POLÍTICAS Y NORMAS DE SEGURIDAD INFORMÁTICA CORRESPONDIENTE A COOPERATIVA PARROQUIAL GUADALUPANA, R.L.

MICOOPE

Unidos para dar vida a tus sueños

POLITICAS Y NORMAS DE SEGURIDAD

CONSIDERANDO

Que la Institución, tiene recursos informáticos actualizados que brindan la oportunidad de potencializar los esfuerzos en pro de la excelencia y calidad en el procesamiento electrónico de datos, buscando la eficiencia y la simplicidad de los procesos gerenciales, administrativos y operativos que contribuyan al alcance de las metas y objetivos definidos en la misión y visión de la institución.

CONSIDERANDO

Los cambios constantes de la tecnología y que la seguridad ha pasado a ser parte inherente de la gestión informática de toda institución. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las instituciones para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de amenazas para los sistemas de información.

CONSIDERANDO

La necesidad de crear políticas de seguridad informática que surjan como una herramienta administrativa para concientizar a los colaboradores de la institución sobre la importancia y sensibilidad de la información y servicios que permiten crecer y mantenerse competitiva.

CONSIDERANDO

Que la presente Política de Seguridad informática aplicada en su justa dimensión, pueden coadyuvar significativamente al fortalecimiento de los sistemas de información y garantizar en gran medida la integridad, confidencialidad, existencia y oportunidad de la información corporativa, lo que conlleva inevitablemente al desarrollo y a la confianza de la gestión cooperativista.

POR TANTO

El Consejo de Administración de la Cooperativa de Ahorro y Crédito Integral Parroquial Guadalupana, R.L. , con base al artículo 36 inciso c) del Estatuto, autoriza la presente Política y Normas de Seguridad informática, en el cual se definen las políticas, normas y procedimientos 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 computarizado, la adquisición y adecuada utilización de programas de apoyo requeridos.

CAPITULO I

OBJETIVOS.

1. Establecer los lineamientos administrativos e informáticos que sirvan como parámetros de referencia para la Institución en la administración, protección y existencia de la información.
2. Establecer un lenguaje común de comunicación documentada entre los usuarios y la Gerencia, para instruir y concientizar a todos y cada uno de los miembros de la Cooperativa sobre la seguridad que se debe proporcionar a la información.
3. Proveer a la Institución, de una herramienta documentada que coadyuve a identificar y clasificar la información, a efecto que la misma sea apropiadamente administrada, protegida y custodiada.
4. Proveer una herramienta que coadyuve a la protección de la información y a su adecuado resguardo como activo importante de su gestión.

CAPITULO II

ALCANCE

La Política de Seguridad Informática es de observancia y aplicación general para todo el personal de la Institución.

CAPITULO III

PERSONAL.

1. La selección y contratación de personal, se realiza cumpliendo las normas y procedimientos de gestión del recurso humano de la Institución, el Estatuto de la Cooperativa y la legislación vigente.
2. La Unidad de Talento Humano ó quien realice esta función y los responsables de las unidades administrativas informan oportunamente al Administrador de Sistemas cuando el personal se ausente temporal o definitivamente de su puesto de trabajo.
3. La Gerencia General a través de la instancia correspondiente capacita y mantiene actualizado al personal de Informática y Control Interno en temas de su competencia, especialmente en control y seguridad informática.
4. En el proceso de inducción al personal de nuevo ingreso, se contempla la observancia de las políticas y normas de seguridad informática.
5. La Institución mantiene y aplica un procedimiento de control estricto de accesos al sistema, en todos aquellos casos en que el colaborador no esté prestando sus servicios de forma permanente o temporal a la Cooperativa y/ó en caso de cambio de puesto.

6. La Institución distribuye e instruye a todo el personal sobre el cumplimiento y observancia de la Política de Seguridad Informática y aplica las sanciones correspondientes en caso de incumplimiento de la misma.

CAPITULO IV

ADMINISTRACION DE ACCESOS.

