

SBS propone medidas para reforzar gestión de seguridad de información

La **Superintendencia de Banca, Seguros y AFP (SBS)** comunicó que ha publicado un proyecto de Reglamento para la gestión de seguridad de la información y ciberseguridad, complementario al Reglamento para la gestión del riesgo operacional, que actualiza los requisitos hoy establecidos sobre seguridad de la información, considerando los estándares y buenas prácticas internacionales.

Ello, con el objetivo de adecuar el marco normativo vigente sobre la seguridad de la información, a las exigencias propias de un entorno cada vez más dinámico e interconectado en el que se desenvuelven las entidades financieras, aseguradoras y **AFP**, que implica una mayor exposición a ciber amenazas y, por ello, demanda de mayores esfuerzos para mantener la seguridad en los servicios ofrecidos a los usuarios.

El proyecto plantea el establecimiento de un marco para el sistema de gestión de seguridad de la información de las entidades supervisadas; la implementación de la autenticación en canales digitales; la subcontratación de servicios de procesamiento de datos, incluyendo el procesamiento en la nube; y, la actualización e incorporación de requisitos en materia de seguridad de la información, asociados a la proporcionalidad de lo exigido.

Respecto al primer aspecto, se establece que las empresas

deberán contar con un plan estratégico de seguridad de la información y de ciberseguridad que prevea el análisis de amenazas y vulnerabilidades de los activos de información, atender necesidades de capacitación y difusión; y efectuar pruebas periódicas de seguridad.

También, deberán contar con un equipo especializado para el manejo de incidentes de ciberseguridad, que tendrá a su cargo de reportar dichos incidentes a la **SBS** y promover el intercambio de información de ciberseguridad con los organismos competentes.

Con relación a los requisitos de autenticación en canales digitales, se requiere que las empresas implementen procesos de autenticación, los que deben ser reevaluados cada vez que se presenten cambios en la tecnología que los soportan, o tras el descubrimiento de nuevas vulnerabilidades en la misma.

También, se requiere de una autenticación reforzada para aquellas operaciones que impliquen una transferencia de fondos, un pago, la solicitud de un trámite o la contratación de un producto o servicio, modificación de límites y condiciones en los que se proveen los servicios, y otros que pueden originar una operación fraudulenta o perjuicio del cliente.

Respecto a la proporcionalidad en materia de seguridad de la información, el proyecto de Reglamento desarrolla requisitos diferenciados en tres niveles.

El primer nivel -denominado aplicación general- requiere de medidas asociadas a la seguridad de información, autenticación, subcontratación del procesamiento de datos y ciberseguridad para bancos, financieras, cajas, aseguradoras, AFP, **Banco de la Nación**, emisores de dinero electrónico y empresas de transporte, custodia y administración de numerario.

El segundo nivel -denominado simplificado- comprende a empresas como las **Edpyme**, Fondo Mivivienda, Fogapi, Agrobanco, Cofide, Derramas y empresas de transferencias de fondos.

El tercer nivel -denominado reforzado- se dirige a las empresas más grandes y con operaciones más complejas sujetas a un requerimiento de patrimonio efectivo por riesgo de concentración de mercado, sin perjuicio de que la **SBS** incluya otras empresas, para las que se especifican requerimientos más exigentes.

Otras medidas propuestas tienen como propósito reforzar las responsabilidades para el directorio, la gerencia, el comité de riesgos y la función independiente de seguridad de la información y ciberseguridad.

El proyecto estará publicado en el portal de la **SBS** (www.sbs.gob.pe) hasta el próximo 17 de setiembre, con la finalidad de recibir comentarios y sugerencias.