

POLÍTICA DE SEGURIDAD INFORMÁTICA

CONSIDERANDO

La necesidad de establecer normativas y disposiciones para el control de los recursos esenciales de la Cooperativa Guadalupana, como lo son los recursos tecnológicos, bases de datos, software y hardware que se administran en todas las oficinas y sedes de la Cooperativa.

POR TANTO

El Consejo de Administración en uso de las facultades que le confiere el artículo No. 36 inciso c) del Estatuto vigente de la Cooperativa:

ACUERDA

Aprobar la Política de Seguridad Informática Versión 3.0

CAPÍTULO I**GENERALIDADES**

ARTÍCULO 1.- OBJETO: Tener el correcto control de los procedimientos realizados por el área de informática, su seguridad análisis, sistemas, software y hardware, según las necesidades que la Cooperativa presente, así como minimizar los riesgos exteriores.

ARTÍCULO 2.- ALCANCE: Aplica a todos los colaboradores que laboren para la Cooperativa, consultores externos, etc.

ARTÍCULO 3.- RESPONSABLE: El Departamento de Informática es el responsable de llevar control del manejo de software y hardware que se utiliza en las instalaciones de la Cooperativa Parroquial Guadalupana, R.L.

ARTÍCULO 4.- DEFINICIONES

Información Sensible: Se toma como información sensible, a toda aquella información que provenga de: CRM, Bases de Datos de los distintos módulos en los que se operan dentro de la Cooperativa, documentos legales o representativos de transacciones, correos electrónicos, archivos y/o expedientes de asociados, colaboradores, expedientes en trámites de los distintos productos, todos los documentos que se cargan al sistema de Cabinet; documentación física de accesos, hojas de responsabilidad; informes de auditoría: gerenciales, legales, investigativos y cualquier otro informe que contenga información de

GUADALUPANA <small>es</small> M <small>MCODES</small>	POLÍTICA DE SEGURIDAD INFORMÁTICA		
	CÓDIGO:	IT-PO-01	VERSIÓN: 03

cualesquiera todo lo relacionado a plazos fijos, créditos y cualquier operación que involucre dinero de los colaboradores y/o asociados.

PERSONAL RESPONSABLE

ARTÍCULO 5.- OBLIGACIÓN CORRESPONSABLE: La responsabilidad por la seguridad de la información no sólo corresponde a las áreas de seguridad informática, sino que es una obligación de cada colaborador.

ARTÍCULO 6.- CÓDIGOS DE IDENTIFICACIÓN Y CLAVES: Los mecanismos de acceso que les sean otorgados a los colaboradores son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona, a menos que exista un requerimiento legal o medie un procedimiento de custodia de llaves. De acuerdo con lo anterior, los usuarios no deben obtener las claves u otros mecanismos de acceso de otros usuarios que pueda permitirles un acceso indebido.

ARTÍCULO 7.- RESPONSABILIDAD DE ACCESO: Los usuarios son responsables de todas las actividades llevadas a cabo con su código de usuario y clave personal.

CONTROL DE LA INFORMACIÓN

ARTÍCULO 8.- CONTROL DE LA INFORMACIÓN: Los usuarios deben informar inmediatamente al área que corresponda dentro de la Cooperativa toda vulnerabilidad encontrada en los sistemas, aparición de virus o programas sospechosos e intentos de intromisión y no deben distribuir este tipo de información interna o externamente.

ARTÍCULO 9.- INSTALACIÓN DE SOFTWARE: Los usuarios no deben instalar software en sus computadores o en servidores sin las debidas autorizaciones.

ARTÍCULO 10.- LÍMITES DE CONTROL: Los usuarios no deben intentar sobrepasar los controles de los sistemas, examinar los computadores y redes de la Cooperativa en busca de archivos de otros sin su autorización o introducir intencionalmente software diseñado para causar daño o impedir el normal funcionamiento de los sistemas.

ARTÍCULO 11.- CONTROL DE LA INFORMACIÓN: Los colaboradores no deben suministrar cualquier información de la Cooperativa a ningún ente externo sin las autorizaciones respectivas. Esto incluye los controles del sistema de información y su respectiva implementación (Ver también contrato de confidencialidad).

