UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
RECTORADO

RESOLUCIÓN Nº 057-2019-CU
Lambayeque, 25 de febrero del 2019

VISTO:

El Oficio Nº 063-2019-OGCU-UNPRG presentado por la Oficina General de Calidad Universitaria y el acta de sesión extraordinaria de Consejo Universitario de fecha miércoles 25 de febrero del 2019; sobre aprobación de Protocolo de Seguridad de los Laboratorios de Informática Versión 2.0.

CONSIDERANDO:

Que, con Oficio Nº 063-2019-OGCU-UNPRG de fecha 22 de febrero del 2019 la señora Directora de la Oficina General de Calidad Universitaria hace llegar al despacho del señor Rector el "Protocolo de Seguridad de los Laboratorios de Informática"- Versión 2.0, elaborado por la Ing. en Computación e Informática Dra. Gisella Luisa Elena Maquen Niño, miembro de la Comisión de Licenciamiento Institucional, a fin de que sea aprobado en consejo universitario;

Que, en el marco del Proceso de Licenciamiento Institucional, dispuesto en la Ley N°30220, Ley Universitaria y a lo requerido por la Superintendencia Nacional de Educación Superior Universitaria – SUNEDU, es pertinente que Consejo Universitario apruebe el pedido formulado por la Directora de la Oficina General de Calidad Universitaria;

Que, en sesión extraordinaria de Consejo Universitario de fecha 25 de febrero del 2019 se acordó aprobar por unanimidad el "*Protocolo de Seguridad de los Laboratorios de Informática"- Versión 2.0*, de la Universidad Nacional Pedro Ruiz Gallo;

En uso de las atribuciones conferidas al Rector, la Ley Universitaria 30220 y el Estatuto de la Universidad y estando a lo acordado por Consejo Universitario en sesión extraordinaria de fecha 25 de febrero del 2019;

SE RESUELVE:

1° APROBAR por unanimidad el PROTOCOLO DE SEGURIDAD DE LOS LABORATORIOS DE INFORMÁTICA- Versión 2.0 de la Universidad Nacional Pedro Ruiz Gallo, propuesto por la Directora de la Oficina General de Calidad Universitaria; en el marco del Proceso de Licenciamiento Institucional, exigido por la Ley Nº 30220, Ley Universitaria y por los motivos expuestos por la parte considerativa.

2° Dar a conocer la presente resolución a la SUNEDU, Vicerrectorado Académico, Dirección General de Administración, Órgano de Control Institucional, Oficina General de Calidad Universitaria y demás instancias correspondientes.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE

Dr. JORGE AURELIO OLIVA NÚÑEZ
Rector

Dr. WILMER CARBAJAL VILLALTA
Secretario General

lyrch

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

PROTOCOLO DE SEGURIDAD DE LOS LABORATORIOS DE INFORMÁTICA

ELABORADO POR:	REVISADO POR: Comisión de Licenciamiento Institucional	APROBADO POR: Consejo Universitario Resolución N° -2019-CU
Dra. GISELLA LUISA ELENA MAQUÉN NIÑO MIEMBRO COMISIÓN LICENCIAMIENTO INSTITUCIONAL	M.Sc. MARÍA ROSA VÁSQUEZ PÉREZ PRESIDENTA	Dr. JORGE AURELIO OLIVA NÚÑEZ RECTOR

ÍNDICE

I. PRESENTACIÓN

La Universidad Nacional Pedro Ruiz Gallo, para asegurar la calidad del proceso formativo, cuenta con el potencial humano, infraestructura, equipos y materiales esenciales para desarrollar el proceso de formación profesional.

Entre las herramientas de apoyo al proceso de enseñanza aprendizaje están los laboratorios de informática, que permiten a los actores educativos acceder a programas informáticos y base de datos para desarrollar sesiones de aprendizaje, trabajos de investigación y extensión que requieren de estas tecnologías, por lo que se hace necesario establecer los lineamientos de seguridad en los laboratorios de informática a través de un Protocolo de Seguridad, para que cada persona comprenda su responsabilidad al efectuar su trabajo en esta área, y así poder brindar un mejor servicio en la enseñanza por parte de los docentes y cumplir con los estándares de seguridad para su funcionamiento.

Para la elaboración del presente Protocolo de Seguridad se tomó como referencia los estándares NTP ISO/IEC 27001, la ISO/IEC 27002 y los Protocolos de seguridad existentes en los laboratorios de la escuela de Ingeniería Electrónica y de la facultad de Ingeniería civil, sistemas y arquitectura.

En este sentido, el presente documento tiene como finalidad la prevención de accidentes en las personas que acceden a estas instalaciones donde se realicen las actividades de docencia, investigación y extensión. El beneficio esperado del Protocolo de Seguridad es permitir un adecuado cumplimiento de las funciones del personal técnico que se desempeña en el Laboratorio de Informática, y que los docentes y estudiantes puedan recibir un mejor servicio en la enseñanza, a través de la infraestructura y equipamiento existente.

II. OBJETIVO Y ALCANCE

a. Objetivos

- Establecer políticas de seguridad en los Laboratorios de Informática de las Escuelas Profesionales de la UNPRG.
- Establecer responsabilidades a cada uno de los usuarios involucrados con el uso y cuidado de los laboratorios.
- Proveer procedimientos para controlar el acceso de personal y los recursos necesarios para la operación de los Laboratorios de Informática de la UNPRG.
- Prevenir riesgos de accidentes a los usuarios y daños al equipamiento e instalaciones.
- Gestionar la seguridad física y ambiental en los laboratorios de Informática.

b. Alcance

El presente protocolo debe ser de conocimiento y aplicación obligatoria de todo el personal: docentes, técnicos administrativos, estudiantes, visitantes y otros; que ingresan a desarrollar actividades académicas de enseñanza – aprendizaje, investigación y extensión en los Laboratorio de Informática de las diferentes Escuelas Profesionales de la UNPRG.

