ACUERDO No. 05
(Noviembre 17 de 2009)

"Por el cual se adopta y aprueba el Modelo de Seguridad de la Información para la Universidad Libre"

La H. Consiliatura de la Universidad Libre, en uso de sus atribuciones y,

C O N S I D E R A N D O:

1. Que en cumplimiento de su función social y fiel al ideario inspirado por su fundador, la Universidad Libre debe impulsar y materializar los cambios que demandan los tiempos modernos, para mantener el posicionamiento y el liderazgo en la formación de talento humano al servicio de la comunidad colombiana;

2. Que la Universidad Libre como organización compleja, que encierra en su ser, en su estructura y en su administración, una naturaleza universitaria nacional combinada con una naturaleza universitaria seccional-regional, requiere de elementos y sistemas que realcen y enriquezcan su espíritu corporativo y su proyección internacional;

3. Que se hace necesaria la modernización y actualización administrativa, transformar la cultura organizacional y empoderar los elementos de la planeación en la gestión gerencial de la Universidad;

4. Que el Modelo de Seguridad de la Información se propuso de acuerdo con las necesidades actuales de la Universidad Libre de protección de la información contra las amenazas del entorno, el aseguramiento de la continuidad de los procesos críticos, la minimización de los riesgos y el ofrecimiento de mejores servicios a la comunidad en general;

5. Que bajo la dirección del Presidente Nacional, la Dirección de Sistemas, presentó a consideración de la H. Consiliatura una propuesta del Modelo de Seguridad de la Información, el cual fue previamente analizado por todos los Presidentes de las Seccionales de la Universidad;

6. Que la H. Consiliatura en su análisis del Modelo de Seguridad de la información, lo encontró ajustado a las necesidades de la Universidad Libre, a su consolidación, proyección y alta calidad académica, razón por la cual lo aprobó en primer debate el día 22 de abril de 2009 y decidió adoptarlo y aprobarlo como norma orgánica de la Institución en la presente sesión.

A C U E R D A:

ARTICULO ÚNICO: Adoptar y aprobar el Modelo de Seguridad de la Información, como se presenta a continuación:

POLITICAS DE SEGURIDAD DE LA INFORMACION

ÍNDICE

0. Objetivo

0.1 Objetivo General

Las Políticas de Seguridad de la Información de la **Universidad Libre** tienen el propósito de definir las bases para promover la planeación, el diseño y la implantación de un Modelo de Seguridad de la Información que establezca una cultura de la seguridad de la información en la universidad.

De igual manera, establecen las reglas básicas con las cuales la **Universidad Libre** debe operar sus recursos de procesamiento de la información, a través del diseño e implantación de normas, procedimientos y estándares de tal manera de aumente la protección de éstos recursos. Así mismo, identifican responsabilidades y establecen requerimientos mínimos para una protección apropiada y consistente de la información de la universidad.

0.2 Objetivos Específicos

- Proteger de manera integral la información de la **Universidad Libre** tratando de salvaguardar la confidencialidad, disponibilidad e integridad de la misma

- Garantizar la utilización de las medidas necesarias para evitar la divulgación no autorizada, pérdida, modificación, o cualquier daño que pueda llegar a sufrir la información.

- Establecer los roles y las responsabilidades referentes al cumplimiento de la Seguridad de la Información.

- Asegurar que la corporación pueda continuar su operación en el evento que se presente un incidente de Seguridad de la Información.

- Asegurar que desde las Directivas hasta los niveles más bajos se cumplan los lineamientos de seguridad de la información

- Enfocar a la **Universidad Libre** en un proceso continuo de gestión de la información.

1. Alcance

Este documento es de obligatoria aplicación para todos los funcionarios de la **Universidad Libre**. Así mismo, proveedores y personal externo que desempeñen labores o le proporcionen algún tipo de servicio o producto a la universidad estarán obligados a cumplir las políticas aquí descritas.

2. Vigencia

El presente documento estará vigente desde la fecha de su publicación y no se considerará obsoleto si no existe una revisión posterior.

3. Sanciones en caso de violación de las Políticas de Seguridad de la Información

En el caso de que se constate alguna violación de las directrices y lineamientos establecidos por las presentes Políticas de Seguridad de la Información, se sancionará al infractor de acuerdo al régimen interno de la **Universidad Libre**.

4. Definiciones

Activo de Información: de acuerdo con la norma ISO 27001, un activo de información es “cualquier cosa que tenga valor para la organización y en consecuencia deba ser protegido”. No obstante, este concepto es bastante amplio, y debe ser limitado por una serie de consideraciones: el impacto que para la universidad supone la pérdida de confidencialidad, integridad o disponibilidad de cada activo, el tipo de información que maneja en términos de su sensibilidad y criticidad y sus productores y consumidores.

Acuerdos de Aceptación de las Políticas de Seguridad: son documentos en los que los funcionarios de la **Universidad Libre** o provistos por terceras partes aceptan acatar las Políticas de Seguridad de la corporación y se acogen a las sanciones establecidas por el incumplimiento de dichas políticas.

Acuerdos de Confidencialidad: son documentos en los que los funcionarios de la **Universidad Libre** o provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la corporación, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la universidad.

Acuerdos de Intercambio: son documentos constituidos entre la **Universidad Libre** y sus proveedores de servicios en donde se concertan las condiciones del intercambio de información, los compromisos de los proveedores de mantener la confidencialidad y la integridad de la información a la que tengan acceso en virtud de la labor que desarrollan para la universidad, las vigencias y las limitaciones a dichos acuerdos.

Acuerdos de Niveles de Servicio: herramientas que ayudan a proveedores y clientes de un servicio determinado a llegar a un consenso en términos del nivel de calidad que se ha de alcanzar en el servicios contratado. Registran el

entendimiento común de servicios, responsabilidades, garantías, tiempos de respuesta, horarios de disponibilidad, entre otros.

Análisis de Riesgos: proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Archivística: es el estudio teórico y práctico de los principios, procedimientos y problemas concernientes al almacenamiento, conservación y restauración de documentos, buscando que dicha documentación, se mantenga en el tiempo, con las condiciones adecuadas y que pueda ser accedida y consultada cuando es requerida.

Arquitectura de software: es un conjunto de patrones y abstracciones coherentes que proporcionan el marco de referencia necesario para guiar la construcción del software para un sistema de información. Estas guías indican la estructura, funcionamiento e interacción entre las partes del software.

Audit trails: conjuntos cronológicos de pistas o registros que contienen los accesos a los sistemas y las operaciones realizadas durante un periodo de tiempo. Los audit trails registran actividades como transacciones o comunicaciones.

Autenticación: es el procedimiento de comprobación de la identidad de un usuario al tratar de acceder un recurso de procesamiento o sistema de información.

Capacity Planning: es el proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita la universidad para satisfacer las necesidades de procesamiento de dichos recursos de forma eficiente y con un rendimiento adecuado.

Centros de Cableado: son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los Centros de Cómputo, los Centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Centros de Cómputo: son zonas específicas para el almacenamiento de múltiples computadoras para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. Los Centros de Cómputo deben cumplir ciertos estándares con el fin de garantizar los controles de acceso físico,

los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones de temperatura y humedad adecuadas.

Cifrado: es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información de la universidad.

Clave criptográfica: es un parámetro que se utiliza junto con un algoritmo criptográfico para transformar, validar, autenticar, cifrar o descifrar datos.

Cola de impresión: estructura lógica utilizada para asignar turnos, almacenar y administrar los trabajos pendientes de impresión en cada impresora.

Confidencialidad: es la garantía de que la información sea accesible solo a aquellas personas autorizadas a tener acceso a ella.

Criptografía: es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

Derechos de Autor: es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Disponibilidad: es la garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella cada vez que se requiera.

Guías de Clasificación de la Información: directrices para catalogar la información de la universidad y hacer una distinción entre la información que es crítica para el negocio y aquella que no lo es y, de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información.

Hacking ético: es el conjunto de actividades para ingresar a las redes de datos y voz de la corporación con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad

Incidente de Seguridad: es un evento adverso, confirmado o bajo sospecha, que afecta a un sistema de información, a una red, o la violación o inminente amenaza de violación de una política o norma o de seguridad.

Integridad: es la salvaguarda de la exactitud y totalidad de la información y los métodos de procesamiento de la misma.

Licencia de software: es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos

Logs de Auditoría: son archivos donde son registrados los eventos que se han identificado en los sistemas de información y redes de datos de la universidad. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

Perfiles de usuario: son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos informáticos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

Plan de contingencia: es un documento que describe en forma clara, concisa y concreta los riesgos, los actores, las responsabilidades y los procedimientos a seguir tendientes a restablecer la operación normal, en casos de eventos adversos. El Plan de Contingencia deberá inventariar los distintos procesos de negocio y determinar la dependencia e importancia que supone para la universidad en términos de disponibilidad. Para los procesos críticos se deberá destinar la máxima atención y recursos.

Plan de recuperación ante desastres: hace parte del Plan de Contingencia y es un conjunto de procedimientos de recuperación de la plataforma tecnológica de la universidad y cubre aspectos como los datos, el hardware y el software crítico, para que la universidad pueda restablecer sus operaciones en caso de un desastre natural o causado por humanos en forma rápida, eficiente y con el menor costo y pérdidas posibles. El Plan también debe incluir las consideraciones necesarias para enfrentarse a la pérdida inesperada o repentina de personal crítico.

Programa de concientización en seguridad de la información: es un conjunto de estrategias que persigue que todos los funcionarios de la **Universidad Libre** y los funcionarios provistos por terceras partes interioricen y adopten las políticas,

normas, procedimientos y guías existentes al interior de la universidad dentro de sus actividades diarias.

Programas de código fuente: son conjuntos de líneas de texto que contienen las instrucciones que deben seguir los servidores o equipos de cómputo para ejecutar dichos programas y describen por completo el funcionamiento de los mismos. El código fuente de un programa está escrito en algún lenguaje de programación; sin embargo, en este primer estado no es directamente ejecutable, sino que debe ser traducido a otro lenguaje (lenguaje de máquina o código objeto) que sí pueda ser ejecutado por el hardware de los servidores o equipos de computo. Para esta traducción se usan los llamados compiladores, ensambladores, intérpretes y otros sistemas de traducción.

Propiedad intelectual: es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluidas las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

Reasignación de derechos de acceso: es la modificación de los privilegios con que cuenta un funcionario sobre un recurso informáticos, la red de datos de la universidad o un sistema de información cuando cambio de labores dentro de la corporación.

Recursos informáticos: son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas académicas y administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la universidad.

Remoción de derechos de acceso: es el bloqueo o la eliminación de los privilegios o de la cuenta de usuario de la cual dispone un funcionario sobre un recurso informático, la red de datos de la universidad o un sistema de información.

Requerimientos de nuevas funcionalidades, servicios o modificaciones: contienen la definición de necesidades y la generación de especificaciones correctas que describan con claridad, en forma consistente y compacta, el comportamiento esperado de las funcionalidades o modificaciones sobre los sistemas.

Sistema de información: es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la

información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno es decir desarrollado por la **Universidad Libre** o de origen externo ya sea adquirido por la universidad como un producto estándar de mercado o desarrollado para las necesidades de la corporación.

Sistemas de aire acondicionado: son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características del mismo, fundamentalmente humedad y temperatura y, de manera adicional, también permite controlar su pureza y su movimiento.

Sistemas de detección y extinción de incendios: son sistemas que reaccionan rápidamente para reducir el impacto y la posibilidad de que se un incendio se propague a otras zonas, contando con algunas de las siguientes características: detección temprana de humo, extinción mediante gas, monitoreo y alarmas contra incendios y sistemas rociadores para zonas comunes.

Software: Cualquier desarrollo realizado por la **Universidad Libre** o por terceras partes para ampliar, mejorar o modificar la funcionalidad de los sistemas de Información existentes o que por si mismos conforman nuevos sistemas de información.

Software malicioso: es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse en o dañar recursos informáticos, sistemas operativos, redes de datos o sistemas de información.

Soporte Técnico: es un servicio que proporciona un único punto de contacto para todos los usuarios de servicios relacionados con tecnologías de información de la universidad, respondiendo a las preguntas y problemas. De igual manera, brinda un apoyo inmediato en línea acerca de los problemas relacionados con el software y hardware de las estaciones de trabajo y equipos portátiles. El Soporte Técnico resuelve requerimientos e indica los pasos a seguir para solicitar los servicios proporcionados por la Dirección de Sistemas y orienta dichas solicitudes al personal apropiado.

Transacción: es una interacción con una estructura de datos, compuesta por varios procesos que se han de aplicar uno después del otro. La transacción debe ser equivalente a una interacción atómica. Es decir, que se realice de una sola vez y, que la estructura a medio manipular no sea jamás alcanzable por el resto del sistema hasta que haya finalizado todos sus procesos.

UPS (Uninterruptible Power Supply): es un sistema ininterrumpido de energía, conjunto de baterías y estabilizador de voltaje conectados al computador, que

detecta pequeñas fluctuaciones eléctricas o cortes de energía, entregando electricidad propia de sus baterías. Estas tienen, dependiendo del consumo, una autonomía de servicio de algunos minutos.

Vulnerabilidades: son características o situaciones inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la universidad, las cuales se constituyen en fuentes de riesgo (amenazas).

5. Política Global de Seguridad de la Información

La información es un activo de valor crítico para el cumplimiento de los objetivos de negocio de la **Universidad Libre** y, por lo tanto, se constituye en el fundamento para la toma de decisiones y la preservación de las ventajas competitivas de la corporación.

Los funcionarios y todos aquellos que tienen responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información de la **Universidad Libre** deben adoptar los lineamientos contenidos en el presente documento, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la misma, así como minimizar los riesgos a los que se encuentra expuesta dicha información.

La Política Global de Seguridad de la Información de la **Universidad Libre** está soportada por políticas, normas y procedimientos específicos los cuales orientan sobre el manejo adecuado de la información de la corporación.

6. Estrategias de seguridad para la Universidad Libre

Las siguientes estrategias resumen los aspectos más relevantes en seguridad de la información para la **Universidad Libre** y son el compendio de las políticas y normas específicas en seguridad de la información que se relacionan en el presente documento a partir del numeral 7.

6.1 Estrategias relacionadas con la plataforma tecnológica

La plataforma tecnológica es el conjunto de software, hardware e infraestructura de comunicaciones y seguridad que proveen los diferentes servicios de información dentro y fuera de la universidad.