GUADALUPANA <small>es</small> M <small>MICROFIN</small>	POLÍTICA DE SEGURIDAD INFORMÁTICA		
	CÓDIGO:	IT-PO-01	VERSIÓN: 03

ARTÍCULO 12.- CONTROL DE DOCUMENTOS: Los colaboradores no deben destruir, copiar o distribuir los archivos de la cooperativa sin los permisos respectivos.

ARTÍCULO 13.- UTILIZACIÓN DE LOS SISTEMAS: Todo colaborador que utilice los recursos de los sistemas tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información ha sido clasificada como crítica.

OTROS USOS

ARTÍCULO 14.- USOS ADICIONALES: Los computadores, sistemas y otros equipos deben usarse sólo para las actividades propias de la cooperativa, por lo tanto, los usuarios no deben usar sus equipos para asuntos personales a menos que exista una autorización respectiva que evalúe el riesgo informático de tal labor.

ADMINISTRACIÓN DEL SOFTWARE

ARTÍCULO 15.- DISPOSICIÓN DEL SOFTWARE: La Cooperativa debe contar en todo momento con un inventario actualizado del software de su propiedad, el comprado a terceros o desarrollado internamente, el adquirido bajo licenciamiento, el entregado y el recibido en comodato. Las licencias se almacenarán bajo los adecuados niveles de seguridad e incluidas en un sistema de administración, efectuando continuos muestreos para garantizar la consistencia de la información allí almacenada. Igualmente, todo el software y la documentación del mismo que posea la Cooperativa incluirán avisos de derechos de autor y propiedad intelectual.

ARTÍCULO 16.- CLASIFICACIÓN DE SOFTWARE: Todas las aplicaciones se clasificarán en una de las siguientes categorías: Misión Crítica, Prioritaria y Requerida. Para las de plan estratégico deberá permanecer una copia actualizada y su documentación técnica respectiva, como mínimo en un sitio alternativo y seguro de custodia.

ARTÍCULO 17.- AMBIENTES DE DESARROLLO: Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad. Los programas que se encuentren en el ambiente de producción de la Cooperativa, se modificarán únicamente por el personal autorizado, de acuerdo con los procedimientos internos establecidos y en todos los casos, y se considerarán planes de contingencia y recuperación.

ADQUISICIÓN DEL SOFTWARE

ARTÍCULO 18.- OBLIGACIÓN CORRESPONSABLE: El software contará con acceso controlado que permita al propietario del recurso restringir el acceso al mismo. El software protegerá los objetos para que los procesos y/o los usuarios no los puedan acceder sin los debidos permisos. Cada usuario se identificará por medio de un único código de identificación de usuario y clave, antes de que se le permita el acceso al sistema.

PARAMETRIZACIÓN

ARTÍCULO 19.- PARAMETRIZACIÓN DE SOFTWARE DE TERCEROS O PROPIOS/DESARROLLADOS: Con el propósito de asegurar la integridad de la información, la función de Parametrización del software estará a cargo de un equipo interdisciplinario. Para el caso de aplicaciones de plan estratégico, el grupo interdisciplinario representará a los diferentes usuarios e incluirá al proveedor. Para el paso del software al ambiente de pruebas, el documento final de Parametrización del software contará previamente con las aprobaciones correspondientes al interior de la Cooperativa.

DESARROLLO DE SOFTWARE

ARTÍCULO 20.- BASES PARA DESARROLLO DE SOFTWARE: La Cooperativa deberá tener una metodología formal para el desarrollo de software de los sistemas de información de plan estratégico, desarrollos rápidos del mismo y las actividades de mantenimiento, las cuales cumplirán con las políticas, normas, procedimientos, controles y otras convenciones estándares aplicables en el desarrollo de sistemas. Los controles desarrollados internamente deberán ser como mínimo el plan de cuentas, el plan de auditoría y el cierre de puertas traseras. Adicionalmente, toda solicitud de modificación al software deberá contar con estudios de factibilidad y de viabilidad al igual que las autorizaciones respectivas dentro de la Cooperativa.

