Lima, 02 de abril de 2009

CIRCULAR Nº G- 140 -2009

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 349º de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley Nº 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, las cuales toman como referencia estándares internacionales como el ISO 17799 e ISO 27001, disponiéndose su publicación en virtud de lo señalado en el Decreto Supremo N° 001-2009-JUS:

Alcance
Artículo 1º.- 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 2º.- Para efectos de la presente norma, serán de aplicación las siguientes definiciones:

a. Evento: Un suceso o serie de sucesos que pueden ser internos o externos a la empresa, originados por la misma causa, que ocurren durante el mismo periodo de tiempo.

b. Factor de autenticación: Información utilizada para verificar la identidad de una persona. Pueden clasificarse de la siguiente manera:

- Algo que el usuario conoce (por ejemplo: una clave de identificación)
- Algo que el usuario posee (por ejemplo: una tarjeta)
- Algo que el usuario es (por ejemplo: características biométricas)

c. Incidente de seguridad de información: Evento asociado a una posible falla en la política de seguridad, una falla en los controles, o una situación previamente desconocida relevante para la seguridad, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

d. Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios, susceptible de ser procesada, distribuida y almacenada.[1]

e. 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.

f. 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.

g. Subcontratación: Modalidad de gestión mediante la cual una empresa contrata a un tercero para que éste desarrolle un proceso que podría ser realizado por la empresa contratante.

h. Subcontratación significativa: Aquella subcontratación que, en caso de falla o suspensión del servicio, puede poner en riesgo importante a la empresa, al afectar sus ingresos, solvencia, o continuidad operativa.

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 aprobada por el Directorio.
b. Definición e implementación de una metodología de gestión de riesgos, que guarde consistencia con la gestión de riesgos operacionales de la empresa.
c. 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.

[1] Literal modificado por la Circular N° G-167-2012 del 05/11/2012.

Estructura organizacional
Artículo 4°.- 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. Asegurar el cumplimiento de la política de seguridad de información y de la metodología definida por la empresa.
b. Coordinar y monitorear la implementación de los controles de seguridad de información.
c. Desarrollar actividades de concientización y entrenamiento en seguridad de información.
d. Evaluar los incidentes de seguridad de información y recomendar acciones apropiadas.

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°.- Como parte de su sistema de gestión de la seguridad de información, las empresas deberán considerar, como mínimo, la implementación de 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.
d) Controles especiales sobre utilidades del sistema y herramientas de auditoría.
e) Seguimiento sobre el acceso y uso de los sistemas para detectar actividades no autorizadas.
f) 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, de conformidad con la legislación laboral vigente.
c) Concientización y entrenamiento.
d) Procesos disciplinarios en caso de incumplimiento de las políticas de seguridad, de conformidad con la legislación laboral vigente.
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, incluyendo 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 y asignar responsabilidades respecto a la protección de estos activos.
b) Realizar una clasificación de la información, que debe indicar el nivel de riesgo existente para la empresa, 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.
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 a suficiente distancia, que evite exponerlos ante posibles eventos que comprometan la operación del 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 incidentes de seguridad de la 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.

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 a terceros ofrecidas por las empresas para su realización a través de canales electrónicos, las empresas deberán implementar un esquema de autenticación de los clientes basado en dos factores como mínimo. Para el caso en que el canal electrónico sea Internet, uno de los factores de autenticación 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[2]
Artículo 7º.- 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 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

[2] Artículo modificado por la Circular N° G-167-2012 del 05/11/2012.

asegurarse que el procesamiento y la información objeto de la subcontratación, se encuentre efectivamente aislada en todo momento.

Subcontratación significativa de procesamiento de datos en el exterior
Artículo 7.Aº.- [3]

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.

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 la 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 marzo de 2010, fecha a partir de la cual quedará sin efecto la Circular SBS Nº G-105-2002.

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 la Superintendencia un plan de adecuación a las disposiciones contenidas en la presente norma.

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

Atentamente,

[3] Derogado por la Resolución SBS N° 504-2021 del 22/02/2021 vigente a partir del 24.02.2021.

FELIPE TAM FOX
Superintendente de Banca, Seguros y
Administradoras Privadas de Fondos de Pensiones

ANEXO A[4]

[4] Derogado por la Resolución SBS N° 504-2021 del 22/02/2021 vigente a partir del 24.02.2021.