# MANUAL DE POLÍTICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA

SEPTIEMBRE 2015

*Cooperativa de Ahorro y Crédito Integral, San Juan Comalapa R.L.*

## ARTÍCULO 1°. INTRODUCCIÓN:

La base para que cualquier organización pueda operar de una forma confiable en materia de Seguridad Informática comienza con la definición de las políticas y estándares. La Seguridad Informática, es una función en la que se deben evaluar y administrar los riesgos, basándose en políticas y estándares que cubran las necesidades de COPECOM R.L. en materia de seguridad informática que son herramientas administrativas para que los colaboradores conozcan la importancia y sensibilidad de la información, así como la optimización en el uso de los recursos tecnológicos que permiten que COPECOM R.L. crezca y mantenga su competitividad.

Así mismo, la razón de ser de la presente política se enmarca en las regulaciones legales y técnicas, la estandarización de procesos, que permite la identificación y aplicación de mejores prácticas y ofrece ser una guía al personal de la Cooperativa.

## ARTÍCULO 2°. JUSTIFICACIÓN

COPECOM R.L., cuenta con recursos informáticos actualizados que brindan la oportunidad de minimizar los esfuerzos para la búsqueda de la excelencia y calidad en el procesamiento de datos, logrando la eficiencia y eficacia de los procesos gerenciales, administrativos y operativos. Por tanto, la administración de los recursos informáticos necesita ser respaldada mediante una política de seguridad informática; esto, con el afán de estandarizar y resguardar las acciones que se toman en cuanto a la generación, divulgación y almacenamiento de la información, así como el manejo de equipo tecnológico, la adquisición y adecuada utilización del software y hardware.

La aplicación de la presente política de seguridad informática ayudará a fortalecer la eficiencia de los sistemas de información y de ésta forma garantizar la integridad, confidencialidad y alta disponibilidad de la información y los servicios. Así como la aplicación de procesos adecuados para la optimización de los recursos.

## ARTÍCULO 3°. OBJETIVO GENERAL:

Establecer medidas técnicas y de organización de las tecnologías de información, para asegurar la integridad, confidencialidad y confiabilidad de la información generada por COPECOM R.L. y minimizar los riesgos en el uso de las tecnologías de información y/o transacción con las que se cuenta y se realizan.

## ARTÍCULO 4°. OBJETIVOS ESPECÍFICOS:

1. Establecer lineamientos administrativos e informáticos que sirvan como parámetros de referencia para la institución en la administración, protección y disponibilidad de la información y recursos tecnológicos.

2. Establecer los canales efectivos de comunicación entre las Gerencias, Jefes de Agencia o Área, Colaboradores y el área de tecnología para la protección de los activos informáticos con los que cuenta COPECOM R.L.

3. Proveer las herramientas de hardware y/o software para la administración, protección y disponibilidad de la información y de los servicios que presta COPECOM R.L.

## ARTÍCULO 5°. ALCANCE:

La presente política debe ser de observancia y aplicación por parte de todo el personal de la Cooperativa, puesto que fue elaborado de acuerdo al análisis de riesgos y de vulnerabilidades a las que pueda estar sujeta COPECOM R.L.

Así mismo, tiene por objeto estandarizar los procesos que atañen al Departamento de Sistemas y contribuir al desarrollo informático de las diferentes áreas de la Cooperativa.

## ARTÍCULO 6°. RESPONSABILIDAD DE LA SUPERVICIÓN, REVISIÓN Y AUTORIZACIÓN DE LAS POLÍTICAS:

Es responsabilidad del Administrador de Sistemas, desarrollar, someter a revisión y divulgar en adición a los demás medios de difusión (intranet, email, sitio web oficial, etc.) los procedimientos, normas y demás contenido de la presente Política. Asimismo, es responsabilidad del Departamento de Sistemas/Informática capacitar a los colaboradores en lo relacionado con los Procedimientos de Seguridad Informática.

La autorización de las políticas propuestas por el departamento de sistemas deberán ser aprobadas por el Gerente General de la Cooperativa quien hará del conocimiento all Consejo de Administración y Comisión de Vigilancia si lo considera necesario.