1. La Gerencia General delega al Gerente Financiero Administrativo, quien a su vez faculta al Administrador del sistema informático la función y responsabilidad de administrar los accesos a los sistemas informáticos de acuerdo al perfil autorizado.
2. Los accesos a los sistemas informáticos son creados en atención a una solicitud documentada y autorizada por los Jefes de las unidades administrativas y asignados en función de las atribuciones y responsabilidades del personal.
3. El uso de los sistemas informáticos y de la documentación confidencial está prohibido a las personas ajenas a la Institución, salvo autorización expresa de la Gerencia General, siempre y cuando convenga a los intereses de la Cooperativa.
4. Cada uno de los accesos a los sistemas informáticos corresponde a una sola persona autorizada y plenamente identificable de la Institución, en quien recae la responsabilidad exclusiva de su utilización.
5. La modificación a la información de las bases de datos se realiza a través de un documento autorizado por personal competente, generándose registro de lo actuado.
6. Los accesos a los sistemas se mantienen activos únicamente si los usuarios que los poseen están activos laboralmente o tienen acceso pre-autorizado corporativo.
7. Los programas de diagnóstico, soporte remoto y otros similares son utilizados exclusivamente por el personal de Informática autorizado.
8. La unidad de Informática implementa procedimientos que garantizan la confidencialidad y existencia de las claves de accesos a los sistemas informáticos.
9. Los empleados de la Institución informan oportunamente al personal de Informática cualquier irregularidad en la seguridad de los sistemas o las sospechas de violación a los mismos.
10. La Gerencia de Investigación y Desarrollo Tecnológico de FENACOAC y la unidad de Informática de la Cooperativa mantienen implementados mecanismos proactivos y reactivos que garantizan la seguridad de los accesos a la información.

CAPITULO V

SEGURIDAD FÍSICA.

1. Las instalaciones de la Institución cuentan con apropiados mecanismos y procedimientos que garantizan la existencia y seguridad de los activos, la información y la integridad del personal que labora en la misma.
2. Los empleados ingresan y permanecen en las instalaciones en días y horas inhábiles con la autorización expresa de la Gerencia General.
3. El área física que resguarda los equipos informáticos sensibles de la Institución está protegida adecuadamente de la intrusión y del medio ambiente.
4. La Gerencia General delega, en un funcionario idóneo o capacitado para su efecto, la responsabilidad de administrar adecuadamente la seguridad física y contingente de la Institución.
5. Contar con una bodega para almacenar materiales inflamables.

CAPITULO VI

SEGURIDAD LÓGICA.

1. La Gerencia de Investigación y Desarrollo Tecnológico de FENACOAC y la unidad de Informática de la Cooperativa, implementan y mantienen mecanismos que protegen la existencia, confidencialidad, disponibilidad e integridad de la información almacenada en los servidores, computadores personales y medios externos de almacenamiento.
2. La información confidencial puede ser transmitida electrónicamente con los mecanismos de seguridad que garanticen su integridad y confidencialidad.
3. Las personas ajenas a la Institución pueden utilizar su equipo informático dentro de las instalaciones siempre y cuando cumplan con las políticas, normas y procedimientos de seguridad informática.
4. El personal de la Unidad de Informática es el único facultado para acceder remotamente a los computadores de la Institución, a través de software autorizado por la Gerencia General y exclusivamente para soporte técnico y situaciones contingentes.

CAPITULO VII

SEGURIDAD ADMINISTRATIVA.

1. El personal de la Institución es responsable de la confidencialidad, existencia y custodia de la información que administra y procesa sin importar el medio que la contenga.
2. Todo software instalado cuenta con su respectiva licencia vigente de uso
3. El responsable de la unidad de Informática mantiene un inventario actualizado del software, hardware y de todo elemento informático utilizado por la Institución.
4. La unidad de Informática es la única autorizada por la Gerencia General para recomendar y definir estándares para la adquisición de equipo informático.

5. Los servidores y computadores personales mantienen instalado únicamente las aplicaciones y productos de software necesarios y autorizados por la Institución.
6. La información impresa de carácter privado y confidencial que no es de utilidad para la Institución es destruida físicamente.
7. La unidad de Informática mantiene estandarizada la configuración de los equipos informáticos.
8. La institución clasifica la información que genera y administra y la protege de acuerdo a dicha clasificación.

CAPITULO VIII

UTILIZACIÓN DE LOS RECURSOS INFORMÁTICOS.

