SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

PREPUBLICACIÓN

Resolución S.B.S.
N° -2020
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, mediante la Resolución SBS Nº 11699-2008 y sus modificatorias, se aprobó el Reglamento de Auditoría Interna;

Que, mediante la Resolución SBS Nº 17026-2010 y sus modificatorias, se aprobó el Reglamento de Auditoría Externa;

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, entre los que se encuentran los publicados por el National Institute of Standards and Technology y la familia de estándares ISO/IEC 27000 sobre seguridad de la información, así como la creciente interconectividad y mayor adopción de canales digitales para la provisión de los servicios del sistema financiero, de seguros y privado de pensiones, y que ante este contexto es necesario que las empresas de dichos sistemas supervisados fortalezcan sus capacidades para el manejo de incidentes de ciberseguridad y procesos de autenticación;

Que, para recoger las opiniones del público, se dispone 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;

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

PREPUBLICACIÓN

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 Quinta 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 recurso que lo soporta, definido y gestionado como una sola unidad de acuerdo con las necesidades de negocios y los requerimientos legales, de manera que pueda ser entendida, compartida y usada eficazmente. Es de valor para la empresa, tiene vulnerabilidades asociadas y 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 conjunto de políticas, procesos y procedimientos, que permiten verificar de manera digital que una entidad sea quien dice ser, para lo cual hace uso de las credenciales y los factores de autenticación. La autenticación puede usar uno, dos o más factores de autenticación independientes, tal que, en términos de la tecnología utilizada, el acceso sin autorización a uno de ellos no compromete la fiabilidad de los otros factores.

d) **Canal digital**: Medio empleado por las empresas para proveer servicios en línea, como internet, teléfonos móviles, cajeros automáticos, terminales de puntos de atención, y otros cuyo almacenamiento, procesamiento y transmisión se realiza mediante la representación de datos en bits.

e) **Ciberseguridad**: Conjunto de políticas, procesos, procedimientos y recursos utilizados por la organización para proteger los activos de información mediante la prevención, detección, respuesta y recuperación ante incidentes 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 para fines de autenticación.

g) **Directorio**: Directorio u órgano equivalente.

h) **Entidad**: Elemento 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 vigente.

j) **Factores de autenticación**: Aquellos factores empleados para verificar la identidad de una entidad, que pueden consistir en:

- Algo que solo la entidad conoce, y sobre lo cual la empresa ha establecido medidas para asegurar su confidencialidad y evitar su divulgación a terceros no autorizados.
- Algo que solo la entidad posee, y sobre lo cual la empresa ha establecido medidas para evitar su replicación y uso por terceros no autorizados.
- Algo que la entidad es, y sobre lo cual la empresa ha establecido medidas para evitar su revelación y uso por terceros no autorizados, así como para asegurar una muy baja probabilidad de que un tercero no autorizado sea autenticado.

Su uso puede reforzarse con la adopción de otros factores relacionados a algo que la entidad regularmente realiza, como el patrón de comportamiento o de ubicación de una entidad.

k) **Identidad:** Una colección de atributos que definen de forma exclusiva a una persona o entidad.

l) **Incidente:** Evento que se ha determinado que tiene un impacto sobre la organización y que requiere de acciones de respuesta y recuperación.

m) **Información**: Datos que pueden ser procesados, distribuidos y almacenados, y representados en cualquier medio electrónico, digital, óptico, magnético u otros, que son el elemento fundamental de los activos de información.

n) **Servicios en nube**: Infraestructura tecnológica que permite el acceso de red ubicuo, 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.

o) **Reglamento:** Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad.

p) **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.

q) **Superintendencia:** Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones.

r) **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, así como detectar y responder ante eventos de seguridad y 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 uso inapropiado, modificación o destrucción, así como que esta sea precisa y completa.

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;
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):

a) Banco de Inversión;
b) Entidad de Desarrollo a la Pequeña y Micro Empresa – EDPYME;
c) Empresa de Transferencia de Fondos;
d) Derrama y Caja de Beneficios bajo control de la Superintendencia;
e) La Corporación Financiera de Desarrollo –COFIDE;
f) El Fondo MIVIVIENDA S.A.;
g) El Fondo de Garantía para Préstamos a la Pequeña Industria –FOGAPI; y,
h) El Banco Agropecuario.