III. POLÍTICAS DE SEGURIDAD

a. Responsables de la Seguridad

Los responsables de la Seguridad Informática en los Laboratorios, según el estatuto de la UNPRG:

- El Decano de la Facultad es el encargado de dirigir administrativamente la Facultad y de designar al encargado o Jefe de Laboratorio.
- El Administrador de la Facultad es el encargado de recepcionar y gestionar los requerimientos de infraestructura y tecnología de hardware y software aplicativos para el cumplimiento de las funciones que brinda el Laboratorio de Informática.
- El Jefe del Laboratorio de Informática es el encargado de coordinar, controlar y supervisar que se brinde un buen servicio para la enseñanza en el funcionamiento adecuado de los equipos de los laboratorios de informática y de realizar la gestión de seguridad de los equipos y copias de seguridad de datos de los sistemas informáticos de la facultad.
- Técnico del Laboratorio de Informática es el encargado de proteger los activos del Laboratorio de Informática y realizar las actividades operativas para brindar un buen servicio.

b. Definición de Responsabilidades para la Seguridad de Datos, Sistemas y Equipos

Para una buena seguridad de datos, sistemas y equipos se deben tener en cuenta las responsabilidades de cada responsable:

El Jefe del Laboratorio de Informática es el responsable de gestionar, controlar, proteger y supervisar los activos que pertenecen al Laboratorio de Informática (datos, sistemas y equipos).

El Encargado (Técnico) del Laboratorio de Informática es el responsable de las actividades operativas, para que los usuarios de los sistemas de información puedan cumplir con sus actividades administrativas y los estudiantes y docentes puedan cumplir con sus actividades académicas. Además, será también el encargado de registrar nuevos requerimientos y reportar los incidentes durante el desarrollo de las actividades académicas y administrativas.

En general, el operador administrativo, estudiante o docente que tenga el control físico de un activo serán los responsables inmediatos de su protección.

c. Responsabilidades del encargado del laboratorio en cuanto a seguridad

- Hacer cumplir las normas del laboratorio.
- No permitir que el usuario trabaje solo en el laboratorio.
- Garantizar el funcionamiento adecuado de los equipos de cómputo para el desarrollo de las clases.
- Iniciar el procedimiento de solicitud de reemplazo de un equipo por alguna falla que se presentara.
- Reportar las condiciones inseguras del Laboratorio de Informática.

- Informar inmediatamente al personal nuevo sobre las normas de trabajo y protocolo existente.
- Mantener los suministros en el botiquín de primeros auxilios y solicitar los implementos faltantes a la Oficina de Administración a la cual pertenece los laboratorios.
- En caso de ocurrir algún incendio será responsable de dirigir a los usuarios por las salidas de emergencias a los puntos de reunión previamente establecidos.
- En caso de ocurrir algún accidente, será responsable de avisar en forma inmediata al docente y llamar a un número de emergencia.
- Dar cumplimiento a las medidas de seguridad (para riesgos Químicos, para riesgos Físicos, riesgos Biológicos) en el área respectiva.

d. Responsabilidades de los docentes del laboratorio en cuanto a seguridad

- Hacer cumplir las normas del laboratorio.
- No permitir que un estudiante o invitado trabaje solo en el laboratorio, es decir, sin la presencia de un docente.
- Supervisar el funcionamiento adecuado de los equipos de cómputo antes del desarrollo de clases.
- No mover los dispositivos o partes del equipo de cómputo de un lugar a otro sin el permiso del encargado o jefe de laboratorio.
- Establecer un manejo eficaz de los materiales que se utilizan, así como formar e informar a los estudiantes sobre los riesgos.
- Informar al jefe o encargado de laboratorio en caso se detectara algún fallo en los equipos o material del laboratorio.
- Informar al jefe o encargado de laboratorio sobre las condiciones inseguras del Laboratorio.
- Se debe Supervisar que los equipos de cómputo estén completos y asegurar la desconexión de equipos y el apagado general del fluido eléctrico en el laboratorio al terminar la clase.
- Se debe cerrar la puerta del laboratorio al terminar la clase.
- Informar al encargado del laboratorio de su salida del laboratorio y entregarle las llaves y controles de los equipos.
- En caso de ocurrir algún incendio en su sesión de clase, será responsable de dirigir a los usuarios por las salidas de emergencias e informar al jefe o encargado de laboratorio.
- En caso de ocurrir algún accidente, será responsable de avisar en forma inmediata al jefe o encargado de laboratorio.

e. Normas generales de conducta de estudiantes e invitados que ingresen al laboratorio

- No está permitido ingresar en pantalón corto, faldas cortas, gorra y con el cabello suelto.
- Si tiene alguna herida, cubrirla para evitar contagiarse.

- Mantener en orden y limpieza los lugares de trabajo antes, durante y después de la ejecución de cualquier tarea.
- No portar e ingerir alimentos ni bebidas en el laboratorio de informática.
- Mantener las zonas de paso libre de obstáculos.
- No jugar ni hacer bromas durante el desarrollo de la clase.
- Transitar por el laboratorio con precaución.
- No correr dentro del laboratorio, en caso de emergencia mantener la calma, transitar rápidamente y conservar su derecha.
- Disponer sus prendas y objetos personales en un lugar destinado para tal fin, nunca dejarlos sobre la mesa de trabajo.
- No mover los dispositivos o partes del equipo de cómputo de un lugar a otro sin el permiso del encargado o jefe de laboratorio.
- Los visitantes, sin importar la razón de su visita, deben de estar autorizados antes de entrar al laboratorio y no deben quedarse en ningún momento solo.

f. Normas generales de seguridad al personal que ingrese a trabajar con los equipos al laboratorio

- Previamente se debe consultar las fichas de seguridad de los protocolos o formatos establecidos por el área de trabajo.
- Al ingresar al laboratorio, se debe revisar que todos los equipos de cómputo estén completos y de acuerdo a los formatos de control del área de trabajo.
- Identificar la ubicación y uso actual de los equipos de cómputo de acuerdo a los formatos de control con las que cuenta el laboratorio.
- Conocer la metodología y procedimientos para el trabajo a realizar en el laboratorio.
- Utilizar los elementos de protección personal, de acuerdo al riesgo al cual está expuesto para el mantenimiento de los equipos de cómputo.
- La vestimenta deberá ser apropiada y cómoda, que facilite la movilidad para la actividad que se desarrolla en los laboratorios.
- Si se provocan quemaduras al tocar algo caliente, se debe lavar con abundante cantidad agua fría, eliminar el calor, aplicar pomada para quemaduras que estará en el botiquín.
- En caso de producirse un accidente, quemadura o lesión, comuníquelo inmediatamente al docente o encargado del laboratorio.
- Se debe asegurar de la desconexión de equipos, y el apagado general del fluido eléctrico en cada uno de los laboratorios al terminar el día.
- No debe recibir visitas durante el desarrollo de su trabajo en el laboratorio.

