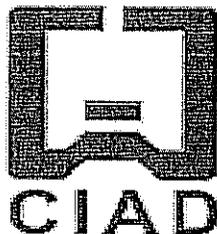




MANUAL DE POLITICAS DE SEGURIDAD
INFORMÁTICA DEL CENTRO DE INVESTIGACIÓN EN
ALIMENTACIÓN Y DESARROLLO, A. C.



***MANUAL DE POLITICAS DE SEGURIDAD
INFORMÁTICA DEL CENTRO DE
INVESTIGACIÓN EN ALIMENTACIÓN Y
DESARROLLO, A. C.***

Última revisión: 23 de octubre de 2009



INDICE

PRESENTACIÓN.....	3
I. AUTORIDAD.....	4
II. DISPOSICIONES GENERALES.....	4
III. POLITICAS.....	4
III.1 Políticas para el uso de la Red.....	4
III.2 Políticas de Software.....	7
III.3 Políticas Página del CIAD(WEB).....	9
III.4 Políticas de Hardware.....	9
III.5 Políticas de Videoconferencia.....	10
III.6 Políticas de Seguridad.....	12
III.7 Políticas de Servicios.....	13
III.8 Impresión en Plotter e Impresión en Impresora Láser a color.....	14
III.9 Administrador de Listas de Correos.....	15
III.10 Soporte técnico.....	15
III.11 Políticas para el uso del Correo Electrónico.....	16
III.12 Políticas para el uso de Internet.....	17
III.13 Políticas de Capacitación.....	17
III.14 Políticas de Desarrollo de Sistemas.....	18
III.15 Políticas Internas del Departamento de Informática.....	19



PRESENTACIÓN

Para cualquier institución es indispensable contar con una infraestructura de informática sólida, esta infraestructura se convierte en parte fundamental del desarrollo y competitividad de las instituciones, sin embargo por lo general se hace uso de ella de manera tan natural que pocas veces se detiene a meditar lo que implica el contar con tal servicio y lo que sucedería si alguna vez no se tiene acceso a él.

Basado en lo anterior, la experiencia nos dice que no es sino hasta el momento que se presenta una falla cuando nos detenemos, a analizar los riesgos y costos involucrados en mantener funcionando la infraestructura de servicios de cómputo, aunque es más común que simplemente nos quejemos por la falla o levantemos el teléfono para pedir una explicación y solicitar la pronta reanudación del servicio.

Actualmente en el CIAD esta infraestructura da servicio aproximadamente a 350 empleados, y 200 usuarios indirectos, entre estudiantes de nuestros programas de posgrado, tesis de licenciatura, prestadores de servicio social y prácticas profesionales. En nuestro centro, se ha adoptado y se desea continuar con una política de libertad en cuanto al uso de los recursos de cómputo, ya que esto, es útil en el desempeño académico, sin embargo, una consecuencia de éstos es el problema de generar la falsa idea de contar con un uso irrestricto de los recursos y una libertad total en la determinación del manejo que se hace de ellos, esto conlleva a que en muchas ocasiones se olvida que el Centro es un organismo descentralizado de investigación, sujeto a leyes y reglamentos específicos.

Así pues, se ha visto la necesidad de contar con una serie de políticas para el uso de los recursos informáticos, no con el fin de tener un control de manera arbitraria, sino con la idea de normar algunos aspectos de su utilización, precisamente como una medida que permita continuar ofreciendo, en la medida de lo posible, un servicio continuo y respetando tanto el derecho de los usuarios como los del equipo responsable de mantener esta infraestructura. Así mismo, es importante mencionar que éstas políticas también contribuyen a mantener dicha infraestructura y los recursos de información en el mejor nivel posible de acuerdo a los recursos económicos destinados.



I. AUTORIDAD

Este documento incorpora los lineamientos y las políticas del CIAD y es publicado por el Departamento de Informática, cuyos servicios han sido autorizados por la Dirección General de acuerdo con lo que establecen los estatutos de CIAD

II. DISPOSICIONES GENERALES

1. Toda persona que utilice los recursos informáticos del CIAD deberá conocer y acatar las disposiciones establecidas por el Comité de Informática en este documento. El desconocimiento del mismo no exonera de las responsabilidades asignadas.
2. Las autoridades académicas y administrativas y de manera específica el Departamento de Informática difundirá estas políticas entre los usuarios de los recursos y bienes informáticos a través de correo electrónico y de su presentación en la página web <http://computo.ciad.mx>.
3. Los casos no previstos por el presente reglamento serán resueltos por la Dirección Administrativa y el Departamento de Informática.

