PROCURADURÍA AGRARIA

SECRETARÍA GENERAL

MANUAL DE OPERACIÓN DEL SISTEMA DE DATOS PERSONALES PARA EL CONTROL DE EXPEDIENTES DEL PERSONAL

Modificaciones realizadas el 9/octubre/2006

MANUAL DE OPERACIÓN DEL SISTEMA DE DATOS PERSONALES PARA EL CONTROL DE EXPEDIENTES DEL PERSONAL

MARCO JURÍDICO

- Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, publicada por el Instituto Federal de Acceso a la Información Pública.
  D.O.F 11-06-2002

- Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, publicado por el Instituto Federal de Acceso a la Información Pública.
  D.O.F 11-06-2003

- Lineamientos de Protección de Datos Personales, publicados por el Instituto Federal de Acceso a la Información Pública.
  D.O.F. 30-09-2005

- Anteproyecto de Estándares mínimos de seguridad para los Sistemas de Datos Personales en custodia de las Dependencias Entidades de la Administración Pública Federal, emitidos por el Pleno del Instituto Federal de Acceso a la Información Pública.

INTRODUCCIÓN

Considerando que la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, publicada el 12 de junio de 2003, tiene como uno de sus objetivos el de garantizar la protección de los datos personales en posesión de los sujetos obligados, así como el acceso y la corrección de los mismos por parte de los titulares, estableciendo autoridades encargadas de dicha protección en cada sujeto obligado.

En atención a la LFTAIPG, se elabora el presente **Manual de Operación del Sistema de Datos Personales para el Control de Expedientes del Personal**, el cual responde al objetivo de crear un instrumento administrativo dinámico y de fácil consulta, que apoye al desarrollo ordenado y eficaz del trabajo de la Dirección de Personal y de la Dirección de Informática en la consecución de sus objetivos.

Para su elaboración se tomaron como base los principios normativos que en la materia establece la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y su reglamento; los Lineamientos de Protección de Datos Personales y el Anteproyecto de Estándares mínimos de seguridad para los Sistemas de Datos Personales en custodia de las Dependencias Entidades de la Administración Pública Federal; disposiciones normativas emitidas por el Instituto Federal de Acceso a la Información Pública.

El presente Manual es una herramienta de carácter administrativo y normativo que permite concientizar a los servidores públicos y usuarios sobre la adecuada y precisa observancia para proteger y conservar el **Sistema de Datos Personales para el Control de Expedientes del Personal**, el que será operado en medios físicos y automatizados, para lo cual se han determinado una serie de medidas para brindar seguridad en la recopilación, protección, manejo y transmisión de los datos personales de los servidores públicos de la Procuraduría Agraria.

OBJETIVOS

Establecer las políticas y procedimientos del **Sistema de Protección de Datos Personales para el Control de Expedientes del Personal** a fin de que los **Responsables**, **Encargados** y **Usuarios** del tratamiento de datos personales, garanticen el manejo, seguridad, protección y destino de datos personales recabados por la entidad, a través de documentos físicos y medios automatizados y que cumplan con los principios rectores de protección de los mismos, apegándose en todo momento al marco normativo establecido en esta materia, con el propósito de evitar su modificación, pérdida y mal uso, así como asegurar su integridad y conservación.

Salvaguardar la confidencialidad del **Sistema de Datos Personales para el Control de Expedientes del Personal de la Procuraduría Agraria** contra cualquier intento de acceso no autorizado o de mal uso de estos.

Establecer y dar a conocer la normatividad, elementos, servicios y recursos implementados en la seguridad informática para el resguardo, protección y manejo de los datos personales en medios automatizados.

ALCANCES

Las Políticas y Procedimientos para el manejo del **Sistema de Datos Personales para el Control de Expedientes del Personal**, son de observancia general y obligatoria y tienen por objeto regular la actividad en cuanto a la seguridad, conservación y resguardo de la Información contenida en este sistema.

Invariablemente, la omisión o incumplimiento de cualquiera de las políticas y procedimientos establecidos en el presente manual, ameritará una sanción administrativa según sea el caso, así como la notificación a las autoridades competentes en caso de ser necesario por la sospecha de pérdida o mal uso de la información contenida en este sistema, como lo marcan los Lineamientos emitidos por el IFAI en esta materia.

