Aprueban Reglamento para Gestión de la Seguridad de la Información y la Ciberseguridad

Lima, miércoles 24 de febrero de 2021

Alerta Legal Financiero

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

Ponemos en conocimiento de nuestros clientes que mediante Resolución SBS No.504-2021, publicada en el Diario Oficial El Peruano el 23 de febrero de 2021, la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (en adelante, "SBS") ha aprobado el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad.

¿Cuál es la finalidad de la norma?

Establecer las normas reglamentarias para la Gestión de la Seguridad de la Información y la Ciberseguridad.

¿A quiénes afecta?

- Las empresas señaladas en los artículos 16 y 17 de la Ley General del Sistema Financiero y el Sistema de Seguros y Orgánica de la SBS – Ley N° 26702 (en adelante, la "Ley General").

- Banco de la Nación, Banco Agropecuario, Corporación Financiera de Desarrollo (Cofide), Fondo MIVIVIENDA S.A., y Derramas y Cajas de Beneficios bajo control de la SBS.

- Empresas corredoras de seguros del segmento 1.

¿De qué manera los afecta?

Sistema de gestión de seguridad de la información y Ciberseguridad (en adelante, "SGSI-C"), es el conjunto de políticas, procesos, procedimientos, roles y responsabilidades, diseñados para identificar y proteger los activos de información, detectar eventos de seguridad, así como prever la respuesta y recuperación ante incidentes de ciberseguridad. El SGSI-C de la empresa debe ser proporcional al tamaño, la naturaleza y la complejidad de sus operaciones.

A. REGIMEN GENERAL

Aplicable a:	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 cuyo volumen promedio de

	activos de los últimos tres (3) años sea mayor o igual a 450 millones de soles. 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; k) El Banco de la Nación
Cambio de régimen	Las entidades indicadas pueden solicitar autorización para la aplicación del Régimen Simplificado, debiendo presentar un informe que sustente la razonabilidad de la solicitud, en términos del tamaño, la naturaleza y la complejidad de sus operaciones, la cual será respondida por la SBS en el plazo de sesenta (60) días hábiles.
Objetivos y requerimientos del SGSI-C	a) 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. b) Revisar periódicamente el alcance y la efectividad de los controles mínimos y contar con capacidades de detección, respuesta y recuperación ante incidentes de seguridad de la información. c) Establecer la relación existente con los planes de emergencia, crisis y de continuidad.
Alcance del SGSI-C	Incluye 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.
Medidas mínimas de seguridad de la información a adoptar por las empresas	a) Seguridad de los recursos humanos b) Controles de acceso físico y lógico c) Seguridad en las operaciones y en las comunicaciones d) Adquisición, desarrollo y mantenimiento de sistemas e) Gestión de incidentes de ciberseguridad f) Seguridad física y ambiental g) Criptografía h) Gestión de activos de información
Programa de ciberseguridad	Toda empresa que cuente con presencia en el ciberespacio debe mantener, con carácter permanente, un programa de ciberseguridad (PG-

	C) aplicable a las operaciones, procesos y otros activos de información asociados.
Reporte de incidentes de ciberseguridad significativos	La empresa debe reportar a la SBS, en cuanto advierta la ocurrencia de un incidente de ciberseguridad que presente un impacto adverso significativo verificado o presumible de: a) Pérdida o hurto de información de la empresa o de clientes. b) Fraude interno o externo. c) Impacto negativo en la imagen y reputación de la empresa. d) Interrupción de operaciones
Implementación de los procesos autenticación	La empresa debe implementar procesos de autenticación, para controlar el acceso a los servicios que provea a sus usuarios por canales digitales.
Enrolamiento del usuario en servicios provistos por canal digital	El enrolamiento de un usuario en un canal digital requiere por lo menos: a) Verificar la identidad del usuario y tomar las medidas necesarias para reducir la posibilidad de suplantación de identidad. b) Generar las credenciales y asignarlas al usuario. Se debe gestionar el ciclo de vida de las credenciales que genere y asigne a sus usuarios, para lo cual debe prever los procedimientos para su activación, suspensión, reemplazo, renovación y revocación; así también, cuando corresponda, asegurar su confidencialidad e integridad.
Autenticación reforzada para operaciones por canal digital	Se requiere de autenticación reforzada para aquellas acciones que puedan originar operaciones fraudulentas u otro abuso del servicio en perjuicio del cliente, como las operaciones a través de un canal digital que impliquen pagos o transferencia de fondos a terceros, registro de un beneficiario de confianza, modificación en los productos de seguro ahorro/inversión contratados, la contratación de un producto o servicio, modificación de límites y condiciones.
Servicios provistos por terceros	En aspectos referidos a gestión de tecnología de la información, a gestión de seguridad de la información o a procesamiento de datos, la empresa, además de cumplir con los requerimientos establecidos en el Reglamento de Gobierno Corporativo y Gestión Integral de Riesgos y el Reglamento para la Gestión de Riesgo Operacional debe: a) Evaluar las amenazas y vulnerabilidades de seguridad de la información en la provisión de bienes y servicios e implementar medidas de tratamiento. b) Asegurar que el arreglo contractual con el proveedor y su implementación le permiten cumplir con las obligaciones establecidas la norma bajo comentario.