III. POLÍTICAS

III.1 Políticas para el uso de la Red

Definición de Red del CIAD

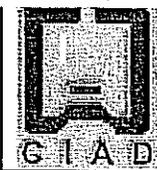
La Red del CIAD es el nombre oficial de un conjunto de facilidades y recursos informáticos, así como la infraestructura de telecomunicaciones y servicios asociados tanto local como remotos, provistos por el Departamento de Informática del CIAD a los usuarios de la misma.

Definición de Usuario

Se entiende por usuario a una división, un departamento, o un individuo ya sea de nuestra institución o ajena a ella, que satisfaga los requerimientos de acceso a la Red del CIAD. El presente reglamento se aplica a todos los usuarios mencionados.

Clasificación del personal autorizado para hacer uso de la RED

Toda persona que trabaje en la Institución, que esté inscrito como alumno, o se encuentre con carácter de becario, o este cumpliendo con su servicio social o prácticas profesionales en la Institución, también profesores o investigadores invitados tienen



MANUAL DE POLITICAS DE SEGURIDAD INFORMÁTICA DEL CENTRO DE INVESTIGACIÓN EN ALIMENTACIÓN Y DESARROLLO, A. C.

derecho a solicitar el uso de los recursos de la red, adicionalmente cuando la situación lo justifique se podrá autorizar el acceso a los recursos de la red para usuarios externos.

Del uso de la Red del CIAD

Los recursos de la Red académica del CIAD únicamente pueden ser usados de acuerdo con lo que establecen las normas de la Institución y la administración pública federal.

- La infraestructura de la Red del CIAD se utilizará únicamente para desarrollos académicos, de investigación, técnicos y administrativos de la Institución, incluyendo los actos promocionales de la misma, así como actividades similares de aquellas entidades con las que exista un convenio vigente.
- Ninguno de los recursos deben ser utilizados para recibir o enviar material ofensivo, ni realizar actos de difamación.
- El Departamento de Informática no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.
- Todos los usuarios que tengan bajo su cargo cualquier tipo de infraestructura informática, acuerdan que dicha infraestructura es sólo para uso institucional y deberán procurar su protección tanto de hardware como de software y deberá permitir el acceso al personal del Departamento de Informática para su verificación.
- No se puede hacer uso de la Red del CIAD para transmitir información de carácter comercial o cualquier otra forma que represente un lucro para la persona que lo origina, o la procura, excepto en caso de que el CIAD lo autorice o se involucre en proyectos de este tipo.
- Ningún usuario de la Red del CIAD esta facultado para otorgar acceso a terceros y mucho menos a aliarse con infractores cibernéticos.
- Todos los usuarios de la Red del CIAD deberán sujetarse a la política de seguridad establecida y difundida por el Departamento de Informática.
- Ninguno de los recursos de la Red del CIAD deberá utilizarse con fines de proselitismo político, ni religioso; respetándose en todo momento las disposiciones y los derechos individuales de las personas.
- No se permite la transferencia de información que afecte los derechos de autor o propiedad intelectual.
- Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos del Centro sin el consentimiento explícito responsable del equipo.
- No se permite interferir o interrumpir las actividades de los demás usuarios por cualquier medio o evento salvo que las circunstancias así lo requieran, como casos de contingencia, los cuales deberán ser reportados en su momento al personal de Informática o a las autoridades correspondientes.



- No se permite el uso de los servicios de la red cuando no cumplan con los trabajos establecidos.
- Todas las cuentas de acceso a los sistemas y recursos de cómputo de la Red-CIAD son personales e intransferibles, se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.
- El uso de analizadores de red es permitido única y exclusivamente para el personal del Centro de Computo o a quien ellos autoricen para monitorear la funcionalidad de la Red del CIAD, contribuyendo a la consolidación del sistema de seguridad bajo las políticas y normatividades del CIAD.
- No se permitirá el uso de analizadores para monitorear redes ajenas a la Red del CIAD y no se deberán realizar análisis de la Red del CIAD desde equipos internos o externos al CIAD.
- Cuando se detecte un uso no aceptable, se cancelará la cuenta o se desconectará temporal o permanentemente al usuario o red involucrados dependiendo de la normatividad del CIAD. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

Conexión a otras redes

Cuando el Centro brinde el acceso a otras redes a través de un convenio establecido con otra entidad, el usuario se sujeta a las normas que la institución receptora tenga estipuladas y las violaciones a las mismas serán penalizadas de acuerdo al reglamento de cada sitio.