4.4. 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.

4.5. 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. Asimismo, la Superintendencia puede incluir a otras empresas cuando la complejidad de sus operaciones o los riesgos en ciberseguridad ameriten mayor control.

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 las principales 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 las medidas de difusión y capacitación periódica 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, proveer los recursos necesarios y una organización para cumplir con sus responsabilidades.

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.
   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). El CSIC se debe encontrar conformado por al menos tres (3) miembros, uno de los cuales debe ser un miembro del directorio que no desempeñe cargo ejecutivo en la empresa, quien lo preside. Asimismo, también deben ser miembros de este Comité el Jefe de la Unidad de Riesgos, el Jefe de la Unidad de Tecnología de la Información y quien desempeñe la Función de Seguridad de Información y Ciberseguridad. Asimismo, el CSIC se rige por las disposiciones sobre comités del directorio del Reglamento de Gobierno Corporativo y Gestión Integral de Riesgos. En caso de no existir un Comité de Riesgos o un CSIC, las funciones antes indicadas son asignadas al directorio.

Artículo 8. Función de Seguridad de Información y Ciberseguridad

8.1. Las empresas deben contar con una función independiente de seguridad de información y ciberseguridad respecto de las áreas de tecnología o sistemas de información, cuyo nivel y relación jerárquica será definido por el directorio a propuesta del Comité de Riesgos, con excepción de las empresas incluidas en el Régimen simplificado del Reglamento, establecido en el Artículo 4 del presente Reglamento. Son responsabilidades de la función de seguridad de la información y ciberseguridad:

1. Proponer el Plan estratégico del SGSI-C y desarrollar los planes operativos.
2. Implementar y manejar las operaciones diarias necesarias para el funcionamiento efectivo del SGSI-C.
3. Implementar procesos de autenticación para controlar el acceso a la información y sistema que utilice la empresa, y a los servicios que provea.
4. Informar al Comité de Riesgos periódicamente sobre los riesgos que enfrenta la empresa en materia de seguridad de información y Ciberseguridad.
5. Informar sobre los incidentes de seguridad 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
6. 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.
7. En general realizar lo necesario para dar debido cumplimiento a lo dispuesto en el presente Reglamento.

8.2. La empresa debe contar con un equipo de trabajo de manejo de incidentes de Ciberseguridad, el cual debe 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.

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, emitido por la Superintendencia, las empresas deben incluir información sobre la gestión de la seguridad de la información.

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

SUBCAPÍTULO I
REGIMEN 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 de nuevos productos y procesos, cambios operativos y asociados a transformación digital.
b) Las relaciones con terceros, en el sentido más amplio, incluyendo proveedores de servicios, empresas con las que se tiene relaciones de subcontratación y en general toda relación con terceros.
c) Los proyectos nuevos o en curso.
d) Las obligaciones de seguridad de la información que se derivan de disposiciones legales, regulatorias, normas internas y de acuerdos contractuales.
e) Toda actividad que exponga sus activos de información por causa interna o externa.

2. Monitorear el alcance y la efectividad de los controles internos, y contar con capacidades de detección, respuesta y recuperación ante incidentes sobre los activos de información de la empresa.

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. Controles de acceso físico y lógico:
   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) Prevenir el acceso no autorizado a la información, así como a los sistemas, equipos e instalaciones mediantes los cuales es procesada, transmitida o almacenada, sea de manera presencial o remota.
   c) Implementar procesos de autenticación para controlar el acceso a los activos de información; y 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 presente Reglamento.
   d) Prevenir la pérdida, el daño, el robo o el compromiso de los activos de información y la interrupción de las operaciones de la empresa.
   e) Utilizar criptografía para el almacenamiento y transmisión de datos, en función a la evaluación de amenazas de conocimiento público en el ámbito técnico.
   f) Revisar periódicamente las políticas de control de accesos existentes y monitorear su efectividad.