Para reducir los riesgos identificados de la plataforma tecnológica, se debe buscar la planeación, implantación, mantenimiento y monitoreo de manera segura de toda la plataforma tecnológica involucrada dentro de la **Universidad Libre**, incluyendo los siguientes aspectos, entre otro: la definición de perfiles, la asignación y establecimiento de controles de acceso, la asignación de privilegios, la

implantación de un software de protección contra código malicioso, la existencia en la red de datos de dispositivos de seguridad como firewall e IDS, la habilitación de filtros de acceso y contenido en internet y en los mensajes de correo, la segmentación de las redes de datos y la realización de pruebas de vulnerabilidades técnicas a la plataforma tecnológica.

6.2 Estrategias relacionadas con los sistemas de información

Los sistemas de información más significativos para la **Universidad Libre** apoyan los objetivos de negocio de la corporación en sus áreas Financiera, Académica y de Recursos Humanos.

Para reducir los riesgos identificados en los sistemas de información se deben considerar los siguientes aspectos: la construcción, pruebas y administración de los sistemas de información de acuerdo con los requerimientos de seguridad definidos, la separación de ambientes de desarrollo, pruebas y producción, la existencia de metodologías y estándares que involucren seguridad en el desarrollo e implantación del software, la documentación de los desarrollos, el control sobre las versiones y los cambios realizados, la existencia de repositorios de software y la existencia de un programa de entrenamiento en las tecnologías de desarrollo utilizadas.

6.3 Estrategias relacionadas con la seguridad física y ambiental

La seguridad física está asociada a toda la infraestructura física de la **Universidad Libre** que involucre el acceso a la plataforma tecnológica y la documentación física de la corporación, siendo ésta última de alta importancia para la universidad.

Para reducir los riesgos relacionados con la seguridad física y ambiental de la plataforma tecnológica y la documentación física se deben considerar los siguientes aspectos: el diseño, mantenimiento y monitoreo de sistemas de control de acceso a todas las instalaciones de la universidad, la definición y mantenimiento de sistemas de control y monitoreo de las instalaciones (alarmas, sistemas de detección de humo, sistemas de detección de incendios, sistemas de vigilancia), la generación y divulgación de los planes de concientización y entrenamiento acerca de las medidas físicas de control de acceso y la actualización y divulgación de los planes de evacuación y emergencias.

Para la plataforma tecnológica se deben considerar, además de los anteriores, los siguientes aspectos: el mantenimiento, protección y continuidad de la plataforma tecnológica y la red de servicios eléctricos y el control y monitoreo de entrada y salida de recursos tecnológicos.

Para la documentación física se deben considerar, de manera adicional, los siguientes aspectos: la existencia de normas de archivística para el adecuado almacenamiento, custodia y destrucción de los documentos y la capacidad física adecuada para el almacenamiento y preservación de los documentos.

6.4 Estrategias para el intercambio de información

El intercambio de información, tanto electrónica como física, entre áreas, entre sedes, entre seccionales y hacia el exterior de la **Universidad Libre** es una constante en la actividad diaria de la universidad.

Para reducir los riesgos relacionados con el intercambio de información se deben considerar los siguientes aspectos: la verificación jurídica y el establecimiento de acuerdos de intercambio con terceras partes como couriers de mensajería, servicios de valores, litógrafos y calígrafos entre otros, la definición de condiciones adecuadas de transporte tanto de recursos tecnológicos como de documentación física y las condiciones y tiempos de entrega.

6.5 Estrategias para la contingencia / continuidad del negocio

La **Universidad Libre** debe garantizar la continuidad de sus operaciones en el evento de un incidente o un desastre de mayores proporciones.

Para reducir los riesgos relacionados con la continuidad de la operación de la universidad se deben considerar los siguientes aspectos, entre otros: la existencia de un plan de continuidad de negocio que involucre a las áreas de la universidad o, por lo menos, la existencia de planes de contingencia para cada uno de los recursos de procesamiento de la información considerados críticos, la realización de pruebas sobre el plan de continuidad o los planes de contingencia y la revisión y actualización permanente de dichos planes.

6.6 Estrategias relacionadas con el personal

La seguridad del personal involucra los controles que permitan un proceso adecuado de selección de personal y contratación, que aseguren la definición e implantación de responsabilidades de los funcionarios de acuerdo con los roles desempeñados, que faciliten el monitoreo adecuado de dichas responsabilidades durante el desempeño del cargo y que garanticen la gestión necesaria durante el proceso de retiro de funcionarios.

Para reducir los riesgos relacionados con el personal de la **Universidad Libre** se deben considerar los siguientes aspectos: el control estricto en la verificación de antecedentes e información del nuevo personal que ingresa a la corporación, la verificación de cumplimiento del reglamento interno de trabajo en materia de protección y seguridad y la gestión de retiro o traslado de funcionarios tomando

las medidas necesarias para garantizar la protección de la información de la universidad.

7. Políticas de la Organización de Seguridad de la Información

Las Políticas específicas de Seguridad de la Información de la **Universidad Libre** se fundamentan en los dominios y objetivos de control de la norma ISO/IEC 27001:2005 y, se enuncian a partir de éste numeral.

7.1 Políticas de la Organización Interna (definición de roles y responsabilidades)

Todos los funcionarios que laboran o realizan actividades para la **Universidad Libre**, son responsables por el cumplimiento de las políticas, normas, procedimientos y estándares vigentes con respecto a la seguridad de la información.

Existen roles definidos en el esquema de seguridad de la información propuesto para la **Universidad Libre** que garantizan una adecuada segregación de funciones para la realización de las actividades de administración, operación y gestión de la seguridad de la información. Estos roles se describen en el documento “Organización de la Seguridad“.

7.2 Políticas que rigen la relación con terceras partes

Cualquier contrato, alianza o convenio con terceras partes debe preservar las políticas y normas de seguridad de la información de la **Universidad Libre**.

La universidad debe establecer mecanismos de control en sus relaciones con terceras partes que le proveen servicios. Se deben establecer o regular los Acuerdos de Niveles de Servicio con los terceros teniendo en cuenta consideraciones de seguridad de la información.

Todo acceso requerido a la información de la **Universidad Libre** por terceras partes deberá ser analizado y aprobado por el área propietaria de la información.

Normas que rigen la relación con terceras partes

Normas Dirigidas a: DIRECCION JURIDICA

- La Dirección Jurídica debe revisar la validez de las condiciones establecidas en los contratos u órdenes de compra suscritos con terceras partes proveedoras de servicios, así como las obligaciones de dichos terceros para con la **Universidad Libre**.

- Así mismo, la Dirección Jurídica debe elaborar modelos de acuerdos de confidencialidad y acuerdos de intercambios con terceros.

- Se deben revisar los Acuerdos de Niveles de Servicio y los requisitos de seguridad a los que los terceros deben acogerse., como es el caso de la constitución de pólizas y la elaboración de los acuerdos de confidencialidad e intercambio con los terceros.

Normas Dirigidas a: DIRECCION DE SISTEMAS

- La Dirección de Sistemas debe generar un modelo de Acuerdos de Niveles de Servicio y divulgarlo a todas las Unidades Académicas y Administrativas que adquieran recursos tecnológicos o de software.

Normas Dirigidas a: JEFES DE LAS UNIDADES ACADEMICAS Y ADMINISTRATIVAS

- Las Unidades Académicas o Administrativas de la **Universidad Libre** que contraten servicios con terceras partes deben realizar un análisis de riesgos antes de conceder acceso a los terceros a la información o los recursos de procesamiento de la misma y establecer una periodicidad para su realización.

- Las Unidades Académicas o Administrativas que adquieran recursos tecnológicos o de software deben establecer Acuerdos de Niveles de Servicio o, incluir en los acuerdos ya existentes, los requisitos de seguridad que deben cumplir los proveedores de servicio, entre los cuales se pueden mencionar, el cumplimiento de las Políticas de Seguridad de la Información, el uso de Acuerdos de Confidencialidad y/o de Intercambio, el uso de hardware y software de los terceros, los niveles de atención según la criticidad, el esquema de escalamiento, los controles de acceso físico, la separación de ambientes de desarrollo y producción, la entrega de reportes que indiquen la disponibilidad de servicio, el esquema de monitoreo y los procesos de manejo del cambio de personal y detección y reporte de incidentes.

- Se deben monitorear de manera permanente el cumplimiento de los Acuerdos de Niveles de Servicio establecidos con terceras partes.

Documentos relacionados con ésta política

- Acuerdos de Niveles de Servicio establecidos con terceras partes

8. Políticas de Administración de Activos de Información

8.1 Políticas de propiedad de la información

La información, tanto física como generada por la infraestructura tecnológica de la **Universidad Libre**, pertenece a la corporación, a menos que en una relación contractual se establezca lo contrario.

Sin embargo, la facultad de otorgar acceso a la información es potestad de los propietarios de la misma, quienes deben asegurar la aplicación de los controles requeridos y una adecuada segregación de funciones durante el flujo de dicha información en los procesos de la universidad

Normas de propiedad de la información

Normas Dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

- Las diferentes Unidades Académicas y Administrativas de la **Universidad Libre** deben actuar como propietarias de sus sistemas de información y de la información generada en ellas, con la facultad para otorgar o revocar el acceso a su información a los perfiles establecidos para éste fin.

- Todos los recursos de procesamiento de la información de la **Universidad Libre** están sujetos a revisiones periódicas por parte de Auditoría Interna o por los funcionarios que la universidad delegue para tal fin.

Normas Dirigidas a: DIRECCION DE SISTEMAS

- La Dirección de Sistemas al ser la propietaria de la plataforma informática donde residen los sistemas de información y la información de negocio de la **Universidad Libre**, debe asegurar su adecuada operación y administración.

8.2 Políticas de clasificación de la información

Se deben definir al interior de la universidad los niveles más adecuados para clasificar su información de acuerdo con su sensitividad, así como generar las Guías de Clasificación de la Información para que los propietarios de la misma puedan catalogarla.

La información de la **Universidad Libre** tanto en forma física como generada por los sistemas de información de la corporación o, generada en las estaciones de trabajo o equipos portátiles de los funcionarios debe ser clasificada con el objeto de determinar controles específicos para la protección de la misma.

Normas de clasificación de la información

Normas Dirigidas a: DIRECCION DE SISTEMAS

- Se deben definir los niveles de clasificación de la información y generar unas Guías de Clasificación de la Información.

- Las Guías de Clasificación de la Información deben ser socializadas y divulgadas a todos los funcionarios de la **Universidad Libre**.

Normas Dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

- Se debe clasificar la información sensitiva de acuerdo con las Guías de Clasificación de la Información.

- Los propietarios de la información o los recursos de procesamiento de la misma son responsables por su clasificación y por la re-clasificación anual de los mismos, con validación de Auditoría Interna durante el primer trimestre del año.

- La información generada por los sistemas de información de la **Universidad Libre** debe estar disponible en el evento que sea requerida, siempre y cuando el nivel de clasificación de ésta información lo permita y, cuya solicitud atienda a un requerimiento formal de la información.

Documentos relacionados con ésta política

- Guías de Clasificación de la Información

8.3 Políticas de administración y protección de la Información

Los funcionarios de la **Universidad Libre** y los funcionarios provistos por terceras partes deben garantizar la oportunidad, veracidad, exactitud, confiabilidad y disponibilidad de la información que generan, así como ser responsables por el buen uso de la información de la universidad, sea que la obtengan de forma física, medios magnéticos o electrónicos.

Así mismo, la corporación debe garantizar la protección de la información, estableciendo las directrices y proporcionando los mecanismos para el adecuado almacenamiento, distribución y destrucción de la información que se encuentre tanto en forma electrónica como en medios de almacenamiento y forma física, cumpliendo con la normatividad vigente para la universidad.

Normas de administración y protección de la información electrónica

Normas Dirigidas a: TODOS LOS USUARIOS

- Los usuarios son responsables por el buen uso de la información de la **Universidad Libre**, sea que la obtengan de medios magnéticos o electrónicos.

- Los funcionarios de la **Universidad Libre** deben garantizar la oportunidad, veracidad, exactitud, confiabilidad y disponibilidad de la información que generan.

- Los funcionarios no deben compartir archivos ni directorios en sus estaciones de trabajo ni equipos portátiles.

- Todos los usuarios deben, al momento de abandonar su puesto de trabajo, bloquear la estación de trabajo o el equipo portátil.

- El protector de pantalla de las estaciones de trabajo y equipos portátiles debe ser activado después de un período de 15 minutos de inactividad. La reactivación del protector de pantalla debe exigir el ingreso de usuario y contraseña.

- No se permite difundir interna ni externamente información confidencial de la **Universidad Libre**, ni transferir electrónicamente programas de software de la corporación a terceras partes sin autorización ni licenciamiento apropiado. Estas infracciones pueden dar lugar a sanciones de tipo administrativo y hasta penal en el caso de violaciones a las leyes de derechos de autor y protección de la propiedad intelectual.

- Los medios electrónicos que contengan información de la **Universidad Libre** deben ser borrados o sobre-escritos antes de que sean reutilizados o destruidos.

- Se deben adoptar los procedimientos para el acceso y divulgación, almacenamiento, generación de copias, transmisión, etiquetado y destrucción de información electrónica y medios de almacenamiento.

- Toda la información de la **Universidad Libre** debe tener un período de almacenamiento asignado que puede ser dictaminado por requerimientos legales o del negocio. Este período debe ser indicado al frente del medio de almacenamiento que la contenga. Cuando expire el período de almacenamiento, todas las copias de los medios de almacenamiento deben ser adecuadamente destruidas.

Normas Dirigidas a: DIRECCION DE SISTEMAS Y ADMINISTRADORES DE LOS RECURSOS INFORMATICOS Y LOS SISTEMAS DE INFORMACION

- La Dirección de Sistemas, en cabeza de los administradores de los recursos informáticos, al igual que los administradores de los sistemas de información, deben implantar los mecanismos de control necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información residente en los recursos informáticos y sistemas de información que se encuentran bajo su custodia.

- Se debe garantizar la aplicación de los mecanismos necesarios para eliminar de manera segura la información contenida en servidores, estaciones de trabajo o equipos portátiles de la **Universidad Libre**, cuando éstos cambian de usuario o son dados de baja por la universidad.

- Se deben destruir los medios de almacenamiento de la información acogiéndose al procedimiento para la destrucción y/o eliminación segura de la información.

- Es responsabilidad de la Dirección de Sistemas garantizar, por medio de mecanismos de cifrado, la confidencialidad e integridad de la información crítica para la universidad, almacenada en los equipos portátiles y estaciones de trabajo de su propiedad.