De las restricciones.

Siendo limitada la cantidad de recursos informáticos con que se cuenta en la Institución también lo es el uso que de ellos pueden hacer los usuarios, los límites establecidos se estarán adecuando continuamente acorde a la situación del CIAD.

Servicios de red.

Los usuarios podrán utilizar libremente los servicios, pero en caso necesario el Departamento de Informática estará regulando el rendimiento de la Red que en el caso de verse afectada, podrá proponer formas para el aprovechamiento óptimo, eliminando algunos de éstos servicios o limitándolos.

No esta autorizada la creación o instalación de servidores que mermen la eficiencia de la red, para su autorización deberán ser solicitadas y analizadas las propuestas que de ser factibles se autorizarán por el Departamento de Informática.



De los servidores de la Red-CIAD

- El Centro de Cómputo tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la Red-CIAD.
- La instalación y/o configuración de todo servidor conectado a la Red-CIAD deberá ser notificada al Centro de Cómputo.
- Durante la configuración del servidor los ATI (Administradores de las Tecnologías de Información) deben normar el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios.
- Los servidores que proporcionen servicios a través de la Red del CIAD e Internet deberán:
 1. Recibir mantenimiento preventivo semanal de software (revisar actualizaciones de seguridad principalmente).
 2. Recibir mantenimiento mensual que incluya depuración de bitácoras.
 3. Recibir mantenimiento semestral que incluya la revisión de su configuración.
 4. Ser monitoreados por el Centro de Cómputo.

III.2 Políticas de Software

- La adquisición de paquetes de licencia se determinará en base a las necesidades actuales de los distintos Departamentos y de acuerdo con las normas establecidas por el Departamento de Adquisiciones.
- Sólo es permitido instalar en los equipos informáticos software con licencia, ya sea de cobertura institucional, de evaluación (shareware) o sin costo (freeware). Será responsabilidad del encargado del equipo que el software instalado en su equipo tenga la licencia correspondiente.
- Queda prohibido instalar software por parte del usuario, principalmente aquel que no cuente con la licencia correspondiente ya que será responsabilidad directa del usuario el software que tenga instalado en su equipo.
- El Departamento de Informática, promoverán la adquisición de licencias "institucionales", de "grupo" y otras modalidades que sean convenientes para la institución.
- Es responsabilidad del usuario informarse sobre los detalles de los tipos de licencia, cobertura, transferibilidad y certificación mediante solicitud de apoyo o asesoría al Departamento de Informática.
- El Departamento de Informática emitirá procedimientos para asegurarse que sólo software con licencia esté instalado en las computadoras del CIAD, y todas las autoridades deberán colaborar con el Departamento para evitar que se instale



software sin licencia en equipos que estén siendo utilizados dentro de la Institución.

- La instalación de paquetes y programas en los servidores generales de la red se llevará a cabo por el personal del Departamento de Informática y en el caso de servidores departamentales por el administrador del sistema particular el cual será responsable de dicha instalación y deberá acatar las disposiciones establecidas en este documento.
- Para la adquisición y/o actualización de licencias (proceso de compra), se deberá hacer una requisición especificando el número de resguardo del equipo (etiqueta CIAD con código de barra, num. entre asteriscos *numero*) y entregar una copia de la requisición al Centro de Cómputo ya sellada por compras, para proceder a la instalación.
- Únicamente se harán instalaciones de software en equipos que sean del CIAD (no se permitirá la instalación de software en equipos personales, aunque estos se estén utilizando en labores del Centro).
- El Centro de Cómputo pone a disposición del personal algunas utilerías de software, de tipo shareware, es decir el usuario las puede instalar y utilizar y en caso de que este software le sea útil, deberá adquirir la licencia correspondiente.
- Todo el software (medios físicos) que sea adquirido por el Centro deberá quedar en resguardo en el Departamento de Cómputo.
- El software original no se utilizará para hacer instalaciones en equipos. El personal del Centro de Cómputo que realiza instalaciones de programas, deberá hacer una copia de los programas originales y hacer las instalaciones a partir de ésta copia.
- Queda prohibido el préstamo de CD's, diskettes y manuales originales a empleados de otras áreas, que no sean del Centro de Cómputo.
- No se harán copias de los programas, solicitados por empleados de otras áreas para uso personal o dentro del CIAD.
- Cualquier copia de un programa de software, excepto copias de seguridad, es una violación a la ley de derechos de autor y a las políticas del CIAD.
- Si la computadora tiene un programa instalado en su disco duro, ese programa no debe ser copiado en ningún otro disco duro o flexible, a menos que se cuente con las licencias correspondientes.
- Se prohíbe ejecutar un programa en dos o más computadoras simultáneamente, a no ser que esté específicamente permitido en la licencia.
- Los empleados de la institución en conocimiento de cualquier uso indebido de software, deberán notificar este hecho al jefe del departamento, investigador o Contraloría Interna.
- Queda prohibido tener instalados programas que no son utilizados para el desarrollo de tus actividades laborales, como juegos, archivos ajenos a los intereses institucionales, etc.