2. 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 segregado el ambiente productivo.
d) Restringir la instalación de software en los sistemas operativos; prevenir la explotación de las vulnerabilidades de seguridad de la información; y minimizar el impacto de las actividades de auditoría en los sistemas operacionales.
e) Contar con protocolos de respuesta y recuperación ente eventos de malware; habilitar y probar copias de respaldo de información, software y elementos que faciliten su restablecimiento.
f) Monitorear las operaciones de la infraestructura tecnológica, para lo cual debe contar con registros de auditoría de la actividad de usuarios, operadores y administradores de sistemas, así como registros de errores e incidentes.

3. 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, desde y hasta redes internas o externas.
   e) Asegurar que el acceso remoto, y que la interconexión que se utilice a través de redes propias y de terceros cuenta con controles acorde a las amenazas de seguridad existentes.
   f) Monitorear y revisar regularmente la efectividad y funcionamiento de los controles de seguridad de redes.

4. 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 los servicios y sistemas informáticos.
   c) Asegurar que se incluyan prácticas de pruebas funcionales en los servicios y sistemas informáticos, así como aquellas que permitan validar la seguridad de estos.
   d) Implementar y verificar el cumplimiento de procedimientos que incluyan prácticas de desarrollo seguro de servicios y sistemas informáticos.
   e) Implementar controles que aseguren la integridad de las transacciones que son ejecutadas en los servicios y sistemas informáticos.
   f) Monitorear y revisar regularmente la efectiva aplicación de prácticas seguras en la adquisición, desarrollo y mantenimiento de servicios y sistemas informáticos.

5. Servicios provistos por terceros:
   a) Evaluar las amenazas y vulnerabilidades de seguridad de la información en la provisión de bienes y servicios, o en la relación con terceros, según sea aplicable.
   b) Establecer requerimientos de seguridad de la información consistentes con las políticas del SGSI-C, cuando corresponda, incorporándolos en los acuerdos suscritos.

c) Establecer los roles y responsabilidades sobre seguridad de la información con los proveedores, según sea aplicable.
d) Monitorear la provisión de servicios de terceros, y evaluar los riesgos que afectan la seguridad de la información ante eventuales cambios, según corresponda.
e) Contar con una estrategia de salida de los servicios a cargo del proveedor, de forma que la información de la empresa pueda ser migrada a un proveedor distinto o a las instalaciones y recursos de la empresa.
f) Asegurar que la información en custodia del proveedor puede ser eliminada definitivamente ante la resolución del acuerdo contractual.
g) Cuando se trate de la provisión del servicio de procesamiento de datos, debe cumplir adicionalmente los requerimientos establecidos en el Subcapítulo IV del presente Reglamento.

6. Gestión de incidentes de seguridad de la información:
   a) Implementar procedimientos para la gestión de incidentes de seguridad la información, y cuando se trate de incidentes en el ciberespacio, estos procedimientos deben incluir las responsabilidades del equipo de manejo de incidentes de ciberseguridad, de acuerdo a lo señalado en numeral 8.1 del Artículo 8 del presente Reglamento; así también, intercambiar información cuando corresponda, conforme al Artículo 17 del presente Reglamento.
   b) Implementar una metodología para clasificar eventos, incidentes de seguridad de la información y de ciberseguridad.
   c) Implementar mecanismos de reporte interno de incidentes de acuerdo con lo señalado en el Artículo 8 del presente Reglamento, y a la Superintendencia conforme al Artículo 16 del presente Reglamento.
   d) Identificar las posibles limitaciones y mejoras en la gestión de incidentes de seguridad de la información luego de la ocurrencia de estos.
   e) Mantener información que permita realizar las investigaciones forenses.

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, analizar las amenazas y vulnerabilidades asociadas a estos, y tomar medidas para reducir la posibilidad de incidentes.
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, según sea aplicable el Subcapítulo IV.

PREPUBLICACIÓN

SUBCAPÍTULO II
CIBERSEGURIDAD

Artículo 14. Programa de ciberseguridad

14.1. Toda empresa que cuente con presencia en el ciberespacio debe contar con un programa específico de gestión de incidentes de ciberseguridad (PG-C), aplicable a las operaciones, procesos y otros activos de información asociados.

