**MANUAL DE POLÍTICAS, PROCEDIMIENTOS DEL DEPARTAMENTO DE SISTEMAS DE CISEPRO CIA. LTDA.**

**DISPOSICIONES GENERALES**

**Artículo 1º** Ámbito de aplicación y fines.

1.1 Las políticas del departamento de sistemas tienen por objeto establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes de telemática [Voz y Datos]) y personas que interactúan haciendo uso de los servicios asociados a ellos y se aplican a todos los usuarios de Cisepro Cía. Ltda.

1.2 El Departamento de Sistemas es quien dará a conocer estas políticas de seguridad internas.

1.3 El Departamento de Sistemas puede agregar guías particulares complementarias de acuerdo a su naturaleza y funciones. Además será el responsable de hacer cumplir y de hacer cumplir este Reglamento.

**Artículo 2º** Definiciones.

**DBA:** Administrador de Base de Datos.

**DS:** Departamento de Sistemas (Áreas de seguridad en: Informática, Telemática). Se encarga de definir esquemas y políticas de seguridad en materia de cómputo para la entidad.

**DS:** Administrador de Tecnologías de Información (Telemática). Responsable de la administración de los equipos de cómputo, sistemas de información y redes de telemática de la Entidad.

**BD:** Base de datos.

**CA:** Central Antivirus.

**Centro de Cómputo:** Cualquier oficina que cuenten con equipamiento de cómputo.

**DS (Departamento de Sistemas):** Es el área que se encarga del funcionamiento y operación de las Tecnologías de Información y comunicaciones (Telemática).

**Contraseña:** Conjunto de caracteres que permite el acceso de un usuario a un recurso informático (password).

**Recurso informático:** Cualquier componente físico o lógico de un sistema de información.

**Red:** Equipos de cómputo, sistemas de información y redes de telemática.

**SGI:** Sistemas de Gestión de Información (Microkey, SMS, Pagupa, SYSCISEPRO).

**Sitio:** Espacio designado en la entidad a los equipos de telecomunicaciones y servidores.

**Solución Antivirus:** Recurso informático empleado para solucionar problemas causados por virus informáticos.

**Telemática:** Conjunto de servicios y técnicas que asocian las telecomunicaciones y la informática ofreciendo posibilidades de comunicación e información.

**TIC:** (Tecnologías de Información y Comunicaciones) conjunto de teorías y de técnicas que permiten el aprovechamiento práctico de la Información.

**Usuario:** Cualquier persona (empleado o no) que haga uso de los servicios de las tecnologías de información proporcionadas por Cisepro Cia. Ltda., tales como equipos de cómputo, sistemas de información, redes de telemática.

**Virus informático:** Programa ejecutable o pieza de código con habilidad de ejecutarse y reproducirse, regularmente escondido en documentos electrónicos, que causan problemas al ocupar espacio de almacenamiento, así como destrucción de datos y reducción del desempeño de un equipo de cómputo.

**Artículo 3º** Frecuencia de evaluación de las políticas.

3.1 Se evaluarán las políticas del presente documento, con una frecuencia anual por el Departamento de Sistemas.

3.2 Las políticas serán evaluadas por el Departamento de Sistemas con una frecuencia semestral.

**POLÍTICAS SEGURIDAD FÍSICA**

**Artículo 4º** Acceso Físico

4.1 Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario no tenga acceso físico directo. Entendiendo por sistema de comunicaciones: el equipo activo y los medios de comunicación.

4.2 El acceso de terceras personas debe ser identificado plenamente, controlado y vigilado durante el acceso portando una identificación que les será asignado por el área de seguridad de acceso a Cisepro.

4.3 Las visitas internas o externas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañadas cuando menos por un responsable del área o con permiso del Departamento de Sistemas.

4.4 El personal autorizado para mover, cambiar o extraer equipo de cómputo del Cisepro son los miembros del Departamento de Sistemas o el superior responsable a través de identificaciones y formatos de Entrada/Salida, el cual notificará al encargado de activos fijos.

**Artículo 5º** Robo de Equipo

5.1 A partir de los procedimientos definidos por el Departamento de Sistemas, el encargado de activos definirá procedimientos para inventario físico, firmas de resguardo para préstamos y usos dedicados de equipos de tecnología de información.