IV. RIESGOS ASOCIADOS A LAS ACTIVIDADES DEL LABORATORIO

- Fatiga visual, fatiga mental y estrés ocasionado por el exceso o deficiencia de la iluminación.
- Muerte por electrocución, paro cardiorrespiratorio y/o quemaduras debido a la exposición a equipos energizados como computadores, impresoras, proyectores y luminaria.

- Lesiones osteomusculares debido a posturas prolongadas y repetitivas durante las prácticas.
- Cefalea, estrés, hipoacusia debido a la exposición a equipos y ruido ambiental.
- Lesiones esqueléticas y de tejidos blandos, accidentes graves o fracturas debido a caídas a nivel o desnivel.
- Disconfort térmico, deshidratación por temperaturas extremas (calor-frio).

V. ESTÁNDARES DE SEGURIDAD

a. Estándares de Seguridad:

- Los tableros y comandos deben ubicarse fuera de las áreas de trabajo, en lugares de fácil acceso y visibles para el personal.
- Los laboratorios deben disponer de un interruptor general para toda la red eléctrica, e interruptores individuales por cada sector, los cuales deben estar identificados y con facilidad de acceso.
- El material eléctrico debe ser a prueba de explosiones por sustancias inflamables.
- No utilizar el mismo terminal eléctrico para equipos que funcionen en forma continua y discontinua.
- Todos los terminales deben contar con una conexión a tierra.
- Los equipos utilizados en área de cómputo deben tener las condiciones necesarias que permitan la movilidad y ajuste para el trabajador.
- La altura y posición del monitor o pantalla del ordenador debe estar ajustado al usuario, permitiendo una distancia cómoda de permitiendo mantener la cabeza posición equilibrada con respecto los hombros, sin tener que doblar o girar el cuello.
- El teclado debe ser móvil y permitir adaptarse a las tareas a realizar en un mismo nivel que el mouse.
- Los usuarios que utilicen USB deberán solicitar al Técnico responsable que se le pase antivirus a sus dispositivos, para evitar que los equipos de cómputo se infecten con virus informáticos.
- Se deberá utilizar estabilizadores de corriente para todos los equipos del Laboratorio de Informática, de esta manera se evitará que las máquinas sufran alteraciones y se puedan conservar en buen estado.
- En caso de derrame de sustancias líquidas en la mesa u otras áreas de trabajo notificar inmediatamente al docente o responsable del laboratorio.
- En caso de electrocutamiento, si la persona queda atrapada en el circuito eléctrico, se debe cortar la fuente de electricidad y liberarla, si no es posible el corte del fluido eléctricos tratar de liberarla utilizando objetos aislantes (madera, plástico, cartón, etc.).

b. Control de acceso a los laboratorios de Informática

- Por el usuario que demanda un servicio (profesores, administrativos, estudiantes, visitantes, otros):

- Esta responsabilidad recae sobre el personal técnico de área de laboratorios, la Jefatura del Laboratorio, Jefatura de Administración y toda la cadena de mando, quienes deben seguir los procedimientos establecidos para estos accesos.
- Personal técnico de área de Laboratorios:
- Solo el personal que labora en estas áreas debe tener acceso en sus horarios respectivos de trabajo. No puede tener acceso a estas áreas fuera de su horario regular de trabajo, a menos que exista una autorización de la autoridad correspondiente o su jefe inmediato.

c. Control de recursos de los Laboratorios de Informática

- Este aspecto de controlar los recursos de estos laboratorios es responsabilidad de todo el personal que labora en estas áreas, desde los técnicos de área de laboratorios, el Jefe de Laboratorio y toda la cadena de mando, siguiendo los respectivos niveles de responsabilidad asignado a cada puesto.
- El encargado directo de estos laboratorios tiene la responsabilidad de que los recursos estén siempre disponibles al máximo de sus capacidades, se usen racionalmente, sean asegurados si fuese el caso, y que su uso en estos laboratorios logre un buen desempeño en las actividades desarrolladas en el mismo.
- También es importante controlar los movimientos que se hagan con el equipo o recursos dentro de los laboratorios de cómputos, llevar seguimiento a estos procesos de circulación, uso y salida de los mismos. Esta labor también es responsabilidad de toda la cadena de mando, desde las autoridades quienes aprueban y desaprueban todos estos movimientos o salidas de equipos de forma temporal o permanente de la instalaciones, siguiendo los correspondientes procedimientos de activos fijos.

d. Elementos de protección general

- Extintor portátil: Es un aparato que contiene un agente extintor (producto cuya acción provoca la extinción) en su interior, que puede ser proyectado o dirigido sobre un incendio por acción de una presión interna, con el fin de apagar el fuego en su fase inicial. Puede transportarse y operarse a mano.
- Botiquín de primeros auxilios: Es el recurso básico para la prestación y atención en primeros auxilios, ya que en él se encuentran los elementos indispensables para dar atención inicial a las personas que sufren alguna lesión o evento y en muchos casos pueden ser decisivos para evitar complicaciones y salvar vidas.

VI. SEGURIDAD FÍSICA DE LOS LABORATORIOS DE INFORMÁTICA.

a. Disposiciones Generales.

Orientados especialmente a la prevención del riego en esta áreas, así como también a la prevención de daños a los recursos tecnológicos y a las instalaciones.

Podemos lograrlo si llevamos a cabo lo siguiente:

- Que las reglas y procedimientos establecidos estén muy bien claras y disponibles para todos, logrando capacitar al personal que dirige o se encargue de los laboratorios de cómputos.
- Es importante que todos vean en la seguridad física un mecanismo de ayuda para sí mismo y para todo el que demande el servicio.
- Todo el personal encargado de los laboratorios debe dar seguimiento de forma dinámica a todas las incidencias que ocurran y que pudiesen ser evitadas por las condiciones que brindan poca seguridad.
- Seguir los lineamientos y procedimientos establecidos en el Plan de Seguridad de la Universidad, es decir, tener personal que activamente se involucre con estos procedimientos y participe activamente en todos los simulacros y formen parte de la brigada de seguridad.
- El Plan de seguridad establece que todo el personal es responsable de la seguridad de la Universidad, por lo que el personal encargado de los laboratorios debe ser parte de esta responsabilidad y asumir su rol en el proceso.
- El Plan de Seguridad establece dentro de sus procedimientos, que todos los encargados de las diferentes áreas de laboratorios deben estar capacitados para saber qué hacer en situaciones de emergencia y cómo actuar para salvaguardar la vida propia y de las demás personas.