DEFINICIONES

I. Sistema Persona: Aplicación informática desarrollada por el Instituto Federal de Acceso a la Información Pública para mantener actualizado el listado de los sistemas de datos personales que posean las dependencias y entidades para registrar e informar sobre trasmisiones, modificaciones y cancelaciones de los mismos.

II. Sistema de Datos Personales: Conjunto ordenado de datos personales que están en posesión de una dependencia o entidad, con independencia de su forma de acceso, creación, almacenamiento u organización.

III. Medios Físicos: Conjunto ordenado de datos que para su tratamiento están contenidos en registros, manuales, impresos, sonoros, magnéticos visuales u holográficos.

IV. Medios Automatizados: Conjunto ordenado de datos que para su tratamiento han sido o están sujetos a un tratamiento informático y que por ende requieren de una herramienta tecnológica específica para su acceso, recuperación o tratamiento.

V. Responsable: El servidor público titular de la unidad administrativa designado por el titular de la dependencia o entidad, que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos personales.

VI. Encargado: El servidor público o cualquier otra persona física o moral facultado por instrumento jurídico o expresamente autorizado por el Responsable para llevar a cabo el tratamiento físico o automatizado de los datos personales.

VII. Usuario: Servidor público facultado por un instrumento jurídico o expresamente autorizado por el **Responsable** que utiliza de manera cotidiana datos personales para el ejercicio de sus atribuciones, por lo que accede a los sistemas de datos personales, sin posibilidad de agregar o modificar su contenido.

VIII: Destinatario: Cualquier persona física o moral pública o privada que recibe datos personales.

IX: Transmisión: Toda entrega total o parcial de sistemas de datos personales realizada por las dependencias y entidades a cualquier persona distinta al Titular de datos, mediante el uso de medios físicos o electrónicos tales como la interconexión de computadoras, interconexión de bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita.

X. Transmisor: Dependencia o entidad que posee los datos personales objeto de la transmisión.

XI. Tratamiento: Operaciones y procedimientos físicos o automatizados que permitan recabar, registrar, reproducir, conservar, organizar, modificar, transmitir y cancelar datos personales.

XII. Titular de datos: Persona física a quien se refieren los datos personales que sean objeto de tratamiento.

MANUAL DE OPERACIÓN DEL SISTEMA DE DATOS PERSONALES PARA EL CONTROL DE EXPEDIENTES DEL PERSONAL

INDICE

ORGANIZACIÓN Y ESTRUCTURA

ESTÁNDARES MÍNIMOS DE SEGURIDAD DEL SISTEMA DE DATOS PERSONALES PARA EL CONTROL DE EXPEDIENTES DEL PERSONAL

1. SISTEMA EN MEDIOS FÍSICOS

1.1. Recepción

- El **Usuario** a cargo de la recepción física de datos personales deberá portar su credencial de identificación vigente emitida por la Entidad.

- El **Responsable** deberá supervisar que el directorio de la entrada de los edificios de la Institución cuente con su nombre como **Responsable** del sistema, del **Encargado** y del **Usuario**, así como la ubicación de cada uno de ellos.

- El **Usuario** deberá contar con el mobiliario y equipo para el resguardo de datos personales, mismos que deberán garantizar su adecuado manejo, seguridad y protección.

- El área en donde se encuentre el sistema deberá contar con los señalamientos de ser área restringida e indicar el nombre del **Usuario** y el horario en que se presta el servicio.

- El **Responsable** deberá supervisar que se lleve a cabo adecuadamente el procedimiento establecido para el "Reclutamiento y Selección de Personal", siendo el **Encargado** quien deberá supervisar que las solicitudes de empleo del personal de nuevo ingreso y los datos personales que se recaben estén completos y sean correctos, debiendo cuidar que sean resguardados en el expediente de cada servidor público.

1.2. Resguardo

- El espacio designado para el resguardo de los datos personales deberá contar con los muebles adecuados y suficientes (anaqueles, archiveros y demás muebles) para el cumplimiento de sus funciones, siendo responsabilidad del Usuario el que se mantenga ordenado y limpio.

- El área de resguardo de los datos personales estará delimitada físicamente (muros y divisiones de mamparas) de manera que se impide el acceso a personas no autorizadas y se cuente con los señalamientos a la vista sobre las limitantes de acceso, para lo cual, la puerta de acceso contará con cerradura para también evitar la salida no autorizada de datos personales.