ARTÍCULO 21.- INFORMACIÓN PARA PRUEBAS DE SOFTWARE: Con el propósito de garantizar integridad y confidencialidad de la información que administrará el software desarrollado y antes del paso a pruebas, se deberán ejecutar las pruebas intrínsecas al desarrollo y a la documentación técnica respectiva. Para todo desarrollo de software se deberán utilizar herramientas, de las cuales se tengan certeza que su comportamiento es seguro y confiable. Solamente las funciones descritas en el documento aprobado de especificaciones de la solución tecnológica podrán ser desarrolladas.

ARTÍCULO 22.- ENCARGADOS DE ACCESO EN PRODUCCIÓN: Los programadores de software no deberán conocer las claves utilizadas en ambientes de producción. Únicamente el Jefe de Informática en conjunción con el Gerente Administrativo.

ARTÍCULO 23.- DOCUMENTACIÓN OBLIGATORIA: Los desarrollos y/o modificaciones hechos a los sistemas de aplicación no deberán trasladarse al ambiente de producción si no se cuenta primero con la documentación de entrenamiento, operación y de seguridad adecuados. La suficiencia de este material deberá ser determinada por los usuarios responsables en la Cooperativa.

PRUEBAS DE SOFTWARE

ARTÍCULO 24.- EQUIPO DE PRUEBAS: Un equipo especializado deberá hacer las pruebas en representación de los usuarios finales. El área de desarrollo de sistemas deberá entregar el software desarrollado con códigos fuentes al área responsable de ejecutar las pruebas, el cual deberá ser revisado para encontrar códigos mal intencionados y debilidades de seguridad utilizando preferiblemente herramientas automáticas, para luego ser compilado e iniciar las pruebas correspondientes.

ARTÍCULO 25.- PRUEBAS A REALIZAR: Los tipos de pruebas deberán ser previamente establecidos. Para garantizar la integridad de la información en producción éstas deberán ser debidamente planeadas, ejecutadas, documentadas y controlados sus resultados, con el fin de garantizar la integridad de la información en producción. Además, el ambiente de pruebas deberá ser lo más idéntico, en su configuración, al ambiente real de producción.

ARTÍCULO 26.- DESARROLLO DE PRUEBAS: Las pruebas sobre el software desarrollado tanto interna como externamente deberán contemplar aspectos funcionales, de seguridad y técnicos. Adicionalmente, se incluirá una revisión exhaustiva a la documentación mínima requerida, así como la revisión de los procesos de retorno a la versión anterior. En caso que se requirieran las claves de producción para ejecutar pruebas, su inserción y mantenimiento se deberá efectuar de manera segura. Se deberá poseer un cronograma para la ejecución de las pruebas con el fin de cumplir con los compromisos institucionales acordados. Éste podrá verse afectado en su calendarización por aquellos eventos en que se tengan que atender desarrollos rápidos únicamente por exigencias mandatarias de entes superiores.

IMPLANTACIÓN DEL SOFTWARE

ARTÍCULO 27.- CONDICIONES DE IMPLANTACIÓN: Para implantar un software mediará una autorización por escrito del responsable para tal fin. Las características que son innecesarias en el ambiente informático se identificarán y desactivarán en el momento de la instalación del software.

ARTÍCULO 28.- PREÁMBULO DE LA IMPLANTACIÓN: Antes de implementar el software en producción se verificará que se haya realizado la divulgación y entrega de la documentación, la capacitación al personal involucrado, su licenciamiento y los ajustes de parámetros en el ambiente de producción. Deberá existir un cronograma de puesta en producción con el fin de minimizar el impacto del mismo.

ARTÍCULO 29.- COMPILACIÓN DE MÓDULOS: Los módulos ejecutables nunca deberán ser trasladados directamente de las librerías de pruebas a las librerías de producción sin que previamente sean compilados por el área asignada para tal efecto, que en ningún momento deberá ser el área de desarrollo ni la de producción.

ARTÍCULO 30.- MODIFICACIONES POSTERIORES: Los programas en el ambiente de producción serán modificados únicamente por personal autorizado y cuando se requiera por fuerza mayor de acuerdo con las normas institucionales establecidas.

ARTÍCULO 31.- ENCARGADOS DE MANTENIMIENTO Y MODIFICACIONES: El área o encargado de programación no hará cambios al software de producción sin las debidas autorizaciones por escrito y sin cumplir con los procedimientos establecidos. A su vez, se contará con un procedimiento de control de cambios que garantice que sólo se realicen las modificaciones autorizadas.

