Ministerio de Agricultura y Ganadería

TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACION

POLÍTICAS Y NORMAS GENERALES

MARZO, 2009

ÍNDICE DE CONTENIDO

Comisión Gerencial de Informática

Román Solera Andara
Presidente
Viceministro

Rafael Espinosa Jiménez
Secretario
Jefe Departamento Informática

Ricardo Zuñiga Cambronero
Miembro
Director Administrativo Financiero

Nils Solórzano Villarreal
Miembro
Director Superior de Operaciones Regionales y Extensión Agropecuaria

Osvaldo Bolaños Víquez
Miembro
Jefe Unidad de Planificación Estratégica

Grupo de Estudio

Rafael Espinosa Jiménez,
Coordinador
Jefe Departamento Informática-MAG

Gerardo Ignacio Quesada Alvarado
Analista de Sistemas
Servicio Fitosanitario del Estado

Juan Luis Vargas Cambronero
Encargado de Informática
Servicio Nacional de Salud Animal

Margie Hernández Carvajal
Analista de Sistemas
Depto. de Informática, Dirección Regional Brunca

Marta Chávez Pérez
Encargada Unidad de Control Interno

Daniel Zúñiga Van der Laat
Jefe Sistema Unificado de Información Institucional

Presentación

Las tecnologías de información y comunicación son hoy en día un tema relevante, tanto para la competitividad de las empresas como para el eficaz desempeño de las instituciones públicas. Para el Ministerio de Agricultura y Ganadería, es importante disponer y poner al servicio del Sector Agropecuario novedosas herramientas tecnológicas, que le permita cumplir con mayor eficiencia, las funciones que le corresponde.

Esta disciplina contiene un rubro muy importante dentro del presupuesto institucional, por lo que es particularmente necesario, vigilar y controlar el eficiente uso de estos recursos, ordenando acciones mediante políticas en materia de tecnologías de información, que sustenten las tareas que requieren el apoyo de las tecnologías informáticas y de comunicación.

En este sentido, además de considerar prioritaria la necesidad de ordenar esta materia, las instituciones públicas tienen la obligatoriedad de acatar la Resolución emitida por la Contraloría General de la República Número R-CO-26-2007, publicada en La Gaceta Nº 119 del 21 de junio de 2007, relacionada con la implementación de la normativa técnica sobre tecnologías de información Nº N-2-2007-CO-DFOE. Para ello, se conformó en este Ministerio un equipo de trabajo para realizar un análisis, estudio y recomendaciones sobre las "Normas Técnicas para la Gestión y Control de las Tecnologías de Información".

El grupo de trabajo planteó, después del análisis respectivo, que el cumplimiento de estas Normas debía orientarse a través de "***Cinco Acciones Estratégicas***"; de las cuales la primera de ellas fue elaborar el presente "**Manual de Políticas Generales sobre Tecnologías de Información y Comunicación**".

Este documento contiene las políticas informáticas institucionales, que son aplicables a todas las Direcciones Nacionales y Regionales, órganos adscritos y en general a la estructura organizativa del Ministerio de Agricultura y Ganadería.

Se definen las políticas administrativas relacionadas con Tecnologías de Información: Sistemas de información, bases de datos, redes y comunicaciones, hardware, software y seguridad informática. Entre otros

La finalidad de este documento es que junto a otro material relacionado, sirva como un instrumento de consulta permanente y como guía especializada, para las áreas usuarias e interesadas dentro de la Institución.

Román Solera Andara
Viceministro
Ministerio de Agricultura y Ganadería
Junio de 2009

Marco Jurídico

La Contraloría General de la República ha emitido leyes y normativas para el control y la administración en materia de tecnologías de información y comunicación, así como la Ley General de Control Interno y otras normativas relacionadas sobre este tema.

En el año 2007 el ente contralor emite las "Normas técnicas para la gestión y el control de las tecnologías de información" las cuales fueron publicadas en el Diario Oficial La Gaceta No 119 del Jueves 21 de junio de ese mismo año y en su Capítulo I, Artículo 1.1 se establece la necesidad que en cada Institución exista un marco estratégico de Tecnologías de Información, constituido por políticas organizacionales que el personal comprenda y con las que esté comprometido.

Por lo tanto, en todas las instituciones del Estado deben existir manuales de políticas internas relativas a la administración de Tecnologías de Información. Para su cumplimiento, se definen en este documento las políticas que en esta materia, deben aplicarse para el Ministerio de Agricultura y Ganadería.

Ámbito de aplicación

Las políticas definidas en este documento son de aplicación para todo el Ministerio, incluyendo las direcciones nacionales, regionales y todas las organizaciones adscritas al MAG, cuyas actividades se apoyan en instrumentos informáticos.

Actualizaciones de este manual

Este instrumento rige una vez que el jerarca institucional lo apruebe y haya ordenado su puesta en marcha a través de una directriz ministerial. Deberá ser revisado y actualizado formalmente por lo menos una vez cada año, siendo responsabilidad de la jefatura de la instancia administrativa de Tecnologías de Información, en adelante denominado Área de TI, realizar este proceso.

Durante el proceso de implementación cualquier usuario podrá hacer observaciones, con el objetivo de mejorar y/o modificar cláusulas o políticas, las cuales se harán llegar a la jefatura del Área de TI.

Marco Filosófico

Del establecimiento de políticas

El término política se define como la guía o principios generales, con que se conduce un asunto o se emplean los medios para alcanzar un fin. De esta manera, las políticas se pueden entender como las orientaciones o directrices que rigen la actuación de una persona o una entidad en un asunto o campo determinado.

El Ministerio de Agricultura y Ganadería define periódicamente el conjunto de políticas generales y normas para la Institución, por lo que las políticas que se definen en este documento pasan a formar parte de este conjunto, como complemento para orientar las actividades apoyadas en tecnologías de información.

Objetivos

Objetivo General

Mantener la confiabilidad, disponibilidad e integridad de la información, así como facilitar el mejor aprovechamiento de los recursos informáticos y las telecomunicaciones, que son propiedad o se encuentran a disposición del Ministerio de Agricultura y Ganadería, para alcanzar la misión institucional.

Objetivos Específicos:

- Utilizar los recursos tecnológicos de información y comunicación en forma responsable y apropiada, de conformidad con las disposiciones dadas en este manual y otras de carácter institucional, legal o emitido por otros órganos del Estado Costarricense, que guarden relación con normativas aplicables a la materia.

- Minimizar las interrupciones de los servicios asociadas a los sistemas informáticos y comunicaciones, ocasionados por uso inapropiado o por daños causados en forma accidental o intencional.

Supervisión de las políticas

La supervisión del cumplimiento de las "Políticas Generales sobre Tecnologías de Información", queda a cargo del Área de TI; razón por la cual está facultada para verificar en cualquier momento el cumplimiento de estas políticas y de las normativas vigentes en materias de tecnologías de información y comunicación.

Violación a las políticas

La infracción o incumplimiento de las políticas sobre tecnologías de información y comunicación, será notificado a la Unidad Administrativa correspondiente a fin de que ésta proceda según corresponda. Durante el proceso de implementación se estará revisando el tema de cumplimiento y sanción con el Departamento de Recursos Humanos.

Este documento se estará revisando y/o actualizando por parte de la instancia administrativa de tecnologías de información en la Sede Central, con la finalidad de estarlo mejorando. Estas modificaciones serán comunicadas a través del Despacho del señor Viceministro.