Normas de administración y protección de la documentación física

Normas Dirigidas a: TODOS LOS USUARIOS

- Los usuarios deben tener en cuenta las siguientes consideraciones cuando impriman documentos, saquen fotocopias o envíen faxes dentro de la **Universidad Libre**:

  - Verificar la fotocopiadora o impresora y las áreas adyacentes para asegurarse de que no quedaron copias adicionales.
  - Asegurarse que tienen el documento original antes de retirarse de la fotocopiadora o la impresora.
  - Si la impresora no está funcionando, borrar el archivo de la cola de impresión.
  - Recoger inmediatamente todos los faxes, impresiones y/o fotocopias que contengan información confidencial para evitar su revelación.
  - No se debe imprimir o fotocopiar al respaldo de una impresión o fotocopia existente.

- Al ausentarse temporalmente de su puesto de trabajo o al final de cada jornada laboral, los funcionarios de la **Universidad Libre** o funcionarios provistos por terceras partes deben garantizar que sus escritorios se

encuentran organizados y que todos los documentos y medios de almacenamiento utilizados durante el desarrollo de sus funciones son almacenados bajo las protecciones de seguridad necesarias.

- Se deben adoptar los procedimientos para el acceso y divulgación, almacenamiento, generación de copias, transmisión, etiquetado y destrucción de la documentación física para garantizar su confidencialidad, integridad y disponibilidad.

- Toda la información de la **Universidad Libre** debe tener un período de almacenamiento asignado que puede ser dictaminado por requerimientos legales o del negocio. Este período debe ser indicado al frente del documento físico que la contenga.

Normas Dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

- Los propietarios de los documentos tienen el deber de controlar la distribución de dichos documentos.

- Así mismo, están en la obligación de impedir el uso no previsto de los documentos obsoletos o no vigentes.

Normas Dirigidas a: SECRETARIA GENERAL

- Se deben generar las directrices de la función archivística para la **Universidad Libre**, que contemplen entre otros, métodos de organización de los documentos, sistemas de codificación de los mismos, tablas de retención, la creación de mecanismos que faciliten la conservación documental y el mantenimiento y seguridad de los documentos.

- De igual manera, se debe divulgar éstas directrices de archivo de documentos a todos los funcionarios de la universidad y funcionarios suministrados por terceras partes que, por razón de sus funciones, interactúan con la documentación física de la corporación.

- Se debe evaluar la capacidad de almacenamiento documental de la universidad y proveer los recursos de almacenamiento necesarios para todas las unidades organizacionales, de acuerdo con las necesidades de retención establecidas.

- La información de la **Universidad Libre** contenida en documentos físicos debe ser destruida de tal forma que quede ilegible una vez se cumplan las vigencias de los períodos de retención. La destrucción de la documentación

física debe ser efectuada por funcionarios de la universidad, acogiéndose al procedimiento establecido para tal fin.

Documentos relacionados con ésta política

- Directrices de la función archivística
- Procedimientos para el acceso y divulgación, almacenamiento, generación de copias, transmisión, etiquetado y destrucción de la información por cada uno de los niveles de clasificación.

8.4 Políticas de uso de los recursos informáticos (servidores, dispositivos de comunicación, estaciones de trabajo, equipos portátiles y otros recursos informáticos)

Los recursos informáticos son provistos por la **Universidad Libre** a sus funcionarios y a los funcionarios provistos por terceras partes, con el único fin de desarrollar actividades relacionadas con la corporación; por lo tanto, estos recursos deben ser utilizados de manera adecuada y eficiente.

Normas de uso de los recursos informáticos

Normas Dirigidas a: TODOS LOS USUARIOS

- Las estaciones de trabajo, equipos portátiles y demás recursos informáticos como impresoras, fotocopiadoras, máquinas de fax y video beams, entre otros, de la **Universidad Libre** no deben ser utilizados para actividades personales o ajenas a la corporación.

- Todos y cada uno de las estaciones de trabajo, equipos portátiles y demás recursos informáticos son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.

- Las estaciones de trabajo, equipos portátiles y demás recursos informáticos de la **Universidad Libre** deben ser operados solamente por personal autorizado y/o el responsable de los mismos.

- La protección física de las estaciones de trabajo, equipos portátiles y demás recursos informáticos corresponde a los responsables de los mismos y, es su deber, notificar cualquier eventualidad que ocurra sobre dichos equipos a la Dirección de Sistemas a través del Soporte Técnico.

- La Dirección de Sistemas es la única área autorizada para realizar movimientos y asignaciones de recursos informáticos, por lo que está

totalmente prohibida la disposición que de éstos pueda hacer cualquier usuario.

- Las estaciones de trabajo, equipos portátiles y demás recursos informáticos asignados a los funcionarios de la **Universidad Libre** y funcionarios provistos por terceras partes deben someterse a todas las instrucciones técnicas que imparta la Dirección de Sistemas.

- En caso de presentarse una falla o problema de hardware o software en una estación de trabajo o equipo portátil propiedad de la universidad, el usuario responsable del mismo deberá informarlo a la Dirección de Sistemas a través del Soporte Técnico, para una asistencia especializada y, por ningún motivo, deberá intentar resolver el problema.

- La instalación de hardware o software, la reparación o retiro de cualquier parte o elemento en las estaciones de trabajo, equipos portátiles y demás recursos informáticos propiedad de la **Universidad Libre**, solo puede ser realizado por los funcionarios autorizados por la Dirección de Sistemas.

- Los funcionarios de la universidad o funcionarios suministrados por terceras partes no deben realizar intencionalmente actos que impliquen el desperdicio o la pérdida de rendimiento de los recursos informáticos asignados a ellos.

- Los computadores portátiles propiedad de la **Universidad Libre**, que estén fuera de las instalaciones de la universidad, no deben ser desatendidos en lugares públicos.

- Todas las estaciones de trabajo y equipos portátiles deben estar protegidos por guaya de seguridad.

- Cuando un funcionario inicie o termine su vinculación laboral con **la Universidad Libre**, sea trasladado entre áreas, sedes, seccionales o, por alguna otra circunstancia deje de utilizar el computador personal o el recurso informático suministrado con carácter permanente, deberá entregar dicho recurso formalmente al Jefe de la Unidad Académica o Administrativa a la que pertenece o, en su defecto, a su Jefe inmediato.

- Los funcionarios de la **Universidad Libre** no deben utilizar sus computadores personales para realizar sus labores de trabajo en las instalaciones de la corporación.

- Los funcionarios de la universidad o funcionarios suministrados por terceras partes deben pedir alistamiento de la estación de trabajo o equipo portátil a la Dirección de Sistemas, a través de Soporte Técnico.

Normas Dirigidas: JEFES DE UNIDADES ACADÉMICAS Y ADMINISTRATIVAS

- Es responsabilidad de los Jefes de Unidades Académicas y Administrativas recibir los recursos informáticos asignados a sus funcionarios cuando éstos se retiran de la universidad o son trasladados entre áreas, sedes o seccionales.

- Así mismo, los Jefes de Unidades Académicas y Administrativas deben informar a la Dirección de Sistemas para realizar el correspondiente borrado y/o alistamiento de los recursos informáticos de funcionarios que se retiran de la universidad o se trasladan

Normas Dirigidas a: DIRECCION DE SISTEMAS

- El ingreso y salida de servidores, dispositivos de comunicación, estaciones de trabajo, equipos portátiles y demás recursos informáticos de las instalaciones de la **Universidad Libre** debe estar debidamente autorizado por la Dirección de Sistemas.

- El alistamiento de las estaciones de trabajo y equipos portátiles es responsabilidad de la Dirección de Sistemas, así como la eliminación segura de la información de los mismos.

- No se permite dar mantenimiento a equipos de cómputo que no sean de propiedad de la **Universidad Libre** con recursos de la corporación.

- Se debe procurar que todos los recursos informáticos tales como servidores, dispositivos de comunicación, estaciones de trabajo, equipos portátiles e impresoras, entre otros, que sean propiedad de **la Universidad Libre** se encuentren continuamente actualizados en aras de conservar e incrementar la calidad del servicio que prestan, mediante la mejora de su desempeño y obtener mayor estabilidad y protección ante amenazas.

Normas Dirigidas a: ALMACEN

- Se debe recibir los recursos informáticos del proveedor y verificar las cantidades y especificaciones de los mismos.

- El área de Almacén es la encargada de hacer entrega de las estaciones de trabajo y equipos portátiles a los funcionarios de la universidad y a los funcionarios suministrados por terceras partes que harán uso de equipos

provistos por la corporación. La asignación de estaciones de trabajo y equipos portátiles debe quedar formalmente documentada.

- Se debe etiquetar y dar salida formal del Almacén a aquellos equipos de cómputo que son asignados a funcionarios de la **Universidad Libre** o funcionarios provistos por terceras partes.

Normas Dirigidas a: SEGURIDAD

- El ingreso y salida de servidores, dispositivos de comunicación, estaciones de trabajo, equipos portátiles y demás recursos informáticos de las instalaciones de la **Universidad Libre** debe estar debidamente controlado por el área de Seguridad.

Normas Dirigidas a: AUDIOVISUALES

- El área de Audiovisuales es la encargada de administrar y custodiar los video beams de la universidad, asegurando las apropiadas medidas de control sobre el préstamo y devolución de dichos recursos.

Normas Dirigidas a: DIRECCION DE SISTEMAS, JEFES DE UNIDADES ACADEMICAS Y ADMINISTRADORES DE LOS RECURSOS INFORMATICOS Y LOS SISTEMAS DE INFORMACION

- Se debe mantener un inventario actualizado del hardware y software de la plataforma tecnológica de la corporación.

Normas Dirigidas a: SERVICIOS GENERALES

- Se debe mantener un inventario actualizado de los recursos informáticos que son propiedad de la **Universidad Libre** y se debe hacer verificación periódica de dicho inventario.

Documentos relacionados con ésta política

- Procedimiento de ingreso y salida de equipos de la universidad
- Procedimiento para la recepción y entrega de puestos de trabajo
- Estándar de seguridad para servidores Windows
- Estándar de seguridad para servidores Solaris
- Estándar de seguridad para routers
- Estándar de seguridad para switches
- Estándar de seguridad para equipos portátiles y estaciones de trabajo

9. Políticas de Seguridad del Personal

9.1 Políticas relacionadas con el ingreso de funcionarios, la confidencialidad de la información y la aceptación de las políticas de seguridad

Se debe garantizar que los nuevos funcionarios de la **Universidad Libre** o, suministrados por terceras partes, son contratados siguiendo un proceso formal de selección y que son orientados en las funciones que deben realizar y en el adecuado manejo de la información de la universidad de acuerdo con sus roles al interior de la misma.

Todos los funcionarios de la **Universidad Libre** y los funcionarios provistos por terceras partes deben firmar un Acuerdo de Confidencialidad y un Acuerdo de Aceptación de las Políticas de Seguridad al momento de su ingreso, para funcionarios nuevos y, en el momento en que la Dirección de Personal lo establezca, para los funcionarios actuales de la corporación.

Todos los usuarios de la información son responsables del manejo adecuado de la misma y mediante el cumplimiento de las políticas, procedimientos y estándares de los procesos operativos y de seguridad informática, se comprometen a respetar su carácter de confidencialidad e integridad.

Normas relacionadas con el ingreso de funcionarios, la confidencialidad de la información y la aceptación de las políticas de seguridad

Normas Dirigidas a: TODOS LOS USUARIOS

- Todos los funcionarios de la **Universidad Libre** deben firmar un Acuerdo de Confidencialidad y un Acuerdo de cumplimiento de las Políticas de Seguridad de la Información, antes de otorgarles su identificación de usuario y contraseña para el uso de los recursos informáticos de la universidad. Únicamente se excluyen de ésta norma aquellos funcionarios que han firmado previamente un Acuerdo de Confidencialidad y un Acuerdo de cumplimiento las Políticas de Seguridad de la Información en el momento de su vinculación laboral con la corporación.

Normas Dirigidas a: DIRECCION DE PERSONAL

- La Dirección de Personal es la encargada de asegurar que todos los funcionarios de la universidad conozcan sus responsabilidades legales con respecto al uso de los recursos informáticos y la información de la **Universidad Libre**. Los acuerdos de Confidencialidad y de cumplimiento de la Políticas de Seguridad de la Información deben ser anexados al contrato de trabajo.

Normas Dirigidas a: JEFES DE UNIDADES ACADEMICAS Y ADMINISTRATIVAS

- Cada Unidad Académica o Administrativa que tenga bajo su responsabilidad personal suministrado por terceras partes es la encargada de solicitar la firma de los Acuerdos de Confidencialidad para terceros y de cumplimiento de las Políticas de Seguridad de la información de la **Universidad Libre**. Dichos acuerdos deben ser anexados al contrato efectuado con el tercero.

- Una vez se vincula un funcionario a la universidad, el Jefe de la Unidad Académica o Administrativa o, en su defecto, el jefe inmediato debe enviar a la Dirección de Sistemas el formato correspondiente debidamente diligenciado, solicitando la creación del usuario y la activación de su cuenta en la red y los sistemas de información de acuerdo con el perfil requerido.

Documentos relacionados con ésta política

- Procedimiento de ingreso de funcionarios
- Manual de funciones
- Acuerdos de Confidencialidad
- Acuerdos de Aceptación de las Políticas de Seguridad

9.2 Políticas de concientización a los usuarios

Es un deber de la **Universidad Libre** diseñar y ejecutar de manera permanente y continua un programa de concientización en seguridad de la información involucrando a todos los funcionarios y funcionarios suministrados por terceros, para garantizar la protección adecuada de su información y los recursos de procesamiento de la misma.

Los funcionarios de la universidad y los funcionarios provistos por terceras partes deben asistir a las capacitaciones y entrenamientos establecidos y deben acogerse a las buenas prácticas en seguridad de la información allí recomendadas.

Normas de concientización a los usuarios

Normas Dirigidas a: TODOS LOS USUARIOS

- Todos los funcionarios de la **Universidad Libre** y los funcionarios provistos por terceras partes que, por sus funciones hagan uso de recursos de información, deberán asistir a los entrenamientos y charlas que se programen en temas relacionados con la Seguridad de la Información. Así mismo, deberán aceptar y cumplir con las Políticas de Seguridad de la Información.

Normas Dirigidas a: DIRECCION DE SISTEMAS

- Es responsabilidad de la Dirección de Sistemas promover constantemente la importancia de la seguridad de la información entre los usuarios de recursos de procesamiento y sistemas de información de la **Universidad Libre**. El programa de concientización en seguridad de la información debe contener continuas capacitaciones y charlas; de manera adicional, se pueden emplear recursos de apoyo como afiches y llaveros, entre otros.