1. Cada empleado es responsable del cuidado y el buen uso del equipo informático que la Institución le ha asignado para realizar sus actividades.
2. El equipo informático de la Institución podrá ser utilizado fuera de las instalaciones con la autorización expresa de la Gerencia General.
3. El personal designado por la Gerencia General tiene autorización para enviar correos electrónicos en forma masiva a todo el personal de la Institución.
4. La Gerencia General a través de la unidad de Informática informa al personal sobre el software permitido instalar en los equipos informáticos.
5. La unidad de Informática es la responsable del mantenimiento continuo y apropiado de los equipos informáticos.
6. El personal autorizado por la Gerencia General, utiliza la mensajería electrónica y la Internet para realizar actividades exclusivas requeridas por sus funciones y atribuciones.
7. El uso inapropiado de los recursos informáticos de la institución es motivo de sanciones que, dependiendo la gravedad, pueden ser administrativas y/o judiciales.
8. Las páginas web de la Cooperativa muestran información no confidencial, respetando las leyes nacionales e internacionales y la dignidad e integridad de las entidades y personas involucradas.
9. El personal comparte los recursos y la información almacenada en sus computadores con la autorización de la Gerencia General y la supervisión del responsable del control interno.

CAPITULO IX

CONTINUIDAD DE LAS OPERACIONES DEL NEGOCIO.

1. La institución cuenta con un plan documentado, probado y aprobado por la Gerencia General de acciones a seguir, para garantizar la continuidad de las operaciones informáticas en situaciones adversas.

2. La Institución protege sus activos informáticos a través de pólizas de seguro vigentes con coberturas apropiadas para su efecto.
3. Los usuarios son responsables de mantener respaldos actualizados de la información de interés institucional almacenada en sus equipos informáticos.
4. La institución mantiene mecanismos y procedimientos que garantizan el suministro de energía eléctrica en situaciones adversas.
5. Los procedimientos para la generación, restauración y custodia de los respaldos de la información están contenidos en un manual actualizado por la unidad de Informática.
6. La Institución mantiene mecanismos que garantizan el reemplazo oportuno del personal clave en caso de ausencia temporal o definitiva de éste.

CAPITULO X

ADQUISICIÓN, DESARROLLO Y MANTIMIENTO DE SISTEMAS.

1. Los sistemas informáticos desarrollados internamente o adquiridos a terceros, están debidamente probados, documentados y con adecuadas pistas de auditoría.
2. El desarrollo o modificación de las aplicaciones estándar para las Cooperativas federadas se centraliza en la Gerencia de Investigación y Desarrollo Tecnológico de FENACOAC y se solicita a través de formularios diseñados y autorizados para su efecto, los cuales forman parte de la documentación de las aplicaciones.
3. El desarrollo o modificación de las aplicaciones específicas de la Institución se centraliza en la unidad de Informática de la Cooperativa y se solicita a través de formularios diseñados y autorizados para su efecto, los cuales forman parte de la documentación de las aplicaciones.

CAPITULO XI

PERSONAL.

1. A los candidatos a optar a un puesto de trabajo dentro de la Cooperativa, se les realizará los estudios y evaluaciones necesarios que confirmen la idoneidad de los mismos al puesto.

CAPITULO XII

ADMINISTRACIÓN DE ACCESOS.

1. No se permite que los practicantes tengan acceso a los sistemas informáticos y a documentos confidenciales.

2. Cuando un empleado finalice su relación laboral o le sean cambiadas sus funciones y atribuciones, se le deben cancelar sus accesos y crearles los que necesite para sus nuevas actividades.
3. En situaciones de despido, al empleado se le debe remover inmediatamente sus claves de acceso a los sistemas y restringirle el acceso a las áreas sensibles de las instalaciones, tales como el área de los servidores, bóveda, telecomunicaciones y otros.
4. El administrador del sistema debe inactivar temporalmente las claves de acceso a los sistemas, a todo usuario que se ausente por: vacaciones, permisos, suspensiones u otros, las cuales podrán ser activadas a su regreso.
5. El periodo de expiración de la contraseña debe ser un máximo de 30 días; sin embargo, el usuario podrá cambiarla a su conveniencia.
6. Los intentos fallidos de acceso a los sistemas deben registrarse en una bitácora e investigarse oportunamente.
7. Debe implantarse un sistema de autorización y control de acceso con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear, o borrar datos importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.
8. Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Administrador de Sistemas debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones.

CAPITULO XIII

SEGURIDAD FÍSICA.

