



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

Lima, XX de XXXXX de 200X

CIRCULAR N° G-XXXX-200X

Ref.: Gestión de la seguridad de la
información

Señor
Gerente General

Sírvase tomar nota que, en uso de las atribuciones conferidas por el numeral 7 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 en adelante Ley General, y por el inciso d) del artículo 57° del Texto Único Ordenado de la Ley del Sistema Privado de Administración de Fondos de Pensiones, aprobado por Decreto Supremo N° 054-97-EF, con la finalidad de establecer criterios mínimos para una adecuada gestión de la seguridad de la información, esta Superintendencia ha considerado conveniente establecer las siguientes disposiciones:

Alcance

Artículo 1°.- La presente Circular será 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.

También será de aplicación a las Cajas Municipales de Ahorro y Crédito (CMAC), la Caja Municipal de Crédito Popular, el Fondo de Garantía para Préstamos a la Pequeña Industria (FOGAPI), el Banco de la Nación, el Banco Agropecuario, la Corporación Financiera de Desarrollo (COFIDE), el Fondo MIVIVIENDA S.A., y las Derramas y Cajas de Beneficios bajo control de la Superintendencia, la Federación Peruana de Cajas Municipales de Ahorro y Crédito (FEPCMAC) y el Fondo de Cajas Municipales de Ahorro y Crédito (FOCMAC), en tanto no se contrapongan con las normativas específicas que regulen el accionar de estas empresas.

Definiciones

Artículo 2°.- Para efectos de la presente norma, serán de aplicación las siguientes definiciones:

- a. Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.
- b. Ley General: 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.
- c. Objetivo de control: Una declaración del propósito o resultado deseado mediante la implementación de controles apropiados en una actividad de tecnología de información particular.
- d. Proceso crítico: Proceso considerado indispensable para la continuidad de las operaciones y servicios de la empresa, cuya realización podría ser razonablemente desarrollada por la empresa supervisada.



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

- e. Seguridad de la información: Característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla los criterios de confidencialidad, integridad y disponibilidad, definidos de la siguiente manera:
- I. Confidencialidad. La información debe ser accesible sólo a aquellos que se encuentren debidamente autorizados.
 - II. Integridad. La información debe ser completa, exacta y válida.
 - III. Disponibilidad. La información debe estar disponible en forma organizada para los usuarios autorizados cuando sea requerida.

Sistema de gestión de la seguridad de la información

Artículo 3º.- Las empresas deberán establecer, mantener y documentar un sistema de gestión de la seguridad de la información (SGSI).

Las actividades mínimas que deben desarrollarse para implementar el SGSI, son las siguientes:

- a. Definición de una política de seguridad de información.
- b. Definición de una metodología de identificación y evaluación de riesgos.
- c. Identificación y evaluación de riesgos asociados con fallas en la seguridad de información.
- d. Identificar y evaluar opciones para el tratamiento de los riesgos.
- e. Selección de controles y objetivos de control para reducir, transferir o evitar los riesgos identificados.
- f. Implementación de los controles seleccionados.
- g. Monitoreo y revisión periódica.
- h. Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la empresa, así como mantener pistas adecuadas de auditoría.

Estructura organizacional

Artículo 4º.- Las empresas deben contar con una estructura organizacional que les permita implementar y mantener el sistema de gestión de la seguridad de información señalado en el artículo anterior.

Asimismo, deben asegurarse que se desarrollen las siguientes funciones, ya sea a través de una unidad especializada o a través de alguna de las áreas de la empresa:

- a. Evaluar los riesgos asociados a fallas en la seguridad de información.
- b. Asegurar el cumplimiento de la política de seguridad de información.
- c. Coordinar y monitorear la implementación de los controles de seguridad de información.
- d. Desarrollar actividades de concientización y entrenamiento en seguridad de información.
- e. Evaluar los incidentes de seguridad de información y recomendar acciones apropiadas.

En caso no se realice una asignación expresa de estas funciones, se entenderá que han sido asignadas a la gerencia general.



SUPERINTENDENCIA DE BANCA, SEGUROS Y AFP

La Superintendencia podrá requerir la creación de una unidad especializada en gestión de la seguridad de información en empresas que a su criterio resulten complejas, y cuando se observe en el ejercicio de las acciones de supervisión que no se cumple con los criterios previstos en la normativa vigente.