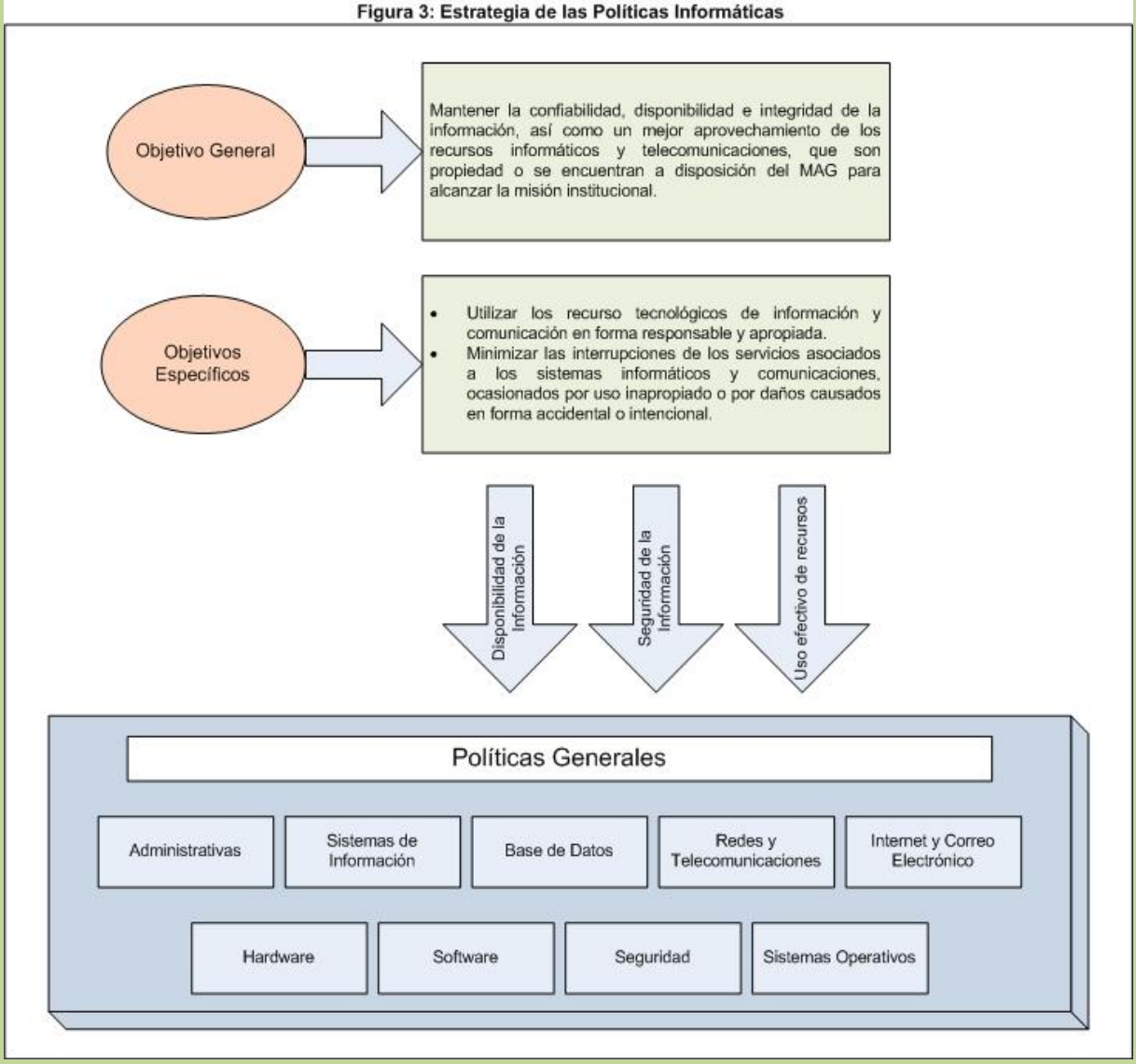
Definición de políticas para los servicios de tecnologías de información y comunicación

Políticas Generales

1. El Área de Tecnologías de Información, o Área de TI, será una unidad administrativa funcionalmente independiente, que le permitirá la ejecución de procesos de planeación, coordinación, ejecución y supervisión estratégica de los proyectos e inversiones de tecnología de información a nivel institucional. Para ello tendrá una dependencia jerárquica adecuada a este propósito, que en el caso de la Sede Central la tendrá con el Despacho del Viceministro, quien cuidará de este tema a nivel institucional.

2. Las políticas de tecnologías de información serán aprobadas por el jerarca del Ministerio y divulgadas adecuadamente a través de los directores nacionales, regionales y sitios web institucionales. Estas políticas será materia obligada en los procesos de inducción a los nuevos funcionarios que ingresen al Ministerio.
3. Debe establecerse una valoración sistemática del riesgo, de aquellos posibles eventos que comprometan el cumplimiento efectivo de las normas vigentes.
4. El Área de TI será responsable por la definición y ejecución de los presupuestos que el Ministerio asigne en esta materia.
5. La jefatura del Área de TI tendrá la responsabilidad de ejercer la Secretaría de la Comisión Gerencial de Informática, la cual tiene funciones definidas por Decreto Ejecutivo.
6. La administración central del MAG, sus direcciones nacionales y regionales brindarán el apoyo logístico, material, presupuestario y los recursos humanos necesarios al Área de TI, para que pueda cumplir adecuadamente sus funciones.
7. La Administración del MAG procurará recursos suficientes en los presupuestos ordinarios, extraordinarios y gestionará mediante proyectos de cooperación; para satisfacer los requerimientos que se deriven de la puesta en ejecución, de los lineamientos dados por el Despacho Ministerial mediante la Directriz DM-574-09, en el tema de implementación de sistemas digitales para el Ministerio de Agricultura y Ganadería

Figura 3: Estrategia de las Políticas Informáticas



Políticas Administrativas

Se definen en este apartado las políticas que enmarcan la forma en que se desarrollarán las actividades administrativas del Área de TI.

Políticas para el planeamiento y administración de actividades

1. El Área de TI contará con un Plan Anual Estratégico con el cual se orientarán las actividades. Para la administración y el control de sus proyectos, se utilizará preferiblemente un software de administración o en su defecto, se utilizará alguna otra herramienta que contenga información de control.

2. En los proyectos relacionados con desarrollo de aplicaciones, deberá aplicarse una metodología formal basada en el ciclo de vida de sistemas, para asegurar la adecuada administración y desarrollo.

Políticas sobre los servicios que ofrece el Área de TI

1. El Área de TI es un área de servicio para las diferentes dependencias del Ministerio, en el desarrollo y la utilización de las tecnologías de información, operando como un órgano asesor, promotor y facilitador.

2. El Área de TI creará un registro de los servicios que ofrece a las dependencias del Ministerio y los informará a través de la web.

3. Los servicios ofrecidos por el Área de TI, se solicitarán formalmente y siguiendo los procedimientos que se emitan para ese fin; los cuales se estarán transmitiendo durante el proceso de implementación

Políticas para el acceso físico al Área de TI

1. En general las oficinas de las Áreas de Tecnologías de Información son de ***acceso restringido***, dadas las características del trabajo que se desarrolla en sus instalaciones.

2. Los funcionarios de las diferentes dependencias podrán ingresar a la recepción del Área de TI, para efectos de solicitar servicios o consultas. Asimismo, podrán ingresar al interno de las oficinas siempre que haya un funcionario de TI que los atienda personalmente, manteniendo visibles sus correspondientes gafetes de identificación.

3. Será necesario un control de visitas al Área, en el cual se registran el nombre del o los visitantes, fecha, hora, persona que atiende y el motivo de la visita.

Políticas para la documentación y mantenimiento de manuales del Área de TI

1. Será política primordial del Área de TI, documentar formalmente todas las actividades que realice en el desarrollo de los servicios que brinda a la Institución.