14.2. El PG-C debe prever un diagnóstico de las capacidades para gestionar un incidente, respecto a un marco de referencia internacional de ciberseguridad, que evalúe por lo menos las siguientes funciones:

a) Identificación de los activos de información.
b) Protección frente a las amenazas a los activos de información.
c) Detección de la ocurrencia de incidentes.
d) Respuesta con medidas que reduzcan el impacto de los incidentes.
e) Recuperación de las actividades de negocio, y capacidades o servicios afectados.

Artículo 15. Reporte de incidentes de ciberseguridad

15.1 La empresa debe reportar a la Superintendencia, en cuanto advierta, la ocurrencia de un incidente de ciberseguridad que tenga un efecto verificado o presumible de:

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

15.2 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 procurar 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 debe suscribir acuerdos con otras empresas del sector o con terceros que resulten relevantes, de forma bipartita, grupal o gremial. El intercambio debe realizarse acorde a criterios previamente establecidos para mantener la confidencialidad de la información y reducir el contenido mínimo necesario, sin que con ello se pierda la utilidad de la información para tomar las acciones preventivas o reactivas.

16.3 Mediante norma de carácter general, la Superintendencia podrá 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) La combinación de factores de autenticación que serán admitidos.
b) Requerimientos criptográficos aceptados, basados en software o en hardware, y sus prestaciones de confidencialidad o integridad esperadas.
c) Plazos y condiciones en las que será obligatorio requerir a la entidad 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, lo que incluye, y no se restringe, al número límite de intentos de autenticación, la prevención de ataques de interceptación y manipulación de mensajes, reproducción de mensajes de autenticación y suplantación.
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 se presenten cambios en la tecnología que los soportan, o tras el descubrimiento de nuevas vulnerabilidades que pueda afectarlos.

17.3 La empresa debe mantener y proteger los registros detallados de lo actuado en cada habilitación y uso del proceso de autenticación, incluyendo información de identificación, credencial asignada, así como los datos de cada operación y los intentos de autenticación.

17.4 La empresa debe contar con los registros de auditoría, herramientas y procedimientos para detectar y remediar los intentos de uso no autorizado de credenciales; así también, implementar el monitoreo de transacciones que permita tomar medidas de reducción de 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. Inscripción y gestión de credenciales

Para la habilitación de la autenticación de una entidad para el acceso a servicios provistos por canal digital, la empresa debe:

a) Recabar la información necesaria para determinar la validez de la identidad de la entidad y corroborarla con un registro de identificación reconocido por el marco legal vigente, o un repositorio bajo responsabilidad de la empresa. Cuando corresponda debe cumplir con los requisitos de debida diligencia en el conocimiento del cliente, establecidos en el Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento del Terrorismo.
b) Para reducir la posibilidad de suplantación de identidad cuando se efectúe lo requerido en el literal anterior por canal digital, la verificación de identidad deberá requerir del uso de dos factores de autenticación, donde por lo menos uno de los cuales debe ser biométrico.
c) Emitir y asignar una credencial a una entidad para la validación de su identificación; además de su emisión, prever procedimientos para su suspensión, reemplazo, renovación y revocación, así también asegurar en todo momento su confidencialidad e integridad.

Artículo 19. Autenticación reforzada para operaciones por canal digital

Para aquellas operaciones que se realicen a través de un canal digital que implique una transferencia de fondos, un pago, la solicitud de un trámite o la contratación de un producto o servicio, modificación de los límites y condiciones en los que se proveen los servicios, y otros que pueden originar una operación fraudulenta u otro abuso en perjuicio del cliente, debe requerirse una autenticación reforzada, que debe contar por lo menos con lo siguiente:

a) Utilizar dos o más factores de autenticación, de los cuales por lo menos dos no podrán ser de ubicación o comportamiento.
b) Lo indicado en el literal a) debe resultar en la generación de un código de autenticación, mediante métodos criptográficos, a partir de los datos específicos de cada operación.
c) Dicho código de autenticación debe utilizarse por única vez para realizar la operación para la que fue generada, no podrá derivarse de él alguno de los factores de autenticación, algún dato de la operación u otro código de autenticación posterior. Su uso y transmisión debe realizarse con controles para prevenir su captura y manipulación no autorizadas, así como el límite a intentos fallidos en el proceso de autenticación.

