MINISTERIO DE AGRICULTURA Y GANADERÍA
GOBIERNO DE EL SALVADOR

Centro Nacional de Tecnología Agropecuaria y Forestal Enrique Álvarez Córdova

GERENCIA ADMINISTRATIVA Y FINANCIERA

UNIDAD DE INFORMÁTICA

POLÍTICAS DE GESTIÓN INFORMÁTICA

SAN ANDRÉS **FEBRERO 2019**

DIRECTOR EJECUTIVO

INDICE

INTRODUCCIÓN

El Centro Nacional de Tecnología Agropecuaria y Forestal "Enrique Álvarez Córdova" (CENTA), con el propósito de optimizar el uso de los recursos informáticos y procurar su desarrollo en esta área, ha considerado necesario contar con lineamientos en temas específicos de la gestión informática; los cuales deberán ser de cumplimiento y aplicación por todo el personal usuario de dichos recursos.

En esta oportunidad se han elaborado Políticas Informáticas en áreas temáticas identificadas como básicas, para la operatividad actual del CENTA, las cuales podrán incrementarse, ampliarse o modificarse de acuerdo a su evolución y complejidad en tecnología de información con el objetivo que constituyan un instrumento de utilidad para administrar, optimizar y desarrollar la capacidad instalada de la entidad;

Las que ahora se aprueban mediante este instrumento se refieren a la administración de recursos, desarrollo informático, estandarización de software, manejo y uso de las comunicaciones, sistemas de información, seguridad y contingencia informática.

DIRECTOR EJECUTIVO

1. **Objetivo General**
   Establecer Políticas y Estándares de Gestión Informática a todo el personal del Centro Nacional de Tecnología Agropecuaria y Forestal "Enrique Álvarez Córdova", para que sea de conocimiento y cumplimiento en los recursos informáticos asignados.

2. **Alcance**
   El documento define Políticas y Estándares de Gestión Informática que deberán observar de manera obligatoria todos los usuarios para el buen uso del equipo de cómputo, aplicaciones y servicios informáticos del Centro Nacional de Tecnología Agropecuaria y Forestal "Enrique Álvarez Córdova".

3. **Base Legal**
   Reglamento de la Corte de Cuentas de la República de El Salvador y Normas Técnicas de Control Interno Específicas, publicado en Diario oficial No 103, tomo No. 371, de fecha 6 de junio del 2006.

1. POLÍTICA DE ADMINISTRACIÓN DE RECURSOS INFORMÁTICOS

Objetivo:

Su objetivo es hacer un uso óptimo de los recursos informáticos de la institución y protegerlos de deterioros o pérdidas a través de una administración adecuada.

Adquisición de Recursos Informáticos

1. La incorporación de cualquier equipo informático a la institución deberá notificarse a la Unidad de Informática inmediatamente, para su administración y registro correspondiente.

2. En la adquisición de computadoras, impresores, servidores, dispositivos de comunicación, etc, la Unidad de Informática emitirá periódicamente estándares de las especificaciones técnicas mínimas aceptables, a fin de maximizar la utilidad de la inversión,

3. En la adquisición de computadoras y servidores se deberá incluir el software necesario instalado con su licencia correspondiente.

4. En la adquisición de impresoras deberán corroborarse la disponibilidad en el mercado local de sus suministros (cartuchos, tóner, cables, etc.) y que su relación precio/rendimiento sea mayor, salvo casos excepcionales que se requiera calidad de impresión.

5. Previa a las adquisiciones de materiales informáticos, se deberá verificar que los requerimientos sean acorde a las especificaciones de los recursos informáticos existentes en la institución y a las necesidades de consumo de acuerdo a información histórica y volúmenes de trabajo vigentes.

6. En la adquisición de software, se procurará adquirir las últimas versiones liberadas de los productos seleccionados, salvo situaciones como falta de disponibilidad financiera o incompatibilidad con la mayoría de los equipos existentes.

7. Dependiendo de la cantidad de equipos en que se va a instalar la versión, se usan licencias individuales o de nivel corporativo, adhiriéndose a las normas y derechos de autor.

8. Todo producto de software que exista en la Institución debe ser legal, adquirido formalmente a un proveedor autorizado y con la documentación necesaria que garantice el buen uso del mismo.

