avisos y subastas

COSSEC

PUBLIC NOTICE ON PUBLICATION OF REGULATION

We hereby notify the public that the Public Corporation for the Supervision and Insurance of Cooperatives of Puerto Rico (COSSEC) intends to adopt the:

Amendment to Articles 4, 5, 6, 10, 11, 23 and 24 of Regulation No. 9444

The purpose of this Regulation is to amend Regulation No. 9444, known as the Procurement Regulation of the Public Corporation for the Supervision and Insurance of Cooperatives of Puerto Rico, to bring it into line with the provisions of Act No. 48-2004, which repealed Section 3.19 of Chapter 3 and amended Section 4.2 of Chapter 4 of Act No. 38-2017. It also amends Articles 4, 10, 22, 25, 31, 32, 35, 42, 46, 50, 51, 53, 64, 66, 72 and 79 of Act No. 73-2019 and incorporates the amendments of Act No. 153-2004. Based on the foregoing, in this Regulation we amend articles 4. Definitions, 5 General Provisions, 6. Types of Purchase, 10. Auction Board, 11. Invitation to Formal Auctions, 23. Notice of Formal Auctions and 24. Administrative Review of Regulation No. 9444 to reflect the changes introduced by Act No. 48-2004 and Act No. 153-2024.

This Regulation is adopted pursuant to Sections 4(d)(5)(11)(B) and 7(a)(i) of the Public Corporation for the Supervision and Insurance of Cooperatives of Puerto Rico Act, Act No. 114-2001, as amended, hereinafter COSSEC or the Corporation, in observance of the principles of Act No. 230 of July 23, 1974, as amended, known as the "Government of Puerto Rico Accounting Act", and Act No. 73-2019, as amended, known as the "General Services Administration Act for the Centralization of Government of Puerto Rico Procurement of 2019", and in accordance with Act No. 38-2017, as amended, "Uniform Administrative Procedure Act of the Government of Puerto Rico".

The text of the Regulation is available for inspection by the public at the facilities of the Public Corporation for the Supervision and Insurance of Cooperatives of Puerto Rico, located at Ave. Américo Miranda # 400, Urb. Villa Nevárez, Edificio Original COSVI, San Juan, PR 00928, between 8:00 a.m. and 4:30 p.m. during weekdays. In addition, they are published on the internet portal www.cossec.pr.gov.

Any person interested in submitting written comments on the proposed Regulation or request a public hearing has 30 days from the publication of this announcement to do so. If an oral hearing is requested, the applicant must present the reasons justifying its necessity. Both the comments and the request for a public hearing may be submitted to the Corporation through the following methods:

EMAIL : reglamento@cossec.pr.gov
MAIL : PO BOX 195449 San Juan, PR 00919-5449.
PERSONALLY: COSSEC's Reception, located on Floor 6 of the address indicated above.

All comments submitted must have the title "Comments on Amendments to Regulation 9444".

In San Juan, Puerto Rico on October 2, 2025.

Mabel Jiménez Miranda, MBA
Executive President

COSSEC

AVISO PÚBLICO SOBRE PUBLICACIÓN DE REGLAMENTO

Se notifica al público en general que la Corporación Pública para la Supervisión y Seguro de Cooperativas de Puerto Rico (COSSEC) se propone adoptar el:

Reglamento de Sistemas de Información y Tecnología

El propósito de este Reglamento es reglamentar los requisitos mínimos de seguridad de la información, manejo de riesgos tecnológicos así como la adquisición de sistemas, programas y servicios tecnológicos, que deben ser implementados por las cooperativas de ahorro y crédito. Además, requiere la presentación de informes y la notificación a la Corporación cuando ocurran incidentes catastróficos que afecten la continuidad de los servicios brindados por las cooperativas de ahorro y crédito así como en los casos en que son víctimas de ataques cibernéticos. Finalmente, dispone el término en el cual todas las cooperativas de ahorro y crédito deberán estar en cumplimiento con las disposiciones de este Reglamento.

Este Reglamento es adoptado en virtud de los Artículos 4(d)(11)(B), 7(a)(i), a(v)(b), 11(a)(3) y 11(b)(7)-(8), de la *"Ley de la Corporación Pública para la Supervisión y Seguro de Cooperativas de Puerto Rico"*, Ley Núm. 114-2001, según enmendada, en adelante COSSEC o la Corporación, por la Ley Núm. 255-2002, según enmendada, conocida como *"Ley de Sociedades Cooperativas de Ahorro y Crédito de 2002"*, por la *"Ley Orgánica de la Comisión de Desarrollo Cooperativo de Puerto Rico"*, Ley Núm. 247-2008, según enmendada, y de conformidad con la Ley Núm. 38-2017, según enmendada, conocida como "Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico".