ARTÍCULO 32.- CONTROL DE VERSIONES: La documentación de todos los cambios hechos al software se preparará simultáneamente con el proceso de cambio. Se deberá considerar, además, que cuando un tercero efectúe ajuste al software, éste deberá firmar un acuerdo de no- divulgación y utilización no autorizada del mismo. Para cada mantenimiento a la versión del software de plan estratégico se actualizará el depositado en custodia en el sitio alternativo y el respaldoado en la institución. Este software y su documentación se verificará y certificará su actualización.

CLASIFICACIÓN DE LA INFORMACIÓN



ARTÍCULO 33.- SEGURIDAD EN LA INFORMACIÓN: Todos los datos de propiedad de COOPERATIVA PARROQUIAL GUADALUPANA, R. L. se deben clasificar dentro de las siguientes categorías para los datos sensibles: SECRETO, CONFIDENCIAL, PRIVADO, y para los datos no sensibles la categoría es PÚBLICO. Para identificar la naturaleza de la información y las personas autorizadas para acceder se deben utilizar prefijos como indicadores generales tales como: 'Financiero', 'Administrativo', 'Comercial', 'Jurídico', 'Tecnológico'. Toda información secreta, confidencial y privada debe etiquetarse según las normas de COOPERATIVA PARROQUIAL GUADALUPANA, R. L. y todos los datos que se divulguen por cualquier medio deben mostrar la clasificación de sensibilidad de la información.

ARTÍCULO 34.- SENSIBILIDAD DE GRUPO DE INFORMACIÓN: Cuando se consolida información con varias clasificaciones de sensibilidad, los controles usados deben proteger la información más sensible y se debe clasificar con el máximo nivel de restricción que contenga la misma.

ARTÍCULO 35.- CLASIFICACIÓN Y FECHA DE CADUCIDAD: La información que se clasifica dentro de las categorías de sensibilidad debe identificarse con la marca correspondiente y se debe indicar la fecha en que deja de ser sensible, esto aplica para la información que se reclasifica tanto en un nivel inferior como en un nivel superior de sensibilidad.

ARTÍCULO 36.- RESPONSABLE DE CLASIFICACIÓN: La responsabilidad para definir la clasificación de la información debe ser tanto del dueño de la información como del área encargada de la seguridad informática en COOPERATIVA PARROQUIAL GUADALUPANA, R. L.

ARTÍCULO 37.- ELIMINACIÓN DE INFORMACIÓN: La eliminación de la información debe seguir procedimientos seguros y debidamente aprobados por el responsable de la seguridad informática y de datos en la cooperativa. Realizando un back-up correspondiente y luego destruyéndola localmente.

ALMACENAMIENTO DE LA INFORMACIÓN

ARTÍCULO 38.- ENCRYPTACIÓN DE INFORMACIÓN: Toda información secreta debe estar encriptada, ya sea que se encuentre al interior de COOPERATIVA PARROQUIAL GUADALUPANA, R. L. o externamente, en cualquier medio de almacenamiento, transporte o transmisión.

ARTÍCULO 39.- DURACIÓN DE LA INFORMACIÓN: Toda información sensible debe tener un proceso periódico de respaldo, tener asignado un período de retención determinado, la fecha de la última modificación y la fecha en que deja de ser sensible o se degrada. Sin embargo, la información no se debe guardar indefinidamente por lo cual se debe determinar un período máximo de retención para el caso en que no se haya especificado este tiempo.

ARTÍCULO 40.- RESPALDO DE INFORMACIÓN CONFIDENCIAL: La información clasificada como sensible (secreta, confidencial o privada) debe tener un respaldo, además debe tener copias recientes completas en sitio externo a COOPERATIVA PARROQUIAL GUADALUPANA, R. L., en un lugar lejano de donde reside la información origen.

ARTÍCULO 41.- ALMACENAMIENTO SENSIBLE: Todos los medios físicos donde la información de valor, sensitiva y crítica sea almacenada por períodos mayores a seis meses (6), no deben estar sujetos a una rápida degradación o deterioro.

