SUPERINTENDENCIA DE LA ECONOMÍA SOLIDARIA
Instrucciones sobre seguridad y calidad de la información para la prestación de los servicios financieros

Circular KRM No. 017 - 22/ 25 de julio, 2022

El pasado 05 de enero del 2022, la Superintendencia de la Economía Solidaria, expidió la Circular Externa No. 36, en la que se modifica el numeral 4.3.4. del Título IV de la Circular Básica Contable y Financiera, Adiciona información en el anexo 2 "Instrucciones sobre seguridad y calidad de la información para la prestación de los servicios financieros" y establece un cronograma para las instrucciones del anexo 2 del Capítulo IV, del Título IV de la Circular Básica Contable y Financiera.

De conformidad con las precisiones anteriormente señaladas, nos permitimos remitir a ustedes esta Circular práctica que les permitirá conocer las modificaciones de mayor impacto efectuadas.

Nuevas instrucciones:

- Teniendo en cuenta el numeral 4.3.4 "Administración de la seguridad de la información" se determina que las entidades, en relación con su estructura tecnológica, tamaño, manejo de información deben establecer lo siguiente:

  - Definir la política de seguridad de la información.
  - Identificar los activos de información.
  - Identificar los riesgos de seguridad de la información.
  - Definir, implementar y probar un plan de gestión de riesgos de seguridad de la información.

- Acorde con el numeral en mención, en el anexo 2 se describen las instrucciones sobre la seguridad y calidad de la información para la prestación de servicios financieros.

- El Anexo 2 del Capítulo IV, del Título IV de la Circular Básica Contable y Financiera, se determina que las entidades deben determinar una política de buenas prácticas en materia de seguridad de la información.

- El Anexo debe ser aplicado por las cooperativas especializadas en ahorro y crédito y multiactivas e integrales con sección de ahorro y crédito vigiladas y podrá ser adoptado por las demás organizaciones solidarias supervisadas, acorde con ciertas características.

- Los elementos claves de la infraestructura de seguridad de la información, son:

  - Gobierno de la Seguridad de la Información.
  - Estrategia de Seguridad
  - Roles y Responsabilidades
  - Riesgos de Seguridad de la Información
  - Sistema de Seguridad de la Información
  - Información Documentada

- De acuerdo con los roles y responsabilidades de los funcionarios, es relevante que la organización estipule y defina claramente las funciones asignadas para cada rol asociados con el riesgo y la seguridad de la información.

- Es conveniente que las entidades establezcan un programa de concientización/educación, concerniente a los directivos y trabajadores; con la finalidad de proveer la información, implementar un proceso disciplinario para incidentes y contar con promociones, cambios de roles, entre otros.

- Acorde con los requerimientos de medios tecnológicos y seguridad de la información, se determina que las cooperativas deben cumplir con la disposición de Hardware, Software y equipos de Telecomunicaciones que minimicen las amenazas del sector.

- Los requerimientos de medios tecnológicos dentro de los requisitos deben gestionar la seguridad de la información bajo el Modelo de Seguridad y Privacidad de la información con sus tarjetahabientes con los estándares de Seguridad de Datos de la Industria de Tarjetas de Pago.

- Los controles criptográficos como los sitios web creados para el procesamiento de la información del negocio, deben ser sitios seguros y utilizar certificados digitales emitidos por un ente certificador legalmente constituido en el país. Así como, Las comunicaciones con terceras partes para la prestación de servicios del negocio y deben utilizar mecanismos de encriptación fuertes.

- Las entidades deben manejar herramientas para los controles criptográficos que cuenten con algoritmos de encriptación en el almacenamiento de la información sensible o crítica en archivos, así como las claves de usuarios a los sistemas de información.

- La protección contra códigos móviles o maliciosos, deben instalar un antivirus para que toda la información descargada sea verificada, es importante mencionar que, se debe restringir el intercambio de medios removibles en la entidad y restringir el acceso de personas ajenas.

- Como buena práctica para el intercambio de información, los empleados deben colocar clave a los archivos sensibles, evitar el envío de documentación sin la debida autorización y/o acuerdo de confidencialidad.

- La entidad para fortalecer su seguridad y calidad de la información, deberán respaldar toda la información que se encuentra en los servidores y equipos de cómputo por medio de: copias de seguridad, medios físicos y/o magnéticos que aseguren el nivel de datos operativos.

- Para los controles de acceso de las instalaciones y áreas críticas, la organización establece los lineamientos para prevenir y preservar la seguridad, así como las restricciones que adopten en el uso de aplicaciones por medio de software, entre otros aspectos.

- En el caso de Teletrabajo, se determina que el acceso remoto de los servidores deber ser autorizado por la organización y las áreas fuera de la sede principal deben cumplir con todas las políticas y controles del sistema de seguridad definido.

- Los inventarios de activos de las organizaciones deberán contar con lo siguiente:

  - Datos digitales
  - Información impresa
  - Software
  - Infraestructura
  - Servicios de información y proveedores de servicios
  - Seguridad física
  - Relaciones comerciales
  - Responsables de los activos.

- En caso de prestar servicios a través de los Cajeros Automáticos, las organizaciones deben verificar y cumplir con los requerimientos establecidos en el Anexo 2.

- Las entidades solidarias que manejen el sistema POS que permite procesar sus transacciones de cara al asociado, deben contar con lectura de tarjeta, establecer procedimientos que le permitan identificar los responsables de los datafonos y velar por la información confidencial del asociado.

- Los centros de Atención Telefónica deben estar regulados por lo establecido con la Ley 1581 del 2012 y cumplir con los requisitos mínimos dando cumplimiento con el tratamiento de datos personales.

- En el caso de Transacciones por Internet, implementar controles descriptivos en los algoritmos y protocolos necesarios, realizar pruebas de vulnerabilidad como mínimo dos (2) veces al año, reducir la posibilidad de información de las transacciones realizadas, informar al asociado el inicio de la sesión, la fecha y hora del último ingreso.

- Los análisis de vulnerabilidades informáticas deben estar basado en un hardware de propósito especifico separado e independiente de cualquier dispositivo, generar un informe consolidado con los planes de acción y vulnerabilidades identificadas.

- Las instalaciones y suministros deben proteger los equipos contra las fallas de energía y otras interrupciones con un sistema de alimentación interrumpida para proporcionar una potencia

adecuada, se debe establecer un plan de mantenimiento y contar con una red de suministro eléctrico.

- La organización debe implementar una política para establecer controles con el propósito de verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.

- La Superintendencia de Sociedades establece el siguiente cronograma para implementar las instrucciones de la circular en mención:

CRONOGRAMA DE IMPLEMENTACIÓN ANEXO 2 INSTRUCIONES SOBRE SEGURIDAD Y CALIDAD DE LA INFORMACION PARA LA PRESTACIÓN DE LOS SERVICIOS FINANCIEROS		
Fases / Actividades	**Plazo máximo implementación**	**Fecha aplicación**
FASE I: Consideraciones generales, ámbito de aplicación, definiciones **Numerales 1, 2, 3**	28-feb-22	1-mar-22
FASE II: Elementos claves de la infraestructura de seguridad de la información, responsabilidades y recursos **Numerales 4, 5**	30-abril-22	1-may-22
FASE III: Requerimientos de medios tecnológicos y de seguridad de la información **Numeral 6**	30-jun-22	1-jul-22

Cronograma de Implementación de la Circular 36 del 2022.

Cordialmente,

COMUNICACIONES
Kreston RM S.A.
Kreston Colombia
Miembros de Kreston Global