UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

LABORATORIOS GENERALES

MANUAL DE SEGURIDAD
PARA LOS LABORATORIOS GENERALES DE COMPUTACIÓN

Julio 2023

ÍNDICE

1. INTRODUCCIÓN 3
2. OBJETIVO 3
3. MARCO LEGAL 3
4. ÁMBITO DE APLICACIÓN 4
5. DEFINICIONES 4
6. NORMATIVAS DE SEGURIDAD PARA EL USO DE LOS LABORATORIOS DE COMPUTACIÓN 5
   6.1. SEGURIDAD FÍSICA 5
   6.2. SEGURIDAD DE DATOS 6
   6.3. SEGURIDAD ELÉCTRICA 7
   6.4. SEGURIDAD DEL HARDWARE 7
   6.5. SEGURIDAD DE SOFTWARE 8
7. CONTROL DE CAMBIOS 10
8. VIGENCIA Y AUTORIZACIÓN 10

1. INTRODUCCIÓN

El presente Manual de Seguridad es creado por los Laboratorios Generales de Computación pertenecientes al Departamento de Ciencias de la Computación, para establecer y promover pautas de seguridad que garanticen un entorno de trabajo seguro y protegido en el laboratorio de computación.

La seguridad es una responsabilidad compartida, por lo que es fundamental que todos los usuarios y miembros del laboratorio se familiaricen con las prácticas de seguridad descritas en este documento.

Al seguir estas directrices, contribuimos a mantener la integridad de los recursos tecnológicos, la confidencialidad de los datos y, sobre todo, a garantizar un ambiente de trabajo seguro y confiable para todos.

2. OBJETIVO

Elaborar un manual de seguridad para los Laboratorios Generales de Computación del DCCO, el cual ayudará a Garantizar la seguridad y protección integral de los usuarios, equipos y datos en el laboratorio de computación, mediante la implementación de procedimientos seguros, con el fin de prevenir accidentes, minimizar riesgos y promover un entorno de trabajo seguro y confiable para todos los usuarios.

3. MARCO LEGAL

- **RESOLUCION ESPE-HCU-RES-2020-109** En la cual resuelve que el “Reglamento interno para la asignación, uso y control de la infraestructura y servicios de tecnologías de la información y comunicaciones de la Universidad de las Fuerzas Armadas – ESPE.”
- **Reglamento Orgánico de la Universidad de las Fuerzas Armadas ESPE**. Art. 38· Gestión de Tecnología de la Información y Comunicación.
- Normas de Control Interno para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que dispongan de Recursos Públicos 410-04 Políticas y procedimientos. - “… Será necesario establecer

procedimientos de comunicación, difusión y coordinación entre las funciones de tecnología de información y las funciones propias de la organización…"

- **Resolución ESPE-HCU-RES-2022-059** Reglamento Interno de Creación y Administración de los Laboratorios.

4. ÁMBITO DE APLICACIÓN

El Manual de Seguridad tiene como lugar de aplicación las instalaciones tecnológicas de los laboratorios generales pertenecientes al Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas – ESPE.

5. DEFINICIONES

- **Laboratorista:** Profesional que trabaja en el campo de la informática siendo este analista o técnico de laboratorio encargado de precautelar la integridad y buen uso de los laboratorios de computación.
- **Periféricos:** Son instrumentos tecnológicos externos a una computadora, que funcionan con la misma siendo estos: teclado, mouse, parlantes, etc.
- **Software:** Son los programas informáticos que hacen posible la ejecución de tareas específicas dentro de un computador.
- **Hardware:** Es la parte física de un sistema informático, que incluye todos los componentes tangibles y visibles, como la CPU, la memoria, el disco duro, el monitor y los dispositivos periféricos.
- **Bitácora:** Conjunto de hojas escritas en las que se recogen toda la información o registros de relevancia para los laboratorios.
- **DCCO:** Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas – ESPE.
- **Franjas Institucionales:** Sirven para clasificar períodos de horarios en los que se divide la institución.

6. NORMATIVAS DE SEGURIDAD PARA EL USO DE LOS LABORATORIOS DE COMPUTACIÓN

La importancia de un manual de seguridad radica en su capacidad para proporcionar pautas claras y procedimientos definidos que garantizan la protección de personas, activos e información dentro de los Laboratorios de Computación. Ayuda a prevenir accidentes, minimizar riesgos y fomentar un ambiente de trabajo seguro y confiable.

Además, promueve la conciencia y responsabilidad en el manejo de recursos, protegiendo el bienestar de todos los involucrados y asegurando la continuidad operativa de los Laboratorios de Computación.