III.3 Políticas Página del CIAD (WEB)

1. El CIAD dispondrá únicamente de una página oficial de información para situarse en la Internet. *http://www.ciad.mx*
2. El material que aparezca en la página de Internet del CIAD deberá ser aprobado por la Dirección General o Dirección Administrativa, respetando la propiedad intelectual (derechos de autor, créditos, permisos y protección, y todos los que se aplican a cualquier material de esta naturaleza).
3. En páginas personales, es responsabilidad del interesado verificar que la información que este en su página sea la correcta y esté actualizada.
4. Para las páginas de áreas, el coordinador será el responsable de la información que ahí aparezca y de preferencia deberá nombrar a un responsable, quien se encargará de proporcionar oportunamente la información al personal del Centro de Cómputo para que la incorpore a dicha página. También deberá seleccionar las fotografías que se insertarán en la página.
5. El formato de la página y subpáginas deberán cumplir con los lineamientos estipulados por el Sistema de Internet de la Presidencia.

III.4 Políticas de Hardware.

- No se le dará servicio a ningún equipo que no cuente con la clave de resguardo del CIAD (código de barras).
- Los equipos en reparación no estarán más de 14 días en el área de Ingeniería Electrónica o el área de Telecomunicaciones. En caso de que la reparación involucre la compra de piezas o refacciones, el equipo se devolverá a su responsable mientras llega la refacción.
- Los equipos que ingresen al área de electrónica solo serán entregados por la persona responsable de su reparación
- El área de electrónica no es responsable de dar de baja los equipos de cómputo o equipos electrónicos del CIAD. Si un equipo ya no cumple con las necesidades del responsable, o se diagnostica que ya no es funcional, el responsable deberá proceder a darlo de baja. El personal de Electrónica solo dará el diagnóstico final del equipo.
- Las llamadas de larga distancia hacia fabricantes o proveedores para consulta o asesoría para solucionar la falla o para autorización de reparación se realizarán desde área de donde pertenece el equipo o con cargo a su proyecto.
- Las garantías de los equipos se tramitarán a través del área de compras, para que esta a su vez trámite la salida del equipo, el área de electrónica emitirá un reporte de la falla.



- Los recursos de cómputo empleados por el usuario:
 - Deberán ser afines al trabajo desarrollado.
 - No deberán ser proporcionados a personas ajenas.
 - No deberán ser utilizados para fines personales.

III.5 Políticas de Videoconferencia

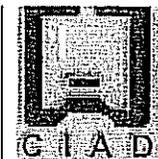
- Este servicio podrá ser utilizado por todo el personal que labora en el CIAD, estudiantes, tesis y maestros, previa autorización y pago del servicio cuando aplique.
- En caso de requerirse autorización, esta deberá de ser otorgada por alguna de las siguientes instancias: El Director General o el Director Administrativo del CIAD.
- Para personas externas al CIAD, deberán obtener una autorización previa y realizar el pago correspondiente del servicio.
- Por ningún motivo el equipo de Videoconferencia (VC) podrá ser prestado dentro o fuera de las instalaciones del CIAD. La instalación y desinstalación del mismo y de los equipos de apoyo (cañón, video casetera, cámaras, micrófonos, computadora y pizarrones) se llevarán a cabo únicamente por el responsable de VC.
- Todas las sesiones de Videoconferencia se llevarán a cabo únicamente en las instalaciones que cumplan con las condiciones de seguridad necesarias para el equipo, como serían: fuente de corriente regulada, bajo nivel de humedad, aire acondicionado, mobiliario apropiado para instalar el equipo de VC, lugar alejado del área de tráfico de personas.
- Para calendarizar una solicitud de una sesión de VC esta deberá solicitarse al encargado de Videoconferencia el cual deberá confirmar la disponibilidad de la fecha y hora especificada por el solicitante. Las solicitudes deberán hacerse al menos una semana antes del evento. En caso de imprevistos en los cuales no se cuente con el tiempo estipulado, el responsable de VC hará los arreglos necesarios para efectuar la VC pero no garantizará la calidad de la misma.
- El establecimiento de las sesiones de VC serán de acuerdo al sistema, “el primero que solicita es el que tiene prioridad sobre la fecha y hora de la misma, sin excepción alguna”.
- En caso de que dos o más eventos se lleven a cabo a la misma fecha y hora dicho conflicto deberá ser solucionado entre las partes en conflicto, la prioridad la tendrá la persona que haya solicitado el servicio en primera instancia.
- El usuario deberá elaborar un programa o una guía del desarrollo de la VC (ej. introducción, exposición, pregunta y respuesta) si es posible con el tiempo estimado, esto con el fin de no tener retrasos, ni pérdida de tiempo y conocer la secuencia de la utilización de los equipos de apoyo y los equipos de la VC (micrófonos, cámaras, etc.).