2. El Área de TI mantendrá un archivo de gestión de documentos, debidamente ordenado y clasificado para el registro y custodia de la documentación administrativa, correspondencia y de actividades técnicas que desarrolla. Mantendrá, como mínimo, dentro de su archivos de gestión, las siguientes documentaciones:

- Correspondencia interna mantenida con todas las dependencias del Ministerio
- Correspondencia con entidades externas
- Documentación de planeamiento estratégico de Tecnologías de información
- Documentación de planes anuales operativos
- Documentación sobre solicitudes de servicio recibidas y satisfechas por el Departamento

- Documentación de inventario de equipos de cómputo, periféricos y de telecomunicaciones
- Documentación de perfiles de usuarios de redes
- Documentación de perfiles de usuarios de bases de datos
- Documentación de inventario de software instalado en equipos
- Documentación relativa a adquisición de equipos de cómputo, periféricos y de telecomunicaciones
- Documentación del mantenimiento correctivo de equipos de cómputo, periféricos y telecomunicaciones
- Documentación de licencias de software adquiridas
- Documentación de proyectos formalmente desarrollados
- Documentación administrativa de los funcionarios del Departamento

3. El Área de TI mantendrá en su archivo de gestión un Compendio de Manuales que contendrá como mínimo:

- Manual de Políticas Institucionales de Tecnologías de Información en general
- Manual de Puestos del Área de TI
- Manual de Procesos y Procedimientos del Área de TI
- Planes de Contingencias de Tecnologías de Información
- Manuales de Sistemas de Información

4. El Área de TI utilizará toda la documentación formal definida en la organización para el desarrollo de trámites administrativos.

Políticas para la adquisición de nuevas tecnologías

1. Todos los procesos institucionales de adquisición de recursos informáticos, deben ser valorados y aprobados previamente por el Área de TI.

2. Para la adquisición de nuevos recursos de hardware, software y otros dispositivos tecnológicos, será política del Área de TI recomendar aquellos que ofrezcan calidad comprobada y sean referentes en el mercado nacional.

3. Para el trámite de adquisición de nuevos recursos informáticos, el Área de TI asesorará y apoyará a la Proveeduría Institucional, en la definición de las características tecnológicas y evaluación de ofertas mediante recomendaciones técnicas.

4. Para la adquisición de nuevos recursos, el Área de TI se fundamentará en los reglamentos y normativas de compras definidos para la Institución.

5. El Área de TI velará porque los recursos informáticos adquiridos sean enviados y utilizados por el mismo sitio en que surgió la necesidad de compra.

Políticas sobre inventario de equipo

1. El Área de TI mantendrá un inventario de equipo con las características de cada uno de ellos, tanto de la sede central como de las direcciones regionales, nacionales, agencias y puestos fronterizos según corresponda.

2. El Área de TI colocará un sello de seguridad en los equipos, los cuales estarán enumerados para el correspondiente control. La finalidad de este sello es controlar la integridad de los equipos que están bajo responsabilidad de los usuarios. En las Direcciones Regionales se contará con el apoyo del enlace de TI (*donde exista y se haya nombrado oficialmente*), quien tendrá el control y la responsabilidad de la ubicación de los equipos. Para ello se gestionará con la Dirección Administrativa la adquisición de los sellos de seguridad durante el proceso de implementación.

3. El sello de seguridad no se podrá remover salvo que sea por los técnicos del Área de TI previamente autorizados, quienes rendirán un informe escrito de los cambios que sufriera el equipo.

4. El Área de TI deberá revisar el inventario del equipo por lo menos dos veces al año, realizando los cambios que sean necesarios. Hará un informe a la Administración sobre las diferencias y/o deficiencias encontradas.

Políticas sobre reparación de equipos

1. Todos los usuarios deben acatar el procedimiento que el Área de TI implemente para controlar los servicios de reparación y la calidad de los mismos.

2. La obtención de fondos presupuestarios para la adquisición de repuestos y accesorios será responsabilidad del usuario.

3. El Área de TI tendrá un control de las garantías de los equipos adquiridos para hacer cumplir los compromisos contractuales. Los equipos no cubiertos se procederán a ser reparados en el sitio mismo o en el taller. Podrá además acudir a talleres especializados cuyo costo será responsabilidad de los usuarios.

4. Se podrán autorizar talleres de reparación en las direcciones regionales para que apoyen el proceso de reparación de equipos. Para ello el enlace de TI regional, hará un reporte a la Sede Central para los controles correspondientes.

Políticas relativas a sistemas de Información

Políticas para el desarrollo interno de sistemas de información

1. El Área de TI desarrollará los sistemas de información que la organización requiera, de acuerdo a los recursos humanos y tecnológicos que tenga a su disposición para este fin.

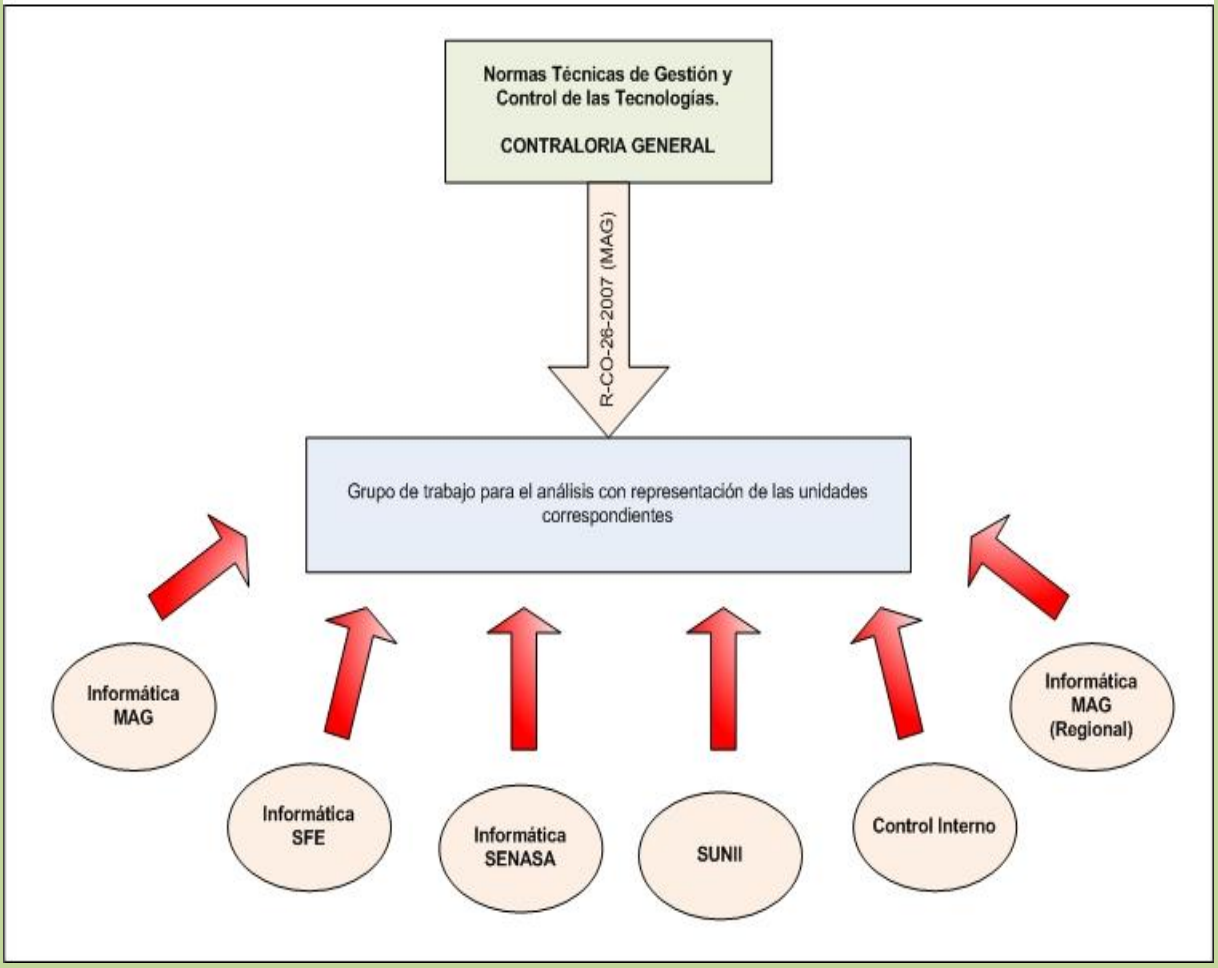
2. El desarrollo de aplicaciones o sistemas se hará bajo el concepto de tecnología web.