El texto del Reglamento se encuentra disponible para inspección por el público en las facilidades de la Corporación Pública para la Supervisión y Seguro de Cooperativas de Puerto Rico, localizada en la Ave. Américo Miranda #400, Urb. Villa Nevárez, Edificio Original COSVI, San Juan, PR 00928, entre las 8:00 am y las 4:30 pm durante días laborables. Además, se encuentra publicado en el portal de internet www.cossec.pr.gov

Los comentarios por escrito o la solicitud de vista oral deberán ser sometidos no más tarde de 30 días a partir de la fecha de publicación de este aviso. En caso de solicitar la vista oral, el (la) solicitante deberá exponer los fundamentos que hacen necesaria su concesión. Tanto los comentarios como la solicitud de vista oral pueden ser remitidos a la Corporación a través de los siguientes métodos:

CORREO ELECTRÓNICO: reglamento@cossec.pr.gov
POSTAL: PO BOX 195449 San Juan, PR 00919-5449.
PERSONALMENTE: Recepción de COSSEC, ubicada en el Piso 6 de la dirección antes indicada.

Todos los comentarios sometidos deben tener por título "Comentarios al *Reglamento de Sistemas de Información y Tecnología*".

En San Juan, Puerto Rico, a 2 de octubre de 2025.

Mabel Jiménez Miranda, MBA
Presidenta Ejecutiva

COSSEC

PUBLIC NOTICE ON PUBLICATION OF REGULATION

We hereby notify the public that the Public Corporation for the Supervision and Insurance of Cooperatives of Puerto Rico (COSSEC) intends to adopt the:

Information Systems and Technology Regulation

The purpose of this Regulation is to regulate the minimum requirements for information security, technological risk management, and the acquisition of technological systems, programs, and services that credit unions must implement. It also requires reporting and notification to the Corporation when catastrophic incidents occur that affect the continuity of services provided by credit unions, as well as in cases where they are victims of cyberattacks. Finally, it establishes the deadline within which all credit unions must comply with the provisions of this Regulation.

This Regulation is adopted pursuant to Sections 4(d)(11)(B), 7(a)(i), a(v)(b), 11(a)(3) y 11(b)(7)-(8) of the Public Corporation for the Supervision and Insurance of Cooperatives of Puerto Rico Act, Act No. 114-2001, as amended, hereinafter COSSEC or the Corporation, by Act No. 255-2002, as amended, known as the "Savings and Credit Cooperative Societies Act of 2002",by the "Organic Law of the Puerto Rico Cooperative Development Commission", Act No. 247-2008, as amended, and in accordance with Act No. 38-2017, as amended, "Uniform Administrative Procedure Act of the Government of Puerto Rico".

The text of the Regulation is available for inspection by the public at the facilities of the Public Corporation for the Supervision and Insurance of Cooperatives of Puerto Rico, located at Ave. Américo Miranda # 400, Urb. Villa Nevárez, Edificio Original COSVI, San Juan, PR 00928, between 8:00 a.m. and 4:30 p.m. during weekdays. In addition, they are published on the internet portal www.cossec.pr.gov.

Any person interested in submitting written comments on the proposed Regulation or request a public hearing has 30 days from the publication of this announcement to do so. If an oral hearing is requested, the applicant must present the reasons justifying its necessity. Both the comments and the request for a public hearing may be submitted to the Corporation through the following methods:

EMAIL : reglamento@cossec.pr.gov
MAIL : PO BOX 195449 San Juan, PR 00919-5449.
PERSONALLY: COSSEC's Reception, located on Floor 6 of the address indicated above.

All comments submitted must have the title "Comments on *Information Systems and Technology Regulation*".

In San Juan, Puerto Rico on October 2, 2025.

Mabel Jiménez Miranda, MBA
Executive President

GOBIERNO DE PUERTO RICO
CORPORACIÓN PÚBLICA PARA LA SUPERVISIÓN Y SEGURO
DE COOPERATIVAS DE PUERTO RICO
(COSSEC)

Reglamento de Sistemas de Información y Tecnología

Índice

Página

GOBIERNO DE PUERTO RICO
CORPORACIÓN PÚBLICA PARA LA SUPERVISIÓN Y SEGURO
DE COOPERATIVAS DE PUERTO RICO
(COSSEC)

Artículo 1. Título

Este Reglamento se conocerá como *Reglamento de Sistemas de Información y Tecnología*.