9. Toda mejora y/o mantenimiento de la Infraestructura tecnológica (Redes) de la Institución debe estar acorde a los estándares establecidos y responder a las necesidades de la Institución.

Adquisición de Recursos Tecnológicos.

10. La Unidad de Informática deberá ser incluida como parte de la comisión, en cualquier proceso, en el que se encuentre inmerso equipo tecnológico (hardware y software), para su administración y registro correspondiente.

11. En la adquisición de equipo tecnológico debe considerarse capacitación para personal de la Unidad de informática, en cuanto uso, instalación y Configuración, para brindar el soporte técnico adecuado.

Asignación y Uso de los Recursos Informáticos:

12. Se deberá evaluar periódicamente y determinar las prioridades de uso de los equipos previo a que éstos sean asignados o para que sean reasignados.

13. Cuando se requiera cambiar a la persona responsable del equipo, el Área de Activos Fijos deberán realizar un inventario de los bienes que el usuario tenga asignados, con la finalidad de verificar que lo registrado sea igual a lo entregado. Una vez entregado el equipo informático al nuevo usuario, éste deberá firmar el formato de asignación.

14. La actualización de la información de los sistemas implantados en la institución es responsabilidad del Usuario respectivamente asignado.

15. Las cuentas de correo electrónico y/o Acceso a internet podrá asignarse o modificarse a los diferentes Usuarios de la Institución, a solicitud del Jefe inmediato con autorización de la Gerencia Administrativa y Financiera.

16. Las cuentas de correo electrónico y/o Acceso a internet podrá suspenderse o revocarse, sea por motivos de mal uso o a solicitud del Jefe inmediato.

17. Por ningún motivo debe usarse los servidores de red como estaciones de trabajo.

18. Los dispositivos de lectura podrán ser desactivados a todos aquellos usuarios que dentro de sus funciones no requiera el uso de estos.

Mantenimiento Preventivo y Correctivo de los Recursos Informáticos

19. La Unidad de Informática comunicará el programa de mantenimiento preventivo a las diferentes dependencias del CENTA; informando a los usuarios la fecha de visita de mantenimiento del equipo.

20. Antes de llevarse a cabo la actividad de mantenimiento, los usuarios deberán respaldar la información almacenada en la computadora.

21. Las oficinas deberán programar sus actividades de tal manera que el equipo esté disponible en la fecha programada para el mantenimiento.

Servicio de Soporte Técnico

22. Todas las solicitudes de soporte técnico deberán plantearse a la Unidad de Informática quién las recibirá y resolverá oportunamente.

23. Sólo se atenderán solicitudes que se refieran al software y hardware propiedad del CENTA, es decir que cuenten con el número de inventario correspondiente, exceptuando aquellos equipos que se encuentran documentados en proyectos, acuerdos, convenios, etc., donde el CENTA esté obligado a brindar el mantenimiento.

24. A través de las solicitudes de servicio se cuantificará el servicio prestado y permitirá establecer programas de capacitación y/o adiestramiento enfocados a áreas o temas deficitarios, sustitución de equipo, etc.

25. Los técnicos de la Unidad de Informática procederán a realizar la desinstalación de programas o recursos no adquiridos por la institución, para los cuales no exista licencia o autorización de uso válido para los fines institucionales.

2. POLÍTICA DE DESARROLLO INFORMÁTICO

Objetivo:

Esta política tiene como objetivo el disponer de lineamientos que contribuyan a realizar inversiones exitosas en beneficio del desarrollo tecnológico informático institucional.

1. Los equipos y dispositivos que se adquieran deberán contar con la garantía de línea del fabricante, con el software y documentación técnica correspondiente.

2. Todos aquellos equipos que son necesarios para el funcionamiento de algún sistema de misión crítica deberán contar con un contrato de servicio de soporte, una vez vencida la garantía.

3. Para la adquisición de computadoras, impresores y servidores se deberá observar que los mismos cubran como mínimo las especificaciones estándar establecidas.

4. Solamente se deben adquirir equipos integrados de fábrica (la totalidad de sus componentes) y cuyas marcas cuente con presencia y permanencia demostradas en el mercado nacional e internacional, y que cuenten con soporte local.

5. Los dispositivos de almacenamiento así como las interfaces de entrada/salida, deberán estar acordes con el estándar establecido.