ARTÍCULO 42.- RESPALDOS SENSIBLES: Los respaldos de información de valor o sensible debe tener un proceso periódico de validación con el fin de garantizar que no ha sufrido ningún deterioro y que se podrá utilizar en el momento en que se necesite.

ARTÍCULO 43.- INFORMACIÓN LEGAL CONTABLE: Toda la información contable, de impuestos y de tipo legal debe ser conservada de acuerdo con las normas y leyes vigentes.

ARTÍCULO 44.- INFORMACIÓN POR CORREO: La remisión de información sensible tanto por correo interno como externo debe cumplir con los procedimientos establecidos de manera que se realice en forma segura.

ARTÍCULO 45.- INFORMACIÓN LIBRE: Para todos los mensajes remitidos en formato libre de texto que contengan información sensible para el negocio debe numerarse cada línea y los documentos oficiales de la Cooperativa que se realicen a mano deben ser escritos con tinta.

ARTÍCULO 46.- CONTROL DE INFORMACIÓN: Todas las copias de documentos secretos deben ser numeradas individualmente con un número secuencial para que las personas responsables puedan localizar rápidamente los documentos e identificar algún faltante de la misma.

ADMINISTRACIÓN DE LA INFORMACIÓN

ARTÍCULO 47.- DERECHO DE TRANSMISIÓN DE LA INFORMACIÓN: Cualquier tipo de información interna de la Cooperativa no debe ser vendida, transferida o intercambiada con terceros para ningún propósito diferente al del negocio y se debe cumplir con los procedimientos de autorización internos para los casos en que se requiera.

ARTÍCULO 48.- PROPIEDAD INTELECTUAL INTERNA: Todos los derechos de propiedad intelectual de los productos desarrollados o modificados por los empleados de la institución, durante el tiempo que dure su relación laboral, son de propiedad exclusiva de COOPERATIVA PARROQUIAL GUADALUPANA, R. L.

ARTÍCULO 49.- MODIFICACIÓN DE DATOS Y PROGRAMAS: Los datos y programas de COOPERATIVA PARROQUIAL GUADALUPANA, R. L. deben ser modificados únicamente por personal autorizado de acuerdo con los procedimientos establecidos, al igual que el acceso a bodegas de información debe restringirse únicamente a personal autorizado.

ARTÍCULO 50.- RESPALDO DE LA INFORMACIÓN: Cuando la información sensible no se está utilizando se debe guardar en los sitios destinados para eso, los cuales deben contar con las debidas medidas de seguridad que garanticen su confidencialidad e integridad.

ARTÍCULO 51.- RECLASIFICACIÓN DE SENSIBILIDAD: En cualquier momento, el propietario de la información con la participación del responsable de la seguridad informática y de datos puede reclasificar el nivel de sensibilidad inicialmente aplicado a la información.


ARTÍCULO 52.- OTORGAR ACCESO: El acceso a la información secreta se debe otorgar únicamente a personas específicas.

ARTÍCULO 53.- CONFIDENCIALIDAD A TERCEROS: Toda divulgación de información secreta, confidencial o privada a terceras personas debe estar acompañada por un contrato que describa explícitamente qué información es restringida y cómo puede o no ser usada.

ARTÍCULO 54.- INTEGRIDAD DE LA INFORMACIÓN: Toda la información de la organización debe contemplar las características de Integridad, Confidencialidad, Disponibilidad, Auditabilidad, Efectividad, Eficiencia, Cumplimiento y Confiabilidad.

ARTÍCULO 55.- SOFTWARE NO AUTORIZADO: Todo software que comprometa la seguridad del sistema se custodiará y administrará únicamente por personal autorizado.

ARTÍCULO 56.- COPIAS DE INFORMACIÓN: La realización de copias adicionales de información sensible debe cumplir con los procedimientos de seguridad establecidos para tal

	POLÍTICA DE SEGURIDAD INFORMÁTICA		
	CÓDIGO:	IT-PO-01	VERSIÓN: 03

fin. La información de COOPERATIVA PARROQUIAL GUADALUPANA, R. L. no debe ser divulgada sin contar con los permisos correspondientes, además, ningún empleado, contratista o consultor debe tomarla cuando se retire de COOPERATIVA PARROQUIAL GUADALUPANA, R. L.