Artículo 2. Base Legal

Este Reglamento se adopta y promulga por virtud de la autoridad conferida a la Junta de Directores de la Corporación Pública para la Supervisión y Seguro de Cooperativas de Puerto Rico, en adelante COSSEC o la Corporación, por los 4(d)(11)(B), 7(a)(i), a(v)(b), 11(a)(3) y 11(b)(7)-(8) de la Ley Núm. 114-2001, según enmendada, (Ley Núm. 114-2001), conocida como la *"Ley de la Corporación Pública para la Supervisión y Seguro de Cooperativas de Puerto Rico"*, por la Ley Núm. 255-2002, según enmendada, (Ley Núm. 255-2002), conocida como *"Ley de Sociedades Cooperativas de Ahorro y Crédito de 2002*", la Ley Núm. 248-2008, según enmendada, (Ley Núm. 247-2008), conocida como "*Ley Orgánica de la Comisión de Desarrollo Cooperativo de Puerto Rico*", y de conformidad con la Ley Núm. 38-2017, según enmendada, (Ley Núm. 38-2017), conocida como "*Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico"*.

Artículo 3. Propósito y Resumen Ejecutivo

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 de la información de los (las) socios(as) y clientes, la seguridad cibernética y la gestión de riesgo tecnológico, entre otras. Este Reglamento tiene el propósito de reglamentar los requisitos mínimos de seguridad de la información, manejo de riesgos tecnológicos así como la adquisición de sistemas, programas y servicios tecnológicos, que deben ser implementados por las cooperativas de

ahorro y crédito. Además, requiere la presentación de informes y la notificación a la Corporación cuando ocurran incidentes catastróficos que afecten la continuidad de los servicios brindados por las cooperativas de ahorro y crédito así como en los casos en que son víctimas de ataques cibernéticos. Finalmente, dispone el término en el cual todas las cooperativas de ahorro y crédito deberán estar en cumplimiento con las disposiciones de este Reglamento.

Cónsono con lo anterior, la Corporación certifica que la aprobación y puesta en vigor de este Reglamento no tiene impacto fiscal adicional para la esta. Un análisis de costo-beneficio del Reglamento evidencia que su adopción es un requisito de ley y no implica mayores costos para el fondo, como tampoco para la ciudadanía.

Artículo 4. Aplicabilidad

Este Reglamento aplica a toda cooperativa de ahorro y crédito organizada bajo las leyes del Gobierno de Puerto Rico, aseguradas por la Corporación.

Artículo 5. Principios Interpretativos

(a) Las disposiciones de este Reglamento se interpretarán liberalmente para permitir a la Corporación llevar a cabo sus funciones reguladoras y asegurar que todos los propósitos de las leyes que administra y este Reglamento sean alcanzados.

(b) Cuando así lo justifique su uso, se entenderá que toda palabra usada en tiempo presente incluye también el pasado y futuro, el singular incluye el plural.

(c) Las palabras usadas en este reglamento deben interpretarse de acuerdo con su contexto y al significado que tengan por su uso común y corriente. Salvo que se indique lo contrario o que de su contexto surja otro significado, los términos, vocablos, frases y definiciones incluidas en cualquier legislación aplicable a la Corporación Pública para la Supervisión y Seguro de Cooperativas de Puerto Rico se aplicarán a este Reglamento.

Artículo 6. Definiciones

1. **Controles de seguridad**- controles formales para proteger la información contenida en documentos, medios de almacenamiento u otros dispositivos externos, el uso e intercambio electrónico de datos contra daño, robo, accesos, utilización o divulgación no autorizada de información para fines contrarios a los intereses de la entidad, por parte de su personal y proveedores.
2. **Gestión de riesgos**- proceso de identificar, evaluar y minimizar el impacto del riesgo.
3. **Información**- todo récord que contenga información personal no pública de un (a) socio(a) o cliente(a) de la cooperativa, conservada en papel, formato electrónico o de cualquier otra forma, por la Cooperativa o por un proveedor de servicios de esta.
4. **Plan de continuidad de negocios y recuperación de desastres**- conjunto de procedimientos que establece protocolos y crea sistemas de prevención y recuperación en caso de un ciberataque, desastre natural u otra disrupción en la cooperativa.
5. **Programa de Seguridad de la información**- es un plan escrito creado e implementado por la cooperativa para identificar y controlar riesgos a la información y sistemas de información y para disponer adecuadamente de la información. Incluye las salvaguardas técnicas, físicas o administrativas establecidas para acceder, recopilar, distribuir, procesar, proteger, almacenar, usar, transmitir, disponer o de cualquier otra forma manejar la información del (de la) socio(a) o cliente.
6. **Reglamento Núm**. **6758-2004**- Reglamento de la Ley de la Corporación para la Supervisión y Seguro de Cooperativas de Puerto Rico.
7. **Reglamento Núm**. **9441-2023-** Reglamento de Procedimientos Investigativos y Adjudicativos.
8. **Sistemas de información** - cualquier método o recurso organizado para la recopilación, procesamiento, mantenimiento, uso, intercambio, difusión o la disposición de información electrónica del (de la) socio(a) o cliente, o que está conectado a un sistema que contiene información del (de la) socio(a) o cliente, así como cualquier sistema especializado, que contenga información del (de la) socio(a) o cliente o esté conectado a un sistema que contenga información del (de la) socio(a) o cliente.