6. Para la adquisición de software como: Sistemas Operativos, Bases de Datos, Lenguajes de Programación, Programas Integrados, Antivirus, Correo Electrónico, Control de Proyectos, Diseño Gráfico y Multimedia se deberá observar que los mismos cubran las especificaciones estándares establecidas.

7. Deberán adquirirse las últimas versiones liberadas del software seleccionado, y solo en determinados casos bajo situaciones específicas, la Unidad de Informática, podrá recomendar su adquisición en forma distinta.

8. Todo Software utilizado en la institución debe ser adquirido de forma legal, respetando la ley de Derechos de Autor y Propiedad Intelectual correspondientes.

9. Los proyectos de desarrollo y/o mantenimiento de sistemas de información de acuerdo a las necesidades de la institución pueden ejecutarse internamente o a través de la contratación de servicios.

10. Los sistemas de información desarrollados interna o externamente deben estar acorde a los estándares establecidos.

11. Todo Proyecto de desarrollo informático debe iniciar con la etapa de planificación, que nos determina el alcance, etapas, tiempo y recursos necesarios para su ejecución.

12. El personal informático debe tener una capacitación continua y permanente, para el uso eficiente de los recursos informáticos e implantación de nuevas tecnologías acorde a las necesidades de la Institución.

13. El personal no informático debe tener una capacitación constante sobre las tecnologías implantadas, para el buen uso y desarrollo de la Institución.

3. POLÍTICA DE SOFTWARE

Objetivo: Mediante esta política se pretende mantener en la institución software estándares que faciliten la operación, flujo de información y comunicación Institucional; mediante la adopción de software de mayor compatibilidad interna y de mayor uso en el mercado mundial.

Estandarización de Software

1. Las diferentes unidades del CENTA deberán contar con software estándar, para facilitar el flujo de información entre los usuarios.

2. El software será clasificado de la siguiente forma:
   a. ***Software básico:***
      a.1) Incluye el Sistema operativo: Es el conjunto de programas que controla las actividades operativas de cada computadora y de la red.

      a.2) Paquete de usuario final: Son aquellos mediante el cual de una manera sencilla elabora sus procesos, entre ellos están: hoja electrónica, procesador de texto, paquete para presentaciones, mensajería, antivirus, etc.

      a.3.) Paquetes Utilitarios: Son aquellos que realizan una función específica, los cuáles facilitan la manipulación y lectura de la

información, entre ellos están: lectura de videos, lectura de música, lectura de imágenes, archivos PDF, etc.

b. ***Software para desarrollo de sistemas:***
Es aquel utilizado para desarrollar aplicaciones o sistemas para satisfacer demandas específicas en el manejo de información, se incluye en esta categoría el lenguaje de programación y la base de datos.

Instalación de Software

3. La instalación será realizada por personal de la Unidad de Informática, haciendo los ajustes y pruebas necesarias a fin de lograr un funcionamiento adecuado de todos y cada uno de los paquetes instalados.

4. La Unidad de Informática tendrá la facultad de limitar el uso de alguna herramienta de software si ésta provoca incompatibilidad con los estándares fijados.

5. En caso de requerir instalar paquetería adicional autorizada en los equipos informáticos, deberá solicitarse a la Unidad Informática; el software será validado con el propósito de revisar que no contenga virus o sea producto de actos de piratería.

6. En caso de existir algún paquete de interés para las Dependencias del CENTA, éstas deberán comunicarlo a la Unidad de Informática, con el fin de realizar la evaluación técnica correspondiente y se consideren los medios para conseguirlo, o se sugieran alternativas para satisfacer la demanda.

7. En caso de que el usuario utilice paquetes no autorizados, se le hará responsable de los daños que esto pueda ocasionar dentro de su estación de trabajo o en la red.

8. Cuando la Unidad de Informática requiera la instalación de nuevas versiones de software, notificará oportunamente a los usuarios la fecha para realizar tal actividad.

9. La instalación de software no aprobado por la Unidad de Informática será responsabilidad del usuario que incurra en la falta, por lo que la pérdida de información, virus en el sistema o la red y cualquier otra resultante será atribuible exclusivamente a éste.

