Reglamento interno para los laboratorios de informática, oficinas y departamentos.

Con el objetivo de prevenir posibles violaciones de la seguridad informática en la Institución y de optimizar el uso de los recursos informáticos puestos a nuestro servicio, se dispone el siguiente reglamento:

1. Laboratorios de Informática.

1.1 Las PC deben cumplir los siguientes requisitos:

- Todas las Pc ubicadas en el laboratorio están en función de la docencia como prioridad. (No hay Pc privativas para el uso de los técnicos)
- Tener configurado el SETUP para que arranque sólo desde el disco duro y a su vez esté protegido por contraseña. (Esta contraseña estará en poder del técnico, el decano de la facultad y el equipo de seguridad informática de la Institución).
- Tener instalados un solo sistema operativo. Tendrán más de uno cuando la actividad relacionada con la docencia lo exija (previa autorización del Jefe de Departamento).
- Tener creados sólo dos sesiones de usuarios para el trabajo.
  - Sesión Usuario "administrador". Este usuario será para el uso exclusivo del técnico de laboratorio, responsable del servicio técnico de la Pc o la red y del equipo de seguridad Informática de la Institución.
  - Usuario "estudiante". Este usuario tendrá propiedades de usuario de avanzada y se utilizará para la docencia y los servicios.

    (En el caso que la actividad docente lo requiera el trabajo con usuarios que posean privilegios administrativos, el técnico previa coordinación, garantizará la creación del mismo y finalizada la actividad lo inhabilitará.)
- Tener instalado, configurado y actualizado correctamente un software antivirus (el acordado por nuestro Ministerio). Para ello se recomienda utilizar los Antivirus NOD32 o KAV Ver 6, el software y actualizaciones periódicas que se publican en el FTP del portal Varona.
- Tener actualizado sistemáticamente el sistema operativo que utiliza con los parches de seguridad.

Para ello podrá descargarlo del FTP del Nodo de la Universidad.

- Al recibir un laboratorio el técnico y el personal designado por el jefe del área, se debe solicitar la clave del servidor al técnico de Copextel, la misma estará bajo la custodia del propio técnico, el decano y el asesor de la seguridad informática del área.
- Si un equipo resulta infestado se deben realizar las siguientes acciones.
  - Desconectar el equipo inmediatamente de la red y hacer una revisión minuciosa con el software antivirus instalado en él.
  - Reiniciar la PC y entrar con la opción de modo seguro.
  - Si es posible, hacer copia de seguridad de sus archivos para poder compararlas con copias anteriores.
  - Ejecutar un programa antivirus.
  - De no ser efectiva la desinfección o eliminación del programa maligno y le sea imposible instalar otro programa antivirus que neutralice la amenaza sin poner en riesgo otros equipos, contacte al equipo de seguridad informática de la Institución. en la siguientes direcciones de correo electrónico: pedroma@ucpejv.rimed.cu o a través del número telefónico 2608284.
  - **Instalar** nuevamente el sistema operativo y restaurar las copias de seguridad
- No pueden instalarse software que violen o intenten violar los servicios de seguridad y trabajo que brinda CICOM (el nodo central).
- Se prohíbe la instalación, así como el uso de los medios informáticos para almacenamiento, ejecución o reproducción de juegos, música, videos, u otro material que no tengan que ver con la actividad docente e investigativa docente, laboral e investigativa de nuestra Institución.
- Tener instalados, configurado y protegido correctamente todo el soporte de Sistema Operativo y de navegación para el trabajo con la Pc del laboratorio.
- Tener instalados el software que se emplean directamente en la docencia, el desempeño laboral o la investigación. El paquete de office, enciclopedias, software educativo, utilitarios y herramientas de programación entre otros.

1.2 Funciones y exigencias que deben cumplir los técnico de laboratorio.

- Deben tener una preparación adecuada en cuanto a conocimientos técnicos informáticos.
- Deben controlar diariamente los recursos Informáticos que están bajo su custodia y hacer

marcado énfasis en la integridad de los sellos de seguridad que coloca el taller central, COPEXTEL u otra entidad que brinde servicios de mantenimiento.

- Para la docencia, debe facilitarle al profesor, el uso de todos los medios informáticos disponibles en el laboratorio y le servirá de apoyo en el desarrollo del proceso docente educativo. Y fiel custodio de la Información almacenada en las Pc por docentes y estudiantes previa coordinación y autorización.

- Debe brindar asesoramiento y protección a los usuarios que acceden a la conectividad y la mensajería electrónica (Intranet, Internet y el correo de la Institución) desde el laboratorio.

  - Evitar que las cuentas y contraseñas de acceso a INTERNET o correo electrónico queden registradas de forma automática en los exploradores de Internet.
  - Garantizar que no existan instalados KEYLOGGER o programas piratas que obtienen esta información.

- Deben revisar con programas antivirus los medios extraíbles que se pretendan introducir en el laboratorio para evitar que sea contaminado por programas malignos.

- Deben apagar y desconectar de la corriente la PC y demás dispositivos de conectividad en caso de descargas eléctricas y posibles tormentas.

- Deben realizar mantenimiento informático y físico sistemático a los medios de cómputos para garantizar el correcto funcionamiento de los mismos, aumentar su eficiencia y rendimiento.

  - Limpiar registros, ficheros temporales, historial de navegación por Internet y contraseñas guardadas.
  - Desfragmentar
  - Quitar elementos innecesarios del menú inicio. Así como información innecesaria (Liberación de espacio en disco)
  - Usar temas y apariencias del sistema operativo acordes con la institución y que no malgasten recursos de memoria.