5.2 El resguardo de los equipos de comunicaciones deberá quedar asignado a la persona que los usa o administra, permitiendo conocer siempre la ubicación física de los equipos.

5.3 La DS, así como las áreas que cuenten con equipos de misión crítica deberán contar con vigilancia y/o algún tipo de sistema que ayude a recabar evidencia de accesos físicos a las instalaciones.

**Artículo 6º** Protección Física

6.1 Las puertas de acceso a las salas de cómputo deben ser preferentemente de vidrio transparente, para favorecer el control del uso de los recursos de cómputo.

6.2 El Sitio de Cisepro Cia. Ltda. Debe:

* Recibir limpieza al menos dos veces por semana, que permita mantenerse libre de polvo.
* Ser un área restringida.
* Estar libre de contactos e instalaciones eléctricas en mal estado
* Contar por lo menos con dos extinguidores de incendio adecuado y cercano al centro de telecomunicaciones.

6.3 El Sitio deberá seguir los estándares vigentes para una protección adecuada de los equipos de telecomunicaciones y servidores.

6.4 Los sistemas de tierra física, sistemas de protección e instalaciones eléctricas del Sitio deberán recibir mantenimiento semestral con el fin de determinar la efectividad del sistema.

6.5 Cada vez que se requiera conectar un equipo de cómputo, se deberá comprobar la carga de las tomas de corriente.

6.6 Contar con algún esquema que asegure la continuidad del servicio.

6.7 Se deberá tener fácil acceso a los procedimientos de contingencias.

6.8 Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).

**Artículo 7º** Respaldos

7.1 Las Bases de Datos de Cisepro serán respaldadas diariamente en forma automática, según los procedimientos generados para tal efecto.

7.2 Los respaldos de Cisepro deberán ser almacenados en un lugar seguro y distante del sitio de trabajo.

**POLÍTICAS DE SEGURIDAD LÓGICA DE LA RED**

**Artículo 8º** De la Red

8.1 La Red de Cisepro tiene como propósito principal servir en la transformación e intercambio de información dentro de la entidad entre usuarios, técnicos, departamentos, oficinas y hacia a fuera de la Entidad, a través de conexiones con otras redes.

8.2 Si una aplicación en la red es coherente con los propósitos de la Red de Cisepro, entonces significa que las actividades necesarias para esa aplicación serán consistentes con los propósitos de la unidad de TIC.

8.3 El Departamento de Sistemas 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.

8.4 Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable del equipo.

8.5 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 a sus superiores correspondientes.

8.6 No se permite el uso de los servicios de la red cuando no cumplan con los quehaceres propios de Cisepro Cía. Ltda.

8.7 Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de Cisepro y se usarán exclusivamente para actividades relacionadas con la entidad.

8.8 Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.

8.9 El uso de analizadores de red es permitido única y exclusivamente por el personal del Departamento de Sistemas, para monitorear la funcionalidad de la Red de Cisepro, contribuyendo a la consolidación del sistema de seguridad bajo las políticas y normatividades de la entidad.

8.10 No se permitirá el uso de analizadores para monitorear o censar redes ajenas a Cisepro y no se deberán realizar análisis de Cisepro desde equipos externos a la entidad.

8.11 Cuando se detecte un uso no aceptable, se cancelará la cuenta o se desconectará temporal o permanentemente al usuario o red involucrada dependiendo de la normatividad. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

**Artículo 9º** Del Departamento de Sistemas.

9.1 El Departamento de Sistemas debe llevar un control total y sistematizado de los recursos de cómputo.

9.2 Los encargados del Departamento de Sistemas son los responsables de calendarizar y organizar al personal encargado del mantenimiento preventivo y correctivo de los equipos de cómputo.

9.3 Los Departamentos deberán reportar al personal al Departamento de Sistemas cuando un usuario deje de laborar o de tener una relación con Cisepro.

9.4 Si un usuario o departamento viola las políticas vigentes de uso aceptable de la Red de Cisepro, el Jefe de Sistemas lo aislará de la misma.

9.5 Para reforzar la seguridad de la información de los usuarios, bajo su criterio, deberá hacer respaldos de la información en sus discos duros dependiendo de la importancia y frecuencia del cambio de la misma.