- Los anaqueles, archiveros y demás muebles tendrán el propósito de resguardar los medios físicos (expedientes) de las inclemencias del clima tales como humedad, polvo, luz, etc.

- El **Encargado** del sistema deberá supervisar que el **Usuario** asegure la conservación de los expedientes físicos, evitando el acumulamiento de polvo, humedad, incendio, etc.

- Las llaves que abren los muebles en donde se resguarden los datos personales estarán identificadas para diferenciar las copias de la llave original, por lo que el **Encargado** deberá supervisar que se encuentren identificadas y resguardadas para su fácil identificación y localización.

1.3. Acceso

- Únicamente tendrá acceso al área del sistema en medios físicos, el **Responsable,** el **Encargado** y los **Usuarios**, quienes siempre deberán portar su credencial a la vista. En el caso de visitantes, se les permitirá el acceso previa autorización escrita del **Responsable**, portando su credencial de visitante que será otorgada por el **Encargado.**

  El **Usuario** deberá registrar a las personas ajenas a la Procuraduría Agraria que acudan al área en donde se resguardan los datos personales, lo cual hará en un libro de visitas y para ello deberán entregar una identificación oficial con fotografía en dicho punto de registro, así como la autorización escrita del **Responsable**.

  Para el caso del personal de la entidad, se deberá registrar en la bitácora correspondiente, entregar la autorización escrita que haya emitido el **Responsable** y portar su credencial oficial vigente.

- El acceso a personal ajeno a las áreas donde se encuentran el sistema será autorizado por el **Responsable** del mismo, siempre y cuando se cuente con la solicitud escrita del interesado y que las razones expuestas justifiquen plenamente su acceso.

- El **Usuario** del sistema será responsable de cumplir con las disposiciones establecidas para permitir el acceso de toda persona ajena a su área.

- El **Responsable** del sistema entregará a través de memorándum al **Encargado** y al **Usuario** del mismo, copia de la llave del área de resguardo, señalando el nombre y cargo, así como la fecha de entrega y el acuse de recibido.

1.3.1. Usuarios autorizados y no autorizados

- El acceso al área de resguardo de datos personales únicamente es sólo para personal autorizado que labora en la Procuraduría y cuentan con llaves para abrir

la puerta de acceso a dicha zona. Las personas ajenas deberán contar con gafete de visitante, autorización escrita del **Responsable** y ser acompañadas por el **Usuario**. La persona que no cumpla con alguno de estos requisitos no podrá accesar al área.

1.4. Registro de actividades

1.4.1. Operación cotidiana

- El **Usuario** dispondrá de una bitácora y un libro de visitantes en donde quedará asentado el registro de toda persona que haya ingresado al área de resguardo de datos personales por haber sido autorizada, para lo cual se registrará el nombre del solicitante, fecha y hora, así como el motivo de su acceso y se anexará el escrito de autorización emitido por el **Responsable**.

- Las personas ajenas al área de resguardo que hayan sido autorizadas para entrar, deben estar acompañadas en todo momento por el **Usuario.**

1.4.2. Incidentes y su divulgación

- En caso de robo, extravío, incursión o divulgación no autorizada de la información contenida en el sistema, el **Usuario**, conjuntamente con el **Encargado**, deberán presentar, el mismo día de ocurridos los hechos, un informe escrito al **Responsable,** quien a su vez, y dentro de los cinco días naturales siguientes de conocer del incidente, se lo comunicará por escrito al C. Procurador Agrario.

- En caso de comprobarse algún incidente o una incursión no autorizada al sistema, la Procuraduría Agraria a través del **Responsable**, en un término no mayor de cinco días naturales de haber ocurrido el incidente, realizará la denuncia penal y/o administrativa según corresponda.

- En caso de haberse detectado el robo o el extravío de datos personales, el **Responsable** del sistema en medios físicos dará aviso por escrito a los ciudadanos afectados en un término no mayor de 30 días naturales de haber ocurrido el incidente. El propósito es pedir a los ciudadanos afectados que tomen precauciones para enfrentar el uso ilegal de su identidad y, si ello llegara a ocurrir, para que realicen la correspondiente denuncia ante las autoridades competentes.

1.4.3. Supervisión

El **Responsable** y el **Encargado** llevarán a cabo la supervisión mensual tanto en la infraestructura como en los procesos y políticas del sistema para, en todo caso, proponer las mejoras que estimen necesarias para incrementar el nivel de seguridad.

