GOBIERNO DE PUERTO RICO
CORPORACIÓN PÚBLICA PARA LA SUPERVISIÓN Y SEGURO DE COOPERATIVAS DE PUERTO RICO
Presidenta Ejecutiva Mabel Jiménez Miranda, MBA mjimenez@cossec.pr.gov

CARTA CIRCULAR NÚM. 2023-02

A LAS COOPERATIVAS DE AHORRO Y CRÉDITO

Rafael Sánchez Rodríguez, CICA, CAMS
Presidente Ejecutivo Interino

RIESGO DE SISTEMAS DE INFORMACIÓN Y TECNOLOGÍA

Reciban un cordial saludo. Como parte de la evaluación de la reglamentación y procesos de supervisión que llevamos a cabo, les enviamos el Cuestionario de Sistemas de Información 2022. Este fue completado por un número significativo de Cooperativas de Ahorro y Crédito, por lo que agradecemos su colaboración.

Los cambios tecnológicos constantes, así como los retos que representan las nuevas modalidades de crímenes cibernéticos a los que se enfrentan las entidades y personas hacen necesario que las Cooperativas de Ahorro y Crédito cuenten con políticas y procedimientos actualizados sobre los sistemas de información, la seguridad cibernética y la gestión de riesgo tecnológico. Dichas políticas y procedimientos deben estar alineadas a su tamaño y la complejidad de sus operaciones y servicios, que les permita diseñar una estructura de control interno adecuada, basada en un proceso de gestión de riesgo tecnológico, que mitigue los riesgos de amenazas y vulnerabilidades asociados a estos.

Las políticas y procedimientos de gestión de riesgo tecnológico deben ser creadas o revisadas para hacerlas compatibles con las mejores prácticas internacionales para el desarrollo de una gestión integral de riesgos. Entre los marcos de referencia que pueden usar se encuentra el Marco Integrado para la Gestion de Riesgo publicado por el *Committee of Sponsoring Organization of the Treadway Commission* (COSO).

Según COSO, la gestión integral de riesgos se define como: un proceso establecido por la junta directiva de una entidad, la gerencia y otro personal, aplicado en un ambiente estratégico y a través de la entidad, diseñado para identificar eventos potenciales que puedan afectarle, gestionar sus riesgos dentro de los niveles de aceptación establecidos, y para proveer seguridad razonable del logro de sus objetivos.

Las medidas preventivas, como lo son mantener un plan de continuidad y de recuperación en caso de un desastre, un plan de manejo de incidentes debidamente actualizado, son el producto de planificación, procesos continuos de gestión de riesgos, inversión en recursos tecnológicos y humanos, capacitación, auditoría y fiscalización de recursos internos y externos, así como de supervisión por la gerencia y Junta de Directores(as).

Por ello, la Corporación, como ente encargado de supervisar y fiscalizar el cumplimiento de las cooperativas de ahorro y crédito con las leyes relativas a sus operaciones, negocios, productos y/o servicios[1] y de conformidad con el Artículo 11 (a) (3) y (b) (7) de la Ley Núm. 114-2001, así como el Artículo 5.10 (a) de la Ley Núm. 255-2002, según enmendada, conocida como *Ley de Sociedades Cooperativas de Ahorro y Crédito de 2002*, requiere que las Juntas de Directores(as) de las Cooperativas de Ahorro y Crédito revisen las políticas y procedimientos relacionadas con los sistemas de información y tecnología, la seguridad cibernética y la gestión de riesgo tecnológico, y procuren que estén actualizadas y sean comunicadas a todos(as) los (las) empleados(as) y personal externo contratado. No se trata de un ejercicio único sino de uno continuo que les permita conocer los riesgos de sus respectivas cooperativas según su tamaño, el perfil de sus socios(as) y depositantes, así como los productos y servicios que ofrecen y cuan preparada está la gerencia para anticiparlos y manejarlos, de ocurrir. Asimismo, tienen el deber de constatar que la gerencia cumpla con su responsabilidad en la implementación de dichas políticas y procedimientos.[2]

Por su parte, los (las) Presidentes(as) Ejecutivos(as) deben asumir un rol proactivo y dinámico enfocado en:

1. Observar que cuenten con los recursos técnicos, tecnológicos y de sistemas necesarios, presupuesto y personal capacitado para mitigar los riesgos y comunicar a la Junta de Directores las necesidades que puedan tener.
2. Proveer informes periódicos a la Junta de Directores(as) sobre la implementación de estas políticas y procedimientos, evaluación de productos y servicios y su impacto en los sistemas de información, riesgos identificados y las medidas implementadas para mitigarlos, situaciones ocurridas y acciones tomadas, entre otros.
3. Periódicamente evaluar los procedimientos conducidos y llevar a la atención de la Junta de Directores(as) de la cooperativa los cambios que sean necesarios.
4. Asegurar que todo el personal recibe adiestramiento continuo sobre las políticas y procedimientos de sistemas de información, seguridad cibernética y la gestión de riesgo, así como de las prácticas de protección al consumidor.
5. Supervisar al personal interno y a los proveedores externos para asegurar que estos cumplen con sus responsabilidades y que sus prácticas son consistentes con los procedimientos adoptados.

---

[1] Artículo 4(b)(1) de la Ley Núm. 114-2001, según enmendada, *Ley de la Corporación Pública para la Supervisión y Seguro de Cooperativas de Puerto Rico*, 7LPRA§1334b

[2] Artículo 5.10(b)(2) de la Ley Núm.255-2002, 7LPRA §1365i

6. Llevar a cabo auto evaluaciones, pruebas periódicas y auditorías externas cuando sea necesario.
7. Observar que se cumplen las leyes federales y estatales de protección al consumidor.
8. Implementar normas sobre el proceso de evaluación y la gestión de riesgos.
9. Colaborar y priorizar en la identificación de los objetivos estratégicos para los que se interesa se realice la evaluación de riesgos.
10. Definir los niveles de aceptación de riesgos, en relación con los objetivos estratégicos, las alternativas disponibles y los mecanismos correspondientes para atenderlos.
11. Organizar un grupo de trabajo multidisciplinario para realizar anualmente la gestión de riesgos tecnológico en la Cooperativa de Ahorro y Crédito. Entre los (las) integrantes del grupo se deben considerar funcionarios(as) o empleados(as) de las áreas que interactúan en el logro del objetivo bajo evaluación, el (la) oficial de cumplimiento y auditor(a) interno(a) o externo(a).

En COSSEC somos conscientes de los retos que representan los riesgos tecnológicos y estamos comprometidos con apoyarles. Si tienen alguna pregunta, pueden comunicarse con el Área de Apoyo Técnico y Supervisión.