# ARTÍCULO 7°. CAPITULO I: NORMAS DE SEGURIDAD INFORMÁTICA

La presente Política está basada en las normas internacionales ISO (Organización Internacional para la Estandarización) y se recogen las normas o estándares de seguridad establecidas tanto por la ISO 27000 y la IEC (Comisión Electrotécnica Internacional) aplicables a la Cooperativa.

Cabe mencionar que las normas ISO/IEC 27000 son un conjunto de estándares de seguridad (desarrollados o en fase de desarrollo) que proporcionan un marco para la gestión de la seguridad.

Contiene las mejores prácticas recomendadas en seguridad de la información para desarrollar, implementar y mantener especificaciones para los sistemas de gestión de la Seguridad de la Información, utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

**Artículo 8°.** Por lo que nuestras normas de seguridad informática se basan en cuatro pilares fundamentales:

- **Confidencialidad**: la información de la Cooperativa no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados por el órgano competente.
- **Integridad**: mantenimiento de la exactitud y completitud de la información y sus métodos de captura o vaciado.
- **Disponibilidad**: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos o procesos autorizados cuando lo requieran.
- **Responsabilidad**: en el uso de los recursos tecnológicos, en la generación de la información, resguardo y uso de la información.

Por tanto, debe considerarse que se tendrá acceso a la información según el perfil autorizado para cada colaborador.

**Artículo 9°.** Así mismo, debe restringirse a las personas que ocupen pasantillas, estudiantes practicantes, ex empleados, entre otros, el acceso a los diferentes sistemas del core financiero y a la base de datos de la Cooperativa, tal y como lo detalla el capítulo VII. Prohibiciones Generales.

# ARTÍCULO 10°. CAPITLUO II: SEGURIDAD FÍSICA, LÓGICA Y ADMINISTRATIVA:

En este capítulo se establece el marco formal de seguridad que debe sustentar la Cooperativa y de ser necesario se debe incluir los servicios o contrataciones externas a la infraestructura de seguridad, Integrando el recurso humano con la tecnología, denotando responsabilidades y actividades complementarias como respuesta ante situaciones anómalas a la seguridad.

## 2.1 SEGURIDAD FÍSICA:

**Artículo 11°.** La seguridad Física es responsabilidad del Departamento de Sistemas en conjunto a la Gerencia General, quienes deben velar para que los activos tecnológicos físicos tengan el resguardo y uso adecuado.

Por tanto:

**Artículo 12°.** Todos los equipos de la Cooperativa que tengan integrado conectores/periféricos/puertos (USB, CD, Dispositivos Móviles, Disco Duro interno y externo) deben estar deshabilitados. Con el objetivo de evitar salida de información no autorizada, ataques de virus en los equipos y servidores y evitar la carga de archivos ajenos a la labor.

**Artículo 13°.** Los equipos autorizados para el uso de dispositivos de almacenamiento externos deben ser supervisados por el área de sistemas, para la entrada y salida de información.

**Artículo 14°.** Debe contarse con una autorización de las Gerencias y/o el Departamento de Sistemas de la salida de los equipos que forman parte del activo de la Cooperativa, tales como: USB's, Discos Duro internos o externos, CD's, Notebooks, Impresoras, CPU's, monitores, teclados, mouses, UPS's, swiches, cables, servidores y otros que no se contemplen en el presente documento bajo criterio de la Gerencia General y Administrador de Sistemas.

**Artículo 15°.** Cada uno de los equipos y/o recursos tecnológicos que representan un Activo para la Cooperativa, deberá estar bajo la responsabilidad de una persona según el área o departamento que corresponda.

**Artículo 16°.** El cableado de red, se instalará físicamente separado de cualquier otro tipo de cableado, llámese a estos de corriente o energía eléctrica, para evitar interferencias.

**Artículo 17°.** Los servidores, sin importar al grupo al que estos pertenezcan, con problemas de hardware, deberán ser reparados localmente, de no cumplirse lo anterior, deberán ser retirados sus medios de almacenamiento.

**Artículo 18°.** Los equipos o activos críticos de información y de proceso, deberán ubicarse en áreas aisladas y seguras, protegidas con un nivel de seguridad verificable y manejable por las personas responsables por esos activos, quienes deberán poseer su debida identificación.

**Artículo 19°.** No se podrán conectar a los equipos de la Cooperativa los dispositivos no autorizados por la Gerencia y/o administrador de sistemas, siendo estos: USB´s, CD´s, teléfonos móviles, cámaras fotográficas y otras bajo el criterio del Administrador de Sistemas.