9.6 Los miembros del Departamento de Sistemas no podrán remover del sistema ninguna información de cuentas individuales, a menos que la información sea de carácter ilegal, o ponga en peligro el buen funcionamiento de los sistemas, o se sospeche de algún intruso utilizando una cuenta ajena.

**Artículo 10º** Políticas de uso aceptable de los usuarios

10.1 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.

10.2 Todo usuario debe respetar la intimidad, confidencialidad y derechos individuales de los demás usuarios.

10.3 El correo electrónico no se deberá usar para envío masivo, materiales de uso no institucional o innecesarios (entiéndase por correo masivo todo aquel que sea ajeno a la institución, tales como cadenas, publicidad y propaganda comercial, política o social, entre otros).

10.4 Para reforzar la seguridad de la información de su cuenta, el usuario –conforme su criterio- deberá hacer respaldos de su información, dependiendo de la importancia y frecuencia de modificación de la misma. Los respaldos serán responsabilidad absoluta de los usuarios

10.5 Queda estrictamente prohibido inspeccionar, copiar y almacenar programas de cómputo, software y demás fuentes que violen la ley de derechos de autor, para tal efecto todos los usuarios deberán firmar un manifiesto donde se comprometan, bajo su responsabilidad, a no usar programas de software que violen la ley de derechos de autor.

10.6 Los usuarios deberán cuidar, respetar y hacer un uso adecuado de los recursos de cómputo y red de Cisepro, de acuerdo con las políticas que en este documento se mencionan.

10.7 Los usuarios deberán solicitar apoyo al Departamento de Sistemas ante cualquier duda en el manejo de los recursos de cómputo de la institución.

**Artículo 11º** De los servidores de la Red.

11.1 El Departamento de Sistemas tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la Red.

11.2 La instalación y/o configuración de todo servidor conectado a la Red será responsabilidad del Departamento de Sistemas.

11.3 Durante la configuración del servidor la DS debe normalizar 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.

11.4 Los servidores que proporcionen servicios a través de la RED e Internet deberán:

* Funcionar 24 horas del día los 365 días del año.
* Recibir mantenimiento preventivo máximo dos veces al año
* Recibir mantenimiento semestral que incluya depuración de bitácoras.
* Recibir mantenimiento anual que incluya la revisión de su configuración.
* Ser monitoreados por el DS.

11.5 La información de los servidores deberá ser respaldada de acuerdo con los siguientes criterios, como mínimo:

* Diariamente, información crítica.
* Semanalmente, los correos y los documentos web.
* Mensualmente, configuración del servidor y bitácoras.

11.6 Los servicios institucionales hacia Internet sólo podrán proveerse a través de los servidores autorizados por el Departamento de Sistemas.

11.7 La DS se encargará de asignar las cuentas a los usuarios para el uso de correo electrónico en los servidores que administra.

11.8 Para efecto de asignarle su cuenta de correo al usuario, éste deberá llenar una solicitud en formato libre y entregarlo al Departamento de Sistemas, con su firma y la del encargado de área.

11.9 Una cuenta de correo deberá estar conformada por la primera letra del primer nombre y su primer apellido. La sintaxis de la cuenta de correo será:

[primeraletradelprimernombreyprimerapellido@cisepro.com.ec](mailto:primeraletradelprimernombreyprimerapellido@cisepro.com.ec) y no deberá contener alias.

11.10 La cuenta será activada en el momento en que el usuario se presente en el Departamento de Sistemas de Cisepro Cía. Ltda., para teclear y verificar de manera personal su contraseña de acceso.

11.11 Los servidores deberán ubicarse en un área física que cumpla las normas para un centro de telecomunicaciones:

* Acceso restringido.
* Temperatura adecuada al equipo.
* Protección contra descargas eléctricas.
* Mobiliario adecuado que garantice la seguridad de los equipos.

11.12 En caso de olvido de la contraseña por parte del usuario, podrá apoyarse con la Dirección de Sistemas para el cambio de contraseña.

**Artículo 12º** De los Sistemas de Gestión de Información

12.1. El DBA tendrá acceso a la información de la Base de Datos únicamente para:

* La realización de los respaldos de la BD.
* Solucionar problemas que el usuario no pueda resolver.
* Diagnóstico o monitoreo.
* Re indexación de la BD.
* Depuración de la BD.

12.2 El DBA no deberá eliminar ninguna información del sistema, a menos que la información esté dañada o ponga en peligro el buen funcionamiento del sistema.