VALIDACIONES, CONTROLES Y MANEJO DE ERRORES

ARTÍCULO 57.- CONTROLES DE VALIDACIÓN PARA INFORMACIÓN: Para reducir la probabilidad de ingreso erróneo de datos de alta sensibilidad, todos los procedimientos de ingreso de información deben contener controles de validación. Se deben tener procedimientos de control y validaciones para las transacciones rechazadas o pendientes de procesar, además de tiempos determinados para dar la solución y tomar las medidas correctivas. Todas las transacciones que ingresan a un sistema de producción computarizado, deben ser sujetos a un chequeo razonable, chequeos de edición y/o validaciones de control. Todos los errores cometidos por los colaboradores de La Cooperativa y que son detectados por los usuarios deben cumplir con un proceso de investigación de acuerdo con los procedimientos y tiempos establecidos.

POLÍTICA DE HARDWARE


ARTÍCULO 58.- MANEJO DE LOS EQUIPOS: Los equipos computacionales de COOPERATIVA PARROQUIAL GUADALUPANA, R. L. no deben ser alterados ni mejorados (cambios de procesador, memoria o tarjetas) sin el consentimiento, evaluación técnica y autorización del área responsable (Soporte Computacional).

ARTÍCULO 59.- REPORTE DE DAÑOS: Los colaboradores deben reportar a los entes pertinentes de La Cooperativa sobre daños y pérdida del equipo que tengan a su cuidado y sea propiedad de La Cooperativa. La intervención directa para reparar el equipo debe estar expresamente prohibida. La Cooperativa debe proporcionar personal interno o externo para la solución del problema reportado.

ARTÍCULO 60.- INVENTARIO DE ACTIVOS: Todos los equipos de la Cooperativa deben estar relacionados en un inventario que incluya la información de sus características, configuración y ubicación.

ARTÍCULO 61.- COMPRAS DE HARDWARE: Todo el hardware que adquiera la Cooperativa debe conseguirse a través de canales de compra y mecanismos establecidos para ello.

A

	POLÍTICA DE SEGURIDAD INFORMÁTICA		
	CÓDIGO: IT-PO-01	VERSIÓN:	03

ARTÍCULO 62.- CONTROL DEL HARDWARE: Todos los productos de hardware deben ser registrados por proveedor y contar con el respectivo contrato de mantenimiento.

ARTÍCULO 63.- UBICACIÓN DE HARDWARE: Los equipos computacionales, sean estos PC, servidores, LAN, etc. no deben moverse o reubicarse sin la aprobación previa del Administrador o jefe del área involucrada.

ACCESO FÍSICO Y LÓGICO

ARTÍCULO 64.- ACCESO A EQUIPOS: Antes de conectarlos a la red interna todos los servidores de Intranet de la Cooperativa deben ser autorizados por el área responsable del hardware.

Todos los accesos que se realicen a las redes, equipos de comunicaciones, servidores o equipos individuales, están limitados exclusivamente a personal del Área de Informática de Cooperativa Guadalupana o usuarios internos designados, asegurando los adecuados niveles de seguridad conforme autenticación de usuario.

Se prohíbe la exploración, monitoreo y divulgación del uso, de la red interna de Cooperativa Guadalupana a cualquier persona, institución o entidad, quedando esta responsabilidad únicamente a cargo del personal designado por el Área de Informática.


ARTÍCULO 65.- USO DE EQUIPOS: Todos los computadores multiusuario y los equipos de comunicaciones deben estar ubicados en lugares asegurados para prevenir alteraciones y usos no autorizados.

ARTÍCULO 66.- RESGUARDO DE INFORMACIÓN LÓGICA: Las bibliotecas de cintas magnéticas, discos y documentos se deben ubicar en áreas restringidas en sitios alternos con acceso únicamente a personas autorizadas.

ARTÍCULO 67.- CONEXIONES: Todas las conexiones con los sistemas y redes de la Cooperativa deben ser dirigidas a través de dispositivos probados y aprobados por la organización y contar con mecanismos de autenticación de usuario.