**Artículo 20°.** Los siguientes equipos deberán contar con el UPS respectivo para garantizar el funcionamiento y resguardo de la información: PC´s, Swiches de Red, Servidores, CCTV, Planta Telefónica, Balanceadores de carga, Routers, SDA, etc.

## 2.2 SEGURIDAD LÓGICA:

**Artículo 21°.** Diariamente se realizan backup´s automáticos a la base de datos según los mecanismos establecidos y se realizan en el horario determinado por Fenacoac.

**Artículo 22°.** Todos los equipos deben contar con usuario y contraseña para acceder respectivamente.

**Artículo 23°.** Los usuarios deberán abstenerse de divulgar o compartir sus datos de acceso a los programas del core financiero y sesiones de Windows a excepción del Administrador de Sistemas.

**Artículo 24°.** Todos los archivos que viajen por correo y que contengan información sensible deberán estar comprimidos con contraseña de uso interno como medida de seguridad de información.

**Artículo 25°.** Se debe realizar una revisión periódica de virus a todos los equipos, incluyendo los siguientes procesos: búsqueda de virus y actualización de la base de datos.

**Artículo 26°.** Todo colaborador que tenga bajo su responsabilidad equipos o recursos tecnológicos, debe contar con una ficha de responsabilidad con los datos siguientes: nombre, fecha de la verificación, código del activo, firma del colaborador y Administrador de Sistemas.

**Artículo 27°.** No podrá instalarse software no autorizado por el Administrador de Sistemas en cada uno de los equipos.

**Artículo 28°.** Todos los equipos deberán tener acceso restringido a las configuraciones internas de la PC.

**Artículo 29°.** Para el resguardo de los diferentes equipos y recursos tecnológicos, se deberá contar con un sistema de circuito cerrado de vigilancia, así como un sistema de alarma.

## 2.3 SEGURIDAD ADMINISTRATIVA/LEGAL:

**Artículo 30°.** Todos los equipos deberán contar con el licenciamiento correspondiente al sistema operativo instalado.

**Artículo 31°.** Todos los equipos que tengan instalado Microsoft Office deberá contar con el licenciamiento correspondiente, independientemente de su versión.

**Artículo 32°.** El Antivirus instalado en los equipos debe contar con el licenciamiento respectivo.

**Artículo 33°.** Se debe realizar por lo menos una vez al año un inventario de los equipos y recursos tecnológicos que represente un Activo para la Cooperativa.

**Artículo 34°.** Se entregará al contratado, toda la documentación necesaria para ejercer sus labores dentro de la institución, en el momento en que se dé por establecido su contrato laboral, dicho contrató debe hacer referencia a la responsabilidad en el uso y

manejo de la información, así como de los recursos y equipos tecnológicos según lo establece el Código de Trabajo.

**Artículo 35°.** La información procesada, manipulada o almacenada por el empleado es propiedad exclusiva de la Cooperativa.

**Artículo 36°.** Deberá restringirse el acceso a páginas web no autorizadas, el contenido del listado estará bajo la responsabilidad del Administrador de Sistemas y Gerencia de IDT del sistema Micoope.

**Artículo 37°.** Se deberán otorgar los accesos respectivos a los usuarios que cumplan con lo requerido en el capítulo IV. Administración de los Accesos.

**Artículo 38°.** Se deberán dar de baja los accesos respectivos de los colaboradores que ya no trabajen para la Cooperativa, se lo establece el capítulo IV. Administración de los Accesos.

## ARTÍCULO 39°. CAPÍTULO III: RECURSOS DE SOFTWARE, HARDWARE Y RED

Para la utilización óptima de los recursos de software y hardware, deben considerarse las siguientes disposiciones:

**Artículo 40°.** Cada empleado es responsable del cuidado y el buen uso del equipo informático que la Cooperativa le ha asignado para realizar sus actividades.

**Artículo 41°.** El equipo informático podrá ser utilizado fuera de las instalaciones con la autorización expresa de las Gerencias o del Administrador de Sistemas.

**Artículo 42°.** El personal en general no podrá utilizar el correo electrónico para enviar archivos o contenidos que representen riesgo de virus para los equipos.

**Artículo 43°.** El departamento de sistemas autorizará al personal sobre el software permitido en los equipos informáticos.