b. Dispositivo de Soporte

Se deben considerar los siguientes dispositivos:

- Aire Acondicionado: Esto permite que los Laboratorios de Informática se mantengan a temperatura adecuada para el buen funcionamiento de los equipos y desarrollo de las clases.
- Sensores de humo: Esto permite que los Laboratorios de Informática no se encuentren vulnerables por cualquier incendio.
- Extintores de Incendio: Se debe contar con uno (01) para cada Laboratorio de Informática y 01 para el ambiente de base de datos.
- Alarma contra robos: Se debe contar con un sistema contra robos.
- UPS (Uninterruptible power supply): Debe existir uno (01) ubicado en el ambiente de base de datos el cual atiende exclusivamente a los servidores de la Facultad.
- Red Eléctrica Trifásica.
- Descarga a Tierra (Pozo a Tierra) por cada laboratorio.

c. Gestión de activos

- Todos los activos deberían ser claramente identificados y deberían prepararse y mantenerse en un inventario de todos los activos importantes.
- Toda la información y los activos asociados con los recursos para el tratamiento de la información deberían ser propiedad de la Facultad.
- Las reglas de uso aceptable de la información y los activos asociados con el tratamiento de la información, deberían ser identificadas, documentadas e implantadas.
- Todos los activos que salgan fuera de la Facultad deberían estar registrado en una orden de salida y de la misma manera deberá documentar su retorno

d. Backup (Data de los Sistemas de Información de la Facultad)

- Se debe contar con un procedimiento para la generación de copias de seguridad de las bases de datos de todos los sistemas de información de la Facultad y el lugar físico donde se deben mantener las copias de seguridad.
- El periodo de la generación de las copias de seguridad debe estar acorde a la criticidad de la información y la frecuencia de cambios.
- El almacenamiento de los backups debe estar en un equipo de respaldo al interior de la Facultad con adecuada medida de seguridad y una copia en discos duros externos que será el Jefe de Laboratorio responsable de su custodia.
- El Jefe de Laboratorio será el encargado de realizar las copias de seguridad y de su restauración.
- No se deben usar los servidores de la Facultad como medios de almacenamiento de las copias de seguridad.

e. Estándares de Seguridad del Equipamiento

- Los equipos de cómputo de los Laboratorios de Informática deben estar en ambientes que solo tengan accesos personas autorizadas alumnos y docentes que pertenezcan a la Facultad y que tengan programados clases dentro del horario de clases alcanzados por la Oficina de Procesos Académicos.
- Los Laboratorios de Informática deben contar con áreas de ventilación y detección de incendios.
- Para protegerlos deben cumplir con los siguientes controles
  - Un (01) extintor manual en cada Laboratorio colocando en un lugar estratégico.
  - Sensores de humo instalados en puntos críticos.
- El personal designado deberá estar capacitado para su uso.

f. Estándares de Seguridad para la red eléctrica

- Los tableros y comandos deben ubicarse fuera de las áreas de trabajo, en lugares de fácil acceso y visibles para el personal.
- Los laboratorios deben disponer de un interruptor general para toda la red eléctrica, e interruptores individuales por cada sector, los cuales deben estar identificados y con facilidad de acceso.
- El material eléctrico debe ser a prueba de explosiones por sustancias inflamables.
- No utilizar el mismo terminal eléctrico para equipos que funcionen en forma continua y discontinua.
- Todos los terminales deben contar con una conexión a tierra.
- Situar a los equipos eléctricos fuera del área en que se utilizan reactivos corrosivos.
- Asegurar que todos los cables eléctricos y las cajas de empalme estén levantados del piso. No existan cables sueltos.
- Procurar que todos estos cables no tengan contacto con líquidos ya que pueden provocarse cortos circuitos y ocasionar un incendio.

- Las instalaciones deben estar acondicionadas para drenar agua en caso de darse situaciones como estas, de no ser así, entonces el técnico debe procurar buscar alternativas para drenar el agua.
- Realizar conexiones de balance de carga, para así prevenir recarga en los circuitos o sobrecarga en un circuito en particular.

g. Estándares de Seguridad de iluminación

Las instalaciones de los laboratorios de cómputos deben tener la iluminación adecuada para evitar que los usuarios del servicio tengan que forzar la visión para realizar sus trabajos.

También debe existir buena iluminación para así controlar el vandalismo de los equipos tecnológicos en estas instalaciones.

Es importante que las instalaciones de cómputos tengan luces de emergencia para que los usuarios puedan salir del laboratorio de cómputo sin riegos de accidentes al darse un apagón por varias horas.

h. Estándares de seguridad para operaciones con presión

Se debe dotar de un sistema que permita medir la presión de trabajo y una válvula de seguridad a todos los equipos que operen encima de 0.5 kg/cm2 de presión.

Evitar el uso de aparatos de vidrio o caso contrario deben estar protegidos.

Utilizar protector facial, gafas protectoras y guantes de cuero cuando se trabajen con equipos sometidos a presión.

Para casos de operaciones con vapor, si se realiza una destilación por arrase de vapor se debe evitar que el vapor circule a altas velocidades en el condensador.

i. Estándares de Seguridad sobre primeros auxilios

El encargado del laboratorio de Cómputo debe verificar que el Botiquín de Primeros Auxilios se encuentre ubicado en un lugar visible del recinto y que sea accesible frente a situaciones de accidentes menores.

Si ocurre una emergencia tal como: Contusiones, cortes o abrasiones se deberá comunicar inmediatamente a los encargados del laboratorio de cómputo quienes deberán brindar a los accidentados los primeros auxilios mediante el uso del Botiquín de Primeros Auxilios ubicado en el recinto del Laboratorio.

También se informará al docente que registrará el evento haciendo constar todas las circunstancias, quien conjuntamente con el responsable del laboratorio efectuarán las acciones para que el lesionado sea atendido con prontitud.

j. Estándares de Seguridad sobre incendios

Los encargados de laboratorio deben:

- Verificar que los extintores se encuentren en buenas condiciones de operatividad y éstos debe servir para cualquier clase de fuego y estar al alcance.
- Enseñar a todos la manera de usarlo.
- Procurar no almacenar productos inflamables, pero si tienen que hacerlo guarden los líquidos inflamables en recipientes cerrados y en sitios ventilados.