1. Resguardar los expedientes de los asociados y del personal en un área restringida y con un control de entradas y salidas.
2. Las instalaciones de la Institución deben mantener las condiciones y elementos de seguridad siguientes:
   - El cableado del sistema eléctrico, telefónico y de datos debe estar protegido con elementos y mecanismos que impidan o dificulten su daño, sustracción o destrucción.
   - Rutas de evacuación debidamente señalizadas.
   - Elementos de primeros auxilios.
   - Mecanismos que supriman o disminuyan el impacto de descargas electromagnéticas.
   - Detectores y alarmas de movimiento y calor.
   - Si la factibilidad lo permite, sistema de vigilancia de circuito cerrado.
   - Acometida eléctrica e interruptores debidamente protegidos.
   - Colocados en las paredes, instructivos de los pasos a seguir en caso de incendio, terremoto, inundaciones y otros relacionados.

- Elementos y procedimiento para el resguardo de objetivos no permitidos tales como: armas, celulares, comunicadores, etcétera.
- Extintores de fuego con mantenimiento apropiado y oportuno.
- Sistema eléctrico certificado y con adecuada tierra física.
- Personal de seguridad debidamente entrenado y capacitado en forma debida y constante.
- Las áreas importantes y las rutas de evacuación deben estar con luces de encendido automático en caso de emergencia.
- Mantener en buen estado y disponible un inversor o planta eléctrica con suficiente capacidad para mantener energía por tiempo prolongados.

3. Todos los equipos informáticos deben estar conectados a los sistemas ininterrumpidos de poder (UPS).
4. Fumigar las instalaciones contra roedores e insectos por lo menos una vez al año.
5. El área de los servidores y equipo de comunicaciones, debe contener las medidas de seguridad siguientes:
   - No estar rotulado.
   - Si la factibilidad económica lo permite con aire acondicionado.
   - Corriente eléctrica regulada.
   - Medidores de humedad y temperatura.
   - Libre de tuberías de aguas negras, pluviales o ductos de alta tensión eléctrica.
   - Prohibición de fumar, beber o ingerir alimentos en su interior.
   - Libre de materiales inflamables y/o elementos que no tengan función dentro del área.

CAPITULO XIV

SEGURIDAD LÓGICA.

1. Se debe deshabilitar en los computadores personales, todo mecanismo que sirva para conectarse fuera de la red interna de la Institución
2. Los computadores personales y equipos informáticos periféricos deben estar configurados de manera estándar a manera de garantizar la compatibilidad, uniformidad y seguridad de la red interna.
3. Los protocolos, servicios y puertos innecesarios deben deshabilitarse en los servidores y computadores personales.
4. Los dispositivos de almacenamiento masivo externo deben ser bloqueados a todos los usuarios, salvo personal autorizado por la Gerencia.
5. Proteger el acceso a la BIOS de la computadora por medio de contraseña.
6. Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto y además deben configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además el

usuario debe activar el protector de pantalla o bloquear la pc manualmente cada vez que se ausente de su oficina.

7. Los computadores deben estar protegidos por un firewall a nivel lógico, el cual debe de contar con una contraseña para poder realizar modificaciones.
8. Se debe delimitar a la utilización de usuarios restringidos en todas las computadoras a nivel de sistema operativo, salvo personal autorizado.
9. Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al Jefe de Seguridad Informática y poner la PC en cuarentena hasta que el problema sea resuelto.
10. Sólo pueden bajarse archivos de redes externas de acuerdo a los procedimientos establecidos. Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otros departamentos de la Cooperativa.
11. No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que haya sido comprobado en forma rigurosa y que esté aprobado su uso por el Departamento de Informática
12. Los usuarios no deben copiar a un medio removible, el software o los datos residentes en las computadoras de la Cooperativa, sin la aprobación previa de la gerencia
13. No pueden extraerse datos fuera de la sede de la Cooperativa sin la aprobación previa de la gerencia. Esta política es particularmente pertinente a aquellos que usan computadoras portátiles o están conectados a redes como Internet.
14. Los usuarios no deben interferir o tratar de interferir con los servicios de cualquier otro usuario, host o red dentro de la Internet. Estas actividades prohibidas incluyen sin limitaciones:
    - Envío de cantidades excesivas de data (exceder con cualquier tipo de tráfico que supere las normas aceptables en cuanto a tamaño y/o frecuencia) con la intención de sobrecargar los sistemas, llenar los circuitos y/o hacer fallar a los hosts.
    - Tratar de atacar o deshabilitar a un usuario, host o sitio.
    - Uso, distribución o difusión de cualquier programa, script o comando diseñado para interferir con el uso, funcionalidad o conectividad de cualquier usuario, host, sistema o sitio dentro de la Internet (como el propagar vía email, mensajes conteniendo virus, caracteres de control, etc.).

