RESOLUCIÓN ADMINISTRATIVA N° 02-010
La Paz, 16 de Marzo de 2016

CONSIDERANDO:

Que el parágrafo I del artículo 2° del Decreto Supremo N° 29710 de fecha 17 de septiembre de 2008, modifica al Decreto Supremo N° 29230 de 15 de agosto de 2007, señala que la Empresa de Apoyo a la Producción de Alimentos - EMAPA, como Empresa Pública, funcionará bajo tuición del Ministerio de Desarrollo Productivo y Economía Plural de acuerdo con el Decreto Supremo N° 29894 de 07 de febrero de 2009; cuya organización y funcionamiento se sujetará a la Ley N° 1178 de 20 de julio de 1990, de Administración y Control Gubernamental.

Que el Decreto Supremo N°1450 de 31 de diciembre de 2012, en la Disposición Adicional Primera modifica el Articulo 3° (ACTIVIDADES) del Decreto Supremo N°29230 de 15 de agosto de 2007, modificado por el Decreto Supremo N°29710 de 17 de septiembre de 2008.

Que el Decreto Supremo N°1694 de 14 de agosto de 2013, modifica el Decreto Supremo N°29230 de 15 de Agosto de 2007, modificado por los Decretos Supremos N°29710 de 17 de Septiembre de 2008 y N°1450 de 31 de Diciembre de 2012.

Que mediante Resolución Administrativa 02-011 de 09 de Julio de 2015, se aprueba el Procedimiento de Control de Documentos versión 8, mismo que establece que la aprobación de manuales y procedimientos se realizan mediante Resolución Administrativa.

CONSIDERANDO:

Que la Unidad de Cartera viene utilizando el Sistema de Control de Cartera contando actualmente con una base de datos confiable la cual registra todos los datos referentes a ls inscripción de beneficiarios, colocación de cartera, recuperación de cartera via acopio , otros granos y depósitos bancarios, pagos a empresas proveedoras por la distribución de insumos, pago a beneficiarios y no beneficiarios por la compra de granos, la cartera por cobrar y mora, asimismo el registro de organizaciones con procesos judicial, pago de impuestos por la compra de grano e informes de cortes contables, finalmente la Unidad de Cartera mediante el Sistema de Control de Cartera lleva el registro de la recuperación de los proyectos de papa y el proyecto de las Seis Federaciones del Chapare.

Que el Informe Técnico EMAPA/GAF/UC/N°02/2016 de 24 de febrero de 2016, señala que por recomendaciones de Auditoría Externa y con la necesidad de contar con un sistema seguro y proteger la información se elaboro un manual con normas y políticas de manejo y acceso a la información en la Unidad de Cartera y concluye recomendando la aprobación del Manual de "GESTIÓN DE LA SEGURIDAD DE LA INFORMACION DEL SISTEMA DE CONTROL DE CARTERA" Versión 1 mediante Resolución expresa para su posterior aplicación por las unidades que intervienen en el proceso.

Que el Informe Legal EMAPA/UAL/INF N°031 de 16 de marzo de 2016 concluye que la aprobación del Manual de "GESTIÓN DE LA SEGURIDAD DE LA INFORMACION DEL SISTEMA DE CONTROL DE CARTERA" Versión 1 de la Empresa de Apoyo a la Producción de Alimentos - EMAPA, no contraviene ninguna norma jurídica en actual vigencia, por lo que se recomienda la emisión de la respectiva Resolución Administrativa.

POR TANTO:

El Gerente General de la Empresa de Apoyo a la Producción de Alimentos – EMAPA en aplicación de las facultades conferidas por la normativa vigente;

RESUELVE:

ARTÍCULO PRIMERO.- Aprobar, el Manual de **"GESTIÓN DE LA SEGURIDAD DE LA INFORMACION DEL SISTEMA DE CONTROL DE CARTERA" Versión 1** de la Empresa de Apoyo a la Producción de Alimentos - EMAPA, el cual forma parte de la presente Resolución Administrativa.

ARTÍCULO SEGUNDO.- La Gerencia General a través de la Unidad de Planificación y Proyectos en coordinación con la Gerencia Administrativa Financiera queda encargada de la difusión, así mismo la Gerencia Administrativa Financiera de la Empresa de Apoyo a la Producción de Alimentos - EMAPA, queda encargada de la implementación y cumplimiento de la presente Resolución Administrativa.

Regístrese, comuníquese, cúmplase y archívese

Ing. Avelino Flores Copa
GERENTE GENERAL
EMAPA

MANUAL
GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DEL S.C.C.