12.3 El DBA es el encargado de asignar las cuentas a los usuarios para el uso. Para tal efecto será necesario seguir el procedimiento determinado para tal efecto.

12.4 Las contraseñas serán asignadas por el Administrador de la Base de Datos en el momento en que el usuario desee activar su cuenta, previa solicitud al responsable de acuerdo con el procedimiento generado.

12.5 En caso de olvido de contraseña de un usuario, será necesario que se presente con el Administrador de la Base de Datos para reasignarle su contraseña.

**POLÍTICAS DE SEGURIDAD LÓGICA PARA ADMINISTRACIÓN DE LOS RECURSOS DE CÓMPUTO**

**Artículo 13º** Departamento de Sistemas.

13.1 El Departamento de Sistemas es el encargado de suministrar medidas de seguridad adecuadas contra la intrusión o daños a la información almacenada en los sistemas así como la instalación de cualquier herramienta, dispositivo o software que refuerce la seguridad en cómputo. Sin embargo, debido a la cantidad de usuarios, la amplitud y constante innovación de los mecanismos de ataque no es posible garantizar una seguridad completa.

13.2 El Departamento de Sistemas debe mantener informados a los usuarios y poner a disposición de los mismos el software que refuerce la seguridad de los sistemas de cómputo.

13.3 El Departamento de Sistemas es el único autorizado para monitorear constantemente el tráfico de paquetes sobre la red, con el fin de detectar y solucionar anomalías, registrar usos indebidos o cualquier falla que provoque problemas en los servicios de la Red.

**Artículo 14º** Administradores de Tecnologías de Información

14.1 El Departamento de Sistemas debe cancelar o suspender las cuentas de los usuarios previa notificación, cuando se le solicite mediante un documento explícito por las Direcciones en los siguientes casos:

* Si la cuenta no se está utilizando con fines institucionales.
* Si pone en peligro el buen funcionamiento de los sistemas.
* Si se sospecha de algún intruso utilizando una cuenta ajena.

14.2 El Departamento de Sistemas deberá ingresar de forma remota a computadoras única y exclusivamente para la solución de problemas y bajo solicitud explícita del propietario de la computadora.

14.3 El Departamento de Sistemas deberá utilizar los analizadores previa autorización del usuario y bajo la supervisión de éste, informando de los propósitos y los resultados obtenidos.

14.4 El Departamento de Sistemas deberá realizar respaldos diarios de la información de los recursos de cómputo que tenga a su cargo, siempre y cuando se cuente con dispositivos de respaldo.

14.5 El Departamento de Sistemas debe actualizar la información de los recursos de cómputo de la entidad, cada vez que adquiera e instale equipo o software.

14.6 El Departamento de Sistemas debe registrar cada máquina en el inventario de control de equipo de cómputo y red de la entidad.

14.7 El Departamento de Sistemas debe auditar periódicamente y sin previo aviso los sistemas y los servicios de red, para verificar la existencia de archivos no autorizados, configuraciones no válidas o permisos extra que pongan en riesgo la seguridad de la información.

14.8 El Departamento de Sistemas debe realizar la instalación o adaptación de sus sistemas de cómputo de acuerdo con los requerimientos en materia de seguridad.

14.9 Es responsabilidad del Departamento de Sistemas revisar periódicamente las bitácoras de los sistemas a su cargo.

14.10 El Departamento de Sistemas reportará a la Dirección los incidentes de violación de seguridad, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de cómputo.

**Artículo 15º** Renovación de Equipo

15.1 Se deberán definir los tiempos estimados de vida útil de los equipos de cómputo y telecomunicaciones para programar con anticipación su renovación.

15.2 Para la adquisición de equipo de cómputo se deberá cumplir con lo establecido en la solicitud de activos.

15.3 Cuando las áreas requieran de un equipo para el desempeño de sus funciones ya sea por sustitución o para el mejor desempeño de sus actividades, estas deberán realizar una consulta al ATI a fin de que se seleccione el equipo adecuado.

**POLÍTICAS DE SEGURIDAD LÓGICA PARA EL USO DE SERVICIOS DE RED**

**Artículo 16º** Servicios en los Departamentos.

16.1 Los Departamentos definirán los servicios de Internet a ofrecer a los usuarios y se coordinará con el Departamento de Sistemas para su otorgamiento y configuración.