1.5. Baja de medios físicos

Par el caso de que se considere dar de baja (destruir) los medios físicos que dan cuerpo a los datos personales que forman parte del sistema, el **Usuario** de los mismos, de acuerdo a los procedimientos y mecanismos que se implanten y con las autorizaciones respectivas por escrito del **Responsable**, podrá realizar la separación de materiales para su destrucción, y en todo caso proceder a su reciclaje.

2. TRANSMISIÓN DE DATOS PERSONALES

2.1. Preparación previa a la transmisión

- El propósito del proceso de preparación previa de los datos personales existentes en medios físicos, es establecer una forma segura de almacenarlos en el medio que será utilizado para su transmisión, es decir, los datos personales no se transfieren en original (a menos que exista solicitud expresa para ello o que así sea necesario) sino que se utilizan fotocopias simples. En este sentido, el expediente resultante de la preparación previa es una copia simple del original.

- Toda solicitud para transmisión de datos personales debe estar respaldada por un escrito del solicitante hacia el **Responsable,** precisando los fundamentos de su solicitud y los datos personales que requiere.

2.2. Transmisión mediante traslado físico

- La transmisión de datos personales a otras instancias, deberá apegarse, para su autorización, a lo establecido en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, así como a su Reglamento, debiendo ser el **Responsable** quién autorizará dicha transmisión.

- La transmisión de datos personales entre la Procuraduría Agraria con dependencias y entidades se realiza mediante entrega en mano por un mensajero autorizado por el **Responsable** del sistema. La entrega se realiza sólo si el

destinatario autentica su identidad y el mensajero recaba nombre, firma y fotocopia de la identificación del solicitante, así como la fecha y hora de recepción.

- La transmisión de datos personales entre la Institución y un particular se realizará mediante correo certificado, verificando que sólo si el destinatario autentica su identidad y el mensajero recaba nombre, firma y fotocopia de la identificación del solicitante, así como la fecha y hora de recepción.

2.3. Usuarios autorizados y no autorizados para la transmisión de datos personales

- Para la transmisión de datos personales mediante traslado físico, las únicas personas autorizadas para intervenir en el son: el **Encargado** que realiza la preparación previa de la información, y el mensajero autorizado que realiza la entrega de los expedientes resultantes.

- Si los datos personales quedan en manos de alguna persona no autorizada, ello es razón suficiente para dar inicio al proceso de atención de un incidente, por lo que es preferible que el mensajero no entregue los datos personales si el solicitante no puede identificarse para recibirlos de manera personal.

3. DOCUMENTACIÓN EN LOS PROCESOS Y POLÍTICAS DEL SISTEMA DE DATOS PERSONALES.

3.1 Manual de operaciones

- Se cuenta con el presente **Manual de Operación del Sistema de Datos Personales para el Control de Expedientes** que describe los procedimientos y documenta los procesos que los **Responsables**, **Encargados** y **Usuarios**, deben llevar a cabo, determinando el nivel de responsabilidad de cada uno de ellos, con lo que se considera cumplir con la observancia de los estándares mínimos de seguridad recomendados por el IFAI para la protección de datos personales, tanto en medios físicos como en medios automatizados.

3.2 Sensibilización y capacitación

- El **Responsable** y/o el **Encargado** sensibilizarán y capacitarán a los **Usuarios** sobre lo establecido en el presente manual. En caso de que exista modificación o actualización en el sistema de datos personales, se llevará a cabo un nuevo curso de capacitación a los **Usuarios**.

3.3 Cartas compromiso, cláusulas y contratos de confidencialidad.

- El titular de la Procuraduría Agraria, recibirá por parte de los **Responsables** de los sistemas en medios físicos y medios automatizados, las cartas compromiso en las que los **Encargado** y los **Usuarios** de los sistemas en medios físicos y en medios automatizados se comprometen a realizar su trabajo en estricta observancia a las diversas disposiciones que integran el marco jurídico en materia de protección de datos personales.

- El personal que sea designado como **Usuario** de datos personales, deberá ser una persona que sea conocida por su alto nivel de honradez, comprometida con la Institución y su trabajo, y que haya demostrado profesionalismo en su desempeño, así como discreción para el manejo de información. Adicionalmente, deberá apegarse a lo establecido en el Código de Ética y acreditar, mediante la aplicación de baterías de valores, ser la persona apta para el desempeño de este encargo.