- Cuidar que los cables de lámparas, CPU. Estabilizadores, proyectores y otros aparatos eléctricos se encuentren en perfectas condiciones. Modere y vigile el uso de parrillas eléctricas, ya que el sistema puede sobrecalentarse.
- No hacer demasiadas conexiones en contactos múltiples, para evitar la sobre carga de los circuitos eléctricos. Redistribuya los aparatos o instale circuitos adicionales.
- Cuidar que por ningún motivo se moje las instalaciones eléctricas. Recuerde que el agua es buen conductor de la electricidad.
- Todo contacto o interruptor debe tener siempre su tapa debidamente aislada.
- Antes de salir, revisar que los aparatos eléctricos estén apagados o perfectamente desconectados.

k. Procedimientos

PROCEDIMIENTO N° 01	
DENOMINACIÓN	MANTENIMIENTO PREVENTIVO Y/O CORRECTIVO DE LOS EQUIPOS DE COMPUTO
EQUIPO DE PROTECCIÓN PERSONAL	**EQUIPOS, HERRAMIENTAS Y MAQUINARIA**
GUANTES, CASCOS, BOTAS DE SEGURIDAD, LENTES PROTECTORES	DESARMADORES, ALICATES DE PINSA, ALICATES DE CORTE, CABLES DE RED PATCH CORD, HERRAMIENTAS DE CONECTORIZACIÓN DE RED, LIQUIDO LIMPIA PANTALLA, BROCHAS PEQUEÑAS, SOPLADORES ELECTRICOS.
DESARROLLO DE LA ACTIVIDAD	
- Correctivo: • Se revisa las conexiones del CPU hacia la salida de energía del estabilizador, la conexión de red, la conexión hacia el proyector. • Si el problema no está relacionado a las conexiones, se revisa el software del equipo. • Si el problema no puede ser detectado con los pasos anteriores se retira el equipo de su ubicación en el mueble para revisarlo internamente, por lo que debe ser trasladado a taller de Soporte Técnico y se procede con la instalación de un equipo de Backup. - Preventivo: • Se retira uno a uno los equipos de los laboratorios y aulas para proceder con su limpieza externa y si el equipo ya no está en garantía se destapa para su limpieza interna utilizando sopladores eléctricos. • Se vuelven a instalar los equipos en sus ubicaciones dentro de los muebles y se inicia el proceso de instalación y configuración de software y pruebas de funcionamiento.	

CONSIDERACIONES
- Utilizar el equipo de protección en todo momento. - Si se realiza limpieza interna por medio de sopladores, se debe utilizar lentes de protección y mascarillas para evitar problemas por exposición al polvo. - Si el equipo se debe trasladar a Soporte Técnico, guardar el debido cuidado al trasladarse por medio de las escaleras de acceso peatonal y las veredas. - Al retirar el equipo de almacén, tener cuidado al sacarlo del apilamiento para no provocar caídas de otros equipos, siempre ir acompañado para tener ayuda en caso de algún accidente. - Es importante que la Oficina General de Proyectos e Infraestructura – División de desarrollo físico, realicen una revisión constante al estado de las llaves diferenciales, conexiones eléctricas y pozos a tierra de cada laboratorio de cómputo.

PROCEDIMIENTO N° 02	
DENOMINACIÓN	MANTENIMIENTO PREVENTIVO, RETIRO E INSTALACIÓN DEL PROYECTOR MULTIMEDIA

EQUIPO DE PROTECCIÓN PERSONAL	EQUIPOS, HERRAMIENTAS Y MAQUINARIA
GUANTES, CASCOS, BOTAS DE SEGURIDAD, LENTES PROTECTORES	ESCALERA, DESARMADORES, LLAVES TUERCAS.

DESARROLLO DE LA ACTIVIDAD

- La actividad requiere de dos personas, primero deben instalar correctamente la escalera, utilizar los dos los equipos de protección personal.
- Uno de los colaboradores sube a la escalera y otro queda de apoyo para evitar que la escalera se mueva.
- Si se requiere cambiar el filtro
  - Se procede retirando el tornillo del filtro para retirar el filtro sucio e instalar el filtro limpito.
  - Se guarda el filtro sucio para llevar a Soporte Técnico.
- Si la actividad requiere retirar el proyector:
  - Se retiran con cuidado los tornillos o pernos de sujeción
  - Se retira el proyector multimedia y se entrega al colaborador de apoyo.
- Si la actividad requiere de instalar el proyector:
  - El colaborador de apoyo alcanza el proyector
  - Se coloca el proyector en los tubos de soporte y se procede a asegurarlo por medio de los tornillo o pernos de sujeción

CONSIDERACIONES

- Utilizar en todo momento los equipos de protección personal
- Desconectar el proyector de la energía eléctrica antes del proceso
- Siempre realizar el trabajo en pareja, ambos con los equipos de protección
- Verificar que el proyector no esté caliente al realizar el procedimiento.

PROCEDIMIENTO N° 03	
DENOMINACIÓN	TRASLADO E INSTALACIÓN DE NUEVOS EQUIPOS

EQUIPO DE PROTECCIÓN PERSONAL	EQUIPOS, HERRAMIENTAS Y MAQUINARIA
GUANTES, CASCOS, BOTAS DE SEGURIDAD, LENTES PROTECTORES	CARRETILLA.

DESARROLLO DE LA ACTIVIDAD

- Se procede con el retiro de las computadoras (CPU, Monitor, Teclado, Mouse) del almacén en grupos de 06 a 08 equipos y se apilan en la carretilla.
- Se desplazan hacia el laboratorio en el cual se realizará la instalación
- Si el laboratorio se encuentra en el 2do o 3er piso, cada colaborador cargará hasta 02 CPU o 04 Monitores LED o utilizando cajas hasta 08 Teclados y 08 Mouse o 02 proyectores multimedia
- Se instalan los equipos de cómputo en sus respectivos muebles
- Se realiza la conexión hacia la energía eléctrica y la red de datos, así mismo se conectan los periféricos hacia la CPU.

CONSIDERACIONES

- Al utilizar la caretilla, no llenar la carretilla al punto de interrumpir la visión del camino, ni al punto que los equipos puedan caerse.
- Al subir las escaleras, no realizar sobre esfuerzos, y tener cuidado al subir, de ser posible solicitar acceso exclusivo a la escalera de acceso peatonal de la zona.
- Al acceder a los muebles realizarlo de tal forma que no se provoquen esfuerzos musculares o articulares excesivos.
- Es importante que la Oficina General de Proyectos e Infraestructura - División de desarrollo físico, realicen una revisión constante al estado de las llaves diferenciales, conexiones eléctricas y pozos a tierra de cada laboratorio de cómputo.