16.2 Los Departamentos pueden utilizar la infraestructura de la Red para proveer servicios a los usuarios externos y/o visitas previa autorización del Departamento de.

16.3 El Departamento de Sistemas es la responsable de la administración de contraseñas y deberá guardar su confidencialidad, siguiendo el procedimiento para manejo de contraseñas.

16.4 No se darán equipos, contraseñas ni cuentas de correo a personas que presten servicio social o estén haciendo prácticas profesionales en la empresa.

16.5 Los Departamentos deberán notificar al Departamento de Sistemas cuando un usuario deje de prestar sus servicios a la empresa.

16.6 El Departamento de Sistemas realizará las siguientes actividades en los servidores de la empresa:

* Respaldo de información conforme a los procedimientos indicados por el centro de operaciones.
* Revisión de bitácoras y reporte cualquier eventualidad al Departamento de Sistemas.
* Implementar de forma inmediata las recomendaciones de seguridad proporcionados y reportar al Departamento posibles faltas a las políticas de seguridad en cómputo.
* Monitoreo de los servicios de red proporcionados por los servidores a su cargo.
* Calendarizar y organizar y supervisar al personal encargado del mantenimiento preventivo y correctivo de los servidores.

16.7 El ATI es el único autorizado para asignar las cuentas a los usuarios con previa anuencia de los departamentos.

16.8 El Departamento de Sistemas aislará cualquier servidor de red, notificando a los Departamentos de la entidad, en las condiciones siguientes:

* Si los servicios proporcionados por el servidor implican un tráfico adicional que impida un buen desempeño de la Red.
* Si se detecta la utilización de vulnerabilidades que puedan comprometer la seguridad en la Red.
* Si se detecta la utilización de programas que alteren la legalidad y/o consistencia de los servidores.
* Si se detectan accesos no autorizados que comprometan la integridad de la información.
* Si se viola las políticas de uso de los servidores.
* Si se reporta un tráfico adicional que comprometa a la red de la Entidad.

**Artículo 17º** Uso de los Servicios de red por los usuarios

17.1. El usuario deberá definir su contraseña de acuerdo al procedimiento establecido para tal efecto y será responsable de la confidencialidad de la misma.

17.2 El usuario deberá renovar su contraseña y colaborar en lo que sea necesario, a solicitud del Departamento de Sistemas, con el fin de contribuir a la seguridad de los servidores en los siguientes casos:

* Cuando ésta sea una contraseña débil o de fácil acceso.
* Cuando crea que ha sido violada la contraseña de alguna manera.

17.3 El usuario deberá notificar al Departamento de Sistemas en los siguientes casos:

* Si observa cualquier comportamiento anormal (mensajes extraños, lentitud en el servicio o alguna situación inusual) en el servidor.
* Si tiene problemas en el acceso a los servicios proporcionados por el servidor.

17.4 Si un usuario viola las políticas de uso de los servidores, el Departamento de Sistemas podrá cancelar totalmente su cuenta de acceso a los servidores, notificando al departament correspondiente.

**POLÍTICAS DE SEGURIDAD LÓGICA PARA LA CREACIÓN Y CAMBIO DE CONTRASEÑAS.**

**Artículo 18º** Son usuarios de la red institucional los empleados de Cisepro y todas aquellas personas, que tenga contacto directo como empleado y utilice los servicios de la red institucional.

**Artículo 19º** Se asignará una cuenta de acceso a los sistemas de la intranet, a todo usuario de la red institucional, siempre y cuando se identifique previamente el objetivo de su uso o permisos explícitos a los que este accederá, junto a la información personal del usuario.

**Artículo 20º** Se creará una cuenta temporal del usuario, en caso de olvido o extravío de información de la cuenta personal, para brindarse al usuario que lo necesite, siempre y cuando se muestre un documento de identidad personal.

**Artículo 21º** No se proporcionará el servicio solicitado por un usuario, departamentos, sin antes haberse completado todos los procedimientos de autorización necesarios para su ejecución.

**Artículo 22º** La longitud mínima de caracteres permisibles en una contraseña se establece en 6 caracteres, los cuales tendrán una combinación alfanumérica, incluida en estos caracteres especiales, combinación de Mayúsculas y minúsculas.