	c) Establecer los roles y responsabilidades que el proveedor asume sobre la seguridad de la información y asegurar que la empresa efectúe las implementaciones complementarias correspondientes.
1. Uso de servicios en nube	Debe implementarse políticas y procedimientos de seguridad de la información que sean de aplicación específica, que tome en cuenta un marco de buenas prácticas internacionales para el uso de estos servicios
2. Servicios significativos de procesamiento de datos	Debe ser considerado como un cambio importante en el ambiente informático, siendo aplicable la definición de servicio significativo establecida en el Reglamento de Gobierno Corporativo y Gestión Integral de Riesgos
3. Autorización para la contratación de servicio significativo de procesamiento de datos provisto por terceros desde el exterior	La empresa debe solicitar autorización de la SBS, previo a la contratación de un servicio significativo de procesamiento de datos provisto por terceros desde el exterior, Para solicitar dicha autorización las empresas deben presentar junto con su solicitud, un informe con los sustentos legales de las limitaciones identificadas y una propuesta de plan de implementación de las medidas compensatorias.

B. REGIMEN SIMPLIFICADO

Aplicable a:	a) Banco de Inversión; b) Empresa de Seguros y/o Reaseguros, no contempladas en el Régimen General; c) Entidad de Desarrollo a la Pequeña y Micro Empresa – EDPYME; d) Empresa de Transferencia de Fondos; e) Derrama y Caja de Beneficios bajo control de la Superintendencia; f) La Corporación Financiera de Desarrollo –Cofide; g) El Fondo MIVIVIENDA S.A.; h) El Fondo de Garantía para Préstamos a la Pequeña Industria –Fogapi; i) El Banco Agropecuario; j) Almacenes Generales.
Actividades anuales mínimas	a) Identificar con las unidades de negocio y de apoyo, cuál es la información de mayor importancia, por las obligaciones normativas o contractuales existentes, y por la necesidad de operar. b) Identificar los dispositivos que se conectan a la red interna y todo software que se encuentre instalado en la infraestructura tecnológica, y

	asegurar que se encuentren acorde a una configuración segura previamente establecida. c) Identificar las cuentas de usuario con permisos de acceso habilitados y en particular las que poseen privilegios administrativos con posibilidad de adicionar software a la infraestructura, y mantener el principio de mínimos privilegios otorgados. d) Implementar y mantener una línea base de seguridad en sistemas operativos y aplicaciones utilizadas. e) Priorizar y gestionar las vulnerabilidades de seguridad identificadas, para cuya identificación oportuna debe contar con los servicios de información necesarios. f) Desarrollar una campaña de orientación para la adopción de prácticas seguras dirigida a los empleados, plana gerencial y de dirección.

C. REGIMEN REFORZADO

Aplicable a:	Obligatoriamente 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.
Requerimientos adicionales para empresa con concentración de mercado	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. La empresa debe someter periódicamente a una evaluación independiente del alcance y la efectividad del SGSI-C.