Software obtenido a través de Internet

10. Se considerarán dos categorías de software que se obtenga por este medio:

    a. **Shareware**: Es aquel que una persona o entidad física que lo desarrolló ha puesto a disposición del público para un período de prueba, al término del cual el usuario se compromete a pagar un cierto monto si desea seguir utilizándolo; caso contrario deberá eliminarlo de su equipo.

    b) **Freeware**: Es aquel que la persona o entidad que lo desarrolló ha puesto a disposición del público de manera gratuita, solicitando en ocasiones un donativo para seguir con los trabajos, que el usuario no está obligado a pagar.

11. Las licencias que se otorgan con este software determinan las condiciones para su uso, debiendo quedar claro para el usuario a que categoría corresponde el programa obtenido, para proceder conforme al marco que se estipule.

12. El usuario deberá notificar a la Unidad de Informática, la existencia de este software, en caso que decida utilizarlo por un período prolongado, incluyendo el nombre, características y funciones del programa, además del motivo para su utilización.

13. La falta de conocimiento de la existencia de dicho software por parte de la Unidad de Informática será responsabilidad del usuario en caso de la realización de una auditoria informática.

4. POLÍTICA DE COMUNICACIONES

Objetivo:

Regular el uso de los servicios de Redes, Correo Electrónico y el acceso a Internet, para lo cual se emiten los siguientes lineamientos para todo el personal que utilice los recursos de la Red.

De Estándares Aplicables en la Instalación de Redes de Datos.

1. Se deberá etiquetar el cableado, las extensiones y los tableros de distribución eléctrica.

2. Se deberá evitar los cableados sueltos o dispersos, éstos deberán entubarse en el caso de los tendidos horizontales no vistos, en el caso de los tendidos horizontales o verticales vistos deben colocarse canaletas adecuadas.

3. Todas las conducciones de comunicaciones deberán separarse un mínimo de 30 cm. de las conducciones eléctricas con menos de 5Kva y fluorescentes. Para líneas de más de 5Kva y transformadores las distancias serán de 60 cm. y 100 cm. respectivamente.

4. Para equipos informáticos es recomendable disponer de circuitos alternos y tableros de distribución eléctrica independientes a cualquier otra conexión.

5. Previo a la instalación de equipos informáticos, es necesario realizar cálculos de la carga eléctrica requerida en la instalación, de los tableros de distribución, así como de los circuitos y conexiones que deben soportar la carga adicional proyectada.

De Uso de Correo Electrónico

6. Herramienta para la comunicación entre personal técnico y administrativo del CENTA y personas relacionadas con las labores desempeñadas en el ámbito nacional e internacional

7. Emplear el correo electrónico para sustituir el uso del teléfono y del fax en la mayor medida posible.

8. Comprimir los archivos anexos (por ejemplo, con el WinZip) cuando éstos se requieran, para disminuir las exigencias técnicas para su transmisión.

9. Verificar que los mensajes que se reciban o se envíen NO incluyan virus, para lo cual su programa antivirus deberá estar activo y mantenerse actualizado a través de la Unidad Informática del CENTA.

10. Liberar espacio en el buzón personal de correo, copiando los mensajes a su computadora personal o bien eliminando los que ya no sean necesarios.

11. El usuario debe respaldar en cualquier dispositivo externo la información que se recibe por correo en forma periódica y eliminar toda aquella información que ya no es pertinente.

12. Si se envía un mensaje dirigido a varias personas, procurar que las direcciones no vayan abiertas para ser conocidas por todos, empleando para ello la línea de "Con Copia Oculta" (CCO).

13. No abrir correos cuyo remitente sea desconocido o cuyo asunto le resulte sospechoso

14. Todos los usuarios tienen derecho a la privacidad del correo electrónico.

De Uso de Internet

El CENTA proporciona el servicio de Internet y los equipos de tecnología de información a los usuarios de la red, con el propósito de fomentar la calidad de sus procesos tecnológicos y administrativos. Y aunque posee una infraestructura adecuada para el acceso a la red mundial, se requiere un uso adecuado para evitar que los canales se saturen. Esto mejorará los tiempos de acceso a la información.

Por ello, los usuarios de Internet deberán observar las siguientes medidas en su operación:

15. El uso de los Servicios de Internet deberá ser, exclusivamente, para apoyar y mejorar la calidad de sus funciones técnicas o administrativas.

16. El CENTA es la propietaria de los equipos y la información que en ellos se maneja, por lo tanto, podrá monitorear en cualquier momento el uso adecuado.