Dentro de los Laboratorios de Computación, es importante considerar varios tipos de seguridad para proteger tanto a los usuarios como los equipos y datos presentes.

A continuación, se enumera los principales tipos de seguridad que se implementa dentro de los Laboratorios Generales del DCCO:

6.1. SEGURIDAD FÍSICA

Implica proteger el acceso al laboratorio y asegurar que solo el personal autorizado, laboratoristas, Director(a) del Departamento de Ciencias de la Computación, Jefe de Laboratorios y Docentes Autorizados, los cuales pueden ingresar al área siendo fundamental el garantizar la seguridad y la confidencialidad de los recursos presentes en el laboratorio de computación.

El Establecer medidas de control de acceso es una estrategia efectiva para evitar intrusiones no deseadas y salvaguardar los activos del laboratorio de computación y por ende de la Institución.

A continuación, se muestra las medidas para este tipo de seguridad:

- **Implementación de sistemas de cerraduras electrónicas** en puertas de acceso basado en tags con códigos de identificación, permite controlar y registrar de manera precisa quiénes pueden ingresar al laboratorio y en qué momentos.
- **El monitoreo constante a través de cámaras de seguridad y sistemas de control de movimiento** proporciona una vigilancia activa que disuade cualquier intento de acceso no autorizado o afectación a algún activo de los laboratorios.

- **El control de visitantes** es igualmente esencial para garantizar la integridad del laboratorio, mediante el correcto acceso de estudiantes junto con el docente que tiene clases dentro de la franja institucional, el cual debe asegurar que los estudiantes cumplan con las normas establecidas dentro del Manual de Uso de Laboratorios Generales del DCCO.
- **Ningún** estudiante o visitante puede permanecer en el laboratorio una vez que haya terminado la clase.
- De acuerdo a la protección física de los computadores: Los estudiantes y profesores **NO** deben consumir ningún tipo de alimento o bebida dentro de los laboratorios, a fin de mantener la limpieza y orden en las instalaciones.

En conjunto, estas medidas de seguridad en el acceso a los Laboratorios se convierten en una barrera efectiva contra posibles amenazas internas y externas, garantizando que solo el personal autorizado y los visitantes debidamente identificados tengan la posibilidad de interactuar con los Laboratorios Generales DCCO.

6.2. SEGURIDAD DE DATOS

Se refiere a la protección de la información y los datos almacenados en las computadoras y servidores del laboratorio, lo cual es crucial para preservar la confidencialidad, integridad y disponibilidad de los activos digitales. A continuación, se muestra las siguientes directrices de seguridad datos implementada en los laboratorios de computación:

- El acceso a los servidores es de **USO EXCLUSIVO** de los Laboratorios, se limita a la modificación de solo el personal de laboratorio autorizado y basado en permisos de administrador otorgados previamente, limitando este acceso con credenciales de red.
- Queda **PROHIBIDO** guardar información importante o delicada en las computadoras del laboratorio, el laboratorista no se hace responsable de la información almacenada por error o intencionalmente.
- Los usuarios **NO** deben usar el computador en actos que vayan en perjuicio de la moral y las buenas costumbres.

En conjunto, estas medidas de seguridad de datos son esenciales para mantener la confidencialidad y la integridad de la información almacenada en el laboratorio de informática. Al proteger adecuadamente los activos digitales, se construye un entorno de confianza y se asegura la continuidad operativa de las actividades del laboratorio.

6.3. SEGURIDAD ELÉCTRICA

Implica garantizar que los sistemas eléctricos sean seguros y estén protegidos contra sobrecargas y cortocircuitos, lo cual es esencial para prevenir daños a los equipos y garantizar la continuidad operativa del laboratorio de Computación. Para ello, se deben realizar las siguientes directrices:

- Inspecciones regulares de las instalaciones eléctricas, asegurándose de que cumplan con las normativas y estándares de seguridad establecidos por la institución.
- El uso de dispositivos de protección en ubicaciones específicas, como reguladores de voltaje y Sistemas de Alimentación Ininterrumpida (UPS). Un UPS proporciona una fuente de energía de respaldo en caso de que se produzca una interrupción del suministro eléctrico principal. Esto permite que los equipos conectados al UPS sigan funcionando temporalmente durante cortes de energía, brindando tiempo suficiente para guardar datos importantes y apagar los equipos de manera segura.

La prevención de problemas eléctricos y la protección de los equipos no solo garantizan la seguridad de los usuarios, sino que también contribuyen a la eficiencia y la productividad del laboratorio de informática.