	Elaborado por:		Revisado por:		Aprobado por:
Nombre:	Lic. Augusto Velásquez	Lic. Norberto Condori	Lic. Aurora Prado Crespo	Lic. Yamile Ibáñez Flores	Ing. Avelino Flores C.
Cargo:	Analista de Sistemas de Cartera	Analista de Sistemas de Cartera	Jefe de la Unidad de Cartera	Gerente Administrativo Financiero	Gerente General
Firma:					
Fecha:	Lic. Augusto Velasquez Pairumani ANALISTA DE SISTEMAS EMAPA	Lic. Norberto Pedro Condori ANALISTA DE SISTEMAS EMAPA	24-02-16	Lic. Yamile Ibañez Flores GERENTE ADMINISTRATIVO FINANCIERO EMAPA	

CONTENIDO

1. INTRODUCCIÓN.

En el presente Manual se establecen y describen las políticas, lineamientos para la Gestión de la Seguridad de la Información del Sistema de Control de Cartera (S.C.C.) de la Empresa de Apoyo a la Producción de Alimentos EMAPA.

El sistema implementado por la Unidad de Cartera presenta un conjunto de actividades preestablecidas y sistemáticas, para dirigir y controlar todas las actividades propias de la Unidad de Cartera que se ha demostrado son necesarias para dar confianza adecuada sobre la información procesada y manejada de productores y proveedores de insumos.

La Unidad de Cartera, con los sistemas propios de esta y la red de información enfrentan amenazas de seguridad que incluyen, entre muchas otras: el fraude por computadora, espionaje, sabotaje, vandalismo, fuego, robo e inundación. Las posibilidades de daño y pérdida de información por causa de código malicioso, mal uso o ataques de denegación de servicio se hacen cada vez más comunes.

Por lo cual la institución ante su compromiso con el proceso de gestión responsable de información que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de este importante activo.

Todo el personal de la Unidad de Cartera involucrado deberá tener acceso para la aplicación del presente Manual.

2. OBJETIVO.

Proteger, preservar y administrar objetivamente la información de la Unidad de Cartera junto a las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

2.1. Objetivos Específicos.

- ✓ Mantener una Política de Seguridad de la Información actualizada y vigente.
- ✓ Definir las normas de la Unidad de Cartera para la correcta valoración, análisis y evaluación de los riesgos de seguridad asociados a la información y su impacto, identificando y evaluando diferentes opciones para su tratamiento con el fin de garantizar la continuidad e integridad del SCC.

3. ALCANCE.

Este manual sobre las normas de seguridad es de aplicación al personal dependiente de la Unidad de Cartera y personal que utilice el Sistema de Control Cartera, para lograr proteger los recursos y la totalidad de los procesos internos o externos vinculados a la Unidad.

4. DEFINICIONES.

4.1. Acceso.

Es el privilegio de una persona para utilizar un objeto o infraestructura.

4.2. Activos de Información.

Se refiere a cualquier información o sistema relacionado con el tratamiento de la información que tenga valor para la organización.

4.3. Equipo informático de Usuario Desatendido.

Es el equipo informático que se encuentra asignado al cuidado de un Usuario sobre el cual no se tiene control.

4.4. Información.

Contenido Almacenado en una base de datos o correspondiente a un sistema.

4.5. Software en Producción.

Software en desarrollo o en elaboración de nuevos requerimientos.

4.6. Usuario.

Personal asignado para el acceso a equipos y sistemas desarrollados, permitiendo su identificación en los registros.

4.7. Usuarios Externos.

Personal autorizado para el uso del SCC, no dependiente de la Unidad de Cartera.

4.8. Vulnerabilidad.

Es una debilidad de seguridad o brecha de seguridad, la cual indica que el activo es susceptible a recibir un daño a través de un ataque ya sea intencional o accidental.

5. ABREVIACIONES.

EMAPA: Empresa de Apoyo a la Producción de Alimentos.

S.C.C.: Sistema de Control de Cartera.

UPS: Uninterruptible Power Supply, que en español significa Sistema de Alimentación ininterrumpida).

6. RESPONSABILIDAD.

6.1. Unidad de Cartera.

Este documento es de aplicación obligatoria para todo el personal de la Unidad de Cartera.

6.2. Analistas de Sistemas de Cartera

Personal responsable de revisar y actualizar este documento.

6.3. Usuarios.

Son los propietarios de activos de información son responsables de la clasificación, mantenimiento y actualización de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia. En general, tienen la responsabilidad de mantener íntegra, confidencial y disponible la información.