3. El desarrollo de sistemas de información se hará mediante proyectos debidamente formalizados, administrados y de acuerdo con la metodología y estándares del Área de TI, los cuales se estarán planteando durante la implementación de estas normas.

4. Las solicitudes de nuevos sistemas de información, solicitadas por las diferentes dependencias del Ministerio, serán evaluadas y aprobadas por la Comisión Gerencial de Informática y el Área de TI de acuerdo con las prioridades que éstos determinen.

5. Las pruebas de los nuevos sistemas de información deberán hacerse en servidores y ambiente de pruebas y con la utilización de bases de datos de prueba antes de ser puestos en producción.

Figura 1: Estructura Operación de Trabajo



Políticas para el desarrollo externo ("outsourcing") de sistemas de información

1. El Área de TI podrá recurrir al desarrollo sistemas de información por "outsourcing", cuando no cuente con el recurso humano y/o tecnológico necesario, para llevar a cabo los desarrollos de forma interna.

2. Las solicitudes de nuevos sistemas de información a desarrollar en la modalidad de "outsourcing", deberán ser formalmente presentadas por las Jefaturas, en forma escrita e indicando en éstas los requerimientos generales por cubrir y la constancia de la existencia de los fondos presupuestarios emitida por el Departamento Financiero. Además, serán evaluados y aprobados por la Comisión Gerencial de Informática y el Área de TI, de acuerdo con las prioridades que la Administración determine.

3. Para los proyectos de desarrollo de sistemas de información por "outsourcing", deberá establecerse un contrato formal entre el Ministerio y la empresa proveedora del servicio, en donde se definan las condiciones de la contratación, el uso de los programas fuente y la reutilización del sistema en el MAG

4. El control y monitoreo del avance de proyectos de sistemas de información por "outsourcing" estará a cargo del Área de TI.

5. Para el desarrollo de proyectos de sistemas de información por "outsourcing", deberán existir uno o más funcionarios que cumplan las funciones de "contraparte" de la Institución, quienes deberán ser preferiblemente profesionales del Área de TI y del área usuaria.

6. El Área de TI estará pendiente que las empresas contratadas para el desarrollo de sistemas de información, brinden la capacitación a sus funcionarios en administración, uso y mantenimiento del nuevo sistema de información, para minimizar la dependencia que se genere del MAG hacia la empresa.

7. Los sistemas de información desarrollados por empresas externas, deberán ser entregados por éstas, de manera formal y debidamente documentados, incluyendo en dicha documentación al menos: el Manual técnico del sistema de información y el manual de los usuarios.

8. Los programas desarrollados o adquiridos externamente serán de uso exclusivo del MAG, y no se permite el uso para funciones que no correspondan a las operaciones normales del MAG.

9. En general para el desarrollo de sistemas "in house" o "outsorcing", "todas las dependencias del MAG, deben armonizar sus procedimientos de captura y registro de información referente a Establecimientos y Actividades Agropecuarias y en particular a Unidades de Producción, de acuerdo con el marco conceptual y el modelo de clasificación que se define para el Sistema Integrado de Registro de Establecimientos Agropecuarios (SIREA)" DIRECTRIZ DM-574-09

Políticas sobre mantenimiento de sistemas de información

1. Será considerado como mantenimiento de sistemas de información todas las acciones que impliquen modificaciones, correcciones, mejoras o adiciones a los sistemas de información, que soliciten los usuarios de cualquier dependencia del Ministerio.

2. El personal del Área de TI será la encargada de dar el mantenimiento ordinario a los sistemas de información que se desarrollen en el Ministerio.

3. El Área de TI definirá el procedimiento y las formalidades necesarias que orienten la forma en que serán desarrolladas las actividades de mantenimiento de sistemas de información.

Políticas relativas a bases de datos.

Políticas para la creación de bases de datos

1. El Área de TI será la encargada de diseñar física y lógicamente las bases de datos, que utilizarán los sistemas de información que se desarrollen internamente.

2. El Área de TI permitirá la creación de bases de datos a empresas contratadas para este fin o para el desarrollo de sistemas de información, siempre que entreguen, en forma completa, toda la documentación técnica de dichas bases de datos que permita su fácil comprensión.

3. En la creación de nuevas bases de datos se deberá generar la documentación necesaria y suficiente, que permita comprender su estructura física y lógica, así como su contenido.

4. En la definición de nomenclatura para las bases de datos, debe respetarse el Manual de Estándares correspondiente elaborado por el Área de TI.

5. El Área de TI hará uso de una herramienta para el modelaje de datos, creación y generación de base de datos, para lo cual debe adquirirse la respectiva licencia y la capacitación para su manejo.

Políticas para la migración de información de bases de datos

1. Toda migración de base de datos deberá ser realizada por personal técnico capacitado interno o personal externo, el cual deberá ser supervisado por un profesional del Área de TI.

2. Antes de cualquier proceso de migración se deberán realizar los respaldos respectivos, así como realizar previamente una prueba de la migración en un servidor de pruebas, para garantizar que el proceso de migración funciona correctamente.

3. En las actividades de migración de información a bases de datos, se deberá seguir el procedimiento definido por el Área de TI para evitar atrasos y complicaciones, así como dejar documentado en una bitácora todo lo realizado para futuras migraciones.

Políticas sobre instalación de bases de datos

1. Toda instalación de base de datos deberá ser realizada por el personal técnico capacitado del Área de TI, o en su defecto por personal de empresas contratadas para estos efectos, bajo la supervisión de Área de TI.

2. Antes de cualquier instalación deberá realizarse los respaldos respectivos para evitar accidentes y garantizar la recuperación de la base de datos.

3. Para la instalación se deberá seguir el procedimiento definido por el Área de TI para prevenir que se den atrasos o complicaciones, así como dejar documentado en una bitácora todo lo realizado.

Políticas sobre administración y mantenimiento de bases de datos

1. Todo mantenimiento a las bases de datos deberá ser realizada por personal técnico capacitado interno o externo, quienes deberán ser supervisados por el profesional responsable de esa tarea del Área de TI.

2. Antes de cualquier proceso de mantenimiento a la base de datos, se deberán realizar los respaldos respectivos para estar prevenidos contra cualquier accidente que se pudiera presentar.

3. Todo cambio o ajuste hecho en el proceso de mantenimiento, se deberá dejar documentado en una bitácora para efectos de control y seguimiento.

Políticas de tiempos de almacenamiento de información en bases de datos

1. El Área de TI deberá garantizar la conservación permanente de toda la información almacenada en las bases de datos de los servidores, que esté directa o indirectamente relacionada con las actividades del Ministerio.

2. La información deberá ser conservada durante el período que se defina en la tabla de plazos de conservación, labor en la cual tendrá concurso el Archivo Central de la Institución.

Políticas de seguridad en bases de datos

1. Todo acceso a las bases de datos del Ministerio deberá contar con los mecanismos adecuados y controlados, que garanticen su seguridad, su integridad y la confidencialidad de la información almacenada.