9. **Proveedores de servicio**- cualquier persona o entidad que mantenga, procese o tenga permitido el acceso a la información de los (las) socios(as) y clientes(as) mediante los servicios que provee directamente a la cooperativa.

Artículo 7. Adopción de Políticas y Procedimientos Relacionados a los Sistemas de Información

A. Deber de la Junta de Directores(as)

1. Es deber de la Junta de Directores(as) de toda cooperativa aprobar políticas y procedimientos sobre los sistemas de información y tecnología que atiendan lo siguiente:
    (a) Seguridad de la información privada de los (las) socios(as) y depositantes.
    (b) Seguridad cibernética.
    (c) Adquisición de sistemas de información, tecnología, programas, equipos y servicios tecnológicos.
    (d) Capacitación del personal.
    (e) Cumplimiento legal relacionado a los productos y servicios manejados, ofrecidos por la cooperativa a través de sus sistemas de información.
    (f) Continuidad de negocios y recuperación de desastres.
    (g) Contratación, supervisión y manejo de proveedores y contratistas.
    (h) Gestión de riesgo tecnológico.
    (i) Cualquier otro elemento que la Junta de Directores determine necesario, alineado a las necesidades estratégicas y operacionales de la institución.
2. Posterior a su aprobación, la Junta de Directores debe procurar que las políticas y procedimientos sobre sistemas de información y tecnología, la seguridad cibernética y la gestión de riesgo tecnológico, estén actualizadas y sean comunicadas a todos(as) los (las) empleados(as) y personal externo contratado. El ejercicio debe ser uno continuo, que le permita conocer los riesgos de su cooperativa según su tamaño, el perfil de sus socios(as) y clientes(as) así como los productos y servicios que ofrecen y cuan preparada está la gerencia para anticiparlos y manejarlos, de ocurrir.

3. Asimismo, tiene el deber de constatar que la gerencia cumpla con su responsabilidad en la implementación de dichas políticas y procedimientos.

B. Deber de los (las) Presidentes(as) Ejecutivos(as)

1. Observar que la cooperativa cuente con los recursos técnicos, tecnológicos y de sistemas necesarios, presupuesto y personal capacitado para mitigar los riesgos anticipados y comunicar a la Junta de Directores(as) las necesidades que puedan tener.
2. Proveer informes periódicos a la Junta de Directores(as) sobre la implementación de las 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 y tecnología, 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.
6. Llevar a cabo auto evaluaciones, pruebas periódicas y auditorías externas cuando sea necesario.

Artículo 8. Oficial de Seguridad de Información

A. Designación

1. El (La) Presidente(a) Ejecutivo(a) de la cooperativa, con la aprobación de la Junta de Directores(as), designará un(a) Oficial de Seguridad de Información.
2. El (La) Oficial de Seguridad de Información podrá ser un(a) empleado(a) de la cooperativa, un(a) empleado(a) de nuevo reclutamiento o una persona natural o jurídica contratada, pero no podrá ser el (la) Presidente Ejecutivo(a) ni algún

miembro de la Junta de Directores(as). Disponiéndose que no será necesaria la designación de un(a) Oficial de Seguridad de Información en los casos en que la cooperativa asigne las responsabilidades de este(a) al puesto de encargado(a) de documentos requerido en el Capítulo III, Sección 3(c)(1) del Reglamento Núm. 6758-2004 siempre y cuando la persona esté capacitada para llevar a cabo las funciones.