CAPITULO XV

SEGURIDAD ADMINISTRATIVA.

1. La información de carácter confidencial o crítica no deberá almacenarse en carpetas compartidas. Si fuese necesario esta práctica, se hará pero aplicando adecuados mecanismos de seguridad.
2. Si una PC tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso especial, preferiblemente por hardware.

3. Todo computador que tenga información confidencial se le debe remover la misma del disco duro, si tiene que ser transportado fuera de la Institución para mantenimiento, reparación u otros.
4. Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina.
5. La información sensible impresa pero ya no útil debe destruirse, preferentemente con un triturador de papel.
6. Las páginas web de la Institución deben observar las siguientes disposiciones:
   - Mostrar únicamente la información necesaria y actualizada para facilitar la consulta por parte de los interesados y para proteger la información.
   - Mostrar las políticas de privacidad de la información publicadas en ella.
   - Respetar las normas internacionales sobre derechos de autor, marcas registradas, propiedad intelectual, dignidad e integridad de las entidades y personas involucradas.

CAPITULO XVI

UTILIZACIÓN DE LOS RECURSOS INFORMÁTICOS.

1. Cada empleado es responsable de mantener su equipo informático apagado antes y después de cada jornada laboral.
2. Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.
3. Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.
4. Cada empleado debe bloquear su computador cada vez que se ausente de su puesto de trabajo.
5. Los equipos no podrán ser reubicados sin permiso del Jefe de Informática. Para llevar un equipo fuera de la Cooperativa se requiere una autorización escrita.
6. La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente
7. A todo usuario que dé un uso inapropiado a la Internet y al correo electrónico se le removerá su acceso a los mismos.
8. El inicio o continuidad de "cadenas" de mensajes por correo electrónico no está autorizado.
9. La unidad de Informática tiene la responsabilidad de dar mantenimiento preventivo al equipo informático por lo menos una vez al año y/o de acuerdo a las especificaciones del fabricante.
10. Los computadores portátiles que son para uso no personalizado, no deben mantener información confidencial o sensitiva. Cada vez que se deje de utilizar este tipo de equipo, su

información se debe guardar en medios externos de almacenamiento y posteriormente ser borrada del disco duro.

11. El correo electrónico debe mantener las condiciones siguientes:
    - Desplegar un mensaje indicando que la Institución no se hace responsable del contenido del correo electrónico, a menos que lo indique expresamente.
    - Ser reconocido como documento oficial, siempre y cuando existan mecanismos que garanticen su genuinidad y validez.
    - Deben ser enviados en formato carácter.

CAPITULO XVII

CONTINUIDAD DE OPERACIONES DEL NEGOCIO.

1. El personal de la Unidad de Informática o personal asignado de la cooperativa es responsable en realizar en forma mensual y detallada el inventario de la información de datos generales, captaciones y colocaciones, formando librerías de información interna en la Cooperativa.
2. El personal de la unidad de Informática es el responsable de la coordinación de las actividades que conlleva un plan de contingencias informáticas.
3. La Institución debe realizar comprobaciones de la eficacia de los planes de contingencias a través de simulaciones de incidencias, las cuales deben documentarse y evaluarse.
4. La unidad de Informática debe mantener documentado y actualizado los datos más importantes de la gestión que realiza, a manera de garantizar en gran medida la continuidad de las operaciones en ausencia prolongada de su personal. Se debe documentar: inventario de equipo, configuración de la red, IP´s, sistema operativo y su versión, inventario de licencias de software, proveedores, etcétera.
5. Todo el personal debe recibir capacitación sobre qué hacer en caso de siniestros y cómo aplicar los mecanismos de emergencia.

CAPÍTULO XVIII

1. La presente Política de Seguridad Informática tomará vigencia a partir del 25 de Marzo de 2013.

Oscar Juan Fuentes Girón
Presidente

Adolfo Maximiliano Rangel Gamas
Vicepresidente

Karin Elisa García Montoya
Secretaria

Erika María Elisa Reina Luther
Vocal I

Oscar Aparicio Segura Monzón
Vocal II