17. Proteger sus recursos significa guardar el secreto de su *password*, no prestar su clave de usuario bajo ninguna circunstancia

De las Informaciones Contenidas en la Red de Internet:

18. El CENTA no controla, ni es responsable del contenido y veracidad de las informaciones obtenidas o recibidas a través de la red de Internet. El CENTA no se hace responsable por la exactitud o calidad de la información obtenida por este medio.

19. Los usuarios de Internet del CENTA son responsables de reportar inmediatamente a la Unidad de Informática (vía electrónica, telefónica o por escrito) cualquier situación en la red que pueda comprometer la estabilidad o seguridad del servicio de cualquier forma, así como cualquier violación a esta política.

20. Los equipos que proporcionan el servicio de Internet debe estar debidamente protegido con un UPS, y es responsabilidad de la jefatura de las diferentes dependencias de la Institución donde estos se encuentren, que mantengan las condiciones adecuadas de conexión para su buen funcionamiento.

21. Los usuarios que tienen asignadas USB inalámbricas, son responsables del cuido y uso adecuado de estos dispositivos, por lo que deben responder en caso de hurto, robo o pérdida.

De Uso de Página WEB

22. Los usuarios que tienen los derechos para la actualización de la página web, deben realizar los procedimientos conforme el manual de usuario de la página web.

23. Es responsabilidad del usuario autorizado informar a la Unidad de Informática a la mayor brevedad, algún daño ocasionado a la página web por mala manipulación de la aplicación de administración de la página web.

24. En todo momento, el usuario es el responsable único y final de mantener en secreto las claves o passwords asignadas, con los cuáles tenga acceso a la aplicación de administración de la página web.

25. El responsable del contenido, calidad y actualidad de los datos publicados en la página web es la persona encargada del área, así dicha información sea obtenida e incorporada por sus colaboradores.

26. La División de comunicaciones es el ente encargado y responsable de revisar la redacción de la información que se publica en la página web.

5. POLÍTICA DE SISTEMAS DE INFORMACIÓN

Objetivo:

Estandarizar los lineamientos básicos que guíen de manera ordenada y sistemática, todos los esfuerzos requeridos para desarrollar, mantener y actualizar Sistemas de Información.

1. Las fases o Ciclo de Vida a considerar en la ejecución de todo proyecto de desarrollo de sistemas de información, deben ser: Especificación de los requerimientos del Usuario, Análisis, Diseño, Desarrollo, Pruebas y Validación, Entrega e Instalación y Puesta en Marcha del Sistema de Información.

2. En el desarrollo y/o mantenimiento de un Sistema de Información debe considerarse como reinventar un proceso ya existente, para hacerlo más eficiente, ágil y oportuno, aprovechando el cambio tecnológico que se dará y aprovechando las facilidades que, en la actualidad, brinda la tecnología.

3. El analista debe entender de una forma total y clara los requerimientos funcionales para satisfacer las necesidades de los Usuarios. Estos deberán ser establecidos con precisión y válidos durante la aceptación del proyecto. Los

requerimientos del usuario deben de ser por escrito y debidamente documentados.

4. Cuando el mantenimiento de un Sistema de Información es requerido por el usuario, el responsable del sistema de información establecerá y mantendrá procedimientos para verificar que tales actividades llenan los requerimientos específicos de mantenimiento.

5. Todo Sistema de Información debe contar con bitácoras en sus operaciones, con el fin de permitir llevar un control de la información que es consultada, actualizada o borrada.

6. El responsable del contenido, calidad y actualidad de los datos de los Sistemas de Información es la persona encargada del área, así dicha información sea obtenida e incorporada por sus colaboradores.

6. POLÍTICA DE SEGURIDAD INFORMÁTICA

Objetivo

Dar protección a los recursos informáticos vitales de la Institución, como son los equipos, software, las bases de datos, los datos e infraestructura tecnológica que permiten realizar las operaciones diarias de la misma.

Sobre el Uso de Claves o passwords

Es necesario fomentar una cultura de confidencialidad de claves o passwords, ya que es un mecanismo que nos permite identificar las acciones realizadas por los diferentes usuarios, siendo así, un elemento que nos ayuda a deducir responsabilidades por algún problema que pueda ocurrir con los diferentes recursos informáticos de la institución.