6.4. SEGURIDAD DEL HARDWARE

Se refiere a la protección física integral de los equipos de computación y periféricos para garantizar su funcionamiento óptimo y prolongar su vida útil. Posteriormente se muestras aspectos importantes relacionados a la seguridad del Hardware dentro de los Laboratorios de Computación:

- Un aspecto crucial de esta protección es asegurarse de que los cables y conexiones de red estén en buen estado, libres de daños o desgastes que puedan causar cortocircuitos o pérdida de conexión.
- Los cables sueltos o desordenados pueden representar un riesgo de tropiezos y caídas, por lo que se promueve el orden y la organización adecuada de los mismos para mantener un entorno seguro y ordenado.
- Es fundamental asegurarse de que no haya obstrucciones en las salidas de aire de los equipos, especialmente en las unidades centrales de procesamiento (CPU) y dispositivos que generen calor.
- Una ventilación adecuada es esencial para evitar el sobrecalentamiento y garantizar el óptimo rendimiento de los equipos. Por lo tanto, se fomenta la colocación adecuada de los equipos y la limpieza periódica de los filtros y ventiladores para mantener una temperatura estable y evitar problemas de funcionamiento causados por el calor excesivo.
- El mantenimiento adecuado de los equipos es una práctica esencial para protegerlos de posibles fallas y asegurar un funcionamiento confiable.
- Por parte de los usuarios finales al uso de los laboratorios se establece que queda prohibido manipular, desconectar y remover, equipos, cables o cualquier otra indumentaria perteneciente a los laboratorios de computación.

La protección física de los equipos de computación y periféricos dentro del laboratorio de computación son una medida preventiva esencial para evitar daños y maximizar la productividad del laboratorio de informática. Al promover la conciencia sobre estas prácticas de cuidado de los activos tangibles del departamento, se contribuye a mantener un ambiente de trabajo seguro, ordenado y funcional, en el que los equipos y recursos tecnológicos puedan desempeñar su papel de manera efectiva y confiable.

6.5. SEGURIDAD DE SOFTWARE

Dentro del entorno de la seguridad de software, es el que se orienta mantener el uso de software actualizado y legitimo. La seguridad del software es esencial para garantizar la integridad y buen funcionamiento en el laboratorio de informática.

Los aspectos importantes ante esta seguridad son los siguientes:

- Se implementa un proceso regular de instalación de actualizaciones para todo el software utilizado en el laboratorio, incluyendo sistemas operativos (imágenes), aplicaciones, herramientas de seguridad y software de terceros autorizados.
- Instalar Software autorizado, código abierto o de Fuentes Confiables, se debe evitar la descarga e instalación de programas de sitios desconocidos o de dudosa procedencia, ya que podrían contener malware o amenazas cibernéticas.
- Se prohíbe instalar software sin licencia y no autorizado por el Departamento de Ciencias de la Computación.
- Se tiene implementado un firewall y antivirus confiable en todos los equipos del laboratorio. El cual se encuentra configurado adecuadamente para bloquear el acceso no autorizado y detectar y eliminar amenazas de seguridad en tiempo real.

Estas directrices contribuyen a fortalecer la seguridad del software en el laboratorio de computación, protegiendo tanto los datos como la infraestructura de posibles ataques cibernéticos y amenazas maliciosas. Al seguir estas prácticas, se promueve un entorno seguro y confiable para el uso de recursos tecnológicos en el laboratorio.

6.6. SEGURIDAD MEDIAMBIENTAL ANTE DESASTRES

Se refiere a la protección física integral de las personas que se encuentren dentro de los Laboratorios Generales del DCCO en caso de un desastre natural como Erupción del Cotopaxi.

- Siga las recomendaciones generadas en el Manual de Seguridad ante Desastres por erupción del Cotopaxi.

7. CONTROL DE CAMBIOS

Fecha	Versión	Elaborado por	Descripción de la modificación
27/7/2023	1.0	Ing. Andrés Quishpe	Generación del documento y contenido

8. VIGENCIA Y AUTORIZACIÓN

Elaborado por:		
Departamento Ciencias de la Computación / Laboratorios de computación	**Departamento Ciencias de la Computación / Laboratorios de computación**	**Departamento Ciencias de la Computación / Laboratorios de computación**
Ing. Andrés Quishpe **Técnico de Laboratorio (TC)**	Ing. Pedro Casame **Analista de Laboratorio (TC)**	Ing. Luis Buri **Analista de Laboratorio (TC)**
Revisado por:	**Aprobado por:**	
Departamento Ciencias de la Computación / Laboratorios de computación	**Departamento Ciencias de la Computación / Laboratorios de computación**	
Ing. Gustavo David Salazar Chacón, PhD. **Jefe de Laboratorio**	Ing. Sonia Elizabeth Cárdenas Delgado, PhD. **Directora del Departamento DCCO**	