


## **POLÍTICA DE COPIA DE SEGURIDAD PARA APLICACIONES INTERNAS**

	POLÍTICA DE COPIA DE SEGURIDAD PARA APLICACIONES INTERNAS		
	CÓDIGO:	IT-PO-02	VERSIÓN: 01

### **CONSIDERANDO**

Que los sistemas informáticos desarrollados por la Cooperativa son recursos esenciales para el funcionamiento de las distintas áreas y que de estos depende el registro y consulta de información de manera oportuna.

### **CONSIDERANDO**

Que existen vulnerabilidades internas y externas que amenazan las aplicaciones y la información que estas manejan, considerada uno de los activos más preciados.

### **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 Copia de Seguridad para Aplicaciones Internas.

## **CAPÍTULO I GENERALIDADES**

**ARTÍCULO 1.- OBJETIVO:** El propósito de la presente política es mantener, mediante un inventario, la identificación de las aplicaciones internas y su clasificación en base al nivel de criticidad para la Cooperativa; así como los responsables de realizar las copias de seguridad y definir el procedimiento para realizar estas copias, su verificación, pruebas de contenido y restauración en caso necesario y conforme Plan de continuidad de la operación.

**ARTÍCULO 2.- ALCANCE:** La Política de Copias de Seguridad para Aplicaciones Internas se limita al resguardo de las aplicaciones desarrolladas por el departamento de Informática y sus datos, no así aquellas aplicaciones provistas en forma de servicio por proveedores externos.

	POLÍTICA DE COPIA DE SEGURIDAD PARA APLICACIONES INTERNAS			
	CÓDIGO:	IT-PO-02	VERSIÓN:	01

### ARTÍCULO 3.- DEFINICIONES

**Copia de Seguridad:** Copia y archivo de los datos de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos.

**Copia de Seguridad Completa:** Se realiza una copia de seguridad de todos los archivos y carpetas seleccionadas.


**Copia Incremental:** Copia de seguridad que incluye los cambios desde la última copia de seguridad completa o diferencial realizada.

**Copia Diferencial:** Copia de seguridad de todos los archivos que se han creado o actualizado desde la última copia completa realizada.

### ARTÍCULO 4.- RESPONSABLES

**a) Personal y sus roles:** Se identifican a las personas que cumplen un rol en la Política de Copia de seguridad para aplicaciones internas:

Ref.	Rol	Marco	Descripción
01	Usuarios	Personal que utiliza los sistemas y servicios de la Cooperativa	Personal de la Cooperativa a quienes se les ha otorgado acceso a los Sistemas informáticos.
02	Soporte técnico	Personal del área de soporte de la Cooperativa (Auxiliares de informática y Asistente de Informática)	Personal de informática que posee la responsabilidad de forma directa de brindar la administración, gestión, monitoreo y soporte primer nivel.
03	Equipo Desarrollo	Personal del área de Desarrollo del departamento de Informática de la Cooperativa.	Personal de informática que posee la responsabilidad de forma directa del análisis, desarrollo, prueba, mantenimiento y soporte segundo nivel.


	POLÍTICA DE COPIA DE SEGURIDAD PARA APLICACIONES INTERNAS		
	CÓDIGO:	IT-PO-02	VERSIÓN: 01

04	Soporte MICOOPE	Personal del área de soporte de Federación.	Personal de informática que posee la responsabilidad de forma directa de brindar soporte de los sistemas y servicios prestados a la Cooperativa.
05	Gerentes	Gerentes de las distintas áreas de la Cooperativa.	Responsables del cumplimiento de los objetivos generales, estrategias, control y evaluación en el ámbito de su competencia.
06	Proveedores	Personal tercerizado que brinda servicios de desarrollo informáticos y servicios complementarios.	Personal que brinda y administra servicios informáticos complementarios para las operaciones de la Cooperativa.

**b) Personal de informática:** Se deberá contar con una agenda de todos los contactos del personal de informática de la Cooperativa con la siguiente información: Nivel de soporte, Puesto, Nombre, Número telefónico.

Dicha agenda es administrada por la Gerencia Administrativa y actualizada por cada modificación del personal por parte de la Jefatura de Informática, se distribuye a las siguientes personas responsables de mantener identificado al equipo técnico en caso de requerir apoyo:

- Gerencia General,
- Jefe de Riesgos,
- Asistente de Gerencia General,
- Auditor Interno,
- Cumplimiento,
- Sub Gerente General,
- Gerente Financiero,
- Gerente de Negocios y Mercadeo y
- Gerente Jurídico.