1. La clave es el primer mecanismo de protección que tiene un usuario ya que es el elemento con el cual se identifica con la Red Informática, Sistemas de Información y los diferentes Servicios; por lo tanto, su manejo y selección debe hacerse con seriedad y estar acorde a los estándares establecidos.

2. En todo momento, el usuario es el responsable único y final de mantener en secreto las Claves o passwords asignadas, con los cuáles tenga acceso a los Servicios y Sistemas de Información.

3. El uso y custodia de la Clave o password es de exclusiva responsabilidad del usuario y no deberá permitir que terceros accedan a ella.

4. Utilizar únicamente la Clave o password que les ha sido asignada para tener acceso a sistemas de información y servicios.

5. Las claves de acceso a Servicios de correo electrónico interno y externo, Internet, Sistemas de Información, etc., deben ser estrictamente confidenciales, no se deberá publicar o tener la contraseña de acceso en un lugar visible, para que otra persona lo pueda utilizar.

6. Es responsabilidad del usuario cambiar periódicamente su clave o password de acuerdo a la criticidad de los servicios o sistemas de información.

7. Las claves de acceso podrán suspenderse o revocarse, sea por motivos de mal uso de ésta, por interés del que autorizó la solicitud del servicio, o por otras circunstancias.

8. El Usuario es responsable de no dejar sesiones activas en su estación de trabajo, cuando se ausente de su escritorio o sitio de trabajo.

9. Las claves de acceso para plataforma informática (red, correo, sistemas, entro otros) deben estar formada de la siguiente manera:

   - ✓ Longitud mínima de 8 caracteres alfanuméricos y símbolos.
   - ✓ No podrá contener el nombre o apellido del usuario.
   - ✓ La contraseña tendrá una validez máxima de 90 días.
   - ✓ No utilizar para generar la contraseña palabras o nombres comunes que puedan figurar en diccionarios.
   - ✓ Modificar la contraseña asignada de forma inicial

   Esta política, no aplica a los servicios TIC adquiridos por CENTA, que por estándar del fabricante no permite esta complejidad de autenticación.

Sobre la Depuración y Respaldo de Información

Es necesario realizar acciones necesarias para salvaguardar la integridad y seguridad de los datos contra pérdida o daño de la información, adoptando las precauciones técnicas para su almacenamiento y recuperación; así como optimizar el espacio de almacenamiento en disco, realizando actividades de depuración de archivos no necesarios.

9. En el modo de trabajo mono usuario, los usuarios son los responsables de hacer el respaldo de su información.

10. En el modo de trabajo multiusuario, el responsable de hacer el respaldo de la información del Servidor, es el administrador de la red, de acuerdo a un calendario establecido

11. La información almacenada en medios magnéticos tendrá al menos una copia de respaldo en CD, DVD o en otro medio de que disponga el CENTA, debido a que el costo de recuperación puede ser demasiado alto.

12. El disco duro es un medio de almacenamiento temporal de la información, el cual debe ser depurado permanentemente de los archivos que no volverán a ser utilizados en forma inmediata, o aquéllos que no sean útiles.

13. Periódicamente deberá efectuarse un respaldo de toda la información útil que se encuentra almacenada en el disco duro, lo cual será realizado por cada usuario responsable del equipo designado.

14. Es responsabilidad de los usuarios que tienen computadoras portátiles asignadas realizar periódicamente un respaldo de toda la información útil que se encuentra almacenada en el disco duro.

15. La información almacenada por el usuario debe ser verificada íntegramente, tanto el original como las copias. Asimismo, debe verificarse que la información no esté contaminada con virus.

16. Debe existir una copia de los archivos importantes que están concluidos, como respaldo preventivo.

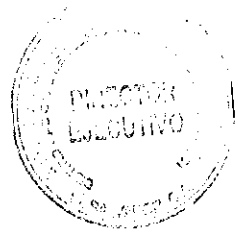
17. Sólo los archivos de datos y no los programas ejecutables deberán ser copiados de una computadora a otra.

19. Cuando se quiera almacenar un archivo de respaldo este deberá guardarse físicamente en otro dispositivo externo diferente a la que contiene el archivo original.

Sobre el almacenamiento físico de los Respaldos:

Los respaldos de información como parte de los activos principales de una institución, por lo tanto se deben considerar ciertos lineamientos básicos en su almacenamiento y protección que nos aseguren el buen funcionamiento de los mismos.

