Descargar: 504-2021.R.pdf

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

Lima, 19 de febrero de 2021

Resolución S.B.S.
N° 504-2021

La Superintendenta de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones

CONSIDERANDO:

Que, el Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos, aprobado mediante la Resolución SBS N° 272-2017, incorpora disposiciones que tienen por finalidad que las empresas supervisadas cuenten con una gestión de riesgos y gobierno corporativo adecuados;

Que, mediante el Reglamento para la Gestión del Riesgo Operacional, aprobado mediante la Resolución SBS N° 2116-2009, se incluyen disposiciones que las empresas deben cumplir en la gestión efectiva del riesgo operacional;

Que, esta Superintendencia emitió la Circular G-140-2009 con la finalidad de establecer criterios mínimos para una adecuada gestión de la seguridad de la información;

Artículo 21. Uso de API para la provisión de servicios en línea

21.1 El uso de interfaces de programación de aplicaciones, para proveer servicios para realizar operaciones, a través de servicios de terceros, requiere que se implementen las siguientes medidas:

a) Análisis de riesgos asociados e implementar las medidas de mitigación.
b) La autenticación mutua de los sistemas y la de los usuarios.
c) La autorización de las operaciones por parte de los usuarios.
d) El cifrado de datos en almacenamiento o transmisión.
e) Prácticas de desarrollo seguro de API y revisión de prácticas de codificación segura.
f) Análisis de vulnerabilidades y pruebas de penetración.
g) La seguridad de la infraestructura tecnológica que lo soporta.
h) Los mecanismos de tolerancia ante fallos y de contingencia.
i) Control de accesos en el entorno de datos, sistemas e infraestructura.
j) Monitoreo de eventos de seguridad de la información y gestión de estos cuando se constituyan en incidentes.

21.2 La empresa debe tomar como referencia estándares y marcos de referencia internacionales, y cuando sea factible adoptarlos en el marco de acuerdos gremiales o sectoriales, para la implementación del intercambio y encriptación de datos, así como la autenticación y la autorización de operaciones, sin que ello sea una lista restrictiva.

21.3 Las especificaciones técnicas de las API utilizadas deben encontrarse documentadas de forma que facilite su auditoría y la implementación necesaria para su uso.

21.4 Las empresas deben implementar las medidas necesarias para garantizar que el tercero autorizado por el usuario, acceda únicamente a la información indicada por este último.

Julio Pari (IT Architect IBM)

Si te ha interesado este artículo y deseas un apoyo o asesoría en algún requerimiento, envíame un mensaje a: (info@juliopari.com) o sino a través de Linkedin: https://www.linkedin.com/in/juliopari/