4. DEL CONTROL DE EXPEDIENTES EN LAS DELEGACIONES ESTATALES

Se atenderá a lo señalado en el marco normativo del MANUAL DE PROCEDIMIENTOS ADMINISTRATIVOS EN MATERIA DE RECURSOS HUMANOS DE LAS DELEGACIONES ESTATALES, señalando que los datos personales recabados serán protegidos de conformidad a lo dispuesto en los lineamientos de protección de datos personales, por lo que el titular de cada Delegación deberá remitir al Director de Personal, la documentación mencionada para la integración del expediente.

Por lo tanto el manejo de datos personales es exclusivo de Oficinas Centrales, a través del **Responsable, Encargado y Usuario**.

5. SISTEMA EN MEDIOS AUTOMATIZADOS

El manejo y resguardo de los datos personales del **Sistema de Datos Personales para el Control de Expedientes del Personal** también se hará en medios automatizados, para lo cual se observarán las disposiciones que a continuación se mencionan, siendo el responsable de la carga de información en el sistema, el **Responsable del Sistema en Medios Físicos.**

5.1 De la instalación del equipo de cómputo.

- Los bienes informáticos asignados para la operación de este sistema, invariablemente deberán ser instalados por el **Encargado del Sistema** en coordinación con el **Usuario** del sistema, de acuerdo a las especificaciones técnicas de los mismos.

- En el caso de equipos de reciente adquisición, éstos serán instalados preferentemente por el personal especializado que defina el proveedor externo en coordinación con el **Encargado del Sistema** con la finalidad de asegurar su correcta instalación, configuración y así asegurar las garantías del equipo adquirido.

- **El Encargado del Sistema** invariablemente resguardará, en las instalaciones de la Dirección de Informática los manuales, discos de instalación y demás documentación relativa al equipo de cómputo y Servidores instalados en el Centro de Cómputo y destinados a la operación del sistema.

- El equipo de cómputo y Servidores destinados a la operación del sistema, invariablemente estarán ubicados en el Centro de Cómputo, a efecto de disponer de seguridad física, condiciones ambientales adecuadas, alimentación eléctrica y acceso solo para el personal autorizado de la Dirección de Informática y del **Encargado del Sistema**.

- El uso y aprovechamiento de los equipos de cómputo y Servidores instalados en el Centro de cómputo estarán destinados únicamente a la Procuraduría Agraria.

- Los **Usuarios** que tengan a su cargo, ya sea la captura de información a través del equipo de cómputo, o bien, la operación de los Servidores que contienen el sistema, tendrán el resguardo de todo el equipo y de los programas de cómputo instalados y autorizados, siguiendo las políticas de la Dirección de Recursos Materiales y Servicios.

- Queda totalmente prohibido, fumar y consumir todo tipo de alimentos o bebidas en el área del Centro de Cómputo donde se ubica el sistema.

- El equipo de cómputo y servidores que contienen el sistema deben estar permanente y debidamente conectados a un regulador, unidad de respaldo de energía o sistema de energía ininterrumpible.

- No debe colocarse ningún tipo de objetos sobre el equipo de cómputo y Servidores que contienen el sistema, y deben de estar alejados de objetos magnéticos, tales como teléfonos celulares e imanes.

5.2 Del mantenimiento del equipo de cómputo.

- Los equipos de cómputo y Servidores cuya garantía se encuentre vigente únicamente recibirán mantenimiento preventivo o correctivo por parte del proveedor o fabricante vendedor, con la finalidad de evitar la pérdida de su garantía.

- Cuando se realice el mantenimiento preventivo de los Servidores, el **Responsable** del sistema le notificará por escrito, y con 48 horas de anticipación, al **Responsable** del sistema físico, el día y la hora de la interrupción del servicio, así como la fecha y hora en que se reanudará completamente su operación.

- El **Encargado del Sistema** supervisará directamente las actividades de mantenimiento preventivo a los equipos de cómputo y Servidores, con la finalidad de verificar su adecuado funcionamiento y en caso de algún problema, este deberá reportar de manera inmediata al responsable del mantenimiento para su pronta solución.