Los usuarios de la información y de los sistemas utilizados para su procesamiento, son responsables de conocer y cumplir normas de Seguridad.

7. ACERCA DE LA SEGURIDAD DE LA INFORMACIÓN.

La seguridad de la información se entiende como la preservación, protección, aseguramiento y cumplimiento de las siguientes características de la información:

- **Confidencialidad:** los activos de información solo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.
- **Integridad:** El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.
- **Disponibilidad:** Los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios que tengan los permisos adecuados.

Para ello es necesario considerar aspectos tales como:

- **Autenticidad:** Los activos de información los crean, editan y custodian usuarios reconocidos quienes validan su contenido.
- **Posibilidad de Auditoría:** Se mantienen evidencias de todas las actividades y acciones que afectan a los activos de información.
- **Protección a la duplicación:** Los activos de información son objeto de clasificación, y se llevan registros de las copias generadas de aquellos catalogados como confidenciales.
- **No rechazo:** Los autores, propietarios y custodios de los activos de información se pueden identificar plenamente.
- **Legalidad:** Los activos de información cumplen los parámetros legales, normativos y estatutarios de la institución.
- **Confiabilidad de la Información:** Es fiable el contenido de los activos de información que conserven la confidencialidad, integridad, disponibilidad, autenticidad y legalidad.

8. GESTIÓN PARA EL ACCESO DE USUARIOS.

El objetivo es evitar accesos no autorizados a los sistemas de información.

8.1. Reglas de los Controles de Accesos.

Se considera las siguientes reglas:

- El Administrador de Base de Datos (Analista de Sistemas - Cartera) es el encargado de registrar a los usuarios.
- El Usuario registrado debe realizar el buen uso de su nombre de usuario y contraseña.
- El registro de usuarios debe ser autorizado por el Jefe de la Unidad.
- Está prohibido el uso del Usuario y contraseña ajeno.
- El Usuario es el encargado de proteger y custodiar sus datos de acceso al sistema.
- La instalación o proporcionar acceso al Sistema es responsabilidad del Analista del Sistema Cartera o Personal Autorizado (regionales).

8.2. Registro de Usuarios.

Se definieron qué perfiles de usuario existen para el sistema, indicando a qué información pueden acceder estos perfiles, qué operaciones o roles pueden realizar sobre esta información y en qué medida pueden ejercer estos roles. El encargado de registrar y administrar estos perfiles es el Administrador de la Base de Datos (Analista de Sistemas - Cartera).

Para realizar una solicitud, se efectúa el llenado del registro **Alta Cambio y/o Baja de Usuario (Ver ANEXO I).**

Pasos a seguir:

- El solicitante llenará el formulario.
- El solicitante pedirá autorización del Jefe de la Unidad.
- El Administrador verificará los roles a habilitar o deshabilitar.
- El Administrador de base de Datos dará conformidad a la Solicitud.

Usuarios externos y personal de empresas externas deben estar autorizados por el Jefe de la Unidad de Cartera quien será responsable del control y vigilancia del uso adecuado de la información.

8.3. Gestión de Contraseñas de Usuario.

Los usuarios deberán mantener en secreto las contraseñas personales y las compartidas.

Se debe tener en cuenta las siguientes consideraciones:

- Inicialmente se asignará una contraseña temporal, que forzosamente debe ser cambiada inmediatamente por el usuario. Se proporcionará también contraseñas temporales cuando un usuario olvide la suya sólo tras una identificación positiva del usuario.
- El administrador dará a conocer al usuario mediante carta de habilitación o Email el usuario y la contraseña respectiva. Los usuarios deben remitir acuse de recibo de sus contraseñas.
- La contraseña deberá estar encriptada en el sistema.
- Se cambiara la contraseña si se tiene algún indicio de su vulnerabilidad o de acceso inadecuado al sistema.
- Seleccionar contraseñas con mayor grado de dificultad.

8.4. Equipo Informático de Usuario Desatendido.

Para garantizar que los equipos desatendidos disponen de la protección apropiada y disminuir la probabilidad de que una vulnerabilidad exista, se recomienda:

- Cancelar todas las sesiones activas antes de marcharse.
- Desconectar los servidores o los computadores centrales cuando se ha terminado la sesión (y no sólo apagar el terminal o el computador personal).
- Proteger el terminal o el puesto de trabajo cuando no estén en uso con un bloqueador de teclado o una medida similar, por ejemplo, una contraseña de acceso.

