ALERTA REGULACIÓN FINANCIERA
Resolución SBS 504-2021
"Aprueban el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad y modifican seis reglamentos y el TUPA de la SBS"

Mediante Resolución SBS N° 504-2021 (la "Resolución"), publicada el 23 de febrero de 2021, la Superintendencia de Banca, Seguros y AFP ("SBS"), aprueba el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, con el fin de hacer frente a la creciente interconectividad y virtualización de productos y servicios del sistema financiero, de seguros y privado de pensiones.

Dicho reglamento recoge diversas disposiciones necesarias para que las empresas supervisadas adapten nuevas políticas de identificación, protección, detección y respuesta:

- Introduce el Sistema de gestión de seguridad de la información y Ciberseguridad (SGSI-C), que asegura la confidencialidad, disponibilidad e integridad de la información, y al ser proporcional a las características de las operaciones puede ser de régimen simplificado o reforzado.
- Establece funciones específicas a los órganos de las empresas supervisadas con el fin de adoptar el SGSI-C, siendo (i) el directorio responsable de aprobar y facilitar la implementación; (ii) la gerencia general de tomar las medidas necesarias para la consolidación; y, (iii) el Comité de Riesgos de aprobar los planes estratégicos y de capacitación para ponerlo en práctica. Para el cumplimiento de las funciones indicadas en el numeral (iii) anterior, se faculta a las empresas a constituir un Comité Especializado en Seguridad de la Información y Ciberseguridad (CSIC).
- Exige que las empresas incluyan información sobre la gestión de la seguridad de la información y ciberseguridad, como parte de los informes periódicos sobre gestión del riesgo operacional requeridos por el Reglamento para la Gestión del Riesgo Operacional.
- Exige a toda empresa que cuente con presencia en el ciberespacio mantener, con carácter permanente, un programa de ciberseguridad (PG-C) aplicable a las operaciones, procesos y otros activos de información asociados.
- Requiere de autenticación reforzada para las acciones que puedan originar operaciones fraudulentas u otro abuso del servicio en perjuicio del cliente.
- Desarrolla medidas que deben cumplir las empresas supervisadas en relación a la gestión de tecnología y seguridad de la información y el procedimiento de datos en los servicios provistos por terceros, uso de servicios en nube y servicios significativos de procesamiento de datos, tomando en cuenta un marco de buenas prácticas internacionales.
- Considera los siguientes plazos:
    - Para la presentación del plan de adecuación ante la SMV (sujeto a previa aprobación del directorio): hasta 60 días calendario posteriores al 23 de febrero de 2021.
    - Para la adecuación: hasta el 1 de julio de 2022.
    - Para informar limitaciones y medidas compensatorias resultantes de un servicio significativo de procesamiento de datos, provisto por terceros, desde el exterior, que dificulten la adecuación: hasta el 25 de marzo del 2021.

Paralelamente, la Resolución modifica el Texto Único de Procedimientos Administrativos de la SBS; y, los seis (6) reglamentos que se mencionan a continuación: (i) Reglamento de Auditoría Interna; (ii) Reglamento de Auditoría Externa; (iii) Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos; (iv) Reglamento de Riesgo Operacional; (v) Reglamento de Tarjetas de Crédito y Débito; y, (vi) Reglamento de Operaciones con Dinero Electrónico.

Reglamento de Auditoría Interna, aprobado por la Resolución SBS N° 11699-2008 y sus modificatorias	Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, aprobado mediante Resolución SBS N° 272-2017	Reglamento de Tarjetas de Crédito y Débito, aprobado por Resolución SBS N° 6523-2013 y sus normas modificatorias
Precisa sus "Actividades Programadas", señalando que las Evaluaciones de (i) gestión del riesgo operacional; (ii) cumplimiento de los procedimientos utilizados para la administración de los riesgos de operación; y, (ii) gestión de los riesgos distintos a los riegos técnicos de seguros, se darían conjuntamente a la evaluación de las disposiciones de la normativa vigente sobre gestión de continuidad del negocio y de seguridad de la información y ciberseguridad.	Desarrolla medidas que deben cumplir las empresas supervisadas en relación a la provisión de bienes y/o servicios por parte de terceros.	Cambia la información mínima que deben incluir las tarjetas de crédito y/o débito, siendo ahora: (i) la denominación social de la empresa que emite la tarjeta; (ii) el nombre comercial que la empresa asigne al producto; y, (iii) la identificación del sistema de tarjeta (marca) al que pertenece, de ser el caso.
Reglamento de Auditoría Externa, aprobado por Resolución SBS N° 17026-2010 y sus modificatorias	**Reglamento de Riesgo Operacional, aprobado por Resolución SBS Nº 2116-2009**	**Reglamento de Operaciones con Dinero Electrónico aprobado por Resolución SBS N° 6283-2013 y sus normas modificatorias**
Establece en uno de los criterios que deberá observar el Informe sobre el sistema de control interno (evaluación de los sistemas de información), que deberán precisarse los sistemas que fueron parte del alcance de dicha evaluación.	Desarrolla medidas que deben cumplir las empresas supervisadas en relación a la provisión de bienes y/o servicios por parte de terceros.	Establece que los soportes para el uso de dinero electrónico deben incluir como mínimo: (i) la denominación social de la empresa que emite el soporte mediante el cual se hace uso del dinero electrónico; (ii) el nombre comercial que la empresa asigne al producto; y, (iii) la identificación del sistema de tarjeta (marca) al que pertenece, de ser el caso; mencionando también que dicha información debe ser mostrada en un espacio visible y de fácil acceso para el usuario.
Texto Único de Procedimientos Administrativos de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones, aprobado mediante Resolución Nº 1678- 2018		
- Modifica el procedimiento N° 123 relativo a la "Autorización del Procesamiento Principal en el Exterior" por "Autorización para la contratación del servicio significativo de Procesamiento de Datos provisto por terceros desde el Exterior" - Incorpora el procedimiento N°198 relativo a "Autorización para aplicar el Régimen Simplificado del Sistema de Gestión de la Seguridad de la Información y la Ciberseguridad"		

La Resolución entra en vigencia con fecha 1 de julio de 2021 -derogando la Circular G 140-2009-, con excepción de determinados artículos señalados en su artículo décimo.