2. Toda transacción que se ejecute en las bases de datos, dejará las pistas adecuadas de auditoría, para poder ejercer un control adecuado, de todas las modificaciones que se hagan en éstas mediante el uso de bitácoras.

3. Deberán de mantenerse y aplicarse sistemas de respaldos para todas las bases de datos del Ministerio, con el fin de garantizar su conservación.

4. Deberán existir planes de recuperación de la información de las bases de datos, para garantizar la continuidad del servicio que se presta por medio de los sistemas de información.

Políticas relativas a redes y telecomunicaciones

Políticas para el uso de las redes de datos

1. El Área de TI será la dependencia responsable de la administración y uso de la red interna de datos.

2. El Área de TI garantizará el acceso controlado en la red interna de datos a los funcionarios del Ministerio que así lo requieran.

3. Los usuarios accederán a la red de datos por medio de un código de acceso que les asignará el administrador de la red.

4. El código de acceso a redes que se asigne será único y exclusivo para cada usuario, el cual será responsable por su uso.

5. Todas las operaciones que se efectúen por medio de las redes internas serán responsabilidad única del usuario al que se le asignó el código relacionado con las mismas.

6. El Área de TI monitoreará periódicamente los accesos a la red interna mediante herramientas de seguridad y administración.

7. No es permitido a ningún funcionario, excepto a los técnicos de redes, manipular los componentes activos de la red (switches, routers, dispositivos inalámbricos, cableado, etc.).

8. No se permitirá la instalación de puntos de acceso de **redes inalámbricas** con conexión a la red del Ministerio sin la debida información y autorización del Área de TI. En caso de detección de un punto de acceso no autorizado se procederá a su inmediata desconexión de la red Institucional.

9. En cualquier caso, nunca se podrá proporcionar acceso permanente a terceros mediante redes inalámbricas conectadas al Ministerio; este hecho será especialmente considerado como infracción a las políticas del MAG.

10. Todos los equipos que se conectan a la red deben recibir una dirección IP y un nombre de red asignados por el Área de TI, además de ser incluidos en el registro correspondiente, junto con la identidad y los datos de contacto del responsable del equipo.

11. No está permitida la conexión de equipos con nombres o direcciones no registrados.

12. No se permite el empleo de mecanismos para la manipulación de direcciones de red o cualquier otro uso que pueda afectar a la topología o a la estructura lógica de la red.

13. El Área de TI solamente prestará apoyo a los equipos conectados a la red institucional; a estos efectos, se consideran conectados a la red del MAG los equipos que accedan a la misma de forma remota a través de los medios proporcionados por el Área de TI.

14. Los equipos electrónicos de gestión e infraestructura de la red del MAG serán instalados, configurados y mantenidos exclusivamente por el Área de TI. Ningún usuario está autorizado a utilizar analizadores del tráfico que circula por la red del Ministerio.

15. Igualmente está prohibido utilizar herramientas de rastreo de puertos o que permitan detectar vulnerabilidades. El uso de estas herramientas sólo está permitido a los administradores de la red y bajo situaciones especiales (incidentes de seguridad, denuncias de usuarios, etc.) que lo justifiquen.

Políticas relativas al servicio de Internet y correo electrónico

Políticas para el acceso a servicios de Internet y correo electrónico

1. Los servicios de Internet y correo electrónico serán administrados por el Área de TI.

2. Para la comunicación oficial del Ministerio debe utilizarse la cuenta de correo institucional, en la medida de las posibilidades.

3. El acceso a los servicios de Internet y correo electrónico estarán disponibles para todos los usuarios del Ministerio, si las condiciones de infraestructura tecnológica y administrativa lo permiten.

4. El uso de los servicios de Internet y correo electrónico deberá ser exclusivamente para apoyar y mejorar la calidad de las funciones administrativas y técnicas.

5. El Área de TI asignará las cuentas de correo de acuerdo a las licencias disponibles. Se asignará con prioridad:

    - Una cuenta para las direcciones o departamento para ser usada en forma general por los funcionarios. Esto incluye una cuenta para las direcciones regionales.

    - Una cuenta para el director, jefe departamental o persona responsable a nivel personal.

    - Funcionarios que por razones muy fundamentadas por el director, requieren de una cuenta personalizada.

- Proyectos que requieren una cuenta particular por razones especiales.

- Todas las licencias deben ser presupuestadas por el usuario en su respectivo CAP.

6. No está permitido facilitar u ofrecer las cuentas de correo a terceras personas.

7. El servidor principal de correo electrónico debe mantener actualizada la herramienta de detección de virus para los correos entrantes y salientes.

8. Se prohíbe a los empleados formar parte de cadenas de mensajes o SPAM, ya que esto contribuye a la saturación de las redes de telecomunicación y facilita la divulgación de su cuenta de correo y la proliferación de virus en la red.

9. Se prohíbe a los funcionarios que tengan acceso al servicio de correo electrónico abrir mensajes de procedencia desconocida.

10. El funcionario que tenga acceso a servicios de correo electrónico debe evitar divulgar su cuenta a personas o entes desconocidos.

11. Ningún equipo que esté designado como servidor debe tener asociada una cuenta de correo electrónica.

12. Los mensajes de correo electrónico deben ser considerados como documentos formales y deben respetar todos los lineamientos referentes al uso inapropiado del lenguaje.

13. Los funcionarios deben realizar revisiones periódicas de los mensajes almacenados con el fin de no mantener información innecesaria.

14. La jefatura inmediata de los funcionarios deberá notificar al Área de TI cuando se deba cerrar o inhabilitar una cuenta de correo electrónico.

15. El usuario debe atender a los avisos de actualización automática del programa de detección de virus e informar al Área de TI, cuando la actualización no se realice satisfactoriamente.

16. Los valores de seguridad, de aceptación de cookies y los certificados de los navegadores o browser no deberán ser cambiados, excepto por indicaciones del Área de TI.

17. Está prohibida la utilización abusiva del correo electrónico y de las listas de distribución incluyendo la realización de prácticas tales como:

    - En caso de que fuera necesario un envío masivo se recomienda usar las listas de distribución o usar el campo de "copia oculta" (Bcc ó Cco) para poner la lista de destinatarios, o bien ponerse en contacto con el Área de TI.

    - Actividades comerciales privadas.

- Propagación de cartas encadenadas o participación en esquemas piramidales o actividades similares.

- El insulto, la amenaza o la difamación a cualquier persona.

- Suscribirse a periódicos, revistas, semanarios, buscadores de parejas, chats; ni a ningún otro tipo de actividades o boletines electrónicos que no sea el estrictamente relacionado con el área profesional de trabajo del funcionario.

- Descargar archivos de música, programas, videos, pornografía y cualquier otro tipo de información que no guarde estricta relación con el área profesional del funcionario. El Área de TI procurará tomar las previsiones del caso para que se bloquee por medio de software especializado, el acceso no autorizado a los servicios antes mencionados.

Políticas relativas al hardware

Políticas de responsabilidad y mantenimiento del hardware instalado

1. El hardware que se encuentra en el área de servidores y los armarios de comunicaciones es responsabilidad directa del personal del Área de TI, que tendrá que velar por su uso y cuidado.

2. Los otros equipos de cómputo quedan bajo la responsabilidad del usuario al que se asignen. Estos tendrán la obligación de cuidarlos, mantenerlos limpios y velar por su buen funcionamiento. En el caso de existir algún problema con el equipo deberán de reportarlo inmediatamente al Área de TI para que se proceda a su revisión.

3. Los usuarios tienen el deber de informar sobre el rendimiento de cada equipo, para que sea valorado y de ser necesario mejorado.