- El costo de la sesión de VC será cubierta por el usuario y dependerá del medio de interconexión, tiempo y equipos requeridos, más la renta del equipo.
- Para los casos en los cuales debido a la naturaleza de la VC y de información que se tratará en la sesión, el solicitante requiera manejar el equipo sin el apoyo del encargado de VC, éste se hará responsable de cualquier daño al equipo, tanto de VC como los equipos de apoyo.
- El horario disponible para llevar acabo las sesiones de VC es de Lunes a Viernes de 8:00 a.m. a 4:00 p.m., solo días laborables (no vacaciones, no días festivos, ni días de descanso) si algún evento estuviera calendarizado fuera de este horario estaría sujeto a la disponibilidad del responsable de VC el que se lleve a cabo. Dichas sesiones se considerarán como trabajo extraordinario sujetándose a lo establecido en el Reglamento Interior de Trabajo.
- El solicitante de la VC deberá dirigirse con el responsable de VC para coordinar la interconexión de salas y proporcionar la siguiente información:

Datos necesarios:

- Título de la Videoconferencia
 - Fecha y hora de inicio y término
 - Responsables del pago de servicios (en caso de que aplique)
 - Equipos periféricos requeridos.
 - Nombre, dirección de correo electrónico y teléfono del contacto técnico del o de los puntos que se conectarán al evento.
- Para poder tener acceso a los servicios de videoconferencia se deberán aceptar las políticas de uso de este servicio.
 - Si el solicitante no está de acuerdo con las políticas de uso, no procederá la organización del evento. (El solicitante se obliga a cumplir y hacer cumplir las políticas de uso de este servicio).
 - Se realizarán las pruebas pertinentes por parte del responsable de VC, y se notificará al solicitante el resultado de su solicitud vía correo electrónico o telefónica, en el caso de que por el tipo de interconexión se generará algún costo extra, éste se le notificará y se emitirá una carta compromiso del pago.
 - Las VC para usuarios externos al CIAD deberán tener la autorización del Director Administrativo o del Director General y los costos o cobro del servicio se hará de acuerdo a las características del evento, etc.



III.6 Políticas de Seguridad

Antivirus en la Red-CIAD

Es obligatorio utilizar la Solución Antivirus Institucional en cada equipo de Cómputo del CIAD

En aquellos equipos que por su naturaleza no acepten la herramienta antivirus institucional se buscará algún otro antivirus que pueda proteger su equipo.

El Centro de Cómputo será el responsable de:

- Implementar la Solución Antivirus en las computadoras del CIAD
- Solucionar contingencias presentadas ante el surgimiento de virus que la solución no haya detectado automáticamente.
- Configurar el analizador de red del CIAD para la detección de virus.
- Notificar al proveedor del antivirus en caso de contingencia con virus.

El Centro de cómputo aislará la red de un área notificando a las autoridades competentes, en las condiciones siguientes:

- Cuando la contingencia con virus no este controlada, con el fin de evitar la propagación del virus a otras redes.
- Si el área viola las políticas antivirus.
- Cada vez que los usuarios requieran hacer uso de discos flexibles o dispositivos de almacenamiento portátil, éstos serán rastreados por la Solución Antivirus en la computadora del usuario o en un equipo designado para tal efecto en las áreas de cómputo del centro.