B. Responsabilidades del (de la) Oficial de Seguridad de Información

En adición a los deberes y responsabilidades que establezca la cooperativa, el (la) Oficial de Seguridad de Información deberá:

1. Velar por el fiel cumplimiento de las políticas y procedimientos de seguridad de información aprobados por la Junta de Directores(as).
2. Rendir informes periódicos al (a la) Presidente(a) Ejecutivo(a) de la cooperativa, los cuales deberán presentarse a la Junta de Directores(as) al menos, trimestralmente. Disponiéndose, que los informes deberán estar disponibles para examen por la Corporación.

   a) Contenido de los informes- Sin que se entienda una limitación, los informes deberán contener lo siguiente:

   i. Situaciones encontradas y su estatus.
   ii. Riesgos, vulnerabilidad o debilidad del sistema de información y tecnología relacionados a la seguridad de la información del (de la) socio(a) y clientes(as).
   iii. Incidentes de accesos no autorizados a, o el uso de información de un(a) socio(a) o cliente(a) que pudiera ocasionarle inconvenientes o daños y acciones tomadas.
   iv. Información sobre querellas presentadas por los (las) socios(as) y clientes(as) de la cooperativa.
   v. Adiestramientos al personal.
   vi. Estatus de cumplimiento con la presentación de informes relacionados a los sistemas de información, requeridos por COSSEC.

Artículo 9. Programa de Seguridad de Información

A. En general

1. Toda cooperativa deberá desarrollar y mantener un programa de seguridad de información a acorde con la complejidad de sus operaciones y riesgos identificados.

B. Objetivos del Programa de Seguridad Informática

1. Las cooperativas deberán asegurase de que los programas de seguridad de información que desarrollen cumplan con los siguientes objetivos:
    (a) Garantizar la seguridad y confidencialidad de la información de los (las) socios(as) y clientes(as).
    (b) Proteger la cooperativa y la información de sus socios(as) y clientes(as) contra el riesgo de amenazas y peligros anticipados.
    (c) Proteger la cooperativas y sus socios(as) y clientes(as) contra accesos no autorizados o la divulgación y uso no autorizado de la información de estos(as).
    (d) Evitar la destrucción de documentos que deban preservarse permanentemente o antes de que finalice el término mínimo de conservación.
    (e) Procurar la disposición adecuada de la información de socios(as) y clientes(as).

C. Controles de Seguridad

1. Como parte del programa de seguridad de información, la cooperativa deberá establecer los controles de seguridad apropiados, basados en la complejidad de su operación, la información así como los riesgos identificados, entre otros factores. Estos deberán incorporar las políticas y procedimientos así como los controles técnicos y físicos necesarios para mitigar los riesgos identificados.

D. Planes de Respuesta a accesos no autorizados o uso no autorizado de información personal de socios(as) y clientes

1. Las cooperativas deberán contar con un plan escrito de respuesta a incidentes de accesos no autorizados o el uso de información de un(a) socio(a) o cliente(a) que pudiera ocasionarle inconvenientes o daños.
2. El plan de respuesta a incidentes debe especificar lo siguiente:
    (a) El propósito del plan.
    (b) Los procesos internos que se activarán en caso de surja un incidente.
    (c) Los roles, responsabilidades y niveles de autoridad en la toma de decisiones.
    (d) Manejo de la comunicación interna y externa.
    (e) El proceso para mitigar, contener y controlar incidentes de accesos no autorizados y /o uso de información de socios(as) y clientes(as).
    (f) Procesos para documentar y reportar los incidentes. Requisito de notificación a COSSEC. En situaciones en que el incidente constituya una violación a leyes federales, la cooperativa deberá radicar el Informe de Actividad Sospechosa o SAR por sus siglas en inglés, ante FinCEN.
    (g) Los parámetros y procedimientos para la notificación de socios(as) y clientes(as).
    (h) Análisis del incidente luego de que ocurra y la revisión de la ejecución del plan para hacer los ajustes necesarios a este.

E. Adiestramientos

1. La cooperativa deberá adiestrar a todos(as) sus directores(as), ejecutivos(as) y empleados(as) sobre la política de seguridad informática y el uso de la internet, las computadoras y los dispositivos electrónicos de la cooperativa. Asimismo, deberá proveer adiestramientos especializados a los (las) empleados(as), dirigidos a reconocer esquemas de fraude, robo de identidad y otros, para que puedan proteger la información privada de los (las) socios(as) y clientes(as) sus instituciones.
    (a) La cooperativa deberá retener evidencia que acredite la participación del personal indicado en los adiestramientos. Los documentos requeridos deberán mostrar el tema del adiestramiento, el nombre del recurso que lo

ofrece, la fecha en que se ofrece así como el nombre y firma de cada asistente. La información deberá estar disponible para inspección de la Corporación.