- Las fallas y/o problemas técnicos de los equipos de cómputo y Servidores que contengan el sistema deberán ser registradas por el **Responsable** en la **Bitácora de Fallas de los servicios de la Red Institucional**.

5.3 De la reubicación de los Servidores y del equipo de cómputo.

- La reubicación de los Servidores tendrá como finalidad actualizar tecnológicamente el sistema y obedecerá a las necesidades de la Institución en materia de optimización, uso y aprovechamiento de la infraestructura informática, debiendo realizarse en fechas programadas para no afectar las actividades de los **Usuarios**.

- La reubicación de los Servidores será facultad exclusiva del **Responsable del Sistema.**

- El **Responsable del Sistema en Medios Físicos** será quien solicite la reubicación del equipo de cómputo que tiene el acceso al sistema, para lo cual será necesario que presente una solicitud escrita al Titular de la Dirección de Informática.

- Una vez realizada la reubicación del equipo de cómputo, el **Responsable del Sistema en Medios Físicos** lo comunicara mediante oficio a la Dirección de Recursos Materiales y Servicios a fin de actualizar los resguardos correspondientes.

- La solicitud de reubicación, cambio y/o baja del equipo de cómputo que tiene acceso al sistema y de los Servidores que lo contienen deberá indicar invariablemente la marca, modelo, y números de inventario y serie.

  En caso solicitar la baja del equipo, la Dirección de Informática deberá emitir el dictamen técnico correspondiente.

6. CONTROL DE ACCESOS.

6.1. Del acceso a las zonas restringidas.

- Están consideradas como zonas restringidas aquellas en donde residen los equipos que contienen el sistema y las que de acuerdo a su naturaleza sean definidas conjuntamente por los **Responsables de los Sistemas**, las cuales deberán estar señalizadas con la finalidad mantener un adecuado control sobre el acceso del personal que opera el Centro de Cómputo, así como de quienes pueden ingresar a este sistema.

- El acceso al Centro de Cómputo y en particular al espacio que ocupan los servidores que contienen el sistema está totalmente prohibido a toda persona no autorizada y su acceso requiere invariablemente autorización del **Responsable y los Encargados del Sistema en Medios Automatizados.**

6.2. Del personal autorizado.

- Las personas autorizadas para tener acceso al equipo de cómputo y Servidores que contienen el sistema son las siguientes:

  1. Los **Responsables de los Sistemas en Medios Automatizados y en Medios Físicos.**
  2. Los **Encargados del Sistema en Medios Automatizados y Medios Físicos.**
  3. Los **Usuarios del Sistema en Medios Automatizados y Medios Físicos.**

6.3. Del acceso al Centro de Cómputo y registro de visitas.

- Solo tendrán acceso al Centro de Cómputo los servidores públicos señalados en el punto anterior, así como las que cuenten con autorización escrita del **Responsable** del sistema.

- La Dirección de Informática es responsable de elaborar y mantener actualizada la Bitácora de Control de Accesos al Centro de Cómputo, así como de las políticas que regulen el acceso de cualquier persona.

- La Bitácora de Control de Accesos al Centro de Cómputo debe estar en lugar visible para que todo el personal autorizado registre correctamente su acceso y salida del mismo.

6.4. Del acceso al equipo de cómputo y a los Servidores.

- El **Responsable del Sistema en Medios Físicos,** se encargará de supervisar el adecuado uso, aprovechamiento y conservación de los equipos de cómputo utilizados para la captura de información.

- El **Responsable del Sistema en Medios Automatizados,** se encargará de supervisar el adecuado uso, aprovechamiento y conservación de los Servidores.

- Todo acceso a los Servidores que contengan el sistema será registrado en la Bitácora de Control de Accesos al Centro de Cómputo, y será responsable de su registro la Dirección de Informática.

6.5. De la creación y asignación de claves de acceso.

- La elaboración y diseño de las claves de seguridad de acceso a los equipos de cómputo que contienen el sistema es actividad propia y única de la Dirección de Informática.

- La Dirección de Informática se reserva el derecho de cambiar, por motivos de seguridad, las claves de acceso al sistema.

- La solicitud de claves de acceso deberá presentarse ante la Dirección de Informática, debiendo estar firmado por el Responsable del Sistema en Medios Físicos.