Artículo 20. Exenciones de autenticación reforzada para operaciones por canal digital
Están exentas del requisito de autenticación reforzada indicado en el artículo 19 del presente Reglamento, las siguientes operaciones realizadas por canal digital:

a) La consulta de información de estados de cuenta, saldos de cuenta, historial de operaciones y movimientos de cuentas; salvo que sea efectuado por primera vez o luego de un periodo sin uso, según lo definido por la empresa.
b) Las operaciones de pago, pagos periódicos o transferencia hacia un beneficiario registrado previamente por el cliente como beneficiario de confianza, de acuerdo con las condiciones de su autorización, salvo a partir de que el cliente excluya a un anterior beneficiario de confianza o modifique las condiciones del pago periódico.
c) Las operaciones de micropago conforme se define en la regulación vigente sobre tarjetas de crédito y débito.

SUBCAPÍTULO IV
PROVISIÓN DE SERVICIOS DE PROCESAMIENTO DE DATOS

Artículo 21. Provisión de servicios de procesamiento de datos a las empresas
Los requisitos establecidos en el numeral 5 del artículo 12 son de aplicación a la provisión de servicios de procesamientos de datos a las empresas. Además, cuando se trate de servicios en nube, es de aplicación también el artículo 22, y cuando sea procesamiento principal y provisto desde el exterior, es de aplicación también el artículo 23.

Artículo 22. Servicios de procesamiento de datos en nube
Las empresas que utilicen servicios de procesamiento de datos en nube deben:

a) Implementar procedimientos para la administración de operaciones y configuraciones del procesamiento en la nube, así como servicios de soporte ante casos de falla, indisponibilidad o incidentes de ciberseguridad.
b) Gestionar las amenazas y vulnerabilidades en el uso de interfaces de programación de aplicaciones (API, por sus siglas en inglés) y otros servicios similares suministrados por el proveedor de nube.
c) Contar con evidencia de que el proveedor de procesamiento mantiene vigente las certificaciones ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018 relevantes a la zona o región desde donde se provee el servicio.

Artículo 23. Autorización de provisión de procesamiento principal de datos en el exterior o en la nube

23.1 Cuando el procesamiento principal de datos se realice fuera del país o en la nube la empresa debe solicitar autorización previa de esta Superintendencia, de acuerdo a los requisitos señalados en el Anexo A del Reglamento.

23.2 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, se requiere de un nuevo procedimiento de autorización ante la Superintendencia.

23.3 Los servicios de procesamiento principal de datos o en la nube autorizados a ser provistos desde el exterior deben ser sometidos anualmente a un examen de auditoría independiente, realizado por una sociedad auditora externa o una firma nacional o extranjera, que acredite contar con el conocimiento y experiencia requerida, debiendo remitir a ésta Superintendencia el reporte SOC 2 tipo 2 resultante de una evaluación realizada conforme a las secciones AT-C 105 y AT-C 205 del estándar de auditoría SSAE 18, emitidos por el Instituto Americano de Contadores Públicos Certificados (AICPA), o el ISAE 3000, emitido por el Consejo de Normas Internacionales de Auditoría y Aseguramiento (IAASB). El alcance periodo del servicio es de doce meses, a cubrir con reportes de por lo menos 6 meses.

SUBCAPÍTULO V
RÉGIMEN SIMPLIFICADO DEL SGSI-C

Artículo 24. Sistema simplificado de gestión de seguridad de la información

24.1 El SGSI-C es responsabilidad de directorio que, para la implementación del régimen simplificado de gestión de seguridad de la información, debe:

a) Aprobar las políticas y lineamientos.
b) Asignar los recursos técnicos, de personal y financieros requeridos para su implementación y adecuado funcionamiento.
c) Aprobar la organización, roles y responsabilidades para las medidas de difusión y capacitación periódica.