**Artículo 44°.** El departamento de sistemas es responsable del mantenimiento preventivo y correctivo, continuo y apropiado de los equipos informáticos.

**Artículo 45°.** El departamento de sistemas y las Gerencias podrán autorizar al personal para utilizar los recursos informáticos (computadoras, internet, impresiones, etc.) en actividades ajenas a las funciones y atribuciones de los colaboradores.

**Artículo 46°.** El uso inapropiado de los recursos informáticos de la institución es motivo de sanciones que, dependiendo de la gravedad, se aplicarán las contempladas en el Reglamento Interno de Trabajo.

**Artículo 47°.** El personal que necesite compartir los recursos y la información almacenada en sus computadoras, deberá contar con la autorización del departamento de sistemas o la Gerencias de la Cooperativa.

**Artículo 48°.** Las plataformas de trabajo autorizadas son:

- ✓ Bankworks
- ✓ Sistema de Pagos a Terceros (Deocsa, Telgua, Claro)

- ✓ Sistema de Pagos de Tarjeta de Crédito (Transtel)
- ✓ Crescor
- ✓ Administrador de ATM (Servitech)
- ✓ Administrador de Tarjetas (Servitech)
- ✓ Multimain (Gestiones de Tarjetas de Crédito)
- ✓ Contadores (contador de billetes Servitech)
- ✓ Micoope en Línea
- ✓ Seguros Columna (Acsel)
- ✓ Coopeseguros

**Artículo 49°.** Es obligación de cada colaborador apagar el equipo a su cargo antes y después de cada jornada laboral.

**Artículo 50°.** Cualquier tipo de falla en los equipos informáticos debe reportarse inmediatamente al departamento de sistemas, para evitar la pérdida de la información, la pérdida del equipo y la indisponibilidad de los servicios.

**Artículo 51°.** Los equipos deben marcarse para su identificación y control de inventario. Para dicho inventario, el departamento de contabilidad deberá asignar el código respectivo del activo y la asignación de la hoja de responsabilidad a cada colaborador.

**Artículo 52°.** El acceso a cada PC debe ser única y exclusivamente del colaborador responsable a excepción del Administrador de Sistemas o quien autorice.

**Artículo 53°.** La instalación o reubicación de los equipos es responsabilidad exclusiva del departamento de sistemas o a quienes autorice el Administrador de Sistemas.

**Artículo 54°.** La pérdida o robo de cualquier equipo, ya sea parcial o total, debe reportarse inmediatamente al departamento de sistemas.

**Artículo 55°.** Solamente las Gerencias o el Administrador de Sistemas deberán autorizar a personas ajenas para instalaciones o reparaciones de los equipos o recursos informáticos.

**Artículo 56°.** El manejador de correo electrónico permitido es Microsoft Office.

**Artículo 57°.** La dirección de correo electrónico de cada colaborador debe mantener las siguientes condiciones:

- Debe conformarse por el primer nombre y primer apellido en concatenación con el dominio en vigencia de la Cooperativa.
- La configuración debe ser por el departamento de sistemas.
- La configuración debe ser de conocimiento exclusivo y único del departamento de sistemas.
- Para el caso de correos que pertenezca a departamentos o áreas que no sean personas físicas, deberá identificarse al colaborador responsable del uso.

**Artículo 58°.** Según el rol o el perfil asignado al colaborador, se le asignará al PC de trabajo una de las IP's de la siguiente clasificación:

- Rango restringido: IP's 0 - 99
- Rango moderado: IP's 100 – 199
- Rango libre: IP's 200 – 244

**Artículo 59°.** Utilitarios de oficinas permitidos:

- Microsoft Office
- Libre Office

**Artículo 60°.** Navegadores de internet permitidos:

- Internet Explorer
- Google Chrome
- Mozilla

## ARTÍCULO 61°. CAPÍTULO IV: ADMINISTRACIÓN DE LOS ACCESOS

Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

El administrador de sistemas definirá procedimientos para la administración de usuarios, creación, cambio de contraseñas, accesos, altas, bajas y bloqueos; considerando las siguientes disposiciones:

**Artículo 62°.** Todos los colaboradores que tenga autorización de acceso a los diferentes sistemas autorizados, deberán hacerlo mediante un usuario y contraseña asignados.