Controles de seguridad de información

Artículo 5°.- En la selección de controles señalada en el literal e del artículo 3° de la presente Circular, las empresas deberán considerar, como mínimo, los controles generales que se indican en el presente artículo.

5.1 Seguridad lógica

- a) Procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios.
- b) Revisiones periódicas sobre los derechos concedidos a los usuarios.
- c) Los usuarios deben contar con una identificación para su uso personal, de tal manera que las posibles responsabilidades puedan ser seguidas e identificadas.
- c) Controles especiales sobre utilidades del sistema y herramientas de auditoría.
- d) Seguimiento sobre el acceso y uso de los sistemas para detectar actividades no autorizadas.
- e) Controles especiales sobre usuarios remotos y computación móvil.

5.2 Seguridad de personal

- a) Definición de roles y responsabilidades establecidos sobre la seguridad de información.
- b) Verificación de antecedentes.
- c) Concientización y entrenamiento.
- d) Procesos disciplinarios en caso de incumplimiento de las políticas de seguridad.
- e) Procedimientos definidos en caso de cese del personal, que incluyan aspectos como la revocación de los derechos de acceso y la devolución de activos.

5.3 Seguridad física y ambiental

- a) Controles para evitar el acceso físico no autorizado, daños o interferencias a los locales y a la información de la empresa.
- b) Controles para prevenir pérdidas, daños o robos de los activos. Esto incluye la protección de los equipos frente a amenazas físicas y ambientales.

5.4 Inventario de activos y clasificación de la información

- a) Realizar y mantener un inventario de activos asociados a la tecnología de información. Deben asignarse responsabilidades respecto a la protección de estos activos.
- b) Realizar una clasificación de la información. Esta clasificación debe indicar el nivel de riesgo existente para la empresa en caso de falla sobre la seguridad, así como las medidas apropiadas de control que deben asociarse a las clasificaciones.

5.5. Administración de las operaciones y comunicaciones

- a) Procedimientos documentados para la operación de los sistemas.



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

- b) Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, las instalaciones de procesamiento y los procedimientos.
- c) Separación de funciones para reducir el riesgo de error o fraude.
- d) Separación de los ambientes de desarrollo, pruebas y producción.
- e) Monitoreo del servicio dado por terceras partes
- f) Administración de la capacidad de procesamiento
- g) Controles preventivos y de detección sobre el uso de software de procedencia dudosa, virus y otros similares.
- h) Seguridad sobre las redes, medios de almacenamiento y documentación de sistemas.
- i) Seguridad sobre el intercambio de la información, incluido el correo electrónico.
- j) Seguridad sobre canales electrónicos.
- k) Mantenimiento de registros de auditoría y monitoreo del uso de los sistemas.

5.6. Adquisición, desarrollo y mantenimiento de sistemas informáticos

Para la administración de la seguridad en la adquisición, desarrollo y mantenimiento de sistemas informáticos, se debe tomar en cuenta, entre otros, los siguientes criterios:

- a) Incluir en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales, controles sobre el ingreso de información, el procesamiento y la información de salida.
- b) Aplicar técnicas de encriptación sobre la información crítica que debe ser protegida.
- c) Definir controles sobre la implementación de aplicaciones antes del ingreso a producción.
- d) Controlar el acceso a las librerías de programas fuente.
- e) Mantener un estricto y formal control de cambios, que será debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios.
- f) Controlar las vulnerabilidades técnicas existentes en los sistemas de la empresa.

5.7. Procedimientos de respaldo

- a) Procedimientos de respaldo regulares y periódicamente validados. Estos procedimientos deben incluir las medidas necesarias para asegurar que la información esencial pueda ser recuperada en caso de falla en los medios o luego de un desastre. Estas medidas serán coherentes con la estrategia de continuidad de negocios de la empresa.
- b) Conservar la información de respaldo y los procedimientos de restauración en una ubicación remota, a suficiente distancia para no verse comprometida ante un daño en el centro principal de procesamiento.

5.8. Gestión de incidentes de seguridad de información

Para asegurar que los incidentes y vulnerabilidades de seguridad sean controlados de manera oportuna, las empresas deberán considerar los siguientes aspectos:

- a) Procedimientos formales para el reporte de los eventos de seguridad de información y las vulnerabilidades asociadas con los sistemas de información.
- b) Procedimientos establecidos para dar una respuesta adecuada a los incidentes y vulnerabilidades de seguridad reportadas.