- Se debe educar y entrenar a los funcionarios en el entendimiento, toma de conciencia y cumplimiento de las políticas, normas, procedimientos y estándares para la seguridad de la información establecidos por la universidad y las responsabilidades legales que la rigen.

- Se debe educar y entrenar a los funcionarios en el uso adecuado y correcto de los recursos de procesamiento y sistemas de información para evitar posibles riesgos de seguridad.

Normas Dirigidas a: DIRECCION DE PERSONAL

- La Dirección de Personal debe proporcionar la logística y facilitar los recursos necesarios para la realización del programa de concientización en seguridad de la información.

- De igual manera, la Dirección de Personal debe convocar a los funcionarios a las charlas y eventos programados como parte del programa de concientización en seguridad de la información y controlar la asistencia a dichas charlas y eventos, aplicando las sanciones pertinentes por la falta de asistencia no justificada.

Documentos relacionados con ésta política

- Material del curso de entrenamiento para los funcionarios de la universidad y funcionarios suministrados por terceras partes que interactúan con información sensitiva o recursos de procesamiento de la misma
- Material de la campaña de concientización para los funcionarios de la universidad y funcionarios suministrados por terceras partes que interactúan con información sensitiva o recursos de procesamiento de la misma

9.3 Políticas relacionadas con la desvinculación y cambio de labores de los funcionarios

La **Universidad Libre** debe asegurar que, sus funcionarios y los funcionarios provistos por terceras partes, se desvinculan de la corporación o cambian de labores de una manera ordenada y controlada.

La Dirección de Personal debe informar de manera oportuna a todas las áreas interesadas de la desvinculación o cambio de labores de sus funcionarios.

Normas relacionadas con la desvinculación y cambio de labores de los funcionarios

Normas Dirigidas a: TODOS LOS USUARIOS

- En el momento de su desvinculación de la **Universidad Libre** o al cambiar de labores, los funcionarios deben entregar su puesto de trabajo al Jefe de la Unidad Académica o Administrativa, a su jefe inmediato o a la persona designada por éste, junto con la copia de la información crítica que manejan. De igual manera, deben entregar todos los recursos informáticos y otros activos que les fueron suministrados en el momento de su vinculación

- Después que un funcionario se ha retirado de la corporación, su ingreso a la misma sólo lo podrá hacer como visitante. En caso que necesite manipular información de la **Universidad Libre**, lo hará con el visto bueno de las Directivas de la universidad bajo un contrato de prestación de servicios.

Normas Dirigidas a: DIRECCION DE PERSONAL

- La Dirección de Personal debe informar de manera inmediata a la Dirección de Sistemas del retiro o cambio de labores de funcionarios de la universidad para la remoción o reasignación de derechos de acceso sobre los recursos informáticos y sistemas de información.

- Así mismo, se debe informar al personal encargado de la vigilancia y seguridad de la universidad del retiro de funcionarios para prevenir el acceso físico no autorizado a las instalaciones de la corporación.

Normas Dirigidas a: JEFES DE UNIDADES ACADEMICAS Y ADMINISTRATIVAS

- Cada Unidad Académica o Administrativa de la **Universidad Libre** que tenga bajo su responsabilidad personal suministrado por terceras partes es la encargada de informar de manera inmediata a la Dirección de Sistemas del retiro de los funcionarios de los terceros, para la remoción de derechos de acceso sobre los recursos informáticos y sistemas de información.

- De igual manera, se debe informar al personal encargado de la vigilancia y seguridad de la universidad del retiro de funcionarios provistos por terceros para prevenir el acceso físico no autorizado a las instalaciones de la corporación.

Normas Dirigidas a: DIRECCION DE SISTEMAS Y ADMINISTRADORES DE LOS RECURSOS INFORMATICOS Y LOS SISTEMAS DE INFORMACION

- Los Administradores de los recursos informáticos, de la Dirección de Sistemas, y administradores de los sistemas de información, deben eliminar, reasignar o bloquear los derechos de acceso otorgados sobre los recursos informáticos y los sistemas de información tanto de los funcionarios de la **Universidad Libre** como de los funcionarios provistos por terceras partes que se retiran de la universidad o cambian de funciones.

Documentos relacionados con ésta política

- Procedimiento de retiro o cambio de labores de funcionarios
- Procedimiento de remoción de derechos de acceso

10. Políticas de seguridad física y del entorno

10.1 Políticas de condiciones eléctricas y ambientales

La **Universidad Libre** debe proveer las condiciones eléctricas y medioambientales adecuadas para la operación de los recursos informáticos. Debe existir documentación del diseño de las instalaciones donde se ubican los componentes tecnológicos de la universidad, a fin de poder realizar una adecuada planeación e implantación de controles para la seguridad de la información.

De igual manera, la corporación debe proveer las condiciones medioambientales adecuadas para el almacenamiento de documentos y medios de almacenamiento.

Normas de condiciones eléctricas y ambientales

Normas Dirigidas a: TODOS LOS USUARIOS

- Las estaciones de trabajo, equipos portátiles y otros recursos informáticos asignados a los usuarios deben estar ubicados en áreas con condiciones de temperatura y humedad adecuadas.

- La documentación física generada, recibida y, en general, manipulada por los funcionarios de la universidad y los funcionarios provistos por terceras partes debe estar ubicada en archivos o repositorios con condiciones de temperatura

y humedad adecuadas, de acuerdo con las Directrices de la función archivística de la corporación.

Normas Dirigidas a: DIRECCION DE SISTEMAS, SERVICIOS GENERALES Y ADMINISTRADORES DE LOS RECURSOS INFORMATICOS Y LOS SISTEMAS DE INFORMACION

- Los Centros de Cómputo y los Centros de Cableado de todas las seccionales deben estar separados de áreas que tengan líquidos inflamables o estén en riesgo de inundaciones e incendios.

- Deben existir mecanismos de revisión y control del ingreso de cualquier tipo de material a los Centros de Cómputo y los Centros de Cableado.

- Todas las instalaciones que se realicen en los Centros de Cómputo y los Centros de Cableado deben seguir los estándares establecidos por la universidad.

- Los trabajos de mantenimiento de redes eléctricas, cableado de datos y voz, deben ser realizados por el personal especialista y debidamente autorizado e identificado.

- Todos los cables de transmisión dentro de los Centros de Cómputo están instalados para propósitos específicos. No se debe manipular ningún cable sin la aprobación de los funcionarios de la Dirección de Sistemas.

- En los Centros de Cómputo deben existir sistemas de detección y extinción automáticas de incendios, control de inundación y alarmas en caso de detectarse condiciones ambientales inapropiadas.

- Los niveles de temperatura y humedad relativa en los Centros de Cómputo deben ser mantenidos dentro de los límites requeridos por la infraestructura de cómputo allí instalada, para lo cual se deben usar sistemas de aire acondicionado.

- Se debe monitorear de manera permanente el estado de los componentes de soporte físico, eléctrico y ambiental que hacen parte de los Centros de Cómputo, como son el sistema de aire acondicionado y el sistema de detección y extinción de incendios, entre otros.

- Los funcionarios de la Dirección de Sistemas deben llevar control de la programación de los mantenimientos preventivos y pruebas de funcionalidad de las UPS, del sistema de aire acondicionado, del sistema de detección y

extinción de incendios y de los recursos informáticos y verificar su realización. Estos mantenimientos deberán realizarse de acuerdo con los contratos establecidos.

Documentos relacionados con ésta política

- Directrices de condiciones eléctricas y ambientales para el Centro de Computo y los Centros de Cableado
- Directrices de la función archivística

10.2 Políticas de seguridad física y control de acceso a los Centros de Cómputo y los Centros de Cableado

La Dirección de Sistemas de la **Universidad Libre** debe garantizar la implantación y efectividad de los mecanismos de seguridad física y control de acceso a los Centros de Cómputo y los Centros de Cableado.

Normas de seguridad física y control de acceso a los Centros de Cómputo y los Centros de Cableado

Normas Dirigidas a: DIRECCION DE SISTEMAS, SERVICIOS GENERALES Y ADMINISTRADORES DE LOS RECURSOS INFORMATICOS Y LOS SISTEMAS DE INFORMACION

- Todos los funcionarios de la **Universidad Libre** que tengan acceso a los Centros de Cómputo y a los Centros de Cableado son responsables por el buen funcionamiento y estado de los mismos.

- Los Centros de Cómputo debe contar con mecanismos de control de acceso tales como cámaras, puertas de seguridad, sistemas de control con tarjetas inteligentes y sistema de alarmas, entre otras, que la universidad considere pertinentes.

- Las puertas de acceso a los Centros de Cómputo y los Centros de Cableado deben permanecer siempre cerradas y aseguradas. De igual manera, todos los gabinetes y puertas de los equipos que se encuentran en los Centros de Cómputo y Centros de Cableado deben permanecer cerrados.

- Los Centros de Cableado deben tener un control de acceso con restricciones especiales.

- Todas las personas que ingresen a los Centros de Cómputo o a los Centros de Cableado deberán tener una autorización previa, de acuerdo con los procedimientos de control definidos para ese propósito.

- El ingreso de terceros a los Centros de Cómputo y a los Centros de Cableado, debe estar debidamente registrado mediante una bitácora ubicada en un lugar visible a la entrada estos lugares.

- Las solicitudes de acceso a los Centros de Cómputo deben ser autorizadas por funcionarios de la Dirección de Sistemas. En cualquier caso, los visitantes siempre deberán estar acompañados por un funcionario de la Dirección de Sistemas durante su permanencia en el Centro de Computo.

- Los ingresos a los Centros de Cómputo deben ser monitoreados regularmente para identificar accesos no autorizados y para confirmar que los controles de acceso son efectivos.

- Los privilegios de acceso físico a los Centros de Computo y los Centros de Cableado deben ser descontinuados o modificados oportunamente a la terminación, transferencia o cambio en las labores de un funcionario autorizado.

- La asignación de espacio, ubicación, movimiento y demás requerimientos físicos para los recursos informáticos de los Centros de Computo deben ser autorizados por el Jefe de la Dirección de Sistemas acogiéndose a los procedimientos de administración y operación del Centro de Computo.

Documentos relacionados con ésta política

- Procedimientos operativos para cada uno de los recursos informáticos y sistemas de información administrados (por ejemplo, administración y operación del Centro de Cómputo y los Centros de Cableado)

10.3 Políticas de seguridad física y control de acceso a las oficinas e instalaciones de la universidad

Todo recurso informático que contenga o procese información de la **Universidad Libre** debe cumplir con las normas de seguridad física que rijan con el fin de restringir el acceso físico no autorizado y asegurar la protección de los recursos.

Cada una de las áreas debe tomar las medidas de control necesarias para asegurar las oficinas e instalaciones de la universidad, utilizando mecanismos de control para evitar el acceso no autorizado.

Normas de seguridad física y control de acceso a las oficinas e instalaciones de la universidad

Normas Dirigidas a: TODOS LOS USUARIOS

- Todos los funcionarios deben portar el carné que los identifica como funcionarios de la **Universidad Libre**, mientras permanezcan en las instalaciones de la corporación.

- Todos los funcionarios deben reportar, a la mayor brevedad, cualquier sospecha de pérdida o robo de carnés de identificación y tarjetas de acceso físico a las instalaciones de la universidad.

- Los funcionarios de la **Universidad Libre** no deben intentar ingresar a áreas a las cuales no tengan la debida autorización.

- Todos los visitantes que ingresen a la universidad, deben presentar en recepción su identificación para ser registrados y cumplir con el procedimiento diseñado para tal fin.

- Todos los visitantes que ingresan a la universidad deben portar una identificación visible la cual es entregada en el momento de registro.

- Todo maletín, bolso o cartera debe ser revisado por el personal de seguridad, tanto cuando se ingresa o se dejan las instalaciones de la universidad.

Normas Dirigidas a: JEFES DE UNIDADES ACADEMICAS Y ADMINISTRATIVAS

- Los Jefes de Unidades Académicas y Administrativas en donde haya atención al público deben garantizar que las áreas de trabajo de sus funcionarios y las propias se encuentran separadas de las áreas de atención al público.

- Las oficinas e instalaciones donde haya atención al público no deben permanecer abiertas cuando los funcionarios se levantan de sus puestos de trabajo, así sea por periodos cortos de tiempo.

- Las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a las oficinas solo deben ser utilizados por los funcionarios autorizados y, salvo situaciones de emergencia, estos no deben ser transferidos a otros funcionarios de la universidad, funcionarios provistos por terceras partes o estudiantes.

- Las oficinas e instalaciones donde se maneje información sensible deben contar con sistemas de alarmas y cámaras.

Normas Dirigidas a: SEGURIDAD

- El área de Seguridad debe brindar asesoría y apoyo a las Unidades Académicas y Administrativas para la instalación de cámaras, sistemas de alarmas u otros sistemas de monitoreo.

- De igual forma, debe administrar los registros de dichas cámaras, sistemas de alarmas u otros sistemas de monitoreo.

Documentos relacionados con ésta política

- Procedimiento de control de acceso físico

11. Políticas de gestión de las comunicaciones y las operaciones

11.1 Políticas de asignación de responsabilidades operativas

La Dirección de Sistemas de la **Universidad Libre**, encargada de la operación y administración de la plataforma tecnológica que apoya los procesos de negocio, debe asignar funciones específicas a sus funcionarios quienes deben garantizar la adecuada operación y administración de dicha plataforma y la documentación de los procesos operativos para la ejecución de dichas actividades.

La Dirección de Sistemas y Auditoría Interna, deben garantizar la eficiencia de los controles implantados en los procesos operativos de la **Universidad Libre** con el objeto de garantizar la integridad, confidencialidad y disponibilidad de la información manejada.

Normas de asignación de responsabilidades operativas

Normas Dirigidas a: DIRECCION DE SISTEMAS Y ADMINISTRADORES DE LOS RECURSOS INFORMATICOS Y LOS SISTEMAS DE INFORMACION

- Se deben documentar todos los procedimientos relacionados con la operación y administración de la plataforma tecnológica que apoya los procesos de negocio. Los procedimientos operativos se deben mantener actualizados y deben llevar un control de versiones.

- Se deben establecer responsabilidades y procedimientos para controlar los cambios en los recursos informáticos y en el software.

- Se deben establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad de la información.

Documentos relacionados con ésta política

- Procedimientos operativos para cada uno de los recursos informáticos y sistemas de información administrados (por ejemplo, soporte, mantenimiento, administración, operación y procesos especiales de cada uno de los recursos informáticos y sistemas de información)

11.2 Políticas para el control de cambios

Todo cambio a un componente de la plataforma tecnológica relacionado con modificación de accesos, modificación o mantenimiento de software, actualización de versiones o modificación de parámetros, debe realizarse de tal forma que no disminuya los niveles de seguridad existentes.