**Artículo 63°.** El personal que no pertenezca a la Cooperativa, siendo estos: estudiantes practicantes, pasantillas, o personas que no pertenezcan al sistema Micoope, no podrán hacer uso de los diferentes sistemas autorizados.

**Artículo 64°.** Deben definirse roles de acceso según el puesto y atribuciones del colaborador y el acceso a sistemas o información que no le competan, deberá ser autorizado por el jefe inmediato.

**Artículo 65°.** Los identificadores para usuarios temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.

**Artículo 66°.** Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.

**Artículo 67°.** Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.

**Artículo 68°.** Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.

**Artículo 69°.** Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al

cambio de su contraseña e informar a su jefe inmediato y éste reportar al responsable del departamento de sistemas.

**Artículo 70°.** El Usuario debe utilizar una contraseña compuesta por un mínimo de ocho caracteres constituida por una combinación de caracteres alfabéticos y numéricos.

**Artículo 71°.** En caso que el sistema no lo solicite automáticamente, el usuario debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.

**Artículo 72°.** En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada 30 días. En caso contrario, se le podrá denegar el acceso y se deberá contactar con el jefe inmediato para solicitar al administrador de la red una nueva clave.

**Artículo 73°.** Utilizar el menor número de listados que contengan datos de carácter personal y mantener los mismos en lugar seguro y fuera del alcance de terceros.

**Artículo 74°.** Cuando entre en posesión de datos de carácter personal, se entiende que dicha posesión es estrictamente temporal, y debe devolver los soportes que contienen los datos inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos.

**Artículo 75°.** Los usuarios deben notificar a su jefe inmediato cualquier incidencia que detecten que afecte o pueda afectar a la seguridad de los datos de carácter personal: pérdida de listados y/o disquetes, sospechas de uso indebido del acceso autorizado por otras personas, recuperación de datos.

**Artículo 76°.** Los usuarios únicamente introducirán datos identificativos y direcciones o teléfonos de personas en las agendas de contactos de las herramientas ofimáticas (por ejemplo, en Outlook).

**Artículo 77°.** Si una contraseña de usuario se olvida o se necesita ingresar a alguna computadora y se desconoce la contraseña de acceso, solamente se podrá efectuar este cambio con la autorización del interesado, del Jefe del departamento o del administrador de sistemas.

**Artículo 78°.** No se instalará correo electrónico a ningún usuario sin la autorización por escrito del jefe inmediato del colaborador o jefatura superior.

**Artículo 79°.** No se dará acceso a internet libre a ningún usuario sin la autorización por escrito del jefe inmediato o jefe superior.

**Artículo 80°.** La utilización del internet está restringida a usos relacionados directamente con las actividades de la Cooperativa, por lo que se eliminará la conexión a las PC's de trabajo que por su naturaleza no requieran de este servicio. Los jefes inmediatos serán responsables de la autorización de los usuarios que cuenten o requieran este servicio.

**Artículo 81°.** Queda prohibida la descarga de música por medio de internet ya que esto degrada considerablemente la velocidad y los servicios dentro de la red de información y por ende el servicio que se presta.

**Artículo 82°.** Cuando un usuario se retira definitivamente de la institución o cambia de puesto, el Jefe inmediato debe reportarlo al Departamento de Sistemas utilizando el proceso definido de "Altas, Bajas y Cambios" con 1 día de anticipación, para que se eliminen o cambien sus niveles de acceso y seguridad o para realizar back'up de archivos.

## ARTÍCULO 83°. CAPÍTULO V: ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SOFTWARE Y HARDWARE

Para la adquisición de hardware y software se observarán las siguientes disposiciones:

**Artículo 84°.** Toda adquisición de tecnología informática se efectuará se basará en la política o manual de compras de la Cooperativa, autorizado por el Consejo de Administración.

**Artículo 85°.** La Administración de Informática, al planear las operaciones relativas a la adquisición de Bienes informáticos, establecerá prioridades y en su selección deberá tomar en cuenta: estudio técnico, precio, calidad, experiencia, desarrollo tecnológico, estándares y capacidad, entendiéndose por:

**Precio**

Costo inicial, costo de mantenimiento y consumibles por el período estimado de uso de los equipos;

**Calidad**

Parámetro cualitativo que especifica las características técnicas de los recursos informáticos.