PROCEDIMIENTO N° 04		
DENOMINACIÓN	DICTADO DE CLASES EN LABORATORIOS DE INFORMÁTICA	
EQUIPO DE PROTECCIÓN PERSONAL		**EQUIPOS, HERRAMIENTAS Y MAQUINARIA**
NO REQUERIDO		LOS EQUIPOS DE CÓMPUTO

DESARROLLO DE LA ACTIVIDAD

- El docente junto con sus estudiantes accede al laboratorio de cómputo
- Si se detecta alguna falla en el funcionamiento de algún equipo se debe llamar al técnico de laboratorio para que pueda realizar la revisión y habilitación del equipo.
- El docente indica y vigila que los estudiantes no manipulen las conexiones eléctricas, video o de red de los equipos de cómputo.
- El docente indica y vigila que no se lleven alimentos sobre todo líquidos a los laboratorios de cómputo
- Al terminar la sesión los estudiantes apagan los equipos, el docente hace lo mismo con su equipo y proyector, y se retiran en orden, el docente revisa que todo quede correctamente apagado y cierra el laboratorio.
- Después el técnico revisa que todo está correctamente apagado y asegura el laboratorio hasta la próxima clase.

CONSIDERACIONES

- Es importante que tanto docente como estudiante no manipulen las conexiones eléctricas, video y red de datos, en caso sea necesario llamar al técnico, él con su equipo de protección personal realizará la revisión y reconexión de ser el caso tomando las medidas de seguridad necesarias.
- Es importante no portar bebidas dentro del laboratorio para evitar el riesgo de electrocución por derrames de líquidos en los equipos electrónicos.
- Es importante que la Oficina General de Proyectos e Infraestructura - División de desarrollo físico, realicen una revisión constante al estado de las llaves diferenciales, conexiones eléctricas y pozos a tierra.

VII. PROTOCOLOS ANTE EMERGENCIAS Y ACCIDENTES

a. PROTOCOLO EN CASO DE SISMO

En caso de sismo el objetivo es proteger la integridad física de los trabajadores, alumnos y posibles visitantes en las zonas de seguridad, es decir, lugares debidamente preestablecidos, para que el personal pueda ubicarse temporalmente.

Antes del sismo o terremoto:

Señalización:

- Se debe identificar y señalizar las zonas de seguridad interna, rutas de escape y salidas de emergencia.
- Identificar los puntos de reunión.
- Hacer de conocimiento a todo el personal a las zonas de seguridad internas, rutas de escape, salidas de emergencia y puntos de reunión.

Rutas de evacuación

- Se debe verificar constantemente que los objetos ubicados en lugares elevados (p.e. ventiladores, aire acondicionado, luminarias) se encuentren firmemente sujetos de tal manera que no puedan caer.
- Se debe verificar permanentemente la buena distribución y ubicación de muebles y objetos.
- Verificar que en todo momento se mantengan las rutas de salida o escape libres de cualquier obstáculo, de tal manera que permita la fluidez de la evacuación.

Durante el sismo o terremoto:

- Una vez iniciado el sismo se procederá a ubicase en las zonas seguras, hasta que cese el movimiento.
- En las zonas de reunión se deberá esperar por lo menos 15 minutos, con la finalidad de prevenir una réplica, en este lapso los brigadistas verificarán que todo el personal de su área ha evacuado a la zona de reunión. De ser necesario, se procederá a la evacuación del establecimiento.
- Los brigadistas de Emergencias determinarán si las condiciones lo permiten, el retorno a las instalaciones.

Al finalizar el sismo o terremoto:

- Luego de terminado el sismo, se debe evaluar los daños a los equipos e instalaciones del local, así como preparar los informes correspondientes.
- Finalmente, se deberá analizar las acciones tomadas para proteger los equipos, las brigadas, los monitores de emergencias, así como la actuación del personal en general durante la evacuación de las instalaciones, a fin de aprovechar la experiencia obtenida para corregir errores

b. PROTOCOLO EN CASO DE ACCIDENTES MAYORES (caídas de altura, electrocución, quemaduras, otros)

El objetivo es proteger al personal accidentado mediante primeros auxilios y traslado de inmediato a un hospital o clínica para su atención médica por profesional médico especializado.

Antes del accidente:

Se debe capacitar al personal responsable del laboratorio en el curso de primeros auxilios, a fin prepararlos para auxiliar al compañero accidentado, alumno o visitante, hasta la llegada del personal médico o paramédico al lugar del accidente o su traslado a un nosocomio para su atención profesional.

Durante el accidente:

- Auxiliar de inmediato al accidentado empleando Acciones Generales de Primeros Auxilios.

Después del accidente:

- Analizar las causas del accidente y las acciones tomadas para auxiliarlo en el lugar, así como la demora en el arribo de la ambulancia o auxilio médico.

c. PROTOCOLO DE INCENDIOS

- Revisar periódicamente el perfecto estado de los extintores.
- Un conato de incendio, puede ser sofocado arrojando un trapo húmedo sobre él, retirar las sustancias volátiles que se encuentren cerca para evitar la propagación del incendio.

- Si se produce un incendio tener en cuenta:
  - Retirar los productos químicos inflamables que se encuentren cerca del fuego y los objetos que sirvan de combustible al fuego en la medida de sus posibilidades.
  - Si usted ha sido capacitado en el uso de extintores y la intervención no extraña peligro, ubíquese entre el fuego y la salida de escape (por ejemplo, la puerta) e intente extinguir el fuego desde su posición, pero se debe asegurar que se pueda salir del área.
  - Escoja el extintor según el tipo de fuego generado para un equipo eléctrico debe utilizarse el extintor de CO_2 (solo para conatos).
  - Si no sabe usar el extintor, cierre puertas y ventanas (si la magnitud del fuego lo permite) y desaloje la zona.
- Si la magnitud del fuego ha pasado de la etapa incipiente, evacue todas las personas del laboratorio de forma ordenada (sin correr).

d. PROTOCOLO DE INUNDACIONES

Antes de la inundación:

- Mantener en buen estado el techo, así como la bajada de agua de los edificios para evitar humedades y que se traspase el agua de un piso a otro.
- Mantener en buen estado las llaves y tuberías de agua de los lavatorios y servicios higiénicos.