Uso del Antivirus por los usuarios

- El usuario no deberá tratar de desinstalar la solución antivirus de su computadora pues podría ocasionar un riesgo de seguridad.
- Si el usuario hace uso de medios de almacenamiento personales, éstos serán rastreados por la Solución Antivirus en la computadora del usuario o por el equipo designado para tal efecto.
- El usuario deberá comunicarse con el centro de cómputo en caso de problemas de virus para buscar la solución.
- El usuario será notificado por el centro de cómputo en los siguientes casos:
 - Cuando sea desconectado de la red con el fin evitar la propagación del virus a otros usuarios de la dependencia.
 - Cuando sus archivos resulten con daños irreparables por causa de virus.
 - Si viola las políticas antivirus.
- Todo usuario debe respetar la intimidad, confidencialidad y derechos individuales de los demás usuarios.



- Los usuarios deberán solicitar apoyo al centro de cómputo ante cualquier duda en el manejo de los recursos de cómputo de la institución.
- El Centro de Cómputo o el CIAD no se hace responsable de la pérdida de la información derivada de un virus, mal funcionamiento del equipo, etc. Es responsabilidad del usuario hacer el respaldo de su información o solicitar el apoyo del personal del Centro de Cómputo.

III.7 Políticas de Servicios

- Para hacer cualquier solicitud a las áreas del Computo y de Electrónica, se cuenta con un sistema de solicitud de servicio vía web.
- Solo se atenderán las solicitudes que se encuentren registradas en este sistema y el personal de Informática no se hará responsable de descuidar solicitudes hechas por otro medio (telefónico o en forma personal)
- El usuario deberá entrar a esta dirección <http://computo.ciad.mx/servicios> y capturar los datos de su solicitud. En este portal también tendrá acceso a la solicitud de otros tipos de servicios a otras áreas (mantenimiento, control patrimonial, desarrollo de sistemas administrativos, etc.)
- Las solicitudes se atenderán por orden de aparición.

III.8 Impresión en Plotter e Impresión en Impresora Láser a color

- Los póster se podrán elaborar en Power Point (recomendado) y Corel Draw preferentemente o algún otro programa siempre y cuando se tenga la licencia correspondiente para instalarse en los equipos que enviarán a imprimir al plotter.
- Se tendrá una lista de espera para la impresión de póster con la política de “el primero en llegar es el primero en atenderse” (no se aparta turno).
- El póster entrará en la lista de espera cuando se haya recibido el archivo y el comprobante autorizado por el Departamento de Presupuestos de que la transferencia del costo del póster al proyecto 6215 de computo se ha realizado.
- Toda impresión de pósters tendrá un costo que dependerá del material que se utilice (tipo de papel), cobertura (porcentaje de color utilizado) y tamaño del mismo. Cabe señalar que éste servicio se puede ofrecer al público en general con un costo competitivo a nivel comercial.
- No es responsabilidad del personal de cómputo elaborar ni revisar errores en los pósters, únicamente hacer recomendaciones. Si el póster tiene errores tipográficos u otro tipo de errores cometidos por el usuario, el póster no se volverá a imprimir, o se volverá a cobrar la impresión. Cuando el error sea por causa de desperfecto del plotter, falta de tinta, etc., entonces el póster se volverá a imprimir sin cargo extra para el solicitante.



- Las impresiones en la láser a color tendrán un costo, el cual será de acuerdo al costo cual estará directamente relacionado al costo que el proveedor cobre por impresión por hoja. Éste costo se le cobrará a cada usuario del servicio, al que se le dará un recibo del número de copias impresas y del costo total para que sea registrado por el departamento de Presupuestos, el cual cargará directamente al proyecto del investigador solicitante del servicio.
- El servicio de impresión en láser a color se hará en las hojas que el proveedor del servicio ofrezca. Si se desea imprimir en algún tipo de hoja especial, el usuario deberá traer las hojas deseadas y el resultado de la impresión no será responsabilidad del Centro de Cómputo.
- Este servicio también tendrá el sistema del primero que lo solicite será el primero que se le atenderá.
- El personal de Cómputo será el responsable de éste equipo y solicitará al proveedor los consumibles, reparaciones y servicios necesarios.