F. Pruebas y Auditorías Externas

1. El programa de seguridad de información deberá contar con pruebas periódicas de los procedimientos, controles técnicos y sistemas. Cada cooperativa deberá establecer en sus procedimientos la frecuencia con la que se realizarán las pruebas y auditorias, basado en sus análisis de riesgo.

G. Supervisión de Proveedores de Servicios

1. En los casos en que la cooperativa vaya a contratar servicios donde los (las) proveedores tengan acceso a la información de socios(as) y clientes(as) la cooperativa deberá:
    (a) Desplegar la debida diligencia en la selección del (de la) contratista.
    (b) Establecer la contratación por escrito.
    (c) Requerir en el contrato que el (la) contratista tome los pasos adecuados para proteger la seguridad y confidencialidad de la información de la cooperativa, sus socios(as) y clientes(as).
    (d) Supervisar el cumplimiento del (de la) contratista con los términos y condiciones del contrato firmado.

Artículo 10. Planes de Continuidad de Negocios y Recuperación de Desastres

Toda cooperativa deberá contar con un plan de continuidad de negocios y recuperación de desastres. Este deberá cubrir todas las contingencias tales como: interrupciones de utilidades, desastres naturales, ciberataques, errores humanos y pandemias locales y globales.

Al preparar el plan la cooperativa deberá velar que este aborde, en relación con los sistemas de información y tecnología, sin que se entienda una limitación, lo siguiente:

1. Que establezca las responsabilidades de cada empleado(a) y personal gerencial durante la emergencia así como la estructura de comunicaciones internas y externas en el manejo de la crisis.

2. La identificación los procesos críticos de sistemas y tecnología, y su prioridad para mantener el funcionamiento de la cooperativa.
3. La identificación de los sistemas, redes y tecnologías esenciales para hacer copias de seguridad de los datos y aplicaciones para permitir las operaciones de forma ininterrumpida.
4. Las situaciones de emergencia que puedan afectar a los proveedores de la cooperativa y los planes de contingencias de estos para mantener el funcionamiento de los procesos y sistemas críticos de la cooperativa.

Artículo 11. Notificación de Incidentes Catastróficos y Cibernéticos

A. Incidentes Catastróficos

1. Para fines de este Reglamento, un incidente catastrófico es cualquier desastre, natural o de otro tipo, que resulte en destrucción física o daño a la cooperativa, o que cause una interrupción en los servicios esenciales a sus socios(as), que se proyecta que dure más de dos (2) días hábiles consecutivos.
2. Toda cooperativa deberá notificar a la Corporación la ocurrencia de un incidente catastrófico que le cause daño y afecte sus sistemas de información dentro de las setenta y dos (72) horas de conocer del incidente.
3. Dentro de un tiempo razonable después de que ocurra un incidente catastrófico, la cooperativa se asegurará de que se prepare y archive un informe del incidente en su oficina principal. En la preparación de dicho informe, sin que se entienda como una limitación, la cooperativa deberá incluir información sobre:
    (a) la oficina donde ocurrió el incidente catastrófico;
    (b) descripción del incidente catastrófico;
    (c) cuándo tuvo lugar;
    (d) el monto de la pérdida, si la hubiere;
    (e) si alguna deficiencia operativa o mecánica podría haber contribuido al incidente catastrófico;
    (f) información sobre profesionales consultados e informes solicitados;
    (g) qué se ha hecho o se planea hacer para corregir la(s) deficiencia(s), y

(h) la(s) gestiones relacionadas a reclamación(es) al (a los) seguro(s) correspondientes;

(i) nombre, posición y firma de la persona que prepara el informe así como la fecha.

B. Incidentes Cibernéticos

Para fines de este Reglamento un **incidente cibernético** es un suceso que pone en peligro real o inminentemente, sin autoridad legal para ello, la integridad, confidencialidad o disponibilidad de información en un sistema de información o pone en peligro real o inminente, sin autoridad legal para ello, un sistema de información.

Por su parte, un **incidente cibernético reportable**, es uno material, que conlleva uno o más de los siguientes elementos:

- Una pérdida de confidencialidad, integridad o disponibilidad de una red o de los sistemas de información de los (las) socios(as) y clientes(as) que resulta del acceso no autorizado o la exposición de datos confidenciales, interrumpe los servicios esenciales a los (las) socios(as) y clientes(as) o tiene un impacto grave en la seguridad y la capacidad de recuperación de los sistemas y procesos operativos de la cooperativa.
- Interrupción de las operaciones comerciales, servicios esenciales a los (las) socios(as) y clientes(as) o del sistema de información para socios(as) y clientes(as) resultante de un ataque cibernético o de la explotación de alguna vulnerabilidad.
- Interrupción de las operaciones comerciales o acceso no autorizado a datos confidenciales facilitados o provocados por un compromiso de un proveedor de servicios, proveedor de servicios en la nube, proveedor de alojamiento de datos de terceros o un compromiso de la cadena de suministros.