ARTÍCULO 68.- SEGURIDAD EN EQUIPOS, DIRECCIONES Y COMUNICACIÓN: Los equipos de computación de La Cooperativa deben ser protegidos por mecanismos de control aprobados por el área de seguridad informática y de datos, Las direcciones internas, configuraciones e información relacionada con el diseño de los sistemas de comunicación y cómputo de la Cooperativa deben ser restringidas. Todas las líneas que permitan el acceso



	POLÍTICA DE SEGURIDAD INFORMÁTICA		
	CÓDIGO:	IT-PO-01	VERSIÓN: 03

a la red de comunicaciones o sistemas multiusuario deben pasar a través de un punto de control adicional (firewall) antes de que la pantalla de login aparezca en la terminal del usuario.

RESPALDO Y CONTINUIDAD DEL NEGOCIO

ARTÍCULO 69.- RESGUARDO ELÉCTRICO: Los equipos electrónicos se deben equipar con unidades suplementarias de energía eléctrica (UPS).

ARTÍCULO 70.- DISEÑO DE RED: El diseño de la red de comunicaciones debe estar de tal forma que se evite tener un punto crítico de falla, como un centro único que cause la caída de todos los servicios.

ARTÍCULO 71.- BACK-UP: Los backups de los sistemas de computación y redes deben ser almacenados en una zona de fuego diferente de donde reside la información original. Las zonas de fuego varían de edificio a edificio y son definidas por el área de seguridad de La Cooperativa.

ARTÍCULO 72.- MANTENIMIENTO DE EQUIPOS: A todo equipo de cómputo, comunicaciones y demás equipos de soporte debe realizársele un mantenimiento preventivo y periódico, de tal forma que el riesgo a fallas se mantenga en una probabilidad de ocurrencia baja.

ARTÍCULO 73.- PLANES DE CONTINGENCIA: Los planes de contingencia y recuperación de equipos deben ser probados regularmente con el fin de asegurar que el plan sea relevante, efectivo, práctico y factible de realizar. Cada prueba debe documentarse y sus resultados y las acciones de corrección deben comunicarse a la alta dirección.

ARTÍCULO 74.- SEGURIDAD EN LOS EQUIPOS: Los equipos portátiles de computación que contengan información sensible deben utilizar software de encriptación para proteger la información.

ARTÍCULO 75.- CONTROL DE EQUIPOS Y DECLARACIÓN DE RESPONSABILIDAD: Todo equipo de cómputo y de comunicaciones de la Cooperativa debe tener un número (lógico y físico) de identificación permanente grabado en el equipo, además, los inventarios físicos se deben realizar en forma periódica, regular y eficiente. Todo equipo portátil debe tener Declaración de Responsabilidad, la cual incluya instrucciones de manejo de información y acato de normas internas y de seguridad para el caso de robo o pérdida.

PROTECCIÓN FÍSICA DE LA INFORMACIÓN

ARTÍCULO 76.- DE LOS COLABORADORES Y TERCEROS: Todas las personas que trabajen para la Cooperativa y/o aquellas designadas por la misma para trabajar en actividades particulares (consultores y contratistas) son responsables del adecuado uso de la información suministrada para tal fin, por lo cual se debe velar por su integridad, confidencialidad, disponibilidad y auditabilidad. Toda información secreta, confidencial y privada debe estar provista de la seguridad necesaria por quien la maneja para evitar el uso indebido por parte de personal no autorizado.

ARTÍCULO 77.- DISPOSICIÓN DEL LUGAR: Al terminar la jornada laboral, los escritorios y áreas de trabajo deben quedar desprovistos de documentos sensibles que puedan comprometer los intereses de La Cooperativa. Estos deben quedar bajo llave en archivadores, cajas fuertes o demás medios de almacenamiento físico seguros.

ARTÍCULO 78.- CÁMARAS EN ÁREAS SENSIBLES: Las áreas donde se maneja información confidencial o crítica deben contar con cámaras que registren las actividades realizadas por los colaboradores.

PLAN DE CONTINGENCIA

ARTÍCULO 79.- CREACIÓN DE PLAN DE CONTINGENCIA: Preparar, implementar y mantener el Plan de Contingencia y de Recuperación de desastres y continuidad del negocio relacionados con tecnología informática.

ARTÍCULO 80.- CONTROL DEL PLAN DE CONTINGENCIA Y EJECUCIÓN: Liderar el proceso de pruebas que se debe ejecutar periódicamente a los Planes de Contingencia y de Recuperación.