La **Universidad Libre** debe asegurar que los cambios efectuados sobre la plataforma tecnológica, considerando tanto el software operativo como los sistemas de información, son adecuadamente controlados y debidamente autorizados por las áreas propietarias. Cualquier tipo de cambio deberá quedar formalmente documentado desde su solicitud hasta su implantación.

Normas para el control de cambios

Normas Dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

- Los propietarios de la información o los activos de información deben solicitar formalmente los requerimientos de nuevas funcionalidades, servicios o modificaciones sobre sus activos de información.

- Así mismo, dichos propietarios son responsables de efectuar las pruebas suficientes de funcionalidad y operación, documentarlas y aprobar formalmente los cambios solicitados.

Normas Dirigidas a: DIRECCION DE SISTEMAS Y ADMINISTRADORES DE LOS RECURSOS INFORMATICOS Y LOS SISTEMAS DE INFORMACION

- Cualquier tipo de cambio sobre la plataforma tecnológica de la **Universidad Libre** debe quedar formalmente documentado desde su solicitud hasta su implantación. Este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos.

- Se debe disponer de manuales de configuración y operación de los sistemas operativos, servicios de red, bases de datos y de los sistemas de información, para toda la plataforma tecnológica de la **Universidad Libre**.

Documentos relacionados con ésta política

- Procedimiento de control de cambios

11.3 Políticas para la planeación y aceptación de sistemas

La Dirección de Sistemas de la **Universidad Libre**, en compañía de las áreas propietarias de los sistemas de información, debe encargarse de hacer las provisiones y proyecciones de crecimiento de la plataforma tecnológica, de manera periódica, con el fin de garantizar la correcta operación de los recursos informáticos y sistemas de información que apoyan los procesos de negocio de la universidad.

De igual manera, deben aceptar nuevos recursos informáticos, servicios o sistemas de información antes de su entrada en producción siguiendo los controles establecidos y cumpliendo con las debidas autorizaciones.

Normas para la planeación y aceptación de sistemas

Normas Dirigidas a: DIRECCION DE SISTEMAS Y ADMINISTRADORES DE LOS RECURSOS INFORMATICOS Y LOS SISTEMAS DE INFORMACION

- Antes de seleccionar y poner en producción un recurso informático se deberá estudiar la demanda y las proyecciones de crecimiento del recurso (capacity planning) para asegurar el desempeño y la capacidad de almacenamiento.

- Las pruebas de aceptación sobre los recursos de procesamiento de información deben ser terminadas antes de la puesta en producción de nuevos sistemas de información o servicios.

- Se debe prever una asignación de espacio en los recursos informáticos para el almacenamiento de los logs de auditoría, de acuerdo con las directrices establecidas por Auditoría Interna.

Documentos relacionados con ésta política

- Proyecciones de crecimiento de la plataforma tecnológica
- Procedimientos operativos para cada uno de los recursos informáticos y sistemas de información administrados (por ejemplo, soporte, mantenimiento,

administración, operación y procesos especiales de cada uno de los recursos informáticos y sistemas de información)

11.4 Políticas de protección frente a software malicioso

La **Universidad Libre** debe proteger su información y los recursos de procesamiento de la misma de divulgación, modificación o daño permanente ocasionados por la contaminación y el contagio de software malicioso; por tal razón, debe tomar las medidas necesarias para evitar éste tipo de contagio en cualquiera de sus formas.

Todos los funcionarios deben acogerse a las buenas prácticas recomendadas por la Dirección de Sistemas en relación con la protección frente a software malicioso.

Normas de protección frente a software malicioso

Normas Dirigidas a: TODOS LOS USUARIOS

- El funcionario no debe cambiar o eliminar la configuración del software de antivirus/ antispyware/ malware definida por la Dirección de Sistemas y, únicamente podrá realizar tareas de escaneo de archivos y directorios.

- Los funcionarios de la **Universidad Libre** y el personal suministrado por terceras partes que se conecte a la red de datos de la universidad, no deben ejecutar programas desconocidos que hayan sido descargados de Internet o copiados de cualquier medio de almacenamiento. De manera adicional, no está permitido el uso de software y hardware de propiedad de los funcionarios de la universidad o del personal provisto por terceras partes.

- Los usuarios únicamente deben descargar archivos adjuntos que provengan de fuentes conocidas para evitar contaminación por virus informáticos y/o instalación de software malicioso en sus estaciones de trabajo o equipos portátiles.

- Todos los archivos que sean proporcionados por estudiantes, proveedores, entidades de control u otras terceras partes con las cuales exista intercambio de información deben ser verificados utilizando el software de antivirus/ antispyware/ malware corporativo.

- Cualquier usuario de la red de datos de la **Universidad Libre** que sospeche o detecte alguna infección por virus informático, debe intentar erradicar los virus en su estación de trabajo o equipo portátil y, en caso de no lograrlo, notificar a la Dirección de Sistemas, a través del Soporte Técnico, para la detección y erradicación del virus.

- El software de antivirus/ antispyware/ malware debe utilizarse para explorar virus en cualquier medio de almacenamiento externo, como diskettes, CDs y dispositivos USB, entre otros, antes de intercambiar información con la estación de trabajo o el equipo portátil.

- El software utilizado en la plataforma tecnológica de la **Universidad Libre** debe ser conocido por la Dirección de Sistemas.

Normas Dirigidas a: DIRECCION DE SISTEMAS Y ADMINISTRADORES DE LOS RECURSOS INFORMATICOS Y LOS SISTEMAS DE INFORMACION

- Todas las estaciones de trabajo y equipos portátiles deben tener instalado un software de antivirus/ antispyware/ malware que mitigue el riesgo de contaminación y contagio de software malicioso, actualizado y debidamente configurado.

- Es responsabilidad de la Dirección de Sistemas mantener licenciado y actualizado el software de antivirus/ antispyware/ malware en todos los servidores, estaciones de trabajo y equipos portátiles de la **Universidad Libre**. Así mismo, es su deber generar actualizaciones permanentes del software de antivirus/ antispyware/ malware.

- Todos los archivos adjuntos en los correos electrónicos deben ser chequeados en busca de virus, spyware y/o malware.

- Se debe utilizar hardware o software antispam que filtre correos electrónicos no deseados.

- El software de dominio público y/o código abierto, debe obtenerse de fuentes reconocidas. Software obtenido de fuentes no confiables no debe ser utilizado en equipos de la **Universidad Libre**.

- Los recursos informáticos de la universidad deben tener instalados todos los parches y las últimas actualizaciones aplicables para bloquear las vulnerabilidades de seguridad conocidas.

Documentos relacionados con ésta política

- Procedimientos operativos para cada uno de los recursos informáticos y sistemas de información administrados (por ejemplo, configuración y administración del software de antivirus)
- Procedimiento de prevención y detección de software malicioso

11.5 Políticas de almacenamiento y respaldo de la información

Se debe garantizar el respaldo de la información crítica de la **Universidad Libre** estableciendo los procedimientos y los mecanismos necesarios para generar copias de seguridad de la información que apoya los procesos de negocio y, para almacenar y resguardar dichas copias. Las áreas propietarias de la información en conjunto con la Dirección de Sistemas deben definir la estrategia a seguir para el respaldo de la información.

Debe existir una definición formal de la estrategia de generación, retención y rotación de las copias de respaldo.

Normas de almacenamiento y respaldo de la información

Normas Dirigidas a: TODOS LOS USUARIOS

- Es responsabilidad de todos los usuarios de recursos informáticos de la **Universidad Libre** identificar que información crítica de sus estaciones de trabajo o equipos portátiles debe ser respaldada y realizar copias de seguridad de dicha información.

- Los usuarios de los recursos informáticos de la **Universidad Libre** son responsables de eliminar toda la información desactualizada, inutilizada o no relacionada con la corporación.

- De igual manera, los usuarios de los recursos informáticos deben solicitar a los Jefes de las Unidades Académicas o Administrativas a las que pertenecen los medios de almacenamiento requeridos para la generación de las copias de seguridad de la información residente en las estaciones de trabajo y equipos portátiles, identificada como crítica para la universidad.

Normas Dirigidas a: DIRECCION DE SISTEMAS Y ADMINISTRADORES DE LOS RECURSOS INFORMATICOS Y LOS SISTEMAS DE INFORMACION

- La Dirección de Sistemas y los Administradores de los recursos informáticos y los sistemas de información deben definir la estrategia de generación, retención y rotación de las copias de respaldo de la información crítica de la universidad.

- La información de los recursos de procesamiento y sistemas de información de negocio debe ser almacenada y respaldada de acuerdo con los procedimientos establecidos, de tal forma que se garantice su integridad y su disponibilidad.

- Los funcionarios de la Dirección de Sistemas tienen la obligación de proteger los discos, diskettes, cintas magnéticas, CD-ROM y DVD que contengan copias de respaldo de la información de la **Universidad Libre** y, se encuentren bajo su custodia, siguiendo el procedimiento de almacenamiento y resguardo establecido.

- La Dirección de Sistemas deberá asegurar la disponibilidad de la información respaldada utilizando mecanismos de comprobación del estado de las copias, tales como secuencias de recuperación de pruebas.

- La Dirección de Sistemas debe definir las condiciones de transmisión y custodia de las copias de seguridad de la información que son almacenadas externamente con una compañía especializada en éste tema.

- Es responsabilidad de la Dirección de Sistemas monitorear el cumplimiento de los Acuerdos de Niveles de Servicio establecidos con el proveedor del servicio de almacenamiento de copias de respaldo.

Documentos relacionados con ésta política

- Procedimientos operativos para cada uno de los recursos informáticos y sistemas de información administrados (por ejemplo, generación de copias de respaldo (backups) y restauración de la información).

11.6 Políticas de uso de las comunicaciones electrónicas (correo electrónico)

El correo electrónico es una herramienta de trabajo que facilita la comunicación entre los funcionarios de la **Universidad Libre** y los estudiantes, proveedores, entidades de control y otras terceras partes interesadas. Se debe garantizar que sea utilizado de manera adecuada y racional para las funciones propias del negocio, respetando los principios de confidencialidad, integridad, privacidad y autenticidad de quienes realizan las comunicaciones.

Las comunicaciones electrónicas tendrán la misma validez que las comunicaciones realizadas en forma impresa y se deberán definir parámetros de seguridad a nivel de los diversos componentes tecnológicos involucrados en el flujo de dichas comunicaciones electrónicas.

Normas de uso de las comunicaciones electrónicas (correo electrónico)

Normas Dirigidas a: TODOS LOS USUARIOS

- La cuenta de correo asignada es de carácter individual; por lo tanto, ningún funcionario bajo ninguna circunstancia debe usar la cuenta de correo de otro funcionario, con excepción de las Autoridades Nacionales.

- Ningún funcionario de la **Universidad Libre** debe utilizar su correo personal para el envío y recibo de información relacionada con las funciones desempeñadas en su trabajo.

- El límite del tamaño de las carpetas personales del buzón de correo para los funcionarios será de 50 Mb y según la necesidad 100 o 150 Mb previa solicitud. Los funcionarios deben mantener sus buzones depurados para evitar que los mensajes reboten por falta de espacio en ellos.

- El tamaño de los archivos adjuntos en los correos será de hasta 10Mb.

- No se debe permitir la entrada ni salida de archivos ejecutables de aplicaciones, música, videos y presentaciones personales.

- El servicio de correo no debe tener restricciones de horario para los funcionarios y estará disponible 24 horas diarias, 7 días a la semana, para todos los usuarios inscritos.

- Se prohíben las cadenas de mensajes de cualquier tipo y la propaganda de tipo comercial, político o religioso entre otros y, cualquier contenido ofensivo para los funcionarios de la universidad.

Normas Dirigidas a: DIRECCION DE SISTEMAS Y ADMINISTRADORES DE LOS RECURSOS INFORMATICOS Y LOS SISTEMAS DE INFORMACION

- Es responsabilidad de la Dirección de Sistemas proveer un ambiente seguro y controlado para el funcionamiento del correo electrónico.

- La Dirección de Sistemas debe asegurar la protección de los canales de comunicación y administrar los aspectos de operación tales como: el tamaño máximo de información transmitida y recibida, la cantidad de destinatarios permitida y el tamaño máximo del buzón de los usuarios, entre otros.

- Se deben establecer procedimientos e implantar controles que permitan:

  - Detectar y proteger contra código malicioso que pudiera ser transmitido a través de los mensajes
  - Evitar interceptación de los mensajes
  - Proteger los archivos adjuntos con información sensible

- Es necesario concientizar a los funcionarios tanto de la **Universidad Libre** como al personal provisto por terceras partes, respecto de las precauciones que deben adoptar cuando intercambien información sensible a través del correo electrónico.

- La Dirección de Sistemas debe informar claramente a los funcionarios de la universidad así como a los funcionarios suministrados por terceras partes, cuál es el uso que se espera que ellos hagan del correo electrónico provisto y, bajo qué condiciones los mensajes pueden ser objeto de control y monitoreo.

- La Dirección de Sistemas debe establecer procedimientos e implantar controles de monitoreo y revisión de la utilización del correo electrónico.

Documentos relacionados con ésta política

- Procedimientos operativos para cada uno de los recursos informáticos y sistemas de información administrados (por ejemplo, configuración y administración del correo electrónico)
- Procedimiento de prevención y detección de software malicioso

11.7 Políticas de acceso a internet

Los funcionarios de la **Universidad Libre** y los funcionarios provistos por terceras partes deben utilizar Internet como una herramienta de consulta, para propósitos de las funciones del negocio, acatando y respetando la normatividad vigente alrededor de su uso.

Normas de acceso a internet

Normas Dirigidas a: TODOS LOS USUARIOS

- Se encuentran restringidos los servicios de FTP (Protocolo para la transferencia de archivos), Telnet (Programa de emulación de terminales remotas) y Chat (Comunicación electrónica interactiva).

- El acceso a sitios web de música, videos, adultos, terrorismo y todos aquellos que puedan afectar la productividad de los funcionarios de la universidad se deben restringir a través de herramientas de control permanente. Los sitios de acceso a correos electrónicos personales (Hotmail, Yahoo, Gmail) tienen restricción de horario. Si por razones de negocio, se requiere el acceso a una página web asociada con un puerto especifico, éste se debe solicitar con dos

horas de antelación a la Dirección de Sistemas, encargada de autorizar y otorgar el acceso de manera temporal.

- La descarga de archivos y ejecución de programas desde internet debe estar restringida a las actividades necesarias para la operación del negocio.