**Artículo 23º** La longitud máxima de caracteres permisibles en una contraseña se establece en 12 caracteres, siendo esta una combinación de Mayúsculas y minúsculas.

**Artículo 24º** La contraseña será modificada cada tres meses y nunca se podrá repetir la misma.

**Artículo 25º** El Departamento de Sistemas, llevará una bitácora del cambio de las contraseñas.

**RESPONSABILIDADES DEL USUARIO**

Art. 1. El usuario es responsable exclusivo de mantener a salvo su contraseña.

Art. 2. El usuario será responsable del uso que haga de su cuenta de acceso a los sistemas o servicios de la intranet e internet.

Art. 3. Se debe evitar el guardar o escribir las contraseñas en cualquier papel o superficie, para así no dejar constancia de ellas, al menos que éste guardada en un lugar seguro.

Art. 4. El usuario es responsable de eliminar cualquier rastro de documentos proporcionados por el Gestor de Seguridad, que contenga información que pueda facilitar a un tercero la obtención de la información de su cuenta de usuario.

Art. 5. El usuario es responsable de evitar la práctica de establecer contraseñas relacionadas con alguna característica de su persona o relacionado con su vida o la de parientes, como fechas de cumpleaños o alguna otra fecha importante que pueda ser fácil de descifrar.

Art. 6. El usuario deberá proteger su equipo de trabajo, evitando que personas ajenas a su cargo puedan acceder a la información almacenada en él, mediante una herramienta de bloqueo temporal (protector de pantalla), protegida por una contraseña, el cual deberá activarse en el preciso momento en que el usuario deba ausentarse.

Art. 7. Cualquier usuario que encuentre un hueco o falla de seguridad en los sistemas informáticos de la institución, está obligado a reportarlo a los administradores del sistema o gestor de seguridad.

Art. 8. La contraseña se la considerará personal e intransferible.

**POLÍTICAS DE OPERACIÓN DE LOS CENTROS DE CÓMPUTO**

El Departamento de Sistemas podrá ofrecer servicios de cómputo, soporte técnico y servicios audiovisuales en las salas de juntas de la entidad.

**Anexo 1.**

El Departamento de Sistemas dará a conocer dicho reglamento mediante diversos mecanismos como pláticas introductorias y la publicación vía Web y la entrega del documento.

La administración de los servicios de la Red deberá llevarse a través de métodos automatizados.

El Departamento de Sistemas verificara el grado de seguridad del software adquirido e instalado en los equipos.

Para optimizar tiempo y recursos de la Red, se deberá contar con los siguientes elementos mínimos: conexión a la Red y equipo portátil de cómputo en cada sala.

Se podrá dar asesoría siempre y cuando no entorpezca las acciones de mayor relevancia.

El personal del Departamento de Sistemas dará soporte técnico únicamente al equipo de cómputo de la entidad.

El Departamento de Sistemas deberá contar con personal para actividades administrativas, para soporte técnico, para administrar los recursos de cómputo, desarrollo de aplicaciones.

El Departamento de Sistemas deberá contar con servicios automatizados que incluya: Mantenimiento preventivo y correctivo al software, publicación de documentos de normatividad, inventario, El Departamento de Sistemas deberá contar con la siguiente documentación: Información técnica: red, edificios, eléctricas, manuales y procedimientos, normatividad, inventarios de hardware y software, que puedan servir en caso de contingencia.

En caso de daño leve en el equipo, el personal de soporte técnico deberá repararlo o de no lograrlo notificará al usuario para que tome las medidas correspondientes, si el equipo se manda a reparación.

La instalación de Software específico deberá ser realizada en conjunto y común acuerdo del usuario que lo solicite y el Departamento de Sistemas.

**SANCIONES**

**Artículo 26º** Generales

Cualquier acción que vaya en contra de las políticas de seguridad en cómputo de Cisepro Cía. Ltda. Debe ser sancionada con la suspensión de los servicios de cómputo y red, por un período determinado por el Departamento de Sistemas y con el Departamento correspondiente y con conocimiento del Departamento en una primera ocasión y de manera indefinida en caso de reincidencia.

**ANEXO 1**

**REGLAMENTO DE LOS CENTROS DE CÓMPUTO**

**INTRODUCCIÓN**

Con el objeto de proporcionar un buen servicio y adecuado manejo de los equipos existentes, el Departamento de Sistemas ha elaborado el presente reglamento.