- Evitar que se introduzcan alimentos en laboratorio, prohibido fumar y mantener una higiene adecuada dentro del mismo.

- No colocar paquetes ni bultos encima de las mesas y/o equipos. Garantizar un área para la

colocación de los mismos.

- Controlar y reportar cualquier incidente de seguridad al grupo central de seguridad informática al cro Irlán vía correo electrónico ic@ucpejv.rimed.cupor.
- Mantener un control estricto sobre las personas que acceden al laboratorio, no permitir que personal ajeno al área de informática y mucho menos a la Institución, instale o configure equipos u opciones en la PC. registrando los siguientes datos en una libreta diseñada para este fin.
  - Nombre y apellidos del usuario.
  - Hora de entrada y salida.
  - Nombre o Nº del equipo que utilizó.
  - Firma.
- Asegurar puertas y ventanas así como la desconectividad eléctrica al concluir la sesión de trabajo.
- Configurar las aplicaciones ofimáticas, el navegador de Internet y el gestor de correo con las opciones de seguridad apropiadas.
- Escribir en el libro o libreta de incidencias cualquier desperfecto o irregularidad detectada e informarlo a la instancia de dirección que se corresponda.

2. Oficinas, departamentos y otros lugares con presencia de recursos informáticos.

2.1 Las PC deben cumplir los siguientes requisitos:

- Tener configurado el SETUP para que arranque sólo desde el disco duro y a su vez esté protegido por contraseña. (Esta contraseña estará en poder del propietario del equipo y el grupo de seguridad informática de la Universidad).
- Tener creados sólo dos usuarios.
  - Usuario "administrador". Este usuario será para el uso exclusivo del equipo de seguridad Informática.
  - Usuario "nombre elegido por el responsable del equipo". Este usuario tendrá propiedades administrativas para garantizar la instalación de software, mantenimiento del equipo, etc.
- Tener instalado, configurado y actualizado correctamente un software antivirus. Para ello se orienta utilizar los antivirus NOD32 o KAV Ver 4 o 6 , los software y actualizaciones periódicas que se publican en el FTP de la Universidad.

- Tener actualizado sistemáticamente el sistema operativo que utiliza con los parches de seguridad. Para ello podrá des cargarlo del FTP del Nodo de la Universidad.

- Si un equipo resulta infestado se deben realizar las siguientes acciones.

  - Desconectar el equipo inmediatamente de la red y hacer una revisión minuciosa con el software antivirus instalado en él.

  - Reiniciar la PC y entrar con la opción de modo seguro.

  - Si es posible, hacer copia de seguridad de sus archivos para poder compararlas con copias anteriores.

  - Ejecutar un programa antivirus.

  - De no ser efectiva la desinfección o eliminación del programa maligno y le sea imposible instalar otro programa antivirus que neutralice la amenaza sin poner en riesgo otros equipos, contacte al equipo de seguridad informática de la Institución. en la siguientes direcciones de correo electrónico: pedroma@ucpejv.rimed.cu o a través del número telefónico 2608284.

  - **Instalar** nuevamente el sistema operativo y restaurar las copias de seguridad

- No pueden instalarse software que violen o intenten violar los servicios que brinda CICOM (el nodo central de la universidad).
- Se prohíbe el uso de los medios informáticos para almacenamiento, ejecución o reproducción de juegos, música y videos que no tengan que ver con el objeto social de la oficina o departamento.
- Al recibir una PC en una oficina o local independiente, se realizarán las pruebas correspondientes a su funcionamiento y será recibida por la persona responsable del medio asignado.

2.2 Exigencias que debe cumplir el responsable del equipo.

- Deben tener una preparación adecuada para el uso del medio informático.

- Deben controlar diariamente los recursos Informáticos que están bajo su custodia y hacer marcado énfasis en la integridad de los sellos de seguridad que coloca el taller central o COPEXTEL.

- Debe brindar protección a los usuarios que acceden a INTERNET y al correo de la Universidad desde su equipo.

  - Evitar que las cuentas y contraseñas de acceso a INTERNET o correo electrónico queden registradas de forma automática en los exploradores de Internet.

  - Exigir a los diferentes usuarios que sus contraseñas sean seguras y cumplan las normas

para su confección.

- Garantizar que no existan instalados KEYLOGGER o programas piratas que obtienen esta información.

- Deben revisar con programas antivirus los medios extraíbles que se pretendan introducir en su equipo para evitar que sea contaminado por programas malignos.
- Deben realizar mantenimiento sistemático al equipo para aumentar su rendimiento.
  - Limpiar registros, ficheros temporales, historial de navegación por Internet y contraseñas guardadas.
  - Desfragmentar
  - Quitar elementos innecesarios del menú inicio. Así como información innecesaria (Liberación de espacio en disco)
  - Usar temas y apariencias del sistema operativo acordes con la institución y que no malgasten recursos de memoria.

2.3 Exigencias que debe cumplir el responsable del equipo respecto a las salvas de información

- Realizar todos los viernes de cada semana, copias de seguridad de la información más importante almacenada en su equipo en CD, DVD y en el espacio del FTP habilitado en los servidores del nodo de la universidad.

Este reglamento forma parte del plan de seguridad informática aprobado para nuestra Universidad. El cumplimiento del mismo será motivo de análisis en los encuentros mensuales del grupo de seguridad informática y se tomará como base para las inspecciones que se realicen a los diferentes laboratorios oficinas y departamentos de la Universidad.

Aprobado por:

Alejandro Miguel Rodríguez Cuervo
Asesor de Seguridad Informática

Georgina Díaz Fernández
Vicerrectora de Tecnología Educativa

Deysí Fraga Cedré
Rectora