La empresa debe contar con políticas y procedimientos apropiados para gestionar los riesgos asociados a los servicios provistos por terceros, y contar con un registro de estos.

La empresa debe implementar un procedimiento para la identificación de aquellos proveedores significativos precisando los casos en los que se encuentren bajo la modalidad de subcontratación.

En los casos de servicios significativos, se encuentren o no bajo la modalidad de subcontratación, y de servicios subcontratados la empresa debe considerar los siguientes aspectos:
a) Implementar un proceso de selección del proveedor del servicio.
b) Contar con un contrato, el cual debe incluir acuerdos de niveles de servicio; establecer claramente las responsabilidades del proveedor y de la empresa; establecer la jurisdicción que prevalecerá en caso de conflicto entre las partes; e incorporar los niveles de seguridad de información requeridos.
c) Gestionar y monitorear los riesgos asociados a estos servicios.
d) Mantener un registro que debe contener como mínimo:
   i) Nombre del proveedor

ii) Giro o actividad principal de negocio del proveedor
iii) Descripción o listado de los servicios provistos
iv) Países, regiones y/o zonas geográficas desde donde se provee el servicio a contratar
v) Niveles de servicio acordados para su provisión
vi) Si la subcontratación es o no considerada significativa por la empresa
vii) Fecha de inicio del servicio
viii) Fecha de última renovación, si corresponde
ix) Fecha de vencimiento del servicio o la próxima fecha de renovación del contrato, según corresponda"

Artículo Séptimo.- Modificar el Reglamento de Tarjetas de Crédito y Débito, aprobado por Resolución SBS N° 6523-2013 y sus normas modificatorias, según se indica a continuación:

1. Sustituir los artículos 6 y 12, de acuerdo con el siguiente texto:

*"**Artículo 6.- Información mínima, condiciones y vigencia aplicable a la tarjeta de crédito***
Las tarjetas de crédito con soporte físico o digital se expiden con carácter de intransferible y deben incluir como mínimo la siguiente información:

1. *Denominación social de la empresa que emite la tarjeta de crédito.*

2. *Nombre comercial que la empresa asigne al producto.*

3. *Identificación del sistema de tarjeta de crédito (marca) al que pertenece, de ser el caso.*

En el caso de las tarjetas con soporte físico se debe incluir el nombre del usuario de la tarjeta de crédito; información de la que se puede prescindir siempre que la empresa cumpla con el Subcapítulo III del Capítulo II del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, aprobado por Resolución SBS N°504-2021.

El plazo de vigencia de las tarjetas de crédito no puede exceder de cinco (5) años, pudiéndose acordar plazos de vencimiento menores.

Artículo 12.- Información mínima, condiciones y vigencia aplicable a las tarjetas de débito
Las tarjetas de débito con soporte físico o digital se expiden con carácter de intransferible y deben incluir como mínimo la siguiente información:

1. *Denominación social de la empresa que emite la tarjeta de débito.*

2. *Nombre comercial que la empresa asigne al producto.*

3. *Identificación del sistema de tarjeta de débito (marca) al que pertenece, de ser el caso.*

Para su uso, requieren adicionalmente la presencia de una clave secreta, firma, firma electrónica u otros mecanismos que permitan identificar al usuario, de acuerdo con lo pactado.

El plazo de vigencia de las tarjetas de débito no puede exceder de cinco (5) años, pudiéndose acordar plazos de vencimiento menores."

Artículo Octavo.- Modificar el Reglamento de Operaciones con Dinero Electrónico aprobado por Resolución SBS N° 6283-2013 y sus normas modificatorias, según se indica a continuación:

1. Sustituir el artículo 4, de acuerdo con el siguiente texto:

*"**Artículo 4.- Soportes para uso de dinero electrónico***
Los soportes mediante los cuales se puede hacer uso del dinero electrónico pueden ser los siguientes:
a) Teléfonos móviles.
b) Tarjetas prepago.
c) Cualquier otro equipo o dispositivo electrónico, que cumpla los fines establecidos en la Ley.

Estos dispositivos deben incluir como mínimo la siguiente información:

1. *Denominación social de la empresa que emite el soporte mediante el cual se hace uso del dinero electrónico.*

2. *Nombre comercial que la empresa asigne al producto.*

3. *Identificación del sistema de tarjeta (marca) al que pertenece, de ser el caso.*

Dicha información debe ser mostrada en un espacio visible y de fácil acceso para el usuario.

Un mismo soporte puede ser utilizado y/o asociado para realizar transacciones con más de una cuenta de dinero electrónico."

Artículo Noveno.- Plazos y Plan de adecuación
1. En un plazo que no debe exceder de sesenta (60) días calendario contados a partir del día siguiente de la publicación de la presente Resolución, las empresas deben presentar a la Superintendencia, un plan de adecuación al Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad aprobado en el Artículo Primero de la presente Resolución, previamente aprobado por el directorio, en el cual incluya: a) un diagnóstico preliminar de la situación existente en la empresa; b) las acciones previstas para la total adecuación al Reglamento; c) los funcionarios responsables del cumplimiento de dicho plan; y, d) un cronograma de adecuación.

2. Las disposiciones señaladas en el Subcapítulo III del Capítulo II y la Tercera Disposición Complementaria Final del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad aprobado en el Artículo Primero de la presente Resolución tienen un plazo de adecuación hasta el 1 de julio de 2022.

3. En un plazo no mayor a treinta (30) días calendario contados a partir del día siguiente de la publicación de la presente Resolución, las empresas que cuenten con un servicio significativo de procesamiento de datos provisto por terceros desde el exterior, cuyo marco legal aplicable impida o limite el cumplimiento de las medidas definidas en el párrafo 24.2 del artículo 24 del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, aprobado en el Artículo Primero de la presente Resolución, deben remitir un informe que contenga: i) las limitaciones presentadas, dicho

informe debe contar con el sustento legal del impedimento de su aplicación y ii) las medidas compensatorias.

Artículo Décimo.- Vigencia
La presente Resolución entra en vigencia el 1 de julio de 2021, fecha en la que se deroga la Circular G 140-2009, con excepción de lo siguiente:

a. Los párrafos 25.1 y 25.2 del artículo 25 del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, aprobado por el Artículo Primero, que entran en vigencia al día siguiente de publicada la presente Resolución, fecha en la cual se deroga el artículo 7A de la Circular G 140-2009.
b. El Artículo Segundo de la presente Resolución entra en vigencia a partir de la auditoría correspondiente al ejercicio 2022.
c. Los Artículos Séptimo, Octavo y Noveno de la presente Resolución, entran en vigencia al día siguiente de la publicación de la presente Resolución, con excepción de lo indicado en el inciso d. del presente Artículo.
d. El requerimiento asociado a la inclusión conjunta de la información sobre la denominación social de la empresa emisora y el nombre comercial que la empresa asigne al producto de tarjeta de crédito y/o débito, señalado en el Artículo Séptimo de la presente Resolución, así como el requerimiento asociado a la inclusión de la dicha información en los dispositivos de soporte al dinero electrónico, señalado en el artículo Octavo de la presente Resolución entran en vigencia el 1 de enero de 2022.

Regístrese, comuníquese y publíquese

SOCORRO HEYSEN ZEGARRA
Superintendenta de Banca, Seguros y Administradoras
Privadas de Fondos de Pensiones