**Experiencia**

Presencia en el mercado nacional e internacional, estructura de servicio, la confiabilidad de los bienes y certificados de calidad con los que se cuente.

**Desarrollo Tecnológico**

Se deberá analizar su grado de obsolescencia, su nivel tecnológico con respecto a la oferta existente y su permanencia en el mercado.

**Estándares**

Toda adquisición se basa en los estándares, es decir la arquitectura de grupo empresarial establecida previamente por el departamento de sistemas o la Cooperativa. Esta arquitectura tiene una permanencia mínima de dos a cinco años.

**Capacidades**

Se deberá analizar si satisface la demanda actual con un margen de holgura y capacidad de crecimiento para soportar la carga de trabajo del área.

**Artículo 86°.** El equipo que se desee adquirir, deberá estar dentro de las listas de ventas vigentes de los fabricantes y/o distribuidores del mismo y dentro de los estándares sugeridas por el departamento de sistemas de la Cooperativa.

**Artículo 87°.** Los equipos complementarios deberán tener una garantía mínima de un año y deberán contar con el servicio técnico correspondiente en el país. Deberán ser equipos integrados de fábrica o ensamblados con componentes previamente evaluados el departamento de sistemas.

**Artículo 88°.** La marca de los equipos o componentes deberá contar con presencia y permanencia demostrada en el mercado nacional e internacional, así como con asistencia técnica y refaccionaria local.

**Artículo 89°.** Los dispositivos de almacenamiento, así como las interfaces de entrada / salida, deberán estar acordes con la tecnología de punta vigente, tanto en velocidad de transferencia de datos, como en procesamiento.

**Artículo 90°.** Las impresoras deberán apegarse a los estándares de Hardware y Software vigentes en el mercado y corroborando que los suministros (cintas, papel, tóner, etc.) se consigan fácilmente en el mercado y no estén sujetas a un solo proveedor.

**Artículo 91°.** Conjuntamente con los equipos, se deberá adquirir el equipo complementario adecuado para su correcto funcionamiento de acuerdo con las especificaciones de los fabricantes.

**Artículo 92°.** Los equipos adquiridos deben contar, de preferencia con asistencia técnica durante la instalación de los mismos.

**Artículo 93°.** En lo que se refiere a los servidores, equipos de comunicaciones, concentradores de medios (HUBS) y otros equipos que se justifiquen por ser de operación crítica y/o de alto costo, deben de contar con un programa de mantenimiento preventivo y correctivo que incluya el suministro de refacciones al vencer su período de garantía.

**Artículo 94°.** En lo que se refiere a los computadores denominados personales, al vencer su garantía por adquisición, deben de contar por lo menos con un programa de servicio de mantenimiento correctivo que incluya el suministro de refacciones.

**Artículo 95°.** Todo proyecto de adquisición de bienes de informática, debe sujetarse al análisis, aprobación y autorización del Departamento de Sistemas.

**Artículo 96°.** Todo proyecto de desarrollo de software para uso interno de la Cooperativa deberá ser aprobado y evaluado previamente por el departamento de sistemas y hará del conocimiento a las Gerencias y de ser necesario al personal. Para la evaluación deberá considerarse los estándares vigentes de seguridad en desarrollo de software.

**Artículo 97°.** En la adquisición de Equipo de cómputo se deberá incluir el Software vigente precargado con su licencia correspondiente considerando las disposiciones del artículo siguiente.

**Artículo 98°.** Para la adquisición de Software base y utilitarios, el departamento de sistemas dará a conocer periódicamente las tendencias con tecnología de punta vigente (Sistemas Operativos, Antivirus, Microsoft Office, etc.)

## ARTÍCULO 99°. CAPÍTULO VI: CONTINGENCIA

El departamento de sistemas creará para los departamentos un plan de contingencias informáticas que incluya al menos los siguientes puntos:

**Artículo 100°.** Continuar con la operación del área con procedimientos informáticos alternos, es decir, manteniendo el servicio a los asociados.

**Artículo 101°.** Tener los respaldos de información en un lugar seguro, fuera del lugar en el que se encuentran los equipos.

**Artículo 102°.** Tener el apoyo por medios magnéticos o en forma documental, de las operaciones necesarias para reconstruir los archivos dañados.

**Artículo 103°.** Contar con un instructivo de operación para la detección de posibles fallas, para que toda acción correctiva se efectúe con la mínima degradación posible de los datos.