Normas Dirigidas a: DIRECCION DE SISTEMAS Y ADMINISTRADORES DE LOS RECURSOS INFORMATICOS Y LOS SISTEMAS DE INFORMACION

- La Dirección de Sistemas debe establecer los procedimientos necesarios para procesar las solicitudes de acceso a Internet y validar las autorizaciones requeridas.

- La Dirección de Sistemas debe otorgar permisos de uso solamente a los servicios de internet permitidos por la universidad, es decir, los que puedan ofrecerse de manera segura.

- Es responsabilidad de la Dirección de Sistemas establecer procedimientos e implantar controles para:

  - Evitar la descarga de software no autorizado
  - Evitar código malicioso proveniente de internet
  - Evitar el acceso a los sitios establecidos como no deseados
  - Evitar el uso de productos y servicios no autorizados

- La Dirección de Sistemas debe generar registros de los accesos de los usuarios a internet y, establecer procedimientos e implantar controles para monitorear dichos registros.

Documentos relacionados con ésta política

- Procedimientos operativos para cada uno de los recursos informáticos y sistemas de información administrados (por ejemplo, configuración y administración de los servicios de internet)
- Procedimiento de prevención y detección de software malicioso

11.8 Políticas de uso de periféricos (scanner, impresoras, mouse, teclado, medios de almacenamiento removibles)

El uso de periféricos y medios de almacenamiento en los servidores, estaciones de trabajo y equipos portátiles de la **Universidad Libre** debe ser aprobado por los Jefes de Unidades Académicas y Administrativas, de acuerdo con las labores realizadas por los funcionarios al interior de cada una de las áreas.

Normas de uso de periféricos

Normas Dirigidas a: TODOS LOS USUARIOS

- Ningún funcionario de la universidad podrá instalar o conectar a su estación de trabajo o equipo portátil, elementos adicionales a los entregados con el equipo. Estos elementos, incluyen, pero no se limitan a: cámaras web, cámaras digitales, grabadoras de sonido, impresoras, scanner. En caso de requerir el uso de cualquier elemento adicional, deberá solicitar autorización a la Dirección de Sistemas.

- Los funcionarios no deberán usar medios de almacenamiento no autorizados para el manejo de la información, donde se incluyen, pero no se limitan a: diskettes, memorias USB, memorias flash, CDs, DVDs, discos externos, que no sean de propiedad de la **Universidad Libre** y que no hayan sido entregados con fines y autorización específicos.

Documentos relacionados con ésta política

- Procedimientos para el acceso y divulgación, almacenamiento, generación de copias, transmisión, etiquetado y destrucción de la información por cada uno de los niveles de clasificación.
- Procedimiento de prevención y detección de software malicioso
- Estándar de seguridad para equipos portátiles y estaciones de trabajo

11.9 Políticas de intercambio de información

Todo intercambio de información sensitiva entre áreas, sedes o seccionales de la **Universidad Libre** o con terceras partes debe realizarse acatando las normas de protección de la confidencialidad, integridad y disponibilidad de la información.

Solo se deben utilizar las formas de intercambio consideradas seguras y se deben establecer Acuerdos de Intercambio con las terceras partes con quienes se realiza el intercambio.

Normas de intercambio de información

Normas Dirigidas a: TODOS LOS USUARIOS

- Los funcionarios de la **Universidad Libre** deben velar por el cumplimiento de los Acuerdos de Intercambio con los proveedores de servicios (courier de mensajería, servicios de valores, calígrafo, entre otros).

Normas Dirigidas a: DIRECCIÓN JURÍDICA

- La Dirección Jurídica debe establecer los requerimientos legales para el intercambio de información con terceras partes.

- De igual manera, debe generar un modelo de Acuerdos de Intercambio y establecerlo con aquellos terceros a los que se les deba entregar o enviar información de la universidad

Normas Dirigidas a: JEFES DE UNIDADES ACADEMICAS Y ADMINISTRATIVAS

- El intercambio de información de la **Universidad Libre** con sus proveedores de servicios debe ser efectuado una vez se hayan establecido los correspondientes Acuerdos de Intercambio.

- Los proveedores de servicios con los cuales haya intercambio de información de la universidad deben acogerse a las políticas de seguridad de la información y deben regirse por los Acuerdos de Intercambio establecidos.

Normas Dirigidas a: SERVICIOS GENERALES

- Se deben definir procedimientos para el intercambio, transmisión y transporte de medios de almacenamiento y documentos que contemplen la utilización de medios de transporte o servicios de mensajería confiables y la adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificaciones.

- De igual manera, se deben implantar mecanismos de control para la protección de la información enviada entre áreas de la universidad utilizando la mensajería interna.

Normas Dirigidas a: DIRECCION DE SISTEMAS

- Se deben definir procedimientos para el intercambio y transmisión de información digital que contemplen la utilización de medios de transmisión electrónica confiables y la adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificaciones.

Documentos relacionados con ésta política

- Acuerdos de Intercambio con terceras partes
- Procedimientos para la transmisión de la información física por cada uno de los niveles de clasificación.

- Procedimientos para la transmisión de la información digital por cada uno de los niveles de clasificación.

11.10 Políticas de monitoreo y auditoria de la plataforma tecnológica

Se debe garantizar el monitoreo permanente del uso que dan los funcionarios de la corporación y los funcionarios provistos por terceras partes a la plataforma tecnológica de la **Universidad Libre**.

De igual forma, se debe realizar la revisión periódica de los archivos de auditoría y velar por su custodia cumpliendo con los periodos de retención establecidos para ellos.

Normas de monitoreo y auditoría de la plataforma tecnológica

Normas Dirigidas a: DIRECCION DE SISTEMAS Y ADMINISTRADORES DE LOS RECURSOS INFORMATICOS Y LOS SISTEMAS DE INFORMACION

- Se debe realizar monitoreo de los recursos informáticos con herramientas que permiten identificar fallas en el software instalado, en el hardware, en los puertos y en la conectividad.

- Se debe contar con archivos de bitácora (logs) y los registros de auditoría (audit trails) que graban los eventos relevantes sobre la seguridad de los recursos informáticos y sistemas de información. Estos archivos se deben almacenar durante el período establecido por Auditoría Interna y se deben proteger para que nadie los pueda alterar y que sólo puedan ser accedidos por las personas autorizadas.

- Se deben habilitar sistemas de monitoreo que permitan: detectar incumplimientos de la Política de Control de Acceso, registrar eventos que proporcionen evidencia en caso de ocurrir incidentes de seguridad y verificar el uso adecuado de los recursos informáticos y los sistemas de información.

Normas Dirigidas a: AUDITORIA INTERNA

- Auditoría Interna debe determinar los periodos de retención de los archivos de auditoría y los eventos a auditar en los recursos informáticos y los sistemas de información.

- Los archivos de auditoría de los recursos informáticos y los sistemas de información (*logs y audit trails*) deben ser revisados periódicamente. Dichos archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoría.

Documentos relacionados con ésta política

- Procedimiento de generación de registros de auditoría para recursos informáticos y sistemas de información.
- Procedimiento de monitoreo y revisión de los registros de auditoría de los recursos informáticos y los sistemas de información

12. Políticas de Control de Acceso

12.1 Políticas de administración de cuentas de usuario y contraseñas

Se debe garantizar que se establezcan las reglas y derechos de control de acceso para cada usuario o grupo de usuarios y se implanten mecanismos de control de acceso lógico sobre los recursos informáticos y los sistemas de información de la **Universidad Libre.**

Normas de administración de cuentas de usuario y contraseñas

Normas Dirigidas a: TODOS LOS USUARIOS

- Se deben asignar códigos de identificación y/o nombres de usuario únicos a todos los funcionarios de la **Universidad Libre** y funcionarios provistos por terceras partes y éstos no deben compartirlas con otros funcionarios de la universidad ni funcionarios suministrados por terceros.

- Los usuarios de recursos informáticos y sistemas de información deben tener un mecanismo de autenticación, por ejemplo, una contraseña. De manera adicional, todos los recursos informáticos y los sistemas de información deben requerir autenticación.

- Cada usuario autorizado es responsable de todas las acciones realizadas por cualquier otra persona a quien haya divulgado su cuenta de usuario y/o contraseña. Se debe recordar que la cuenta de usuario y/o contraseña de acceso es individual e intransferible.

- Las contraseñas deben requerir una configuración compleja adaptándose a las restricciones técnicas de cada uno de los recursos informáticos y sistemas de información de acuerdo con el estándar de contraseñas.

- Una vez le han sido asignadas las contraseñas de acceso, es responsabilidad del usuario modificarlas en su primer uso de cada uno de los recursos informáticos y/o sistemas de información según las indicaciones de los

Administradores de los recursos informáticos y sistemas de información y los Propietarios de los activos de información.

- El acceso a recursos informáticos y sistemas de información propiedad de la **Universidad Libre** mediante el uso de contraseñas compartidas está prohibido.

- Las contraseñas de los usuarios de la red de datos y los sistemas de información de la **Universidad Libre** deben ser cambiadas periódicamente de acuerdo con el estándar de contraseñas.

- Bajo ninguna circunstancia, se debe escribir las contraseñas en papel o almacenarlas en medios digitales no cifrados.

- Los usuarios deben solicitar cambio de contraseñas siempre que exista un posible indicio de compromiso del recurso de procesamiento o sistema de información y/o utilizar el mecanismo de cambio de contraseña que le sea provisto.

Normas Dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION, DIRECCION DE SISTEMAY ADMINISTRADORES DE LOS RECURSOS INFORMATICOS Y SISTEMAS DE INFORMACION

- Todos los recursos informáticos y sistemas de información que procesen cualquier información perteneciente a la **Universidad Libre** deben requerir autenticación.

- Las cuentas de usuario definidas sobre los recursos informáticos y los sistemas de información deben contar con aprobación para su creación y con especificación de tareas. Por ningún motivo se deben crear cuentas de usuario genéricas.

- La creación de cuentas o modificación de perfiles de usuario debe ser solicitada y documentada por el nivel superior al funcionario que lo requiere.

- Los recursos informáticos y los sistemas de información de la **Universidad Libre** no deben mostrar las contraseñas en pantalla.

- Las cuentas de usuario que no hayan sido utilizadas consecutivamente deben ser inhabilitadas y no reactivadas hasta que la identidad del usuario haya sido verificada de acuerdo con el estándar de contraseñas.

- La cuenta de un usuario debe ser deshabilitada si ha habido un máximo de intentos de acceso consecutivos sin éxito de acuerdo con el estándar de contraseñas; esto con el propósito de evitar posibles ataques de intrusión.

- Los recursos informáticos deben ser configurados y los sistemas de información desarrollados de tal manera que al primer ingreso a ellos se exija al usuario modificar la contraseña asignada por defecto.

- La pantalla de inicio de sesión en todos los recursos informáticos y sistemas de información de la **Universidad Libre** debe advertir a los usuarios que están entrando a un sistema propietario y el acceso es permitido solamente a personas autorizadas.

- Debe definirse la periodicidad de cambio de contraseñas y solicitar este cambio de manera automática utilizando algún mecanismo que la Dirección de Sistemas y los Propietarios de los activos de información definan, de acuerdo con el estándar de contraseñas.

Documentos relacionados con ésta política

- Procedimiento de control de acceso lógico

12.2 Políticas de verificación y mantenimiento de los derechos de acceso

Los funcionarios de la **Universidad Libre** y los funcionarios suministrados por terceras partes deben tener acceso únicamente a la información necesaria para el desarrollo de sus funciones y el otorgamiento de los derechos de acceso debe estar regulado por las normas y procedimientos establecidos para tal fin.

Normas de verificación y mantenimiento de los derechos de acceso

Normas Dirigidas a: TODOS LOS USUARIOS

- La creación o modificación de perfiles de usuario y/o accesos a los recursos informáticos y sistemas de información debe ser solicitada, aprobada y documentada por el nivel superior al usuario que lo requiere.

- El acceso a los recursos informáticos y sistemas de información de la **Universidad Libre** está permitido únicamente para soportar las actividades relacionadas con el negocio.

- Las responsabilidades y obligaciones de los funcionarios con acceso a recursos informáticos y sistemas de información de la **Universidad Libre** deben estar claramente definidas. El acceso otorgado a un usuario debe ser

restringido solamente a la información específica para las funciones de su cargo.

Normas Dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

- Es responsabilidad de los propietarios de los recursos informáticos y sistemas de información definir los perfiles de usuario y autorizar las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos.

- Así mismo, los propietarios de los activos de información deben verificar y ratificar periódicamente todas las autorizaciones sobre sus recursos informáticos y sistemas de información.

Normas Dirigidas a: DIRECCION DE SISTEMAS Y ADMINISTRADORES DE LOS RECURSOS INFORMATICOS Y LOS SISTEMAS DE INFORMACION

- Se debe establecer un procedimiento que asegure la eliminación de derechos de acceso de manera oportuna, cuando los funcionarios se retiran de la **Universidad Libre** o cambian de cargo.

- Los usuarios o perfiles de usuario que traen por defecto los sistemas operativos y las bases de datos deben ser suspendidos, renombrados o limitados en sus autorizaciones.

- Así mismo, las contraseñas que traen por defecto los recursos informáticos deben ser cambiadas.

- Para todos los equipos de cómputo se deben establecer bloqueos o terminación de sesiones automáticas, en el caso de que queden desatendidos.

Documentos relacionados con ésta política

- Procedimiento de control de acceso lógico

12.3 Políticas de control de acceso a sistemas operativos, redes de datos y sistemas de información

La **Universidad Libre** debe garantizar que los sistemas operativos, las redes de datos y los sistemas de información que apoyan los procesos de negocio son debidamente protegidos de accesos no autorizados por medio de mecanismos de control de acceso lógico.

Normas de control de acceso a sistemas operativos, redes de datos y sistemas de información

Normas Dirigidas a: TODOS LOS USUARIOS

- Tanto los funcionarios de la **Universidad Libre** como los funcionarios provistos por terceras partes, al recibir una nueva cuenta o nivel de acceso a los recursos de la red de datos, deben firmar un documento donde declaran conocer las Políticas de Seguridad de la Información, y aceptan sus responsabilidades con relación al uso de la cuenta o acceso otorgados.

- La utilización de los recursos y servicios de red debe ser limitada a usuarios autorizados únicamente para los propósitos establecidos.

- El uso de herramientas de administración remota de estaciones de trabajo o equipos portátiles, que incluyen, pero no se limitan a: VNC, NetMeeting, Terminal Server, estarán bajo la responsabilidad de la Dirección de Sistemas; por lo tanto, ningún usuario podrá hacer uso de estas herramientas sin la debida autorización.