- Las claves de acceso se crearán mediante la asignación de un Usuario y una Clave de Seguridad de Acceso (**Password**), y de acuerdo a la actividad a desarrollar dentro de este sistema, pudiendo ser, altas, bajas, cambios, reportes o la combinación de alguna de ellas.

- La creación de las claves de seguridad se realizará de acuerdo a los modelos utilizados para cada Servicio o Sistema Informático, de acuerdo a las siguientes características:

  a. Longitud mínima de 4 campos.
  b. Longitud máxima, la soportada por la aplicación, sistema o servicio utilizado.

c. Compuesta de "Caracteres Numéricos, Alfabéticos y Caracteres Especiales".

d. Caracteres intercalados de manera aleatoria.

- La Dirección de Informática entregará las claves de acceso al sistema en sobre cerrado y a través de oficio al **Responsable del Sistema en Medios Físicos**.

6.6. De la actualización o cambio de claves de acceso.

- La actualización o cambio de las claves de seguridad de acceso es actividad propia y única de la Dirección de Informática, y será llevara a cabo a petición escrita del **Responsable en Medios Físicos.**

- La Dirección de Informática entregará las claves de acceso actualizadas en sobre cerrado y a través de oficio al **Responsable del Sistema en Medios Físicos.**

6.7. De la cancelación de claves de acceso.

- Por razones de seguridad e integridad de los datos contenidos en el sistema, el **Responsable del Sistema en Medios Físicos,** solicitara a la Dirección de Informática por escrito, la cancelación temporal o definitiva de las claves de seguridad de acceso al Sistema.

6.8. De la responsabilidad del usuario en el uso y resguardo de claves de acceso.

- Los **Usuarios** a quienes se les haya proporcionado clave de acceso al sistema serán los responsables de utilizarla adecuadamente y resguardarla. En caso de extravío, deberá notificárselo de manera inmediata al **Responsable del Sistema en Medios Físicos.** para evitar que se haga mal uso de ella y pueda ponerse en riesgo la seguridad de los datos personales contenidos en el sistema.

- **Responsable del Sistema en Medios Físicos**, dentro de las siguientes 24 horas de que tuvo conocimiento del extravío de la clave de acceso, solicitará de manera escrita a la Dirección de Informática su cancelación definitiva.

6.9. De la divulgación, pérdida o posible mal uso de la información.

- En el caso de divulgación, pérdida o mal uso de la información contenida en el sistema o una incursión no autorizada al mismo, el **Usuario**, conjuntamente con el **Encargado**, deberán presentar, el mismo día en que ocurrieron los hechos, un informe escrito a los **Responsables de los Sistemas en Medios Automatizado y en Medios Físicos,** quienes a su vez, y dentro de los cinco días siguientes de conocer del incidente, se lo comunicarán de manera conjunta y por escrito al C. Procurador Agrario quien instruirá al Servidor Público facultado para presentar la denuncia correspondiente.

- En caso de haberse detectado el robo o el extravío de datos personales, los **Responsables de los Sistemas en Medios Automatizado y en Medios Físicos**, en un término no mayor de 30 días naturales de haber ocurrido el incidente, darán aviso por escrito a los ciudadanos afectados,. El propósito es que los ciudadanos afectados tomen precauciones para enfrentar el uso ilegal de su identidad y, si ello llegara a ocurrir, para que realicen la correspondiente denuncia ante las autoridades competentes.

7. EQUIPO DE SEGURIDAD.

7.1. Del equipo de detección y extinción de incendios.

- La Dirección de Informática será la responsable en definir las características y especificaciones técnicas adecuadas del equipo de detección y extinción de incendios.

- La Dirección de Informática será la responsable de supervisar la correcta instalación del equipo de detección y extinción de incendios, así como, de verificar su óptimo funcionamiento.

- Es responsabilidad de la Dirección de Informática el requerir la contratación del mantenimiento preventivo y correctivo del equipo de detección y extinción de incendios, así como establecer el calendario de eventos que debe realizar el proveedor externo de mantenimiento, debiendo verificar que el equipo funcione correctamente una vez concluidas las acciones de mantenimiento.

- La Dirección de Informática debe coordinar las acciones de las revisiones, capacitación y uso de los equipos de seguridad física con el Personal de Vigilancia en turno.

- El Jefe de Telecomunicaciones debe registra en la **Bitácora de Revisión de Equipos de Seguridad** los eventos que se realicen de mantenimiento (efectuado por personal externo) y revisión (realizado por él mismo); en las fechas programadas.