24.2 El régimen simplificado de gestión de seguridad de la información requiere la planificación y ejecución de las siguientes actividades, acorde a una periodicidad definida por el directorio, que 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 legales, regulatorias 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.
c) Identificar las cuentas de usuario y en particular las que poseen privilegios alternativos con posibilidad de adicionar software a la infraestructura.
d) Priorizar y cerrar las brechas de seguridad identificadas mediante las acciones detalladas en el numeral previo.
e) Configurar e implementar una línea base de seguridad en sistemas operativos y aplicaciones utilizadas. Identificar y evaluar la habilitación de las funciones de seguridad integradas en los sistemas operativos.

f) Desarrollar una campaña de orientación para la adopción de prácticas seguras dirigida a los empleados, plana gerencial y de dirección.

24.3 En caso provea servicios a usuarios por canales digitales que implique una transferencia de fondos, un pago, la solicitud de un trámite o la contratación de un producto o servicio, modificación de los límites y condiciones en los que se proveen los servicios, y otros que pueden originar una operación fraudulenta u otro abuso en perjuicio del cliente, debe requerirse una autenticación reforzada, la empresa deberá implementar las disposiciones establecidas en el Subcapítulo III del Capítulo II.

24.4 En caso utilice servicios significativos provistos por terceros, la empresa debe implementar las disposiciones establecidas en el numeral 5 del artículo 12 y, cuando se trate del procesamiento de datos, las indicadas en el Subcapítulo IV del Capítulo II.

24.5 La empresa debe mantener un programa de ciberseguridad, conforme al Subcapítulo II del Capítulo II, con un alcance que por lo menos incluya los servicios indicados en los párrafos 24.3 y 24.4. del presente artículo.

SUBCAPÍTULO VI
DISPOSICIONES ADICIONALES APLICABLES A EMPRESAS CON CONCENTRACIÓN DE MERCADO

Artículo 25. Requerimientos adicionales para empresa con concentración de mercado

25.1 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.

25.2 La empresa debe someter periódicamente una evaluación independiente el alcance y efectividad del SGSI-C.

DISPOSICIONES COMPLEMENTARIAS FINALES

Primera.- La empresa puede contar con un marco especializado para la gestión de los riesgos asociados a la seguridad de la información, que deber 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 ciberseguridad, es aplicable lo señalado en el Artículo 15 del Reglamento para la Gestión de la Continuidad del Negocio, sobre Reporte de Eventos de Interrupción significativa.

Cuarta.- Sin perjuicio de lo señalado en el Artículo 4 del presente Reglamento, la Superintendencia puede disponer el cambio de régimen, del sistema de gestión de seguridad de la información y la ciberseguridad, que una empresa debe cumplir.

Quinta.- 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, sobre la base de las siguientes consideraciones.

1. Se les aplica el Régimen Simplificado del Sistema de Gestión y Seguridad de la Información y Ciberseguridad con excepción de los párrafos 24.4 y 24.5 del artículo 24.
2. En el caso de los párrafos 24.1 y 24.2 del artículo 24, las empresas corredoras desarrollarán las actividades requeridas, de acuerdo al tamaño y volumen de sus operaciones.
3. En el caso del párrafo 24.3 del artículo 24, aplica solo cuando la empresa corredora desarrolle con alguna compañía de seguros, sistemas que involucren la contratación de seguros y pago.
4. Finalmente, dependiendo del nivel de riesgo al que se encuentre expuesta la empresa corredora en aspectos de seguridad de información o de ciberseguridad, la Superintendencia podrá realizar requerimientos adicionales señalados en el presente Reglamento.