4. Las computadoras, impresoras y otros dispositivos del MAG serán sometidos a un mantenimiento preventivo por lo menos una vez al año, incluyendo los equipos que tengan vigente la garantía, con la finalidad de aumentar su vida útil, mejorar el rendimiento, detectar a tiempo posibles causas de fallas y determinar su necesidad de mejora o reemplazo.

5. El mantenimiento preventivo del equipo de telecomunicaciones se realizará por lo menos una vez al año, por el Encargado de Soporte Técnico, quien deberá establecer un programa de trabajo y llevar los respectivos controles.

6. Es responsabilidad del Área de TI hacer cumplir las garantías respectivas de cada uno de los equipos; para tal razón se deberán respetar los sellos de garantía que vienen adheridos a los equipos, y velar porque el usuario final no los despegue.

7. Es responsabilidad del Área de TI valorar la necesidad de sustituir algún equipo cuando ya éste no garantice la funcionalidad y operatividad adecuada.

Políticas relativas al software

Políticas sobre el uso de licencias de software

1. Según Decreto Ejecutivo Nº 30151-J del 01 de febrero de 2002, en su Artículo 1 se indica: "Se ordena que todo el Gobierno Central se proponga diligentemente prevenir y combatir el uso ilegal de programas de cómputo, con el fin de cumplir con las disposiciones sobre derechos de autor que establece la Ley Nº 6683 y sus reformas…" Así las cosas, los programas que se utilizarán en los equipos del Ministerio tendrán licencia, de lo contrario es ilegal y debe eliminarse de inmediato.

2. El Área de TI dará la asesoría necesaria a los funcionarios del MAG en el tema de licencias. Los usuarios deben asegurarse que disponen de las licencias adecuadas al uso que hagan del respectivo software, ya sea mediante licencias adquiridas de forma centralizada por el Ministerio (para software de uso común), por la adquisición individual de las correspondientes licencias, o bien por el uso de software libre. De no ser así, la responsabilidad recaerá totalmente sobre el usuario.

3. El Área de TI llevará un registro actualizado de los equipos y las licencias vigentes en el Ministerio para informar a la Administración a este respecto.

4. El Área de TI dará de baja todos los equipos que estén al margen de la ley, en lo que respecta al cumplimiento de la Ley de Derechos de Autor, lo cual se hará en un plazo razonable, que será comunicado al responsable de la dirección o departamento respectivo.

5. La Dirección Administrativa y Financiera gestionará mediante los presupuestos ordinarios y extraordinarios con cargo a los Centros de Asignación Presupuestaria, la compra de licencias de "software" con la finalidad de que siempre el Ministerio se mantenga al día con el uso de licencias. Esta función la hará mediante el concurso y petición del Área de TI.

6. El Área de TI removerá cualquier programa de las máquinas cuando no exista licencia, sin responsabilidad para ésta de los problemas que ocasione directa o indirectamente. Llevará un registro de los programas instalados ilegalmente, para que, ante la reincidencia de mantener programas instalados en forma ilegal, se proceda a reportar el asunto al Departamento de Recursos Humanos o ante las autoridades superiores, para aplicar la sanción que corresponda por desobediencia según el Reglamento Interno del MAG, lo cual debe tipificarse como falta grave. Para ello, el Área de TI cuidará de no violentar el derecho a la privacidad de las personas, solicitando previamente la autorización al usuario para proceder con la remoción del programa ilegal.

7. Las licencias básicas para todo equipo son: el Sistema Operativo ("Windows"), paquete de Oficina ("Office") y el acceso a la red interna (CAL), así como el respectivo antivirus.

8. Los medios de instalación originales serán custodiados por el Área de TI.

Políticas para la instalación de Software

1. El Área de TI es la responsable de la instalación de los programas de software en cada una de las computadoras del Ministerio.

2. Queda completamente prohibido que los usuarios realicen instalaciones de cualquier tipo de software en sus computadoras. De requerir un software específico debe solicitarse al Área de TI para que se valore la necesidad de su instalación.

3. Todo software que se instale en las computadoras del MAG deberá contar con su respectiva licencia y su instalación deberá ser autorizada por la jefatura del Área de TI.

4. Queda prohibida la instalación del software adquirido por el MAG en equipos que no sean de su propiedad.

5. El personal del Área de TI deberá mantener un inventario de software y programas instalados en cada una de las computadoras. Este inventario deberá revisarse y actualizarse una vez al año.

6. Para la administración y el manejo seguro de la información que se almacena en los computadores del Ministerio y para evitar su utilización por personas no autorizadas, se utilizarán los sistemas operativos que ofrezcan mayor seguridad.

Políticas relativas a seguridad

Políticas generales de seguridad de acceso

1. El Área de TI es la responsable de la seguridad de acceso a los sistemas operativos, sistemas de información, bases de datos, y redes que operen en los equipos de cómputo del Ministerio.

2. El Área de TI establecerá los mecanismos adecuados para el control, verificación y monitoreo de cambios en passwords, número de sesiones activas, seguridad lógica, física de todas las actividades relacionadas con el uso de tecnologías de información.

3. Para evitar situaciones de peligro para el MAG, se desactivarán o bloquearán las cuentas de usuario a aquellas personas que estén en vacaciones, con permisos o incapacidades mayores a una semana, para lo cual debe informar la jefatura respectiva.

4. En caso de despido de un funcionario, el permiso de acceso deberá desactivarse o bloquearse previamente a la notificación de la persona sobre la situación.

5. En todos los casos, el Departamento de Recursos Humanos debe notificar al Área de TI para la desactivación de la cuenta de algún usuario.

6. El administrador de los sistemas operativos, sistemas de información, bases de datos o redes asignará la clave de acceso al usuario.

7. Las jefaturas deben solicitar formalmente la apertura, modificación o cierre de las cuentas de usuario. Cuando sea solicitada una apertura, deben indicar el perfil que se le debe asignar.

8. El encargado de seguridad informática no cambiará ninguna clave de acceso, si no es por solicitud expresa de su dueño. En caso de ser necesario y a solicitud de la jefatura se congelarán los accesos de un usuario específico.

9. El Área de TI establecerá un procedimiento especial para la creación de perfiles y roles de usuario, tomando en consideración los criterios de las jefaturas departamentales, las recomendaciones de control interno y las políticas de seguridad establecidas en este documento de políticas.

Políticas de seguridad de acceso a sistemas operativos

1. La activación y desactivación de usuarios de sistemas operativos estará a cargo del personal técnico del Área de TI.

2. En la activación de usuarios de sistemas operativos, se crearán identificadores de usuario utilizando el estándar de la letra inicial del nombre seguida del primer apellido.

3. Siempre que los sistemas operativos utilizados lo permitan, deberá controlarse el número de intentos de ingreso fallidos. Luego de tres intentos, deberá bloquearse la cuenta del usuario y no permitir su ingreso al sistema. La cuenta debe estar bloqueada por 30 minutos y el administrador de seguridad podría desbloquearla antes por solicitud del usuario involucrado.

4. En el caso que el sistema operativo lo permita, se deberán implementar las bitácoras de seguimiento a los accesos, donde se registren los ingresos al sistema y los intentos fallidos.

5. El responsable por la seguridad del Área de TI revisará periódicamente esta bitácora y reportará a su Jefatura cualquier anomalía que encuentre. La información de esta bitácora debe estar disponible para cualquier autoridad que lo requiera.

Políticas de seguridad de acceso a sistemas de información

1. La activación y desactivación de usuarios de los sistemas de información estará a cargo del personal técnico del Área de TI.

2. El administrador del sistema de información asignará la clave de acceso al usuario.

3. Para otorgarle acceso a las diferentes aplicaciones del sistema, de acuerdo con las funciones que debe desempeñar el usuario, la jefatura correspondiente deberá hacer la solicitud formal al encargado de seguridad.