1. Las cooperativas deberán notificar a la Corporación aquellos incidentes cibernéticos reportables tan pronto como sea posible, pero a más tardar setenta y dos (72) horas después de que ocurra.

    (a) La notificación a la Corporación deberá incluir la siguiente información:

i. Descripción del incidente cibernético reportable incluyendo las funciones que fueron, o razonablemente se sospecha que fueron, afectadas.
ii. El periodo durante el cual ocurrió el incidente cibernético reportable.
iii. Descripción de las vulnerabilidades explotadas en el incidente cibernético reportable y las técnicas usadas por los (las) perpetradores, si se conocen.
iv. Cualquier información que identifique a las personas que puedan ser responsables del incidente.
v. El impacto del incidente en las operaciones de la cooperativa.

2. En casos de incidentes de cibernéticos reportables constitutivos de delito, la cooperativa deberá radicar ante la Policía de Puerto Rico y/o la agencia de ley y orden federal que corresponda una querella sobre el incidente.
3. La cooperativa someterá cualquier otro informe relacionado con el incidente cibernético que requiera la Corporación.

C. Método de Notificación

Las notificaciones de incidentes catastróficos o cibernéticos reportables serán notificadas a la Corporación completando el formulario_____, el cual deberá enviarse al correo electrónico **incidentes@cossec.pr.gov**.

D. Confidencialidad

Todas las investigaciones, señalamientos, conclusiones y recomendaciones que haga o reciba la Corporación o sus agentes con relación a cualquier medida o mecanismo de seguridad informática de alguna cooperativa, se considerarán confidenciales.

Artículo 12. Gestión de Riesgo

Una gestión de riesgo adecuada es pieza integral de la administración responsable de una cooperativa de ahorro y crédito. Esta provee a la Junta de Directores(as) y gerencia de la

cooperativa la estructura para determinar: dónde se encuentran los riesgos, la cantidad de riesgo por exposición, los niveles máximos de riesgos que está dispuesta a asumir, la manera en que cambian los riesgos y los controles apropiados para limitar la exposición a estos. Cónsono con ello, las cooperativas deberán:

1. Crear, revisar e implementar políticas y procedimientos de gestión de riesgo tecnológico, compatibles con las mejores prácticas internacionales para el desarrollo de una gestión integral de riesgos.
2. Establecer los objetivos de riesgo estratégicos.
3. Definir los niveles de riesgos aceptables, en relación con los objetivos estratégicos.
4. Organizar un grupo de trabajo multidisciplinario para realizar anualmente la gestión de riesgos tecnológicos en la cooperativa. 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) de la cooperativa.
5. Rendir un informe a la Junta de Directores(as) de la cooperativa sobre el resultado de la gestión de riesgos tecnológicos anual, dentro de los cuarenta y cinco días (45) de concluida.

Artículo 13. Planificación Presupuestaria y Adquisición de Equipos, Programas y Tecnologías

1. El presupuesto anual de cada cooperativa deberá considerar las necesidades de adquisición, reparación y sustitución de equipos, programas y servicios tecnológicos.
2. La cooperativa deberá llevar a cabo el análisis y planificación de las necesidades de sistema, equipos o tecnología a corto, mediano y largo plazo; alineado a las necesidades estratégicas y operacionales de la institución, los productos y servicios que ofrece y el análisis de los riesgos que estos representan.

3. Toda compra deberá seguir el procedimiento para la adquisición de sistemas, programas, equipo y servicios tecnológicos aprobado por la Junta de Directores(as), el cual deberá ser compatible con las guías promulgadas por la Corporación.
4. Las cooperativas deberán mantener un inventario actualizado de los sistemas, programas, equipos y servicios tecnológicos adquiridos, sus garantías, licencias así como la asignación y disposición de estos.

Artículo 14. Seguros

El (La) Presidente(a) Ejecutivo(a) de toda cooperativa deberá procurar y mantener los seguros necesarios, aplicables a su actividad de tecnología, de acuerdo con sus operaciones y los riesgos identificados, de acuerdo con lo dispuesto en la Sección 2(a) (1-3) del Capítulo III del Reglamento Núm. 6758-2004. Asimismo, deberán requerir a sus proveedores de servicios los seguros apropiados, según el servicio contratado, para proteger los intereses de la institución.