**Artículo 104°.** Contar con un directorio del personal interno y del personal externo de soporte, al cual se pueda recurrir en el momento en que se detecte cualquier anomalía.

**Artículo 105°.** Ejecutar pruebas de la funcionalidad del plan.

**Artículo 106°.** Mantener revisiones del plan a fin de efectuar las actualizaciones respectivas.

## ARTÍCULO 107°. CAPÍTULO VII: PROHIBICIONES GENERALES

Con el fin de evitar que nuestros recursos tanto tecnológicos y datos de información sean vulnerables, deben cumplirse las siguientes prohibiciones:

**Artículo 108°.** Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los Recursos Informáticos. El departamento de sistemas, tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los Sistemas de cualquier elemento destinado a destruir o corromper los datos informáticos.

**Artículo 109°.** Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos propiedad de la Cooperativa.

**Artículo 110°.** Albergar datos de carácter personal en las unidades locales de disco de los computadores de trabajo.

**Artículo 111°.** Cualquier fichero introducido en la red corporativa o en el puesto de trabajo del usuario a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual y control de virus.

**Artículo 112°.** Todo el personal que accede a los Sistemas de Información de la Cooperativa debe utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de utilización.

**Artículo 113°.** Todo el personal tiene prohibido instalar copias ilegales de cualquier programa, incluidos los estandarizados.

**Artículo 114°.** También tiene prohibido borrar cualquiera de los programas instalados legalmente.

**Artículo 115°.** Ninguna persona debe conectar a ninguno de los recursos, ningún tipo de equipo de comunicaciones (Ej. Módem, celulares, etc.) que posibilite la conexión a la Red Corporativa.

**Artículo 116°.** Ninguna persona debe conectarse a la Red Corporativa a través de otros medios que no sean los definidos.

**Artículo 117°.** Ninguna persona debe intentar obtener otros derechos o accesos distintos a aquellos que les hayan sido asignados, para ello deberá solicitarlo mediante el proceso definido.

**Artículo 118°.** Ninguna persona debe intentar distorsionar o falsear los registros en bitácoras de los Sistemas de Información.

**Artículo 119°.** Ninguna persona debe intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos.

**Artículo 120°.** Ninguna persona debe poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros Usuarios, ni dañar o alterar los Recursos Informáticos.

**Artículo 121°.** La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todos los colaboradores tienen las mismas responsabilidades en cuanto al uso de Internet.

**Artículo 122°.** El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello, es decir, por medio del sistema de seguridad con cortafuegos incorporado en la misma. No está permitido acceder a Internet llamando directamente a un proveedor de servicio de acceso y usando un navegador, o con otras herramientas de Internet conectándose con un módem sin la previa autorización del departamento de sistemas.

**Artículo 123°.** Todas las actividades en Internet deben estar en relación con tareas y actividades del trabajo desempeñado.

**Artículo 124°.** En caso de tener que producirse una transmisión de datos importante, confidencial o relevante, sólo se podrán transmitir en forma encriptada.

**Artículo 125°.** Es responsabilidad de cada uno de los colaboradores de la Cooperativa la lectura y conocimiento de la Política de Seguridad más reciente.

**Artículo 126°.** Debido a la propia evolución de la tecnología y las amenazas de seguridad, y a las nuevas aportaciones legales en la materia, el departamento de sistemas de COPECOM R.L. se reserva el derecho a modificar esta Política cuando sea necesario. Los cambios realizados en esta Política serán divulgados a todos los colaboradores de la Cooperativa.

**Artículo 127°.** Así mismo, las disposiciones aquí enmarcadas, entrarán en vigor a partir del día siguiente de su aprobación y difusión.

**Artículo 128°.** Por otra parte, las disposiciones aquí descritas constarán de forma detallada en los manuales de políticas y procedimientos específicos.

**Artículo 129°.** Y la falta de conocimiento de las normas aquí descritas por parte de los colaboradores no los libera de la aplicación de sanciones y/o penalidades por el incumplimiento de las mismas contenidas en el Reglamento Interno de Trabajo.

APROBADO Y AUTORIZADO SEGÚN:

ACTA DE CONSEJO NO. 16-2015

RECTIFICADO Y RATIFIACADO EN EL ACTA DE CONSEJO NO. 12-2016