20. Los ambientes donde se depositan los medios magnéticos deben contar con adecuadas condiciones de temperatura y no presentar humedad.



21. Los medios magnéticos (CD, DVD, cintas, etc.) en los cuales se almacena la información histórica, deben ser completamente nuevos (es decir de primer uso), verificándose su buen estado operacional.

22. Los medios magnéticos donde está grabada la información deben recibir mantenimiento de limpieza cada tres meses como mínimo.

23. Sólo el personal responsable de la seguridad de los archivos tendrá acceso al ambiente donde se encuentren estos medios magnéticos que contengan copias de respaldo.

24. Todas las copias de respaldo deberán estar claramente identificadas, debidamente etiquetadas.

Protección contra virus

Los datos e información de la institución, como parte de sus activos principales, deben ser protegidos de la principal causa de pérdida o daño de los mismos, como son los virus informáticos, con los siguientes lineamientos básicos.

25. Se debe salvaguardar la integridad y seguridad de la información, adoptando las precauciones técnicas del caso, a fin de evitar, detectar o eliminar virus informático, en los equipos.

26. Utilizar racionalmente los recursos informáticos asegurando un adecuado control contra el daño producido por virus informático en la información procesada en los equipos.

27. Nunca se deben ejecutar programas de origen desconocido.

32. Si por razones de trabajo fuera necesario la utilización de un medio magnético proveniente del exterior, éste deberá necesariamente pasar por los controles de chequeo y registro correspondientes.

33. Los medios de detección de virus deben ser actualizados en las diferentes dependencias de la institución con el apoyo de los enlaces de informática, de acuerdo a las nuevas versiones de los detectores de virus que se adquieran.

34. El personal que tiene acceso a computadoras que se encuentran integradas a la red, el programa de detección de virus debe ser instalado en la memoria, a fin de que permanentemente se controle cualquier medio de almacenamiento que sea utilizado con el equipo.

Protección Física de los Equipos Informáticos

Es necesario considerar en la protección de los equipos informáticos, el medio ambiente y físico en que se encuentran, para evitar cualquier deterioro o daño que puedan sufrir por cualquier evento o contingencia que pueda ocurrir.

35. Se recomienda verificar periódicamente el estado de las griferías y cañerías a fin de evitar posibles inundaciones.

36. Es recomendable contar con servicio de aire acondicionado, evitando que esté próximo a material inflamable; asimismo se deberá contar con las instrucciones de operación visibles.

37. Asegurar que los tomas de aire de los equipos se encuentren ubicados en zonas no susceptibles de ser obstruidas.

38. Capacitar al personal en el uso y mantenimiento del equipo contra incendio.

39. Evitar que las paredes, pisos y techos contengan material inflamable, recomendándose instalar equipos de alarma, detectores de humo.

44. Para combatir los incendios producidos por equipos eléctricos se deben utilizar extintores, hechos preferentemente de bióxido de carbono, productos químicos secos y líquido vaporizado. Estos estarán al alcance inmediato, preservando la vigencia química del extintor e identificando su localización en el respectivo plano.

45. No se deberá abrir los equipos, ni intercambiar componentes internos de éstos, sin previa autorización de la Unidad de Informática; se llevará un control del equipo al que se le extrajo dicho componente y dónde se alojó.

46. Es recomendable que todas las computadoras tengan un soporte logístico mínimo, filtros para pantalla y cubierta protectora que deberá ser colocada diariamente al finalizar la jornada de trabajo.

47. Las computadoras deberán tener instalado un software de protección de pantalla con criterio institucional.

48. Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.

49. Es recomendable que durante el período de garantía los equipos deberán contar con un programa de mantenimiento preventivo. Este Servicio es recomendable contratarlo con el proveedor que suministró los equipos

50. Los usuarios deben verificar que se lleve a cabo el mantenimiento preventivo de forma periódica.

51. Es recomendable realizar Fumigaciones Periódicas en las Oficinas y Dependencias del CENTA, para evitar daños en los Equipos Informáticos e instalaciones de red generados por roedores, plagas, insectos, etc.