III.9 Administrador de Listas de Correos

- El administrador de listas (Adminlistas) es una herramienta de comunicación para el personal del CIAD, pero solo se utilizará para enviar correos de carácter laboral y de servicio social.
- Los correos solicitados por el personal del CIAD para ser enviados a través del administrador de listas (Adminlistas) deberán estar redactados.
- Preferentemente no se enviarán archivos adjuntos (attached), debido a que esta práctica puede saturar el ancho de banda de acceso a internet.
- En los casos en que se necesite enviar algún archivo adjunto, éste se pondrá en la intranet y solo se hará referencia de la dirección del archivo en el correo mediante un hipervínculo.
- Los envíos masivos de correo electrónico ("broadcasts") y que incluyan a todos los usuarios de la red, sólo podrán ser transmitidos por el administrador de las listas. Así mismo la utilización inadecuada de listas individuales como un sustituto no está permitido.
- Para enviar comunicados a todo el personal del CIAD o para ciertos grupos se utilizará este medio. También existen algunos grupos o áreas que pueden enviar correos masivos a través de los grupos de cuentas. La responsabilidad del contenido de los mismos será solo del usuario que envíe el correo.

III.10 Soporte técnico

- El personal de Informática ofrecerá el servicio de asesoría de software solo concerniente a la plataforma de software institucional.
- Es responsabilidad del usuario tener un respaldo actualizado de su información, el personal de cómputo realizará los respaldos solo cuando el usuario lo solicite y lo hará únicamente de la información solicitada.
- El personal de Informática no se hace responsable de la pérdida de ningún archivo, el hará los movimientos necesarios para asegurar que el respaldo quede bien y será responsabilidad del usuario revisarlo y dar el visto bueno de que su respaldo quedó bien.
- En los casos en que se haga un cambio de equipo de cómputo primero se hará el respaldo y se pedirá que se revise en el equipo nuevo, ya que se le da el visto bueno se procederá a borrar la información del equipo anterior.
- El personal de Informática deberá brindar el servicio de forma respetuosa.
- El personal de Informática podrá negar el servicio si el personal solicitante no se dirige de una manera respetuosa hacia el.



III.11 Políticas para el uso del Correo Electrónico

- El Departamento de Recursos Humanos es responsable de solicitar las altas, bajas y cambios a las cuentas de correos del personal, proporcionando para esto los siguientes datos al Administrador de la Red:
 - Nombre completo
 - Puesto
 - Área
 - Nombre de la cuenta
- Una cuenta deberá estar conformada por un nombre de usuario y su contraseña asignada. El nombre de usuario deberá contar como máximo de 8 caracteres y no deberá contener alias.
- En caso de olvido de la contraseña por parte del usuario, el Centro de Cómputo podrá apoyar para el cambio de la misma siempre y cuando el usuario se identifique plenamente.
- El Departamento de Docencia es responsable de recibir y registrar los datos de los estudiantes y darles de alta su cuenta de correo electrónico y darles de baja cuando los estudiantes hayan terminado o se de la baja.
- Se considera que el correo Electrónico es una comunicación directa y confidencial entre el que envía y el (los) que recibe(n), y no debe ser observado o reproducido por nadie más que los implicados.
- El administrador de la red es responsable de configurar y dar de alta o baja, en el sistema de red, las cuentas de usuario y los permisos autorizados, para todos los usuarios de la red.
- Es responsabilidad del usuario mantener los respaldos de su cuenta. El Departamento de Informática no se hace responsable por pérdidas de información en su correo.
- Queda prohibido, el uso de la cuenta para fines ajenos a los intereses del CIAD, tales como: comerciales, el envío o contestación de cadenas de correo, enviar o reenviar SPAM (correo basura), enviar anexos o adjuntos que pudieran contener información nociva para otro usuario como virus o pornografía, vocabulario ofensivo;
- Queda prohibido el uso de la cuenta de otro usuario sin su consentimiento.
- La información que se envíe por correo electrónico debe siempre responder a un comportamiento profesional y ético.

Vigencia de las cuentas.

Las cuentas creadas en la Red-CIAD tendrán una duración finita la cual queda determinada por las siguientes reglas:

- Las cuentas de estudiantes tendrán una duración máxima igual al período límite establecido para terminar los estudios, a partir del momento en que el alumno se



inscribe, estas cuentas deberán ser renovadas cada año. Una vez concluidos sus estudios podrán solicitar que la cuenta se conserve durante un plazo máximo de 3 meses.

- Las cuentas del personal que se separe del Centro se conservarán por un período máximo de 3 meses.
- Se podrá suspender o eliminar inmediatamente y sin previo aviso, cualquier cuenta de correo que ponga en peligro la integridad de la red del CIAD, o cualquier cuenta de usuario que se separe del Centro y que pueda ser utilizada de forma indebida, para lo cual se solicitará autorización del Director General.
- La baja de las cuentas de correo se hará a solicitud del Departamento de Recursos Humanos.