- Bajo ciertas condiciones, la **Universidad Libre** permite a usuarios externos acceder a las redes corporativas desde redes externas. Los usuarios externos deben ser autorizados por la corporación antes de permitirse el acceso. La autorización debe ser documentada y aprobada.

- El acceso remoto al correo electrónico de la **Universidad Libre** debe estar restringido a los funcionarios de la universidad y funcionarios provistos por terceras partes que tengan cuenta de correo electrónico.

Normas Dirigidas a: DIRECCION DE SISTEMAS Y ADMINISTRADORES DE LOS RECURSOS INFORMATICOS Y LOS SISTEMAS DE INFORMACION

- Se deben establecer procedimientos de autorización y controles para proteger el acceso a los sistemas operativos, los recursos y servicios de red y los sistemas de información.

- Se deben adoptar medidas para garantizar la disponibilidad de los recursos y servicios de red de la **Universidad Libre** y la permitir la conexión a ellos.

- Los recursos y servicios de red ofrecidos deben contar con los niveles o atributos de seguridad requeridos por la universidad.

- Se debe definir el horario de conexión y el tipo de información a la cual es posible acceder remotamente.

- La instalación de un nuevo componente en la red de datos de la **Universidad Libre** debe estar autorizada por el jefe de la Dirección de Sistemas.

- Todos los equipos de computo clientes que deseen conectarse a la red de datos de la universidad deberán pasar por todos los controles de red para poder autenticarse en ella.

- Se deben establecer mecanismos para la identificación y autenticación de usuarios externos antes de permitir su ingreso a los recursos informáticos y sistemas de información de la corporación.

- Se debe asegurar que los usuarios externos a la **Universidad Libre** entienden y aceptan sus responsabilidades para la adecuada utilización y protección de los recursos y servicios de red mediante la aceptación de las Políticas de Seguridad de la Información.

- Los controles de acceso para usuarios externos, deben revisarse periódicamente. Tanto el Propietario del activo de información como Auditoría Interna y la Dirección de Sistemas deben revisar estos controles para garantizar que los usuarios externos tengan acceso permitido solamente a aquellos recursos y servicios de red para los cuales han sido aprobados y solamente por el tiempo que haya sido acordado.

- Los accesos remotos a los servidores deben estar restringidos únicamente a personal autorizado y con base en la necesidad de las labores de los funcionarios que lo requieran.

- La utilización de programas para el control remoto de equipos está permitida, únicamente haciendo uso del software aprobado por la **Universidad Libre**.

- Los privilegios especiales para administración de servidores, dispositivos de red, bases de datos y sistemas de información sólo deben otorgarse a aquellos directamente responsables de la administración o de la seguridad de dichos recursos informáticos y sistemas de información. El Administrador de cada recurso de procesamiento o sistema de información es el responsable de otorgar los accesos al mismo.

- Las contraseñas de usuarios administradores deben modificarse periódicamente siguiendo el estándar para las contraseñas críticas. Las contraseñas de estos usuarios deben ser entregadas al Jefe de la Dirección de Sistemas en sobre cerrado, cada vez que son modificadas, y deben ser almacenadas en caja fuerte.

- Las conexiones desde estaciones de trabajo no autorizadas son una fuente potencial de intrusión en un entorno de red. La conexión a la red de datos que no sea requerida debe ser inhabilitada.

- Las sesiones de usuario inactivas, es decir, las que no han tenido intercambio de información hacia o desde el usuario por cierto período de tiempo, deben ser terminadas.

- La red de datos de la **Universidad Libre** deberá estar protegida por la implantación de un sistema de firewall, que permitirá filtrar por puerto, protocolo, aplicación y tipo de tráfico, entre otros.

- Los enrutadores de la red de datos deben tener políticas de filtrado de paquetes.

- El esquema de direccionamiento interno de la red de datos de la **Universidad Libre** no debe ser visible desde redes o equipos externos y el acceso desde internet hacia la red de datos interna no debe ser permitido o, solo debe ser permitido a través de un dispositivo fuerte de autenticación.

- La **Universidad Libre** deberá mantener las redes de datos segmentadas por dominios, grupos de servicios, usuarios o sistemas de información.

- Se deben activar las facilidades de seguridad que ofrecen los sistemas operativos para restringir el acceso a los recursos informáticos.

- Los Administradores de los recursos informáticos no deben tener acceso a sistemas de información en producción y transacciones en línea.

- Solamente el DBA (administrador de las bases de datos) puede tener acceso a los datos desde fuera de los sistemas de información. Se debe controlar y monitorear dichos accesos.

- Para protegerse de software malicioso, todas las estaciones de trabajo y equipo portátiles que se vayan a conectar a la red de datos de la **Universidad Libre** deben tener un software de antivirus/ antispyware/ malware actualizado, el cual debe ser verificado antes de permitir la conexión.

- Las redes inalámbricas deben contar con métodos de autenticación para su acceso.

Documentos relacionados con ésta política

- Procedimiento de control de acceso lógico

13. Políticas de adquisición, desarrollo y mantenimiento de los sistemas de información

13.1 Políticas para el establecimiento de requerimientos de seguridad

Se debe asegurar que el software adquirido, desarrollado por terceras partes o al interior de la **Universidad Libre** cumpla con los requisitos de seguridad establecidos por la corporación. Cualquier sistema de información o software que se adquiera o se desarrolle debe acogerse a ésta política.

Todas las áreas propietarias de sistemas de información deben incluir requisitos de seguridad en la definición de requerimientos y deben asegurarse de que estos sean cumplidos a cabalidad durante las pruebas realizadas sobre los desarrollos.

Normas para el establecimiento de requisitos de seguridad

Normas Dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION Y DIRECCION DE SISTEMAS

- Las especificaciones para la adquisición o desarrollo de sistemas de información o software para la **Universidad Libre** deberán incluir unos requerimientos de seguridad de la información, los cuales contemplan pero no se limitan a, estandarización de herramientas de desarrollo, controles de autenticación como contraseñas y autorización como perfiles, controles de acceso al código, controles de acceso a los datos, controles de manejo de sesiones, cifrado, arquitectura de las aplicaciones y recomendaciones de codificación y configuración.

- Se deben generar metodologías para la definición de requerimientos de software, las cuales deben contener buenas prácticas y principios que deben utilizar los desarrolladores de software para entender de forma precisa el producto de software que se va a construir. Así mismo, se deben utilizar dichas metodologías para la definición de requerimientos de software

- Se deben identificar los riesgos asociados al desarrollo de sistemas de información o software y buscar que sean mitigados utilizando los controles apropiados.

- La identificación de requerimientos para sistemas de información o software deben mantener el balance entre la funcionalidad y la seguridad.

- Se debe garantizar que los sistemas de información o software adquiridos, desarrollados por terceras partes o al interior de la **Universidad Libre**

cumplan con todas las políticas, procedimientos y estándares de seguridad definidos al interior de la universidad.

Normas Dirigidas a: DESARROLLADORES (GRUPO INTERNO Y TERCEROS PROVEEDORES DE SOFTWARE)

- Se debe identificar la arquitectura de software más conveniente para cada sistema de información o software que la **Universidad Libre** requiera desarrollar de acuerdo con los requerimientos de seguridad y los controles deseados.

- Todo sistema de información o software adquirido, desarrollado por terceros o al interior de la **Universidad Libre** debe usar herramientas de desarrollo ampliamente reconocidas en el mercado, suficientemente documentadas y que cuenten con licencia.

- Ningún software desarrollado por funcionarios de la **Universidad Libre** o por terceras partes debe tener la habilidad de obtener accesos privilegiados.

Documentos relacionados con ésta política

- Metodologías para la definición de requerimientos de software (tanto desarrollado por terceros como internamente)
- Metodologías para la realización de pruebas al software desarrollado
- Procedimiento de control de cambios
- Procedimiento de control de acceso lógico

13.2 Políticas de control al procesamiento de los sistemas de información

Todas las áreas propietarias de sistemas de información al interior de la **Universidad Libre** deben velar por el correcto procesamiento de los sistemas de información y por la calidad y veracidad de la información tanto ingresada como generada por dichos sistemas.

Los funcionarios que operan los sistemas de información deben hacer validaciones periódicas de la información contenida en éstos sistemas.

Normas de control al procesamiento de los sistemas de información

Normas Dirigidas a: TODOS LOS USUARIOS

- Los usuarios son responsables por la información ingresada en los sistemas de información.

- Así mismo, tienen responsabilidad de verificar la calidad de la información procesada y generada por dichos sistemas de información.

Normas Dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

- Se debe revisar de manera periódica y continua la calidad de los datos ingresados a los sistemas de información o software de la **Universidad Libre**. De la misma forma, se debe validar la información generada por dichos sistemas de información que se encuentren en formas de reportes o consultas.

- Toda migración de datos entre ambientes de desarrollo, pruebas y producción o entre sistemas de información debe ser aprobada por los propietarios de los activos de información.

Normas Dirigidas: AUDITORIA INTERNA

- Auditoría Interna tiene la responsabilidad de monitorear y validar los controles efectuados sobre la calidad de los datos ingresados y generados por los sistemas de información.

Normas Dirigidas a: DESARROLLADORES (GRUPO INTERNO Y TERCEROS PROVEEDORES DE SOFTWARE)

- A cada transacción procesada por un sistema de información o software en producción se le debe asignar un número de secuencia que permita identificarla de manera única.

- Se deben establecer validaciones sobre la información de entrada a los sistemas de información y software desarrollados para la **Universidad Libre** que permitan facilitar que los datos suministrados sean adecuados y correctos.

- Si una transacción de un sistema de información falla, debe rechazar los datos de entrada y generar una notificación de la falla, la cual debe ser corregida o, de lo contrario, se debe mantener la transacción suspendida.

- Todos los sistemas de información tanto adquiridos como desarrollados por terceros o al interior de la **Universidad Libre**, en el caso de una falla no esperada, deben presentar a los usuarios un mensaje de error e indicarles como deben proceder.

- Los archivos y recursos temporales utilizados por los sistemas de información o software deberán ser liberados una vez el proceso que los está utilizando culmine su tarea.

- La salida de datos generados por los sistemas de información o software tales como consultas y reportes debe ser validada para garantizar que el procesamiento de la información es el adecuado para la cada situación.

- Los sistemas de información tanto adquiridos como desarrollados por terceros o al interior de la universidad deben contemplar el bloqueo de manera temporal o definitiva de una cuenta por número de intentos fallidos de acceso, así como prohibir múltiples sesiones con una cuenta de usuario.

- Los sistemas de información adquiridos, desarrollados por terceros o al interior de la **Universidad Libre** deben manejar el concepto de definición de roles y perfiles, de tal forma que solo se habiliten la funciones, y/o menús a los cuales se autoriza el acceso a los usuarios.

- Desde los sistemas de información se debe impedir la ejecución de comandos de los sistemas operativos.

- Bajo ninguna circunstancia debe existir una conexión directa entre los usuarios y las bases de datos. Dichas conexiones siempre deben realizarse a través de los sistemas de información.

- Todo sistema de información de la **Universidad Libre** debe mantener de manera separada los módulos de configuración de los módulos de funcionalidad.

- Cuando las migraciones de datos son realizadas por un tercero, éste debe adjuntar el plan de migración completamente documentado, donde se debe incluir la metodología a utilizar y los planes de contingencia en caso de falla. De igual forma, se deben documentar los inconvenientes y resultados de cada migración.

Normas Dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION Y DIRECCION DE SISTEMAS

- Las transacciones de los sistemas de información adquiridos a terceros que generen errores deben ser identificadas, y la evidencia de dichos errores debe ser documentada, para ser enviada al proveedor del sistema de información o software.

- Así mismo, errores de software, omisiones y problemas de seguridad que son atribuibles a los sistemas de información desarrollados al interior de la **Universidad Libre** se deben retornar a los diseñadores y desarrolladores internos para que estas situaciones sean corregidas.

Normas Dirigidas a: ADMINSTRADORES DE LOS RECURSOS INFORMATICOS

- Se debe mantener la integridad y disponibilidad de las bases de datos y los sistemas operativos de los dispositivos que soportan a los sistemas de información de la universidad.

- Los utilitarios de los sistemas de información o las bases de datos no deben ser utilizados para pasar por alto la seguridad de los mismos.

- Los Administradores de los recursos informáticos deben documentar las metodologías utilizadas, los problemas presentados y los resultados obtenidos de cada migración de datos que lleven a cabo.

Documentos relacionados con ésta política

- Metodologías para la definición de requerimientos de software (tanto desarrollado por terceros como internamente)
- Metodologías para la realización de pruebas al software desarrollado
- Procedimiento de control de cambios
- Procedimiento de control de acceso lógico

13.3 Políticas para el manejo de información cifrada

La información de la **Universidad Libre** clasificada como sensitiva o restringida debe ser cifrada al momento de almacenarse y transmitirse.

Se debe seleccionar un tipo de herramienta de cifrado, que se va a utilizar para el envío y/o almacenamiento de información, evaluando las condiciones técnicas y de costos del software de cifrado.

Se debe capacitar a los funcionarios seleccionados en el manejo de la herramienta y los procedimientos para el envío o transmisión de la información.

Normas para el manejo de información cifrada

Normas Dirigidas a: DIRECCION DE SISTEMAS

- La información sensitiva de la **Universidad Libre** debe ser almacenada y/o transmitida bajo técnicas de cifrado con el propósito de salvaguardar su

confidencialidad y para proteger la integridad de los mensajes. Se debe identificar el nivel requerido de protección y, de acuerdo con ello, elegir el tipo de algoritmo de cifrado.

- Se espera que todo software, tanto construido por la universidad como por un tercero, que requiera transmisión electrónica de información sensible utilice un sistema de cifrado de datos.

- Deberá usarse un sistema de cifrado cuando un requisito legal así lo exija.

- Se debe prestar atención a los algoritmos utilizados por el software de cifrado ya que el uso de algunos de ellos es ilegal fuera del territorio norteamericano o europeo.

- Las llaves de cifrado nunca deben residir en memoria principal, buffers o registros en los sistemas de información donde funcionan para garantizar la seguridad de los procesos.

- Se deben utilizar controles criptográficos para
  - la protección de contraseñas de acceso a recursos informáticos y sistemas de información.
  - el almacenamiento y transmisión de información sensitiva en estaciones de trabajo y equipos portátiles catalogados como críticos.
  - información sensitiva que es trasladada en medios removibles

- Si se requiere el uso de firmas digitales, estas se deben implantar mediante el uso de una técnica criptográfica sobre la base de dos claves relacionadas (llave privada para crear la firma y llave pública para verificar la firma).