8.5. Control de Acceso a la Red.

Con el objetivo de proteger los servicios de la red interna en la cual se encuentra implementada el SCC, se llevará un control de acceso de los usuarios a la red y sus servicios para no comprometer la seguridad del negocios, por medio de:

- Interfaces adecuadas entre la red de la Unidad y las redes públicas o las privadas de otras Unidades.
- Fijar mecanismos adecuados de autenticación para los usuarios y los equipos.
- Controlar accesos de los usuarios a los servicios de información.

8.6. Control de acceso al Sistema Operativo.

El objetivo es evitar accesos no autorizados a los computadores que tengan implementados el S.C.C.

Se utilizarán las prestaciones de seguridad a nivel de sistema operativo para restringir el acceso a los recursos del computador. Estos servicios deberían ser capaces de:

- Proteger cada computador, terminal y servidor con una contraseña asignada por el Usuario.
- El computador personal que tiene acceso al sistema debe estar claramente identificado su procedencia y/o ubicación.
- La conexión a la red es restringida y/o autorizada por el Analista de Sistemas - Cartera.

9. SEGURIDAD FÍSICA Y DEL ENTORNO.

9.1. Acceso.

Se debe tener acceso controlado y restringido a los servidores principales y subsidiarios.

9.2. Seguridad en los Equipos.

Los servidores que contengan información deben ser mantenidos en un ambiente seguro y protegido por los menos con:

- Controles de acceso y seguridad física.
- Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

Toda información institucional en formato digital debe ser mantenida en servidores designados o asignados por el Área de Sistemas. No se permite el alojamiento de información institucional en servidores externos.

10. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN.

Para garantizar la seguridad de la información es necesario desarrollar los procesos de respaldo y de recuperación que, en caso de fallo del sistema informático, permitan recuperar y en su caso reconstruir los datos.

10.1. Obtención de Copias de Respaldo.

El Administrador o el personal expresamente designado o autorizado, será responsable de obtener periódicamente una copia de seguridad de los Datos, a efectos de respaldo y posible recuperación en caso de fallo.

Estas copias deberán realizarse diariamente o en caso de Solicitud, el procedimiento esta descrito en el Manual del Sistema de Control de Cartera.

Las copias de respaldo deben ser almacenadas en el servidor, y ser copiadas en un medio magnético semestralmente.

10.2. Recuperación de Datos.

En caso de fallo del sistema con pérdida total o parcial de los datos, se deberá seguir el procedimiento indicado en el Manual de Usuario, que partiendo de la última copia de respaldo realizada, se reconstruirán los datos al estado en que se encontraban antes de la falla.

El responsable de los datos deberá verificar la correcta definición y funcionamiento del procedimiento de respaldo y recuperación efectuado.

10.3. Controles periódicos de Verificación del Cumplimiento.

Se comprobará al menos con periodicidad anual, por los administradores, la existencia de copias de respaldo que permitan la recuperación de Datos según lo estipulado en el apartado 10.1. de este documento, enviando en un medio magnético los respaldos a la Unidad de Cartera de la oficina central.

11. GESTIÓN EN EL MANTENIMIENTO DEL SISTEMA.

El objetivo es asegurar la confiabilidad en la información y también evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones.

11.1. Validación de los Datos de Entrada.

Los datos de entrada a las aplicaciones del sistema deben ser validados para garantizar que son correctos y apropiados. Se deberán aplicar verificaciones a la entrada del registro de datos. Los controles siguientes deberían ser considerados:

- Revisión periódica del contenido de la Base de Datos para confirmar su validez e integridad.
- Verificación de los documentos físicos de entrada para ver si hay cambios no autorizados a los datos de entrada (todos deberían estar autorizados).
- Comprobar la integridad de los datos transferidos desde las regionales.
- Comprobaciones que aseguren que los programas de las aplicaciones se ejecutan en el momento adecuado.
- Controlar que los programas se ejecutan en el orden correcto, que finalizan en caso de falla y que no sigue el proceso hasta que el problema se resuelve.

11.2. Validación de los Datos de Salida.

Validar los datos de salida del SCC para garantizar que el proceso de la información ha sido correcto y apropiado a las circunstancias. Los controles siguientes deberían ser considerados:

- Validar la credibilidad para comprobar que los datos de salida son razonables.
- En casos de fallos verificar la consistencia de los datos al ser restaurados.
- Los cambios solicitados al Administrador serán validados por el usuario solicitante.