- No dejar productos peligrosos ni documentos importantes en zonas propensas a quedar afectados por el agua y se deterioren.
- Identificar la ubicación de las llaves principales de Agua y de fluido eléctrico.
- Identificar una ruta de evacuación, y otras vías alternativas y estar preparado para evacuar.
- Cortar la luz, agua y gas y evacuar si la situación lo amerita o las autoridades así lo indican.

Durante la inundación:

- En caso de inundación, abandonar lo antes posible los recintos de los laboratorios. Además, debemos cortar la corriente eléctrica.
- Ubicarse en un lugar seco y permanecer allí. Evitar caminar sobre el agua.

Durante una evacuación:

- Si la situación así lo amerita o las autoridades lo indican, evacuar lo antes posible los laboratorios.
- No acercarse a cables ni aparatos eléctricos.
- No caminar cerca de donde está el agua.

Después de la inundación:

- No regresar a los laboratorios de cómputo hasta que las autoridades indiquen que lo puede hacer.
- Limpiar sustancias como medicamentos, y productos inflamables.
- No tocar ni pisar cables eléctricos caídos.

En un lugar visible y de fácil acceso dentro del laboratorio debe mantenerse:

- Horario de atención del laboratorio
- Líneas de emergencia
- Número telefónico de la Dirección/ Jefatura de la cual depende el laboratorio

Universidad Nacional Pedro Ruiz Gallo
Calle Juan XIII N° 391 – Lambayeque
(074) 283146 / 283115 / 282120 / 282356

EMERGENCIAS	
ENTIDAD	***TELÉFONO***
Oficina de Bienestar Universitario	*Anexo 2460 / 2461*
Puerta Principal/ Garita de Control Empresa de Vigilancia VISEN SRL	*947566556 / 945281771*
Hospital Belén de Lambayeque	*(074) 281190*
Policlinico ESSalud "Agustin Gavidia salcedo" - Lambayeque	*(074) 283719*

EMERGENCIAS	
ENTIDAD	***TELÉFONO***
Hospital Nacional Almanzor Aguinaga	*(074) 237776*
Hospital Regional las Mercedes	*(074) 229341*
Hospital Naylamp	*994158008*
Hospital Privado Metropolitano	*(074)228802*
Clínica El Pacífico	*(074)228585*
Clínica Max Salud	*(074)226201*
Cia. de Bomberos "Salvadora Lambayeque" N° 88	*(074)283520*
Cia. de Bomberos Nº 27 -Chiclayo	*(074)222422 / (074)23333*
Electronorte S.A.	*(074) 481200*
Comisaria Sectorial de Lambayeque	*(074) 282119*
Comisaria San Martín de Porras	*(074) 281673*

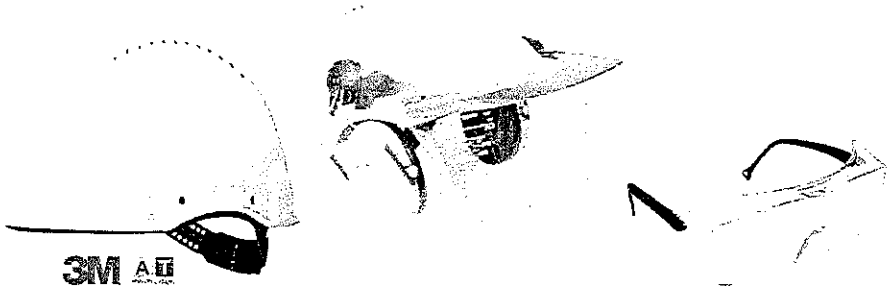
VIII. ELEMENTOS DE PROTECCIÓN PERSONAL

En el laboratorio se realizan operaciones muy diversas, de corta duración, en las que se manipulan gran variedad de productos con diferentes características de peligrosidad, siendo a menudo, difícil adoptar medidas de protección colectiva eficaces y resultando en muchos casos, riesgos residuales. Es en estas circunstancias cuando debe recurrirse a los equipos de protección individual, que han de ser adecuados frente a los riesgos de los que se quiere obtener protección mediante su correspondiente certificación (marca CE). Los EPI más utilizados en el laboratorio son los protectores de los ojos, de la piel y de las vías respiratorias.

a. Protección de cabeza, la cara y los ojos

Los equipos destinados a la protección de la cara y los ojos permiten protegerse frente a los riesgos causados por proyecciones de partículas sólidas, proyecciones

de líquidos (corrosivos, irritantes) y exposición a radiaciones ópticas (infrarrojo, ultravioleta, láser). Se pueden clasificar en dos grandes grupos: pantallas y gafas-



Los cascos protegen la cabeza, ante la caída de objetos contundentes. Es alta mente recomendable su uso en trabajos en altura

Las gafas protegen los ojos del trabajador. Se recomienda su uso permanente en los laboratorios.

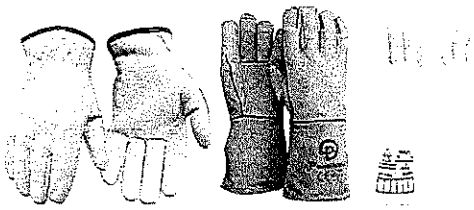
Las pantallas cubren la cara del usuario, no solamente los ojos. Existen dos tipos de pantallas, faciales y de soldador.

Si el uso de pantallas o gafas está destinado a la protección frente a algún tipo de radiaciones deben estar equipadas con visores filtrantes a las mismas.

b. Protección de la Piel

- **Protección de las Manos**

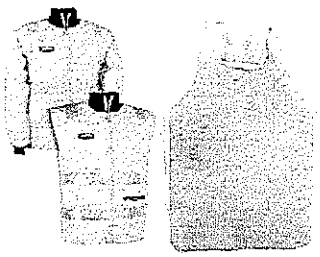
Los guantes son el sistema de protección de las manos y brazos más utilizado ante la posibilidad de riesgos de corte, golpes, contacto dérmico o contacto térmico y contacto eléctrico.



- **Protección del Cuerpo**

Para la protección del cuerpo frente a proyección de chispas o metal emplear mandiles de cuero. El riesgo de impregnación de la ropa se puede prevenir empleando delantales, mandiles, batas, ropa de trabajo o protección adecuada a las características de peligrosidad del agente manipulado. En caso de contacto con un

producto químico debe procederse al lavado inmediato de la protección y si se ha impregnado la ropa de trabajo, quitársela inmediatamente y proceder a su lavado.