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

PREPUBLICACIÓN

ANEXO A

DOCUMENTACIÓN A REMITIR JUNTO CON LA SOLICITUD DE AUTORIZACIÓN PARA REALIZAR PROCESAMIENTO PRINCIPAL EN EL EXTERIOR

Documento	Tradicional	Procesamiento en la nube
1. Información general del proveedor y del servicio	• Razón social del proveedor. • Giro del negocio y años de experiencia. Indicar a qué empresas brinda actualmente el mismo servicio que prestará a la empresa supervisada. • Estados financieros del proveedor correspondientes a los dos últimos años. • Relación de accionistas del proveedor y funcionarios principales. • Relación con la empresa supervisada (indicar si pertenecen al mismo grupo económico). • Servicios que serán provistos por el proveedor y el tipo de información a ser procesada. • Ubicación (país y ciudad) del centro de procesamiento principal. • Evaluación realizada por la empresa para la elección del proveedor.	• Razón social del proveedor. • Años de experiencia e indicar a qué empresas brinda actualmente el mismo servicio que prestará a la empresa supervisada. • Descripción del proveedor y de los servicios de nube a ser provistos. • Relación de servicios que serán provistos por el proveedor y el tipo de información a ser procesada. • Ubicación (región y zona de disponibilidad) del centro de procesamiento principal. • Evaluación realizada por la empresa para la elección del proveedor.
2. Borrador del contrato	<u>Aspectos a considerar:</u> • Acuerdos de niveles de servicio. • Cumplimiento de las normas sobre secreto bancario y confidencialidad de la información. • Prestación del servicio en regímenes especiales (vigilancia, intervención, liquidación). El proveedor debe seguir brindando el servicio como mínimo un año después de que la empresa ha ingresado a un régimen especial. • Compromiso de cumplimiento de la normativa de la Superintendencia. • Aseguramiento del acceso adecuado a la información con fines de supervisión, en tiempos	<u>Aspectos a considerar:</u> • Contrato con el proveedor de Procesamiento en la nube, que incluya: ▪ Región (es) geográfica (s) y país donde se alojará físicamente la información. ▪ Definición de responsabilidades del proveedor(es). ▪ Acuerdo de niveles de servicio (SLA) definidos. ▪ La jurisdicción donde se almacene la data no debe inhibir el acceso efectivo a la data por parte de la empresa, sus auditores o el regulador. ▪ Cumplimiento de las normas sobre secreto bancario y confidencialidad de la información. ▪ Prestación del servicio en regímenes especiales (vigilancia, intervención,

	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. Este aspecto debe ser aplicable sobre cualquier otra empresa que el proveedor subcontrate para brindar servicios a la empresa supervisada. • Cláusulas que faciliten una adecuada revisión por parte de la Unidad de Auditoría Interna, la Sociedad de Auditoría Externa y la Superintendencia.	liquidación), hasta por un año después de que la empresa ha ingresado en alguno de ellos. ▪ Aseguramiento del acceso adecuado a la información con fines de supervisión, 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. Este aspecto debe ser aplicable sobre cualquier otra empresa que el proveedor subcontrate para brindar servicios a la empresa supervisada ▪ Cláusulas que faciliten una adecuada revisión por parte de la Unidad de Auditoría Interna, la Sociedad de Auditoría Externa y la Superintendencia.
3. Informe de la plataforma tecnológica	<u>Aspectos a considerar</u>: (Señalar qué equipos y aplicaciones estarán a cargo del proveedor) • Inventario de equipos de cómputo. • Inventario de software base. • Herramientas y/o manejadores de base de datos. • Aplicaciones críticas. • Esquema de comunicaciones a ser implementado entre el proveedor y la empresa supervisada.	<u>Aspectos a considerar</u>: (Señalar qué servicios estarán a cargo del proveedor) • Informe de arquitectura de sistemas a implementar, donde detalle las modalidades de servicio de nube a utilizar. • Relación de servicios a contratar con el proveedor de servicios de nube, incluyendo una breve descripción de ellos. • Diagrama de implementación de la solución en nube. • Esquema de comunicaciones con el proveedor de servicios de nube. • Métodos de cifrado sobre la transmisión y almacenamiento de data, en función a su criticidad.
4. Gestión de continuidad de negocios	Relativo a la empresa: • Estrategia de continuidad del negocio de los servicios que serán provistos por el tercero, incluyendo esquema de contingencia y planes asociados, de ser el caso. • Tiempos objetivos de recuperación de los servicios que serán provistos por el tercero. • Planificación de pruebas de continuidad del negocio que incorpore los servicios provistos por el proveedor. • Estrategia de salida para retomar operación por cuenta propia o mediante otro	