5.9. Cumplimiento normativo

Las empresas deberán asegurar que los requerimientos legales, contractuales, o de regulación sean cumplidos, y cuando corresponda, incorporados en la lógica interna de las aplicaciones informáticas.



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

5.10. Privacidad de la información

Las empresas deben adoptar medidas que aseguren razonablemente la privacidad de la información que reciben de sus clientes y usuarios de servicios, conforme a la normatividad vigente sobre la materia.

Seguridad en operaciones de transferencia de fondos por canales electrónicos

Artículo 6°.- En el caso de las operaciones de transferencia de fondos ofrecidas por las empresas para su realización a través de canales electrónicos, como el Internet, las empresas deberán implementar un esquema de autenticación de los clientes basado en, por lo menos, dos factores uno de los cuales deberá ser de generación o asignación dinámica. Las empresas podrán utilizar otros factores de autenticación, en tanto éstos proporcionen un nivel de seguridad equivalente o superior respecto a los dos factores señalados, en particular cuando se trate de operaciones importantes según los límites que el banco determine de acuerdo a las características del producto o servicio ofrecido.

La empresa deberá tomar en cuenta los riesgos operacionales asociados, en el diseño de los procedimientos, las definiciones de límites y las consideraciones de seguridad e infraestructura requeridas para un funcionamiento seguro y apropiado en las operaciones de transferencia de fondos.

Subcontratación

Artículo 7°.- Las empresas son responsables y deben verificar que se mantengan las características de seguridad de la información contempladas en la presente norma, incluso cuando ciertas funciones o procesos críticos puedan ser objeto de una subcontratación. Para ello se tendrá en cuenta lo dispuesto en el artículo 21° del Reglamento de la Gestión Integral de Riesgos. Asimismo, las empresas deben asegurarse y verificar que el proveedor del servicio sea capaz de aislar el procesamiento y la información objeto de la subcontratación, en todo momento y bajo cualquier circunstancia.

En caso que las empresas deseen realizar su procesamiento principal de datos en el exterior, requerirán de la autorización previa y expresa de esta Superintendencia. Para ello, deberán cumplir con los siguientes requisitos:

- a) La empresa debe asegurar un adecuado cumplimiento de la presente Circular, en lo que sea aplicable al servicio de procesamiento contratado.
- b) La empresa debe estar clasificada en la categoría de riesgo A y haber tenido dicha clasificación durante los dos semestres anteriores a la presentación de su solicitud.
- c) El proveedor del servicio en el exterior debe encontrarse sujeto a una supervisión efectiva por parte de la autoridad supervisora del país en el cual se brindará dicho servicio.

En el Anexo A de la presente Circular se detalla la información que debe remitir la empresa adjunta a su solicitud de autorización. Una vez recibida la documentación completa, dentro de un plazo que no excederá de sesenta (60) días útiles, la Superintendencia emitirá la resolución que autoriza o el oficio que deniega la solicitud presentada por la empresa.

Información a la Superintendencia

Artículo 8°.- Como parte de los informes periódicos sobre gestión del riesgo operacional requeridos por el Reglamento para la gestión del riesgo operacional, emitido por la SBS, las empresas deberán incluir información sobre la gestión de la seguridad de la información.



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

Información adicional

Artículo 9°.- La Superintendencia podrá requerir a la empresa cualquier otra información que considere necesaria para una adecuada supervisión de la gestión de la seguridad de la información de la empresa.

Asimismo, la empresa deberá tener a disposición de esta Superintendencia todos los documentos a que hace mención la presente Circular, así como la información de auditoría o revisiones realizadas por la casa matriz en caso de ser aplicable.

Sanciones

Artículo 10°.- En caso de incumplimiento de las disposiciones contenidas en la presente norma, la Superintendencia aplicará las sanciones correspondientes de conformidad con lo establecido en el Reglamento de Sanciones.