Normas aplicables a todos los regímenes

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.
Responsabilidades de la gerencia	La gerencia general es responsable de tomar las medidas necesarias para implementar el SGSI-C de acuerdo a las disposiciones del directorio.
Funciones del comité de riesgos	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 Para ello se puede constituir un Comité Especializado en Seguridad de la Información y Ciberseguridad (en adelante, “CSIC”). Para las empresas comprendidas en el régimen simplificado, que no cuenten con un Comité de Riesgos o un CSIC, las funciones antes indicadas son asignadas a la Gerencia General.
Información a la SBS	Como parte de los informes periódicos sobre gestión del riesgo operacional requeridos por el Reglamento para la Gestión del Riesgo Operacional, las empresas deben incluir información sobre la gestión de la seguridad de la información y ciberseguridad.
Plazos y plan de adecuación	a) En un plazo que no debe exceder de sesenta (60) días calendario contados a partir del 24 de febrero de 2021, las empresas deben presentar a la SBS, un plan de adecuación a la norma bajo cometario, previamente aprobado por el directorio, en el cual incluya: i) un diagnóstico preliminar de la situación existente en la empresa; ii) las acciones previstas para la total adecuación al Reglamento; iii) los funcionarios responsables del cumplimiento de dicho plan; y, iv) un cronograma de adecuación b) Hasta el 1 de julio de 2022: Las disposiciones referidas a Ciberseguridad c) En un plazo no al 25 de marzo de 2021, las empresas que cuenten con un servicio significativo de procesamiento de datos provisto por terceros desde el exterior, deben remitir un informe que contenga: i) las limitaciones presentadas, dicho informe debe contar con el sustento legal del impedimento de su aplicación y ii) las medidas compensatorias.

Modificaciones a normativa vinculada

a. Reglamento de Auditoría Interna, aprobado por la Resolución SBS N° 11699-2008

Respecto de las actividades programadas que debe realizar la Auditoría Interna, se ha establecido que debe incluir la 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.

Estas disposiciones entran en vigencia a partir de la auditoría correspondiente al ejercicio 2022

b. Reglamento de Auditoría Externa, aprobado por Resolución SBS N° 17026-2010

El informe sobre el sistema de control interno debe contener adicionalmente la 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 la SBS, precisándose los sistemas que fueron parte del alcance de dicha evaluación.

c. Reglamento de Riesgo Operacional, aprobado por Resolución SBS Nº 2116-2009

Se ha establecido requisitos y condiciones vinculadas a la contratación de bienes y/o servicios provistos por terceros, entre otros se ha indicado que 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.

d. Reglamento de Tarjetas de Crédito y Débito, aprobado por Resolución SBS N° 6523-2013

Se ha modificado lo siguiente:

(i) Información mínima, condiciones y vigencia aplicable a la tarjeta de crédito

Las tarjetas de crédito con soporte físico o digital se expiden con carácter de intransferible y deben incluir como mínimo la siguiente información:

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

2. Nombre comercial que la empresa asigne al producto.

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

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

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

(ii) Información mínima, condiciones y vigencia aplicable a las tarjetas de débito

Las tarjetas de débito con soporte físico o digital se expiden con carácter de intransferible y deben incluir como mínimo la siguiente información:

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

2. Nombre comercial que la empresa asigne al producto.

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

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

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

Estas disposiciones entran en vigencia a partir del 24 de febrero de 2021. Salvo el requerimiento asociado a la inclusión conjunta de la información sobre la denominación social de la empresa emisora y el nombre comercial que la empresa asigne al producto de tarjeta de crédito y/o débito, que entra en vigencia el 1 de enero de 2022

e. Reglamento de Operaciones con Dinero Electrónico aprobado por Resolución SBS N° 6283-2013

Los soportes mediante los cuales se puede hacer uso del dinero electrónico pueden ser los siguientes:

a) Teléfonos móviles.

b) Tarjetas prepago.

c) Cualquier otro equipo o dispositivo electrónico, que cumpla los fines establecidos en la Ley.

Estos dispositivos deben incluir como mínimo la siguiente información:

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

2. Nombre comercial que la empresa asigne al producto.

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

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

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

Estas disposiciones entran en vigencia a partir del 24 de febrero de 2021. Salvo el requerimiento asociado a la inclusión en los dispositivos de soporte al dinero electrónico sobre la denominación social de la empresa emisora y el nombre comercial que la empresa asigne al producto, entra en vigencia el 1 de enero de 2022

¿Cuándo entra en vigencia?

La Resolución bajo cometario entra en vigencia el 1 de julio de 2021, con excepción a la autorización para la contratación de servicio significativo de procesamiento de datos provistos desde el exterior, entran en vigencia el 24 de febrero de 2021 y aquellas que hemos precisado en el presente documento.

La presente alerta legal señala los lineamientos generales de la norma comentada y no debe ser considerada como una opinión legal ante una consulta específica.