	proveedor ante la eventualidad de incumplimiento o terminación abrupta, de acuerdo a los tiempos objetivos de recuperación definidos por la empresa. Relativo al proveedor: • Estrategia de continuidad del negocio de los servicios a proveer a la empresa, incluyendo esquema de contingencia, tiempos objetivos de recuperación y planes asociados. • Prioridad asignada al procesamiento de la información de la empresa supervisada respecto al resto de clientes del proveedor. • Forma en que se dará aviso a la empresa y las acciones que debe desarrollar la empresa en caso de una contingencia en el proveedor. • Frecuencia y alcance de las pruebas de la estrategia de continuidad del negocio de los servicios provistos a la empresa. • Inventario de los servicios subcontratados (subcontratación en cadena) que se encuentren relacionados a los servicios provistos a la empresa.
5. Informe de comunicación con la Superintendencia (SUCAVE, RCD, otros)	• Descripción de la forma de envío de información a la Superintendencia luego de que se implemente el servicio de procesamiento en el exterior. Asimismo, indicar los cambios que se aplicarán sobre los procedimientos asociados a la generación, consolidación y reporte de dicha información.
6. Informe de evaluación de riesgos	• Evaluación de los riesgos operacionales asociados con el esquema propuesto por la empresa, tradicional o computación en la nube, realizada por la Unidad de Riesgos.
7. Informe Legal	• Informe respecto al marco legal y regulatorio aplicable a los servicios subcontratados, y sobre la eventual resolución de contingencias legales.

8. Informe de seguridad de información	• Informe donde evalúe las condiciones de seguridad en las que se proveería el servicio, que incluya por lo menos:
	  • Las políticas de seguridad de información.
	  • Estructura organizativa para la gestión de la seguridad de información.
	  • Reportes periódicos que la empresa recibirá sobre las condiciones de seguridad en que operaría el servicio.
	  • Esquema de coordinación y contrapartes definidas entre la empresa y el proveedor para el manejo de incidentes de ciberseguridad.
	  • Forma en que se aislará el procesamiento y la información objeto de subcontratación.
	  • Procedimientos y controles a implementar la empresa en materia de seguridad de la información, lo que incluiría los aspectos de monitoreo del servicio y operación en contingencia.
	  • Definición de responsabilidades de supervisión del cumplimiento de los servicios subcontratados.
	• La Superintendencia podrá requerir la presentación de los sustentos del informe que presente.

9. Plan de	• Alcance, forma y periodicidad de las revisiones de auditoría de sistemas de la

Auditoría de Sistemas	Unidad de Auditoría Interna, considerando el nuevo esquema de procesamiento principal de la empresa.
10. Gestión del proyecto	• Cronograma de actividades, incluyendo plazos, responsables y principales hitos de control. • Costo estimado de implementación del proyecto.

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 de Procesamiento de Datos en el Exterior" por "Autorización de Procesamiento de Datos en el Exterior y en la Nube" 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:

"*mm) 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 éste 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 En el caso de subcontratación significativa se debe cumplir con los siguientes requisitos:

a) *Realizar una evaluación de los riesgos asociados, el cual debe ser puesto en conocimiento del directorio para su aprobación.*
b) *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.*

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

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

PREPUBLICACIÓN

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) La contratación del servicio significativo del procesamiento principal de datos en el exterior o en la nube, de acuerdo con lo establecido en el Reglamento de Gestión de la Seguridad de la Información y Ciberseguridad o norma que lo sustituya;
c) 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 éste 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***
14.1 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.

14.2 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.

14.3 En los casos de servicios principales, 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) País(es), 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.- Vigencia

1. La presente resolución entra en vigencia el 1 de enero de 2021 y se deroga la Circular G 140-2009.

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

Regístrese, comuníquese y publíquese