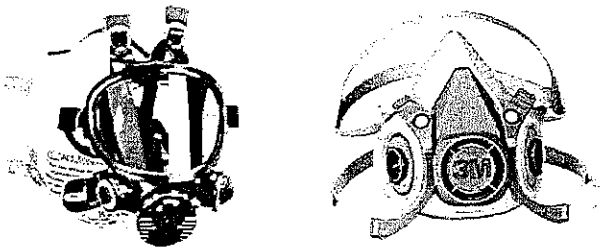


c. Protección de las vías respiratorias

Los equipos de protección individual de las vías respiratorias son aquellos que tratan de impedir que el contaminante penetre en el organismo a través de esta vía. Técnicamente se pueden clasificar en equipos dependientes e independientes del medio ambiente.

- **Equipos dependientes del medio ambiente**

Son equipos que utilizan el aire del ambiente y lo purifican, es decir retienen o transforman los contaminantes presentes en él para que sea respirable. Estos equipos no pueden utilizarse cuando el aire es deficiente en oxígeno, cuando las concentraciones de contaminante son muy elevadas o se trata de sustancias altamente tóxicas o cuando existe el peligro de no detectar su mal funcionamiento (por ejemplo, un gas sin olor como el monóxido de carbono). Presentan dos partes: el adaptador facial y el filtro. El adaptador facial crea un espacio herméticamente cerrado alrededor de las vías respiratorias, de manera que el único acceso a ellas sea a través del filtro. Existen diferentes filtros según los productos químicos que se utilicen y se tienen diferentes tamaños de poro según el tamaño de partícula.



IX. SEGURIDAD LÓGICA

La Seguridad Lógica consiste en asegurar que personas autorizadas solo podrán tener acceso a los datos y sistemas.

Los objetivos que se plantean son:

- Restringir el acceso a los programas y archivos.
- Asegurar que el operador administrativo pueda tener acceso al sistema de información (Sistema de Contabilidad y Sistema de Gestión Académica Ficsa).
- Restringir que los estudiantes y docentes puedan modificar archivos del sistema operativo, las aplicaciones instaladas o instalar nuevas aplicaciones.
- Asegurar que los usuarios (estudiantes y docentes) estén utilizando los datos, archivos y aplicaciones correctas.

a. Procedimientos Formales para la concesión de Identificador de Usuarios y Contraseñas

i. Identificador de Usuario

Es la que permite a un usuario de forma individual acceder a un sistema como se detalla a continuación:

- Operador Administrativo podrá acceder al sistema de información.
- Estudiante y docente podrá acceder al sistema operativo para el uso de las aplicaciones instaladas.

ii. Autenticación al Sistema Operativo

En la interfaz del sistema se mostrará los siguientes datos:

- Nombre de usuario
- Password

El password se mostrará de manera oculta por su seguridad.

Cuando el usuario (estudiantes y docentes) se loguea correctamente podrá acceder al Sistema Operativo y hacer uso de las aplicaciones instaladas.

iii. Autenticación al Sistema de Información (Por parte del encargado o jefe de laboratorio)

En la interfaz del sistema se mostrará los siguientes datos:

- Nombre de usuario
- Password

El password se mostrará de manera oculta por su seguridad.

Cuando el operador administrativo logra conectarse al Sistema de Información podrá hacer uso del sistema y desarrollar sus actividades administrativas.

iv. **Contraseña**

La contraseña de acceso es la principal protección porque valida al usuario y deja hacer uso del sistema. Para la protección de los Activos de Información del Laboratorio de Informática y la protección del usuario mismo se debe considerar que las contraseñas deben tener las siguientes características:

- Es secreta y personal
- No se visualiza en pantalla mientras se teclea
- Tiene una longitud mínima de 08 y máxima de 12 caracteres.
- Es alfanumérica

v. **Modificación de Usuarios**

El acceso de cada usuario (estudiantes y docentes) en los laboratorios se modificará cada vez que se vea en riesgo su conocimiento de la contraseña o cada mes se cambiará por una nueva contraseña.

En el caso del operador administrativo se modificará su contraseña cuando sea cambiado a otra oficina o facultad, o no recuerde, o crea que está en riesgo el conocimiento de su contraseña.

b. Administración de Roles

i. **Roles**

Para una buena seguridad lógica se deberá considerar la creación de los siguientes roles:

- Rol de administrador permitirá realizar las tareas de administrar los usuarios, instalación y desinstalación de software, Actualizar el sistema operativo según sea accesibles a nuevas versiones, configuración de las políticas de seguridad para los usuarios, crear políticas de copias de seguridad y recuperación.
- Rol de docente permitirá acceder a las aplicaciones instaladas y además compartir carpetas para que los estudiantes puedan acceder al material otorgado por el docente.
- Rol del estudiante permitirá solamente el uso de las aplicaciones instaladas.

X. SEGURIDAD EN LA COMUNICACIONES

a. Antivirus

- En todos los equipos de los Laboratorios de Informática deberá existir un antivirus ejecutándose permanentemente y en continua actualización.
- La actualización de los antivirus de todos los equipos de cómputo se debe realizar según lo requiera el antivirus a través de un procedimiento formal. El técnico del laboratorio es el responsable de cumplir dicho procedimiento.
- Deberá existir un procedimiento formal a seguir en caso que se detecte un virus en algún equipo de cómputo.

b. Firewall

- Deberá existir una solicitud formal hacia la Oficina Central de Informática especificando todo lo que está prohibido.

XI. SEGURIDAD DE APLICACIONES

a. Control de las Aplicaciones en PC's

- Deberá existir un procedimiento donde se especifique que aplicaciones deberán ser instaladas en cada uno de los laboratorios por solicitud de los docentes para el desarrollo de sus clases.
- Antes de realizar algún cambio en la configuración de los servidores se debe realizar una copia de seguridad. Una vez hecho el cambio se debe documentar el motivo de la configuración.
- Se deben documentar los procedimientos de instalación, la reparación de equipos y cada uno de los mantenimientos que se les realicen.
- La instalación de una nueva aplicación por parte del docente se deberá solicitar 48 horas antes de su clase, una vez hecha la instalación se deberá documentar en el registro de instalación.

XII. CUMPLIMIENTO DEL PROTOCOLO

El Decano es la autoridad responsable de velar por el cumplimiento del protocolo de seguridad en los laboratorios de informática, así como brindar los recursos necesarios para la adecuación de los laboratorios en cuanto las normas de seguridad, así como de capacitar al personal directamente involucrado.