7.2. Del aire acondicionado.

- La Dirección de Informática definirá las características y especificaciones técnicas que debe cumplir el equipo de clima artificial a instalar en el lugar donde operarán los equipos de cómputo y Servidores que contendrán el sistema, siendo responsabilidad de la Dirección de Recursos Materiales y Servicios su adquisición.

- La Dirección de Informática debe supervisar la correcta instalación del equipo de clima artificial, así como, de verificar su óptimo funcionamiento.

- La Dirección de Informática debe requerir la contratación del mantenimiento preventivo y correctivo del equipo de clima artificial, así como, establecer el calendario de eventos que debe realizar el proveedor externo de mantenimiento y verificar, una vez concluidas las acciones de mantenimiento, su óptimo funcionamiento.

- Es responsabilidad del Jefe del Departamento de Telecomunicaciones supervisar la correcta operación del equipo de clima artificial ubicado en el Centro de Cómputo y Conmutador Central, con la finalidad de asegurar su óptimo funcionamiento.

- El Jefe del Departamento de Telecomunicaciones debe registrar en la Bitácora de **Revisión de Equipos de Seguridad** los eventos que se realicen de mantenimiento (efectuado por personal externo) y revisión (realizado por él mismo) en las fechas programadas.

7.3. De la unidad de respaldo de energía (UPS).

- Es responsabilidad de la Dirección de Informática determinar las características técnicas que deberán cumplir los equipos de respaldo de energía (UPS) para la protección de los Servidores que contienen dicho sistema.

- Corresponde a la Dirección de Informática supervisar la correcta instalación de la unidad de respaldo de energía (UPS), así como, de verificar su óptimo funcionamiento.

- La Dirección de Informática debe requerir la contratación del mantenimiento preventivo y correctivo de la unidad de respaldo de energía (UPS)., así como, establecer el calendario de eventos que debe realizar el proveedor externo de mantenimiento y verificar, una vez concluidas las acciones de mantenimiento, su óptimo funcionamiento.

- Es responsabilidad del Jefe del Departamento de Telecomunicaciones supervisar la correcta operación de la unidad de respaldo de energía (UPS). ubicado en el Centro de Cómputo y Conmutador Central, con la finalidad de asegurar su óptimo funcionamiento.

- El Jefe del Departamento de Telecomunicaciones debe registra en la Bitácora de **Revisión de Equipos de Seguridad** los eventos que se realicen de mantenimiento (efectuado por personal externo) y revisión (realizado por él mismo); en las fechas programadas.

8. RESPALDO, RECUPERACIÓN Y PROTECCIÓN DE INFORMACIÓN EN SU TRASLADO.

8.1. Del respaldo de información.

- La Dirección de Informática a petición del **Responsable del Sistema en Medios Físicos** efectuará el respaldo de información contenida en el sistema de acuerdo a sus procedimientos técnicos establecidos para tal caso y de conformidad con el calendario establecido.

- Las cintas que se generen con motivo del respaldo de la información de manera semanal, y de acuerdo al calendario previsto, serán depositadas por la Dirección de Informática en la Bóveda de Seguridad Bancaria para su protección.

8.2. De la recuperación de información.

- La Dirección de Informática es la responsable de efectuar la recuperación de la información del sistema de acuerdo a sus procedimientos técnicos establecidos para tal caso, incluyendo la recuperación de las cintas de respaldo depositadas en la Bóveda de Seguridad Bancaria.

- Una vez recuperada la información, y para los efectos procedentes, la Dirección de Informática dará aviso por escrito al **Responsable del Sistema en Medios Físicos.**

8.3. De la protección de información en caso de traslado.

- El **Responsable del Sistema en Medios Automatizados** verificara que la solicitud y/o el mandato para el traslado de los datos personales en medios electrónicos, cumpla con la normatividad establecida.

- El **Responsable del Sistema en Medios Automatizados**, asegurará que la información a trasmitir en medios electrónicos sea protegida mediante claves de seguridad con la finalidad de evitar el acceso por personas no autorizadas.

- El **Responsable del Sistema en Medios Automatizados**, trasmitirá electrónicamente la información solicitada, verificando la recepción de la misma por el solicitante, mediante el acuse correspondiente. Asimismo verificará el cumplimiento de la vigencia y el destino final de la información.