Objetivo: Proporcionar servicios de cómputo integral y eficiente para los empleados de Cisepro Cía. Ltda.

**CAPÍTULO I**

**GENERALES**

**Artículo 1.**

Únicamente pueden ser usuarios de los recursos de TIC:

* Los empleados de la entidad.
* Las personas externas previa firma de convenio o autorización de un mando superior.

**Artículo 2.**

El Personal del Departamento de Sistemas estará disponible para contingencias mayores o críticas las 24 horas del día durante los 365 días del año.

**Artículo 3.**

Para tener derecho a los servicios:

Se atenderán las peticiones de los usuarios asignándole el equipo que cubra las expectativas para desarrollar sus actividades, las cuales podrán ser de manera individual o por grupo. En caso de:

* Solicitud de soporte Individual: El usuario deberá utilizar el sistema de Soporte Informático, que para tal efecto estará disponible en todos los equipo de la red.
* Solicitud de soporte para eventos especiales: Las realizará en forma de memorándum el Director correspondiente señalando el detalle del soporte y con un mínimo de 24 horas previo al evento.

**Artículo 4.**

Tiempo de respuesta a solicitudes de soporte:

Las Solicitudes de soporte individual serán atendidas, sin ninguna excepción, el mismo día que se realicen, siempre y cuando sean en horas de oficina.

**Artículo 5.**

Cancelación de solicitudes de soporte:

El personal del Departamento de Sistemas en común acuerdo con el usuario podrá cancelar una solicitud que no proceda, señalando la causa en el cuerpo de la misma.

**Artículo 6.**

Servicios:

Los usuarios deberán respetar las especificaciones que los equipos tengan con respecto al software instalado en general.

El equipo de cómputo asignado, son de uso exclusivo para un usuario.

Los usuarios solo podrán utilizar el equipo de cómputo que les sea asignado. En caso que éste tenga alguna anomalía, deberán reportarlo inmediatamente, para que se le corrija la anomalía.

* El usuario que requiera el uso de software especial que no se encuentre instalado o provisto de manera institucional, deberá solicitarlo al Departamento de Sistemas, previa justificación que la sustente.
* Los usuarios deberán contar con sus discos de trabajo para efectuar los respaldos de su información.

**Artículo 7.**

La instalación y desinstalación de programas es facultad exclusiva del personal del Departamento de Sistemas, si el resguardatario del equipo instala un programa sin previa autorización, cualquier consecuencia por dicha instalación será responsabilidad del usuario.

**Artículo 8.**

Derechos de autor.

Queda estrictamente prohibido inspeccionar, copiar y almacenar software que viole la ley de derechos de autor.

**Artículo 9.**

El Departamento de Sistemas no se hace responsable de la información de los usuarios ajena a los fines de Cisepro almacenada en los discos duros de los equipos de cómputo.

**Artículo 10.**

El Departamento de Sistemas se reserva el derecho de cancelar el servicio total de la TIC en caso de una emergencia mayor.

**Artículo 11.**

Equipo ajeno a la institución:

El usuario que requiera conectar equipos personales a la red o periféricos a las computadoras, deberán contar con la autorización correspondiente de la Dirección de Sistemas, y no será responsabilidad de esta, si el equipo sufre un daño o contaminación por virus. En caso de que un usuario, sin autorización, conecte un equipo o periférico personal al sistema de red de la entidad y este ocasione un daño o contaminación de virus, será total responsabilidad del usuario y se aplicaran las sanciones correspondientes.

**CAPITULO II**

**DERECHOS Y ATRIBUCIONES**

**Artículo 12.**

Son derechos de los usuarios de los recursos de TIC:

* Hacer uso de los servicios de cómputo proporcionados por la entidad
* Reservar el equipo de cómputo para su uso.
* Solicitar una cuenta personalizada a la Dirección de Sistemas.
* Respaldar información en su cuenta personalizada y/o unidades extraíbles.
* Disponer del equipo de cómputo durante el tiempo establecido por la entidad.
* Recibir la capacitación requerida de los programas alojados en su equipo en la fecha y horario que estipule la subgerencia de Informática.
* Recibir este reglamento