4. En toda transacción que se realice en el sistema se deberá grabar el nombre del usuario, la fecha y la hora en que se realizó.

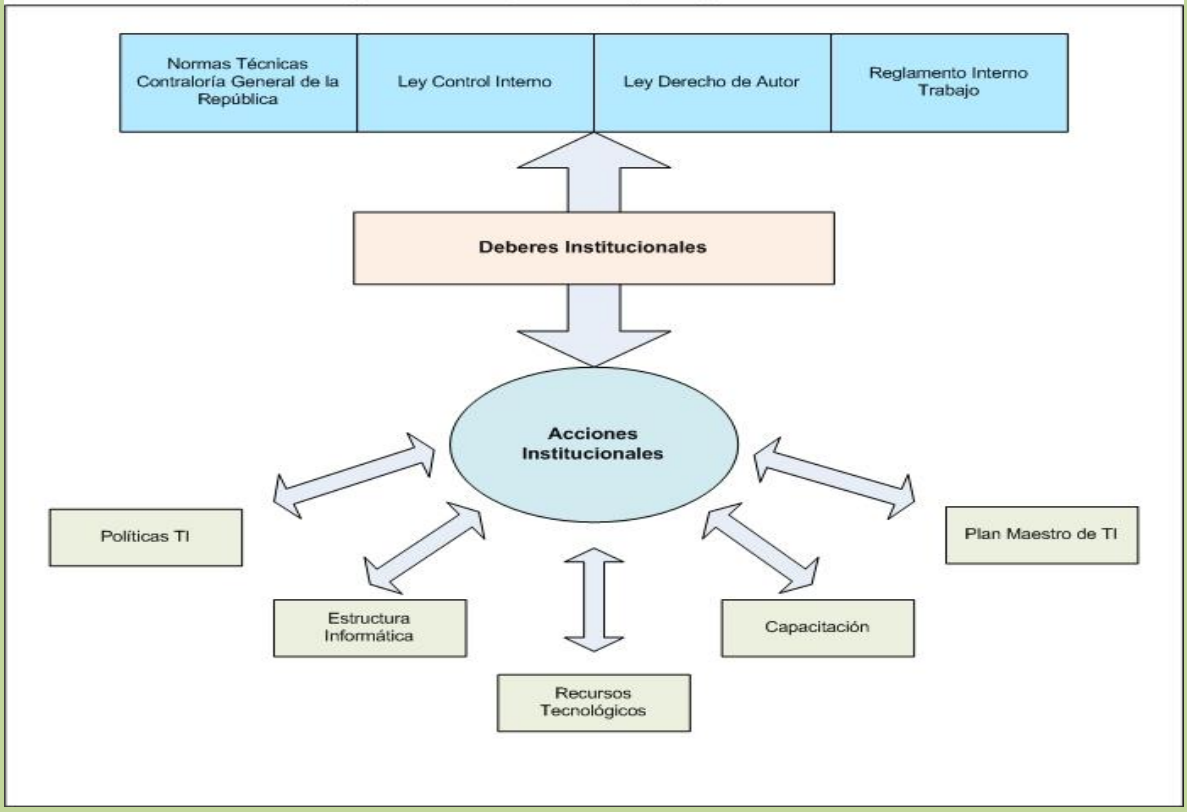
Políticas de seguridad de acceso a bases de datos

1. El Área de TI velará porque toda base de datos que sea instalada, cuente con los controles de seguridad que garanticen la confiabilidad de la información.

2. Los códigos de acceso de los usuarios de las bases de datos utilizarán el estándar indicado en el respectivo de base de datos.

3. El administrador de la base de datos asignará la clave de acceso al usuario.

Figura 2: Estrategia de trabajo. Grupo de estudio.



4. El sistema de seguridad deberá contemplar el bloqueo de claves luego de tres intentos fallidos de acceso, cuando la base de datos lo permita.

5. El acceso a la información de las bases de datos deberá controlarse por medio de roles y nunca se otorgarán privilegios de acceso a tablas u objetos directamente a un usuario.

6. El Área de TI implementará controles para que todos los respaldos de información, se encuentren almacenados en medios externos como cintas de respaldo, CD´s o DVD´s.

7. Los diferentes centros de datos del MAG se respaldarán mutuamente en sus servidores y los medios físicos se resguardarán en los diferentes sitios.

Políticas de seguridad de acceso a redes

1. El administrador de redes asignará las claves de acceso a los usuarios, además procederá conforme con la activación y desactivación de usuarios de las redes del Ministerio.

2. Para la utilización de las redes de datos, los nombres de usuario para las mismas se crearán siguiendo el esquema de letra inicial del nombre seguido por el primer apellido.

3. Para otorgarle acceso a las redes de datos, de acuerdo con las funciones que debe desempeñar el usuario, la jefatura correspondiente deberá enviar la solicitud formal al Área de TI.

Políticas de ubicación de los centros de procesamiento de información y comunicaciones

1. Los centros de procesamiento de información y comunicaciones deberán estar ubicados dentro del edificio del MAG, a menos que se disponga instalarlos en sitios externos especializados con la seguridad necesaria.

2. Debe estar completamente cerrada y con una única puerta de acceso, la cual deberá permanecer siempre cerrada. Las llaves de acceso estarán en custodia del personal del Área de TI y una copia de ellas estará en el Departamento de Bienes y Servicios.

3. Todo el cableado eléctrico que sea utilizado en los equipos de los centros de procesamiento de información y comunicaciones deberá ser totalmente independiente al cableado normal del edificio.

4. Para efectos de cableado eléctrico y de datos se utilizarán las normas de cableado que se fundamenten en las mejores prácticas utilizadas en el mercado.

Políticas de ambiente de los centros de procesamiento de información y comunicaciones

1. El área asignada para los centros de procesamiento de información y comunicaciones debe estar dotada con las condiciones ambientales necesarias para garantizar un entorno físico conveniente para su funcionamiento.

2. Este espacio de los centros de procesamiento de información y comunicaciones deberá estar climatizado permanentemente a una temperatura que se encuentre entre los 18º y 20º para garantizar el mejor rendimiento de los componentes electrónicos y alargar la vida útil de los mismos.

3. El MAG procurará la entrega de sus desechos tecnológicos a empresas recicladoras que cumplan con las normativas vigentes de protección al medio ambiente

Políticas sobre "Responsabilidad de funcionarios por uso de los equipos"

1. Los funcionarios del MAG usarán el equipo de cómputo en labores exclusivamente de trabajo y serán responsables por el uso adecuado de las herramientas (como son el PC, los periféricos y los programas instalados).

2. El usuario del equipo mantendrá el equipo en un estado razonable de limpieza, para lo cual gestionará con su jefatura directa, los aditamentos necesarios (líquidos, franela, etc.) para el mantenimiento del mismo. No deberá consumir ni preparar alimentos en la mesa destinada para el computador, para evitar derrame de los mismos sobre los equipos, que pueden ocasionar trastornos en su operación.

3. El usuario del equipo es responsable de acatar las disposiciones del Área de TI, en cuanto a los programas que puede tener su equipo. Es responsable directo si es detectado en su equipo, un software no autorizado, ilegal o "pirateado", por lo cual debe responder ante las autoridades del Ministerio o quien corresponda.

4. Es prohibido a todos los funcionarios de cualquier nivel, utilizar el equipo de la oficina para bajar de internet ni ejecutar: juegos, música, videos, fotos, "screensavers" y todo archivo que provenga de fuentes no confiables; así como todo tipo de material pornográfico, que atenta contra el trabajo o el honor de las personas.