7. POLÍTICA DE AUDITORIAS INFORMÁTICAS.

Objetivo:

Para dar un seguimiento a la aplicación de las políticas y procedimientos de la gestión informática, por el personal de la institución, se hará uso de las auditorías programadas y no programadas, que permitan evitar problemas a la institución.

1. Las Auditorías informáticas internas podrán ser efectuadas por personal de la Unidad de Informática en conjunto con personal de Auditoría Interna o en forma independiente.

2. Se realizará periódicamente de acuerdo a calendario establecido por la Unidad de Informática o cuando fuesen necesarias.

3. Se determinará si podrían llevarse a cabo mejoras en la asignación de los recursos informáticos para una mejor o más amplia utilidad del mismo.

4. Se verificará el software que contengan los equipos informáticos.

5. Se verificarán las condiciones del local donde esté alojado el equipo informático, y demás elementos complementarios.

6. Se verificará que las oficinas realicen las actividades de depuración y respaldo de acuerdo a las normas y políticas relacionadas.

7. Se elaborará un informe para consignar las observaciones y recomendaciones pertinentes.

9. Se validarán permanentemente las políticas y procedimientos a efecto de determinar si cumplen con los objetivos para las que fueron diseñadas.

8. POLÍTICA DE CONTINGENCIAS

Objetivo:

Estar preparados para enfrentar la Interrupción o falta de continuidad en el procesamiento de información, Servicios, etc. Debido a fallas generadas por causas naturales, error humano, sabotaje, siniestro, etc.

1. Disponer de equipamiento alternativo completo que permita superar una contingencia por destrucción en los equipos o dispositivos principales.
2. Disponer de un Stock de repuestos mínimo que permita superar una contingencia por fallas en los equipos o dispositivos principales o secundarios.
3. Todo Sistema de Información en producción deberá tener documentada las acciones de recuperación de servicio, ante cualquier tipo de emergencia.
4. Se debe tener una copia de respaldo de aplicaciones, programas y licencias que exista en la institución, para ser utilizadas en las acciones de recuperación que sean necesarias.
5. El Plan de Contingencias deberá tener acciones de emergencia a seguir, en forma clara y precisa, tal que puedan ser ejecutadas con el personal jerárquico de las diferentes áreas, a fin de contemplar los casos de cambios y/o emergencias, con el fin de llegar al punto de recuperación antes de ocurrir la falla o siniestro.
6. El Plan de Contingencias tendrá asignado el responsable de su generación y actualización.

9. POLÍTICA DE SEGURIDAD INFORMACIÓN

Objetivo:

Salvaguardar la información generada por las diferentes dependencias de la institución. Ya que esta es un activo fundamental para la prestación de los servicios y la toma de decisiones eficientes.

1. Todos los funcionarios serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
2. Únicamente se permitirá el uso de software autorizado que haya sido adquirido legalmente por la Institución.

3. Es responsabilidad de todos los funcionarios reportar los incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.

10. POLÍTICA DE CREACIÓN DE USUARIO

1. Todos los recursos de información críticos del CENTA tienen asignados los privilegios de acceso de usuarios con base en los roles y perfiles que cada empleado requiera para el desarrollo de sus funciones.

2. Tendrán usuario administrador todos aquellos usuarios que por naturaleza de sus funciones lo requieran.

3. Los equipos se entregaran con usuario restringido, así como con bloqueo de Panel de control, salvo en aquellos casos que el usuario por la naturaleza de sus funciones lo requiera.

11. DISPOSICIONES GENERALES

1. La violación a lo dispuesto en las presentes Políticas, será resuelto por las leyes laborales, leyes de la administración pública y demás disposiciones legales aplicables.

2. Lo no previsto en las presentes Políticas se resolverá de conformidad con las leyes mencionadas en el artículo anterior.

3. Las presentes Políticas entrará en vigencia, después de su aprobación por la Dirección Ejecutiva.

12. VIGENCIA Y MODIFICACIÓN

El contenido de este documento podrá ser modificado conforme a las reformas que se realicen a la base legal referida o a iniciativa de la Gerencia Administrativa y Financiera con el propósito de introducir mejoras.

Aprobado a los veintiocho días del mes de Febrero del año dos mil diecinueve, en la Dirección Ejecutiva del Centro Nacional de Tecnología Agropecuaria y Forestal "Enrique Álvarez Córdova".

Aprobado:

Ing. Rafael Alemán
Director Ejecutivo