Vigencia

Artículo 11°.- Las disposiciones de la presente Circular entran en vigencia al día siguiente de su publicación en el Diario Oficial "El Peruano", otorgándose para su cumplimiento un plazo de adecuación hasta el 31 de diciembre de 2009, fecha a partir de la cual quedará sin efecto la Circular SBS N° G-105-2002, salvo los artículos 11° al 13° que dejarán de tener vigencia una vez concluya el plazo de adecuación contemplado en la Circular referida a Gestión de la Continuidad del Negocio.

Adecuación de las AFP

Artículo 12°.- En un plazo que no excederá de noventa (90) días calendario de haberse publicado la presente Circular, las AFP deberán remitir a esta Superintendencia un plan de adecuación a las disposiciones contenidas en la presente norma.

Dicho plan deberá incluir un diagnóstico preliminar de la situación existente en la AFP, las acciones previstas para la total adecuación y el cronograma de las mismas, así como los funcionarios responsables del cumplimiento de dicho plan.

Atentamente,

FELIPE TAM FOX

Superintendente de Banca, Seguros y
Administradoras Privadas de Fondos de Pensiones



ANEXO A

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

Documento	Contenido mínimo requerido
1. Información general del proveedor y del servicio	<ul style="list-style-type: none">• Razón social del proveedor.• Giro del negocio y años de experiencia. Indicar a qué empresas brinda servicios actualmente.• 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.• Razones para seleccionar al proveedor.• Carta de la autoridad supervisora competente del país donde el proveedor desarrollará el servicio de procesamiento informático que acredite que dicha entidad la supervisa de manera efectiva.
2. Borrador del Contrato	<p><u>Aspectos a considerar:</u></p> <ul style="list-style-type: none">• Acuerdos de niveles de servicio.• Procedimientos de monitoreo.• Procedimientos de contingencia.• 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 esta Superintendencia.• Aseguramiento del acceso adecuado a la información con fines de supervisión, en tiempos razonables y a solo requerimiento, por parte de esta Superintendencia, Auditoría Interna y 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 entidad supervisada.• Cláusulas que faciliten una adecuada revisión por parte de la Unidad de Auditoría Interna, la Sociedad de Auditoría Externa y esta Superintendencia.
3. Informe de la Plataforma Tecnológica	<p><u>Aspectos a considerar:</u> (Señalar qué equipos y aplicaciones estarán a cargo del proveedor)</p> <ul style="list-style-type: none">• 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.



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

4. Informe de Comunicación con esta Superintendencia (SUCAVE, RCD, otros)	<ul style="list-style-type: none">• Descripción de la forma de envío de información a esta 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.
5. Informe de Evaluación de Riesgos	<ul style="list-style-type: none">• Evaluación de los riesgos de operación asociados con el esquema propuesto por la empresa, realizada por la Unidad de Riesgos.
6. Gestión de la seguridad de información	<ul style="list-style-type: none">• Política de seguridad de información de la empresa.• Estructura organizativa para la gestión de la seguridad de información.• Asignación de responsabilidades asociadas con la seguridad de información en la entidad y el proveedor.• Forma en que se aislará el procesamiento y la información objeto de la subcontratación.• Procedimientos y controles a implementar, considerando el procesamiento en el exterior, en los siguientes aspectos:<ul style="list-style-type: none">- Seguridad lógica.- Seguridad de personal.- Seguridad física y ambiental.- Administración de las operaciones y comunicaciones.- Desarrollo y mantenimiento de sistemas informáticos.- Administración de las copias de respaldo.
7. Gestión de continuidad de negocios	<ul style="list-style-type: none">• Plan de Contingencia del proveedor, para asegurar la continuidad del servicio de procesamiento informático.• Señalar la prioridad asignada al procesamiento de la información de la empresa supervisada respecto al resto de clientes del proveedor.• Señalar la forma en que se dará aviso a la empresa supervisada, y las acciones que deberá desarrollar la empresa en caso de una contingencia en el proveedor.• Frecuencia y alcance de las pruebas al Plan de Contingencia del proveedor.
8. Plan de Auditoría de Sistemas	<ul style="list-style-type: none">• Señalar el alcance, forma y periodicidad de las revisiones de auditoría de sistemas considerando el nuevo esquema de procesamiento principal de la empresa.
9. Gestión del proyecto	<ul style="list-style-type: none">• Cronograma de actividades, incluyendo plazos, responsables y principales hitos de control.• Costo estimado de implementación del proyecto.