III.12 Políticas para el uso de Internet

- Queda prohibido navegar en sitios ajenos a los intereses del Centro, los cuales puedan poner en peligro la integridad de la Red y la información de los usuarios.
- Esta prohibido la descarga de archivos tales como: música, programas, imágenes, ajenos a los intereses del Centro, los cuales puedan poner en peligro la integridad de la Red, la información de los demás usuarios o el detrimento del ancho de banda de CIAD.
- No está permitido la instalación de software tipo spyware o malware que pueda obtener información personal de los usuarios de la red.

III.13 Políticas de Capacitación

- Tener acceso a un presupuesto que permita la capacitación y el desarrollo del personal del área de informática.
- Plan de capacitación, asesoría y apoyo informático para personal operativo, mandos medios y superiores.
- Ofrecer cursos del software utilizado en el Centro a los empleados y estudiantes del CIAD.
- Se dará asesoría personalizada de cualquier software y hardware utilizado en el Centro, a todos los usuarios que las solicitan en el sistema del departamento.



III.14 Políticas de Desarrollo de Sistemas

Desarrollo de sistemas

- Solo se brindará mantenimiento a aplicaciones desarrolladas por esta área.
- Todas las aplicaciones desarrolladas por esta área deberán acompañarse con manuales de usuario al momento de la implantación.
- Las solicitudes de desarrollo de aplicaciones serán atendidas de acuerdo al orden de llegada.
- Las solicitudes de corrección tendrán prioridad respecto a las solicitudes de desarrollo.
- Las solicitudes de mantenimiento se atenderán respecto al criterio del responsable del desarrollo del sistema.
- Las solicitudes para el desarrollo de una aplicación, deberá especificar:
 - Todos los Requerimientos de la aplicación
 - El impacto de la aplicación
 - El proyecto
 - Así mismo, el responsable deberá por lo menos aparecer en los agradecimientos o como coautor en el proyecto y publicaciones derivadas de esta aplicación.
- El solicitante deberá emitir una carta de conformidad una vez implantada la aplicación solicitada.
- Todas las operaciones internas que impliquen borrado de información deberán quedar excluidas de los menús de usuarios en todos los sistemas de cómputo administrativos.
- Todos los sistemas desarrollados deberán contar con su manual técnico, el cual debe incluir, la estructura de la base de datos y descripción detallada de las operaciones realizadas por los mismos.

III.15 Políticas Internas del Departamento de Informática

- Todos los servidores deberán manejar esquemas de almacenamiento redundantes que impliquen la utilización de, al menos, 2 discos físicos diferentes (arreglo en espejo).
- Todos los equipos deberán tener, al menos, un software de diagnóstico del estado de los discos duros y correrlo al menos una vez por semana.
- Se deberán realizar respaldos diarios de los archivos de datos manejados por los sistemas instalados en los servidores. Estos respaldos diarios podrán realizarse en discos duros, siempre que se encuentren en equipos localizados en oficinas distintas a las de los servidores a respaldar.



MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA DEL CENTRO DE INVESTIGACIÓN EN ALIMENTACIÓN Y DESARROLLO, A. C.

- Se deberán hacer pruebas mensuales de los respaldos, a fin de comprobar su buen funcionamiento.
- Se deberán realizar respaldos semanales, en medios magnéticos, de los archivos de datos de todos los sistemas informáticos administrativos. Estos medios magnéticos deberán resguardarse en cajas fuertes a prueba de fuego, localizadas en edificios distintos a los de los equipos que se están respaldando.
- Todos los equipos deberán contar con fuentes de suministro auxiliares del tipo "No Break", con un tiempo de respaldo mínimo de 10 minutos.
- Todos los servidores contarán con el software y equipo requerido para apagarse por si mismas en caso de interrupción del suministro eléctrico.
- Todos los servidores deberán contar con tierra física debidamente instalada en sus tomacorrientes.
- Todos los servidores estarán en áreas permanentemente cerradas con llave.
- Todos los servidores estarán en áreas con aire acondicionado permanente.
- Todos los servidores estarán en áreas sin ventanas.
- Todos los servidores estarán en áreas a prueba de incendios.
- Las áreas en donde se encuentren los servidores deberán contener, únicamente, dichos equipos y los aparatos estrictamente indispensables para su operación y protección.
- Todas las operaciones internas que impliquen borrado de información deberán quedar excluidas de los menús de usuarios en todos los sistemas de cómputo administrativos.