5. Los funcionarios deben velar porque su equipo tenga protección contra fallas de energía eléctrica o reducciones de voltaje. Para ello, deben prevenir a las jefaturas para que intercedan ante la Administración, mediante la correcta planificación presupuestaria para procurar estos dispositivos de seguridad.

6. Los usuarios deben utilizar antivirus actualizados para revisar todo medio antes de ingresarlo al equipo, con el propósito de evitar que éste sea contagiado al igual que la red institucional. Si no tienen instalado los antivirus tienen la responsabilidad de notificarlo al Área de TI por escrito.

7. Los usuarios de equipos deben procurarse los conocimientos imprescindibles para el manejo de sus programas, así como realizar copias de seguridad de los datos que considere relevante, lo cual puede resultar verdaderamente importante cuando los discos duros colapsen por cualquier razón.

8. Todo usuario es responsable de mantener respaldos de la información de acuerdo a sus necesidades. En caso de las aplicaciones cliente-servidor el responsable por los respaldos es el administrador de la red y si es del caso, el Administrador de la Base de Datos.

9. Por razones de seguridad se prohíbe el uso de mensajería instantánea, chat o similares a menos que se justifique el uso para lo cual debe solicitarse por la jefatura, manifestándose los cuidados y supervisión que ejercerá sobre su uso.

10. Está prohibido conectarse a Internet utilizando equipos diferentes a los que oficialmente se encuentren en servicio.

Glosario de términos utilizados

A continuación se presentan en orden alfabético una serie de términos que son utilizados en el presente reglamento:

Ambiente de Desarrollo:

Conjunto de software y hardware utilizado por personal del Área de desarrollo de software, en el cual se simula la operación normal de los sistemas con el fin de desarrollar nuevos requerimientos o pruebas a módulos existentes.

Ambiente de Producción:

Conjunto de software y hardware utilizado en el trabajo diario de la institución, donde se maneja la información real de la misma, el cual no es afectado por ningún proceso de prueba.

Base de Datos:

Conjunto de datos organizados de tal modo que permita obtener con rapidez diversos tipos de información.

BD:

Base de datos.

Browser:

Programa o aplicación informática que se usa para navegar por las redes informáticas y acceder a documentos, imágenes y demás información.

CD:

Siglas en inglés de Disco Compacto (Compact Disk), placa circular de material plástico donde se graba información por medio de láser codificado.

Centro de Procesamiento de Información y Comunicaciones:

Áreas de tecnologías de información en donde se encuentran los servidores, equipo de comunicación y UPS.

Chat:
Conversación interactiva en tiempo real, en Internet.

Cookies:

Archivo que se implanta en el disco duro del usuario por el sitio visitado en Internet, contiene información acerca del usuario.

Correo Spam:

Se utiliza este término para identificar todo aquel correo denominado como "Correo Basura" o correo no deseado.

Firewall:

Sistema diseñado para prevenir el acceso no autorizado a o desde una red privada, en general para prevenir intrusos desde Internet.

Hardware:

Conjunto de componentes que integran la parte material de una computadora, impresora o equipo de comunicación.

Incluir, modificar, consultar, eliminar, imprimir:

Transacciones que se realizan a las tablas de una base de datos, normalmente a través de los sistemas de información.

Internet:

Red informática de comunicación internacional que permite el intercambio de todo tipo de información entre sus usuarios. El nombre proviene del acrónimo de las palabras inglesas International Network (red internacional).

Migración de datos:

Proceso de pasar información de una base de datos a otra diferente, ajustándola a nuevas estructuras de datos.

Normativa:

Conjunto de normas aplicables a una determinada materia o actividad.

Parches:

Arreglo de un programa que agrega o cambia una pequeña parte del mismo.

Perfil de usuario:

Grupo de privilegios o roles de trabajo que se asignan a una persona, de acuerdo con las características que tenga su puesto con el fin de que pueda desempeñar sus funciones.

Rol:

Grupo de derechos o privilegios para el uso de recursos informáticos que asignan a uno o más usuarios, por ejemplo: derechos de lectura, escritura, modificación o borrado sobre una tabla de datos.

Recuperación:

Es la tarea que se lleva a cabo cuando es necesario volver al estado de la aplicación al momento del último respaldo, a partir de los datos de la última copia de seguridad realizada.

Respaldo:

Es la obtención de una copia de los datos en otro medio magnético, de tal modo que a partir de dicha copia es posible restaurar el sistema o la información.

Seguridad lógica:

Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

SI:

Sistema de información.

SO:

Sistema operativo.

Software:

Es un término genérico que designa al conjunto de programas de distinto tipo (sistema operativo y aplicaciones diversas) que hacen posible el funcionamiento y la operación del computador.

TI:

Tecnología de Información.

UPS:

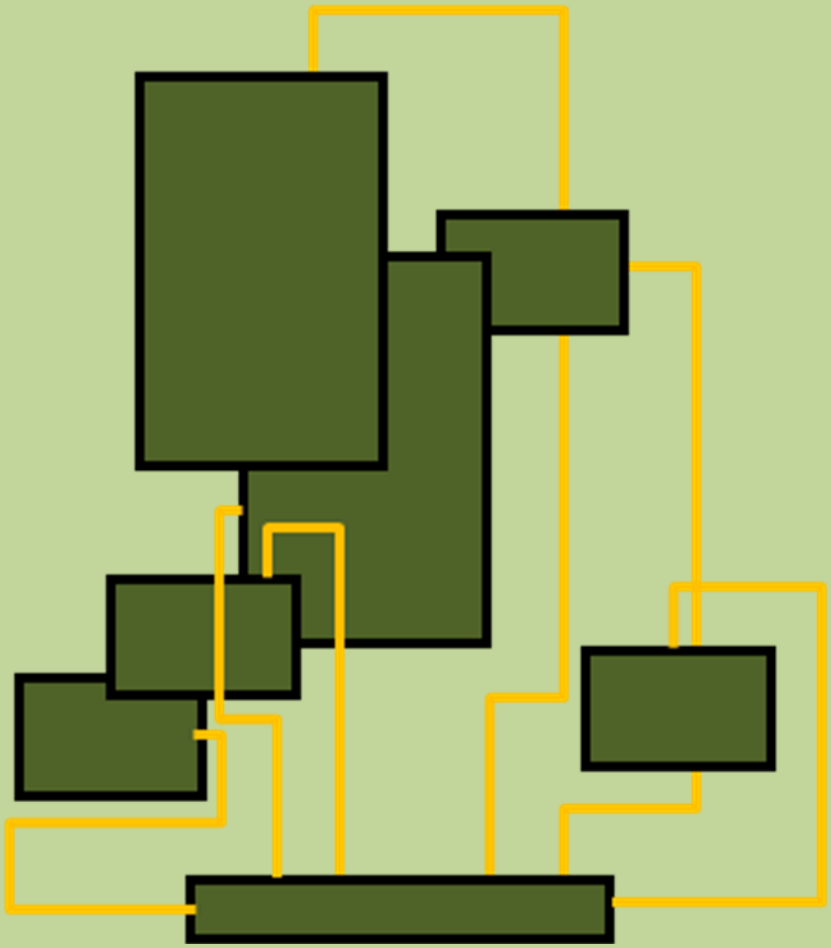
Abreviatura de "Uninterruptible Power Supply", aparato que suple corriente eléctrica al sistema en caso de apagones.

Virus:

Es un programa informático que se ejecuta en el ordenador sin previo aviso y que puede corromper el resto de los programas, archivos de datos e incluso el mismo sistema operativo.

MINISTERIO DE AGRICULTURA Y GANADERÍA

ÁREA DE TECNOLOGÍAS DE INFORMACIÓN



POLÍTICAS GENERALES SOBRE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

2009