	POLÍTICA DE COPIA DE SEGURIDAD PARA APLICACIONES INTERNAS		
	CÓDIGO:	IT-PO-02	VERSIÓN: 01

La agenda tiene el propósito de identificar al equipo técnico de informática para tener comunicación vía telefónica en horas laborales y no laborales para gestionar una emergencia.

- c) Servicios tercerizados – Proveedores:** Se deberá contar con un inventario de los Sistemas que son brindados por proveedores para mantener la continuidad de las operaciones de estos, en la que se identifica: Sistema, Proveedor, Técnico (Contacto, Teléfono y Correo) y Administrativo/Comercial (Contacto, Teléfono y Correo).

Este inventario es administrado por el Jefe de Informática y se actualiza trimestralmente para su distribución a las siguientes personas:

- Gerente Administrativo y
- Personal de Informática.


- d) Equipos relacionados de la Cooperativa:** En la Cooperativa se cuenta con los siguientes equipos para reaccionar ante una contingencia:

- **Brigada de Primer respuesta:** Coordinan las diferentes actividades de preparación y reacción ante una contingencia. Esta estará conformada por los Auxiliares de Informática, Asistente de Informática, Jefe de Informática y Gerencia Administrativa.
- **Comité de Divulgación:** Vela por la divulgación de la presente política y está integrado por departamento de Procesos y departamento de Informática.

## CAPITULO II

### POLÍTICA GENERAL

**ARTÍCULO 5.- INVENTARIO DE ACTIVOS DE INFORMACIÓN:** En conjunto con “Gerencia Administrativa” se han identificado las aplicaciones necesarias para reanudar la operación de la Cooperativa en caso de desastre o incidente grave. Se incluye el software necesario y los datos críticos, los dispositivos que los albergan, responsables y ubicación:

	POLÍTICA DE COPIA DE SEGURIDAD PARA APLICACIONES INTERNAS		
	CÓDIGO:	IT-PO-02	VERSIÓN: 01

Ref.	Aplicación	Descripción	Dispositivo	Ubicación
<b>01</b>	<b>KB Guadalupana</b>			
01.01	Parametrización general	Sistema principal de gestión de los restantes Sistemas, contiene catálogos generales y seguridad.	Servidor de aplicaciones	Data center
01.02	Estado patrimonial	Sistema del área de Cumplimiento para la gestión de los estados patrimoniales del personal de la Cooperativa.	Servidor de aplicaciones	Data Center
<b>02</b>	<b>Herramientas</b>			
02.01	Sistema operativo Linux	Sistema operativo donde se alberga la instalación de la base de datos.	Servidor base de datos Producción	Data Center
02.02	Servidor Web	Sistema de servicios que ofrecen los sistemas web.	Servidor de aplicaciones	Data Center
02.03	Sistema de virtualización VMware	Sistema de virtualización donde se alberga sistema operativo de base de datos y Servidor web.	Servidor físico de aplicaciones	Data Center
02.04	Sistema de backup	Herramienta para realización de copias de seguridad.	Servidor físico de aplicaciones	Data Center / Equipo backup

**ARTÍCULO 6.- CONTROLES DE ACCESO:** La siguiente tabla muestra las amenazas más comunes que podrían impactar en la continuidad y componentes de los Sistemas internos de la Cooperativa:


Ref.	Responsable	Nivel de acceso		
		Realización	Resguardo Interno	Resguardo Externo
01	Auxiliares de Informática.	X		
02	Asistente de Informática.	X	X	
03	Jefe de Informática.		X	X
04	Gerente Administrativo.			X

**ARTÍCULO 7.- PERIODICIDAD:** Se define la frecuencia de la realización de las copias de seguridad teniendo en cuenta la variación de los datos generados, el costo de almacenamiento y las obligaciones legales:

Ref.	Backup	Frecuencia			Resguardo	
		Diario	Semanal	Mensual	Interno	Externo
01	Lunes	X				X
02	Martes	X				X
03	Miércoles	X				X
04	Jueves	X				X
05	Viernes	X				X
06	Sábado	X				X
07	Semanal 01		X			X
08	Semanal 02		X			X
09	Semanal 03		X			X
10	Mes 1			X	X	
11	Mes 2			X	X	
12	Mes 3			X	X	

**ARTÍCULO 8.- TIPO DE COPIA:** Se establece el tipo de copia de seguridad idóneo estimando los recursos y tiempo necesarios para llevarlos a cabo:

Ref.	Responsable	Tipo		
		Diferencial	Incremental	Completo
01	Lunes			X
02	Martes			X
03	Miércoles			X
04	Jueves			X
05	Viernes			X
06	Sábado			X
07	Semanal 01			X
08	Semanal 02			X
09	Semanal 03			X
10	Mes 1			X
11	Mes 2			X
12	Mes 3			X

	POLÍTICA DE COPIA DE SEGURIDAD PARA APLICACIONES INTERNAS		
	CÓDIGO:	IT-PO-02	VERSIÓN: 01

**ARTÍCULO 9.- COPIA EN LA NUBE:** Las copias de seguridad de resguardo externo, podrán almacenarse en un servidor ubicado en la nube, considerando las siguientes precauciones para garantizar su resguardo:

- Copia deberá estar cifrada.
- Los acuerdos de nivel de servicio con el proveedor, deberán garantizar la disponibilidad, integridad, confidencialidad y control de acceso a las copias.

**ARTÍCULO 10.- COMPROBACIÓN DE COPIAS DE SEGURIDAD:** Se establece una periodicidad diaria para la realización de verificación de la copia de seguridad, quedando bajo responsabilidad del Asistente de Informática el verificar y certificar la revisión a través de la “FORMA – VALIDACIÓN COPIA DE SEGURIDAD” la cuál deberá ser diseñada por el Jefe de Informática.

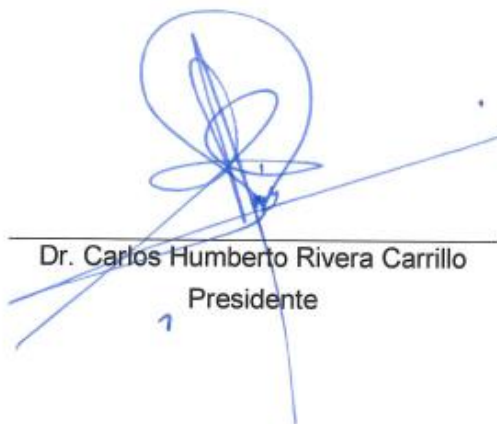
**ARTÍCULO 11.- SIMULACRO:** Se establece una periodicidad de seis meses para la ejecución de una simulación de pérdida de las Herramientas detalladas en el inciso 2) del “ARTÍCULO 5.- INVENTARIO DE ACTIVOS DE INFORMACIÓN”. Este simulacro se realizará hacia un equipo alternativo, fuera del entorno productivo, para evitar conflicto con el servidor principal y estará coordinado por el Asistente de Informática.

Debiendo documentarse, por parte de la Jefatura de Informática, los tiempos desde el inicio del Diagnóstico, manejo de la falla hasta habilitación de copia en equipo alternativo y Personal interno y externo involucrado.

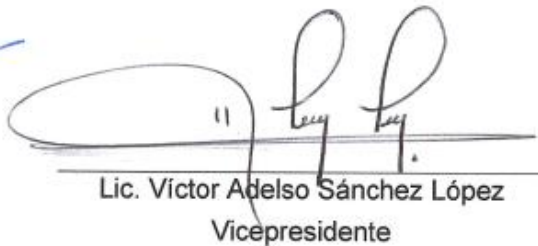
**ARTÍCULO 12.- REVISIÓN:** La Política de Copia de seguridad de aplicaciones internas está sujeta a revisión y cambios por lo menos una vez cada año, en caso de no existir modificaciones el Gerente General podrá ratificarlo para la continuidad de su aplicación.

**ARTÍCULO 13.- VIGENCIA:** La presente Política de Copia de seguridad de aplicaciones internas entra en vigencia treinta días después de su aprobación.





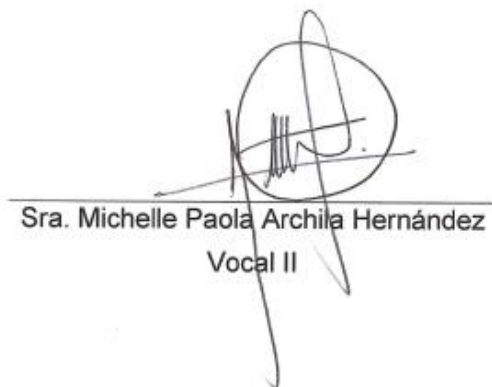
Dr. Carlos Humberto Rivera Carrillo  
Presidente



Lic. Víctor Adolfo Sánchez López  
Vicepresidente



Lic. Luis Estuardo Batres Montenegro  
Vocal I



Sra. Michelle Paola Archila Hernández  
Vocal II