CAPACITACIÓN Y ENTRENAMIENTO

ARTÍCULO 81.- MEJORA CONTINUA DEL ÁREA: Establecer y apoyar a las áreas encargadas en la ejecución de un plan de Capacitación continuo que permita actualizar a los colaboradores en aspectos de seguridad informática fortaleciendo la cultura sobre el tema.

ARTÍCULO 82.- CAPACITACIÓN A USUARIOS: Dar un entrenamiento adecuado a los usuarios, custodios y usuarios dueños de la información en cuanto a los requerimientos y responsabilidades sobre la seguridad de la información.

INDICACIONES FINALES

GUADALUPANA <small>es</small> M <small>MACOCHES</small>	POLÍTICA DE SEGURIDAD INFORMÁTICA	
	CÓDIGO: IT-PO-01	VERSIÓN: 03

ARTÍCULO 83. DEL INCUMPLIMIENTO DE LA POLÍTICA: Es de suma importancia mantener la integridad de la información elaborada dentro de la Cooperativa, por este motivo cualquier persona que infrinja algún artículo contenido dentro de este documento será causal de despido, según la gravedad de los mismos.

CONTROL DE ACCESOS

ARTÍCULO 84.- CREACIÓN DE USUARIOS: El departamento de Informática, deberá mantener los registros donde los líderes de los procesos hayan autorizado a los colaboradores a su cargo, el acceso a los diferentes sistemas de información de la Cooperativa de acuerdo a sus perfiles.

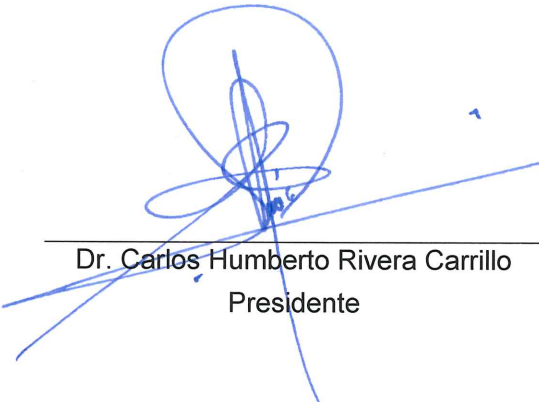
Cuando se retire o cambie de puesto a un colaborador, se deberá de aplicar la eliminación de los usuarios y accesos a los que estaba autorizado.

Por motivo de vacaciones, permisos, permisos sin goce de salario o suspensiones de los colaboradores deberán de inactivarse o bloquearse temporalmente los accesos a los sistemas de la Cooperativa, siendo responsabilidad de los jefes inmediatos notificar al departamento de Informática la fecha de inicio y finalización de la ausencia, así como el requerimiento de desvío de sus correos para atención por otro usuario.


ADMINISTRACIÓN DE CUENTAS DE CORREO ELECTRÓNICO

ARTÍCULO 85.- CADUCIDAD DE LAS CUENTAS: Talento Humano debe notificar al departamento de Informática, mediante correo electrónico, la desvinculación de los colaboradores, para que este proceda a realizar la desactivación de la cuenta de correo electrónico de cada colaborador y active el desvío de correos a la(s) cuenta(s) designada(s) por el jefe inmediato del área a la que pertenecían los colaboradores. Esta medida tendrá una vigencia de dos meses, finalizado el plazo el departamento de informática procederá con la eliminación definitiva del correo y desvío aplicado en el servidor de correos.

ARTÍCULO 86.- RELACIÓN DE CONFIDENCIALIDAD: Está política se relaciona directamente con el contrato de confidencialidad y las normativas que ahí se pactan con cada colaborador, Está política no exime de ninguna cláusula allí estipulada, sino complementa la seguridad e integridad de la información, diferentes equipos, conexiones, hardware, y todo aquello que asegura la continuidad de la operación.




Dr. Carlos Humberto Rivera Carrillo
Presidente



Lic. Víctor Adolfo Sánchez López
Vicepresidente



Lic. Luis Estuardo Batres Montenegro
Vocal I



Sra. Michelle Paola Archila Hernández
Vocal II