11.3. Control del Software en Producción.

La implementar de nuevos requerimientos en el SCC debe ser controlada para minimizar el riesgo de corrupción, se consideran los siguientes controles:

- La actualización de las librerías de programas operativos será realizada por el responsable del Control y Administración del Sistema.
- Se debe implementar código ejecutable que tenga evidencia del éxito de las pruebas, la aceptación del usuario y la actualización de las librerías de programas fuente.
- Mantener registro de todas las actualizaciones de librerías de programas en producción.
- Se debe retener las versiones anteriores de software como medida de precaución para contingencias.

11.4. Procedimientos de Control de Cambios del sistema y datos.

Para minimizar la corrupción de los sistemas de información, se deberán mantener estrictos controles sobre la implantación de cambios. Este proceso debería incluir:

- Garantizar que los cambios se realizan por usuarios autorizados.
- Realizar la revisión de los controles y los procedimientos de integridad para asegurarse que los cambios no los debilitan.
- Registrar la Solicitud de cambio con la aprobación formal y detalle de la propuesta antes de empezar el trabajo según el registro **Solicitud de Cambios en el Sistema (Ver ANEXO II).**
- Garantizar y registrar la aceptación por el usuario autorizado, de los cambios antes de cualquier implantación.
- Garantizar que la implementación de un cambio, minimice la interrupción en el uso del Sistema.
- Garantizar de actualización de la documentación del sistema al completar cualquier cambio y del archivo o destrucción de la documentación antigua.
- Notificar los cambios en datos utilizando el registro **Inclusión y/o Edición de Datos (Ver ANEXO III).**

12. ANEXOS.

Anexo I: Alta, Cambio y Baja de Usuarios.
Anexo II: Solicitud de Cambios en el Sistema.
Anexo III: Solicitud de Inclusión y/o Edición de Datos.
Anexo IV: Modelo de Carta de Habilitación de Usuario.

ANEXO I

emapa	**REGISTRO**	**E-EMP/UC/I/521 R01**
	ALTA, CAMBIO Y BAJA DE USUARIOS	**Versión 3**

INFORMACIÓN SOLICITANTE

FECHA SOLICITUD	/ /
NOMBRE SOLICITANTE	
FECHA DEL EJECUCION	/ /

INFORMACIÒN

ALTA ☐ **CAMBIO** ☐ **BAJA** ☐

USUARIOS

CI	NOMBRES	PATERNO	MATERNO	TELEFONO

PROGRAMA	☐ARROZ ☐MAIZ ☐SOYA ☐TRIGO ☐OTRO
OPCIONES	☐INSERTAR ☐MODIFICAR ☐ELIMINAR ☐VISTAS
APLICACION	☐SCC ☐ACOPIO ☐CLIENTE
OBSERVACIONES	

INFORMACIÓN EJECUCIÓN

NOMBRE DEL EJECUTOR	
FECHA	/ /

Autorizador por:

Solicitado por:

ANEXO II

	REGISTRO	**E-EMP/UC/I/521 R01**
	SOLICITUD DE CAMBIOS EN EL SISTEMA	**Versión 3**

Fecha de Solicitud:	Solicitado por:
Sistema:	Modulo:
DESCRIPCIÓN DE LA SOLICITUD	
Autorizador por:	Solicitado por:
Fecha de Entrega:	Realizado por:
CONFORME ☐	**NO CONFORME** ☐
OBSERVACIONES:	
Firma del Solicitante:	Firma del Analista de Sistemas Cartera:

ANEXO III

	REGISTRO	**E-EMP/UC/I/521 R03**
	SOLICITUD DE INCLUSIÓN Y/O EDICIÓN DE DATOS	**Versión 3**

Fecha de solicitud:		Solicitado por:	
Programa:	Campaña:	Sistema:	Modulo:
DESCRIPCIÓN DE LA SOLICITUD			
DESCRIPCION DE LOS CAMBIOS REALIZADOS EN EL SISTEMA (Encargado de sistemas)			
Fecha de entrega:		Realizado por:	
Duración(Días):			

Autorizado por: Solicitado por:

ANEXO IV
Modelo de Carta de Habilitación de Usuario.
(EJEMPLO)

La Paz, 23 de abril del 2015.

Señor:
Lic. xxxxxx
xxxxxxxxxxxxxx
EMAPA

Ref.: ASIGNACION DE USUARIO Y PASSWORD

De mi consideración:

De acuerdo a requerimiento enviado en el Formulario de alta, cambio y baja de usuarios, se le asigna:

Usuario:…….....
Password……..

Se le recomienda cambiar su password para su próximo ingreso, para su seguridad destruirlo una vez memorizado o guardar a buen recaudo toda vez, que el manejo de este acceso en el Sistema de Control de Cartera es de entera responsabilidad del usuario.
Atentamente,

AFP/apv
CC. Archivo