**CAPITULO III**

**OBLIGACIONES**

**Artículo 15.**

Son obligaciones del usuario de los recursos de TIC:

* Cuidar su equipo de no sufrir daño físico.
* Notificar al Departamento de Sistemas cualquier anomalía en su equipo y/o programas de cómputo.
* Vacunar sus discos y cuidar que no contaminen el sistema de red de la entidad.
* Cerrar correctamente su sesión como usuario de la red.
* Limpiar y acomodar su área de trabajo al término de su sesión y apagar el equipo de cómputo (CPU, Monitor, Periféricos, Reguladores y Fuentes de Poder).
* Comunicar al DS el retiro de los colaboradores cuando dejen de laborar para Cisepro Cía. Ltda., para que se realicen las configuraciones correspondientes con el fin de que nadie pueda utilizar las contraseñas y accesos de la persona que dejo de laborar, con un plazo máximo de 24 horas.

**CAPITULO IV**

**RESTRICCIONES**

**Artículo 16.**

Queda estrictamente prohibido al usuario:

* Divulgar, vender, negociar, publicar, extraer cualquier tipo de información sensible para Cisepro Cía. Ltda.
* Consumir alimentos, bebidas, fumar y tirar basura, mientras está usando la computadora.
* Conectar cualquier equipo ajeno a la empresa sin autorización.
* Transferir su cuenta asignada por el Departamento de Sistemas.
* Modificar los parámetros de configuración de hardware y software instalado.
* Mover el equipo de cómputo y cambiar los cables de conexión a la red.
* Conectarse a equipos no autorizados.
* Realizar trabajos con fines de lucro.
* Utilizar cualquier tipo de juego.
* Utilizar programas de plática en línea (chat’s) sin autorización.
* Utilizar la infraestructura de la entidad para lanzar virus.
* Utilizar la infraestructura de la entidad para realizar ataques internos o externos.
* Introducir cualquier objeto que genere o emita magnetismo o electromagnetismo.
* Acceder a información que pueda dañar la imagen de la Entidad: faltas a la moral y a las buenas costumbres.
* Ingresar a las áreas exclusivas del personal del Departamento de Sistemas.

**CAPITULO V**

**SANCIONES**

**Artículo 17.**

Las sanciones a que están sujetos los usuarios por incumplimiento de sus obligaciones e incurrir en las restricciones señaladas, son las siguientes:

* Llamada de atención de manera verbal o escrita.
* Suspensión temporal de los servicios de la Red.
* Suspensión definitiva de los servicios de la Red.
* Reposición o pago de los bienes extraviados, destruidos o deteriorados.

**Anexo Recomendaciones para Centros de Cómputo**

**Recomendaciones de uso para el Equipo Multimedia y Equipo de Cómputo.**

1. Usarse en áreas con aire acondicionado
2. Conectarse a tomas de corriente regulada, si están disponibles.
3. Mantenerse alejados de alimentos y bebidas.
4. No forzar las conexiones de los dispositivos de los equipos (éstos sólo pueden conectarse de una forma).
5. Ubicar los equipos de tal forma que el calor generado por éstos no incida sobre equipos de cómputo.
6. No mover ni golpear los equipos cuando están encendidos.
7. Poner los equipos en modo de reposo (stand-by) durante al menos 5 minutos antes de apagarlos de manera definitiva.
8. Al terminar, enrollar los cables y acomodarlos para un transporte seguro. Sin embargo, los cables no deben enrollarse con radios de curvatura muy pequeños, ya que pueden fracturarse.
9. No colocar los proyectores o cañones sobre computadoras portátiles ya que la pantalla líquida puede dañarse.
10. Evitar dejar sin vigilancia los equipos.

**De las Impresiones**

Impresión de trabajos.

1. Para impresiones de “trabajo” se utilizarán hojas recicladas.
2. Solo se utilizará tonners, cintas y tintas originales.
3. No se imprimirán trabajos con fines de lucro ni aquellos que no tengan relación con la Entidad.

**Imprevistos**

Los casos no previstos en este reglamento serán resueltos por el Departamento de Sistemas.

**Vigencia**

Este reglamento entra en vigor a partir del 1 de Agosto del año 2012 y por tiempo indefinido.

Elaborado Por:

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Ing. Jorge Aguirre V.**

**Jefe de Sistemas y seguridad Electrónica**