Artículo 15. Cumplimiento con Leyes Estatales y Federales

Las cooperativas deberán asegurarse de que todas las operaciones que realizan a través de sus sistemas de información están en cumplimiento con las leyes estatales y federales aplicables.

Artículo 16. Término de Transición y Certificación de Cumplimiento Inicial

1. En el plazo de ocho (8) meses contados a partir de la fecha de efectividad del presente Reglamento, todas las cooperativas de ahorro y crédito deberán contar con las políticas y procedimientos requeridos en este Reglamento, debidamente aprobadas por sus Juntas de Directores(as).
2. Vencido el plazo, todas las cooperativas vendrán obligadas a someter ante la Corporación, una certificación de cumplimiento inicial acreditativa de ello.
3. Aquella cooperativa que incumpla con la adopción de las políticas y procedimientos de sistemas de información y tecnología dispuestos en este Reglamento y/o con presentar la certificación requerida, estará sujeta a una multa de hasta cien dólares

($100) por cada día de incumplimiento, a tenor con el Artículo 35 de la Ley Núm. 114-2001, además de cualesquiera otras sanciones que por ley o reglamento se puedan imponer. En estos casos, la Corporación seguirá el procedimiento establecido en el Capítulo II del Reglamento 9441-2023.

Artículo 17. Certificación Anual de Cumplimiento

1. Anualmente, el (la) Presidente(a) Ejecutivo(a) y el (la) Presidente(a) de la Junta de Directores(as) deberá certificar a la Corporación, en el formulario creado para ello, lo siguiente:
    (a) La fecha de la última revisión de las políticas y procedimientos de sistemas de información y tecnología.
    (b) Que el (la) Presidente(a) Ejecutivo(a) ha rendido los informes periódicos requeridos por los Artículos 7(B)(2) y 8(B)(2) de este Reglamento.
    (c) Que el presupuesto anual aprobado por la Junta de Directores(as) consideró las necesidades relacionadas a los sistemas de información y tecnología a corto, mediano y largo plazo.
    (d) Que la cooperativa realizó la gestión de riesgos tecnológicos anual y el (la) Presidente (a) Ejecutivo(a) presentó el informe anual a la Junta de Directores(as).
2. La certificación de cumplimiento deberá presentarse de forma electrónica (subirla a AITSA o email) _____, en o antes del _____.
3. La Corporación podrá imponer una multa de hasta cien dólares ($100) por cada día de incumplimiento, a tenor con el Artículo 35 de la Ley Núm. 114-2001, además de cualesquiera otras sanciones que por ley o reglamento se puedan imponer, a la Junta de Directores(as) y al (a la) Presidente(a) Ejecutivo(a) de toda cooperativa que incumpla esta disposición. En estos casos, la Corporación seguirá el procedimiento establecido en el Capítulo II del Reglamento 9441-2023.

Artículo 18. Guías, Formularios y Medios de Presentación Electrónica

La Corporación podrá emitir guías interpretativas sobre el contenido de este Reglamento, modificar los formularios, así como el método electrónico de presentación de las certificaciones e informes requeridos en él. Toda guía o modificación deberá contar con la aprobación de la Junta de Directores de la Corporación y notificarse a las cooperativas de ahorro y crédito mediante carta circular.

Artículo 19. Disposiciones Reglamentarias Incompatibles

Todas las disposiciones contenidas en cualquiera de los reglamentos vigentes de la Corporación deberán estar en conformidad con este Reglamento. De resultar incompatibles prevalecerán las disposiciones de este Reglamento.

Artículo 20. Separabilidad

Si cualquier artículo, frase, párrafo o cláusula de este Reglamento fuera declarada nula o inconstitucional por un tribunal con jurisdicción, dicho pronunciamiento no afectará ni invalidará el resto de sus disposiciones.

Artículo 21. Vigencia

Este Reglamento entrará en vigor a los treinta (30) días de su radicación en el Departamento de Estado, de conformidad con las disposiciones de la Ley Núm. 38-2017.

Aprobado en San Juan, Puerto Rico a ____ de_____de 2025.

Dra. Liza I Alfaro Mercado	**Miguel Colón Robles**, **CPA**
Presidenta Junta de Directores	Secretario Junta de Directores

Mabel Jiménez Miranda, MBA
Presidenta Ejecutiva