- Cuando la información deba ser protegida durante su transmisión, se deben considerar algoritmos de cifrado como MD5 o SHA1 para garantizar y firmar el mensaje de manera que su receptor pueda confirmar la autenticidad del mismo al comparar las firmas criptográficas.

- En caso de implantar firmas digitales, se debe desarrollar y establecer un procedimiento para el manejo y la administración de las llaves de cifrado, considerando aspectos como la solicitud, revocación y recuperación de la información cifrada así como el reemplazo de las llaves de cifrado.

- Así mismo, se deben definir roles y responsabilidades para el sistema de cifrado, considerando los siguientes:
  - Analista: encargado de medir el impacto de la utilización de controles criptográficos en la universidad y de los estándares (algoritmos) a ser utilizados en el proceso.

- Administrador del Sistema de cifrado: encargado de la creación, administración y revocación de llaves de cifrado.
- Implantador: encargado de la gestión de la política de cifrado y del software de apoyo

Documentos relacionados con ésta política

- Resultados de evaluación de herramienta de cifrado
- Manual de capacitación en el uso de la herramienta de cifrado
- Procedimiento para el manejo y la administración de las llaves de cifrado (condicional)

13.4 Políticas de seguridad en los sistemas de archivos

Se deben mantener ambientes separados de desarrollo, pruebas y producción con los controles de acceso establecidos para cada uno de dichos ambientes y una adecuada segregación de funciones para evitar accesos no autorizados a los ambientes productivos.

Así mismo, se debe asegurar la protección de los archivos de programas fuente de los sistemas de información o software tanto adquiridos como desarrollados al interior de la **Universidad Libre**.

Normas de seguridad en los sistemas de archivos

Normas Dirigidas a: DESARROLLADORES (GRUPO INTERNO Y TERCEROS PROVEEDORES DE SOFTWARE)

- Las actividades realizadas por usuarios con privilegios de administración en los sistemas de información o software desarrollados deben ser registradas.

Normas Dirigidas a: DIRECCION DE SISTEMAS Y ADMINISTRADORES DE LOS RECURSOS INFORMATICOS

- Los desarrolladores, tanto internos como los proveedores externos de sistemas de información y software, deben tener acceso limitado y controlado a los datos y programas que se encuentren en ambiente de producción.

- Los programas de código fuente de los sistemas de información y desarrollos de software de la **Universidad Libre** se deben encontrar en repositorios con acceso controlado y restricción de privilegios y, se deben registrar todos los accesos a dichos programas de código fuente.

- A los ambientes de producción de los sistemas de información, sólo se tendrá acceso de forma limitada, autorizada y controlada de acuerdo con los procedimientos establecidos.

- Los registros de auditoría de los sistemas de información no deben estar disponibles para personal no autorizado. Únicamente podrán acceder a éstos registros los funcionarios de Auditoría Interna y los Administradores de los recursos informáticos.

Documentos relacionados con ésta política

- Procedimiento de control de cambios
- Procedimiento de control de acceso lógico
- Procedimiento de administración de código fuente

13.5 Políticas de seguridad en los procesos de desarrollo y soporte

Se debe velar porque los sistemas de información adquiridos o desarrollados al interior de la **Universidad Libre** cumplan con el ciclo de vida de desarrollo y con los requerimientos de funcionalidad y seguridad esperados y se acojan a las metodologías para la definición de requerimientos de software y para la realización de pruebas al software desarrollado.

Todo sistema de información o software adquirido, desarrollado por terceros o al interior de la universidad debe contar con el nivel adecuado de soporte para garantizar que la corporación no se vea afectada. El soporte debe garantizar que cualquier problema que se presente en el sistema de información o software debe ser resuelto de la manera más eficaz y en un tiempo aceptable para la universidad.

Normas de seguridad en los procesos de desarrollo y soporte

Normas Dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION Y DIRECCION DE SISTEMAS

- Todos y cada uno de los sistemas de información o desarrollos de software de **la Universidad Libre** deben tener un área propietaria al interior de la universidad formalmente asignada y, dentro de dicha área debe haber un responsable y/o un custodio del sistema de información o software.

- Con el propósito de garantizar integridad y confidencialidad de la información, antes del paso a producción, los propietarios de los sistemas de información son responsables de efectuar las pruebas suficientes para asegurar que se han cumplido los requerimientos de funcionalidad y seguridad.

- Se deben utilizar las metodologías establecidas para la realización de pruebas al software desarrollado y dichas pruebas deberán contemplar aspectos funcionales, de seguridad y técnicos.

- Se debe efectuar el entrenamiento funcional y técnico necesario para cualquier nuevo sistema de información o software que vaya a ser implantado en la **Universidad Libre**.

- Se debe ejercer supervisión y control en todo proceso de compra, desarrollo y mantenimiento de sistemas de información o software.

Normas Dirigidas a: DESARROLLADORES (GRUPO INTERNO Y TERCEROS PROVEEDORES DE SOFTWARE)

- Para todos los sistemas de información o software a desarrollar, los diseñadores y desarrolladores deben considerar la seguridad durante el ciclo de vida de los mismos, desde el diseño del software hasta su puesta en producción.

- Cada desarrollo o sistema de información debe generar alertas de seguridad mediante las cuales pueda llamar la atención del administrador hacia un posible problema de seguridad de la información.

- Los mecanismos de seguridad definidos para cada sistema de información de la universidad no deben ser alterados, pasados por alto o comprometidos. Así mismo, dichos controles de seguridad deben ser documentados y deben permitir probar su efectividad.

- Todos los cambios a programas deben realizarse en el ambiente de desarrollo.

- Se debe generar la documentación mínima requerida por cada uno de los sistemas de información o software desarrollados (manual técnico, manual de operación y manual de usuario) como requisito para la entrada en producción de éstos.

- De la misma manera, todas las actualizaciones y/o cambios en los sistemas de información o software desarrollados deben estar documentados.

- Los sistemas de información y software adquiridos o desarrollados por terceros o al interior de la universidad deben suministrar el nivel adecuado de soporte para garantizar la resolución de problemas que se presenten en el

software de la manera más eficaz y dentro de unos rangos de tiempo aceptables para la corporación.

Normas Dirigidas a: DIRECCION DE SISTEMAS Y ADMINISTRADORES DE LOS RECURSOS INFORMATICOS Y LOS SISTEMAS DE INFORMACION

- Cualquier software adquirido o desarrollado para la **Universidad Libre** no debe usar funciones privilegiadas del sistema operativo.

- Los sistemas de información adquiridos a terceras partes deben estar a cargo de un responsable de la **Universidad Libre** quien deberá ser capacitado para dar un primer nivel de soporte técnico.

- Los ambientes de desarrollo, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad.

- Deben existir controles para asegurar que todos los movimientos entre los ambientes de desarrollo, pruebas y producción han sido autorizados de acuerdo con el procedimiento de control de cambios.

- Se debe contar con la documentación actualizada de todos los sistemas de información y desarrollos de software y ésta debe estar disponible para cuando se requiera. Las copias impresas o en medios magnéticos de dicha documentación deben ser almacenadas en lugares seguros.

- Los nuevos desarrollos y/o modificaciones realizadas a los sistemas de información o software no deberán trasladarse al ambiente de producción, si no se cuenta con la aprobación del propietario y con la documentación de operación actualizada.

- Se deben efectuar las actualizaciones de parches para el software de base (sistemas operativos y bases de datos) donde residen los sistemas de información, previo estudio del impacto de los mismos, en ambientes de pruebas.

- Se debe contar con un sistema de control de versiones el cual debe ser utilizado para administrar las modificaciones, cambios y documentación de los sistemas de información y desarrollos de software de la universidad.

- Se debe garantizar que exista una clara segregación de funciones referente a la administración, operación y desarrollo de sistemas de información o software de la **Universidad Libre**.

- Todo nuevo sistema de información o desarrollo de software, tanto adquirido

como desarrollado por terceros o al interior de la universidad que vaya a entrar en producción deberá someterse a las debidas pruebas de carga de datos y pruebas de capacidad.

- Los sistemas de información adquiridos o desarrollados por terceros deben poseer un acuerdo de licenciamiento el cual debe especificar las condiciones de utilización del software y los derechos de propiedad que deben ser tenidos en cuenta.

- Se deben generar metodologías para la realización de pruebas al software desarrollado, las cuales deben contener las pautas para la selección de escenarios, niveles, tipos y datos de pruebas y las sugerencias de documentación de las mismas.

Normas dirigidas a: AUDITORÍA INTERNA

- Auditoría Interna debe verificar que las pruebas de funcionalidad y seguridad sobre los sistemas de información se realicen acorde con las metodologías definidas, contando con casos de prueba debidamente documentados.

Documentos relacionados con ésta política

- Metodologías para la definición de requerimientos de software (tanto desarrollado por terceros como internamente)
- Metodologías para la realización de pruebas al software desarrollado
- Procedimiento de control de cambios
- Procedimiento de control de acceso lógico
- Acuerdos de Niveles de Servicio establecidos con terceras partes

13.6 Políticas para la administración de vulnerabilidades

Los funcionarios de la Dirección de Sistemas de la **Universidad Libre** deben revisar de manera periódica la aparición de vulnerabilidades técnicas y reportarlo tanto a los administradores de los recursos informáticos como a los desarrolladores internos y externos de software.

De igual manera, se deben realizar pruebas de vulnerabilidades con una periodicidad establecida y aplicar los correctivos necesarios de acuerdo con los resultados arrojados por las pruebas.

Normas para la administración de vulnerabilidades

Normas Dirigidas a: DIRECCION DE SISTEMAS Y ADMINISTRADORES DE LOS RECURSOS INFORMATICOS

- Los servidores, dispositivos de comunicación y seguridad, las estaciones de trabajo, equipos portátiles y las bases de datos de la **Universidad Libre** deben ser configurados de manera segura.

- Se deben realizar pruebas de vulnerabilidades, escaneo de sistemas de información y hacking ético con una periodicidad anual.

- Se debe indagar permanentemente por la aparición de nuevas vulnerabilidades y notificar a los administradores de los recursos informáticas para prevenir la exposición al riesgo de los recursos informáticos de la **Universidad Libre** o para la remedición de dichos riesgos.

- De ser posible, se debe adquirir un software de gestión de vulnerabilidades que permita la recolección, comparación y notificación de éstas. Se deberá asignar un responsable para su operación y administración.

Documentos relacionados con ésta política

- Resultados de las pruebas de vulnerabilidades
- Estándar de seguridad para servidores Windows
- Estándar de seguridad para servidores Solaris
- Estándar de seguridad para routers
- Estándar de seguridad para switches
- Estándar de seguridad para bases de datos Oracle

14. Políticas de gestión de incidentes de seguridad

14.1 Políticas para el reporte de incidentes de seguridad

Es un deber de la **Universidad Libre** promover entre la comunidad usuaria de recursos informáticos y sistemas de información el reporte de los incidentes relacionados con la información y sus medios de procesamiento.

Todos los funcionarios de la universidad están en la obligación de informar acerca de cualquier violación o problema de seguridad de la información encontrado.

Normas para el reporte de incidentes de seguridad

Normas Dirigidas a: TODOS LOS USUARIOS

- Es responsabilidad de todos los funcionarios de la **Universidad Libre** y funcionarios provistos por terceras partes reportar cualquier tipo de incidente

relacionado con la información y/o los recursos informáticos a la mayor brevedad posible.

- ❖ En caso de conocer la pérdida o divulgación no autorizada de información sensible, se debe notificar al propietario de la misma así como a la Dirección de Sistemas.

- ❖ Cualquier intento de interferencia, obstrucción o de disuadir a quien reporta una posible violación de seguridad está terminantemente prohibido y será motivo de una acción disciplinaria. De igual manera cualquier retaliación o amenaza contra la persona que realiza la investigación o un proceso de investigación.

Normas Dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

- ❖ Los propietarios de los activos de información deben informar los incidentes de seguridad que les hayan sido reportados.

- ❖ Toda falla aparente de cualquier sistema de información o software debe ser reportada a la mayor brevedad al proveedor del software en caso de tratarse de un sistema de información adquirido o a los desarrolladores en caso de tratarse de un desarrollo interno.

Normas Dirigidas a: COMITÉ DE SISTEMAS, DIRECCION DE SISTEMAS Y AUDITORIA INTERNA

- ❖ Los incidentes de seguridad de la información que estén relacionados con requerimientos legales o regulatorios deberán ser reportados a autoridades externas por personal autorizado de la **Universidad Libre**.

- ❖ El uso de los recursos informáticos debe ser monitoreado regularmente, al igual que cada sistema de información debe ser auditado.

Documentos relacionados con ésta política

- ❖ Procedimiento de gestión de incidentes de seguridad

14.2 Políticas para el tratamiento y administración de incidentes de seguridad

Se deben asignar responsables para el tratamiento de los incidentes de seguridad en la **Universidad Libre**, quienes tienen la responsabilidad de investigar y solucionar de la manera más expedita y efectiva aquellos incidentes reportados, tomando las medidas necesarias para prevenir su re-ocurrencia e informando a sus niveles superiores de acuerdo con la criticidad de los incidentes.

Normas para el tratamiento y administración de incidentes de seguridad

Normas Dirigidas a: PRESIDENCIA SECCIONAL, DIRECCION DE SISTEMAS, SEGURIDAD Y AUDITORIA INTERNA

- Después de recibir la notificación de un incidente de seguridad o vulnerabilidad de la información, quien reciba la notificación es responsable de asegurar que el propietario del activo de información y todas las personas involucradas con el incidente, estén informadas.

- Todos los incidentes de seguridad deben ser evaluados de acuerdo con su circunstancia particular; esto puede requerir o no la acción de varias áreas de la **Universidad Libre**. Cuando sea necesario se deben aplicar sanciones disciplinarias a partir de la falta cometida.

- Los incidentes de Seguridad de la información deben ser apropiadamente investigados por personal calificado. Es necesario identificar las causas y planear como prevenir su re-ocurrencia. La evidencia debe ser apropiadamente recolectada.

- Deben ser creadas unas bases de datos de incidentes con sus respectivas soluciones para que permitan reducir el tiempo de respuesta en caso de ocurrencia de nuevos incidentes.

Documentos relacionados con ésta política

- Procedimiento de gestión de incidentes de seguridad

15. Políticas de los planes de contingencia

15.1 Políticas de contingencia y recuperación de la normalidad

La **Universidad Libre** debe responder de manera efectiva ante los eventos catastróficos que se presenten según la magnitud y grado de afectación de los mismos sobre la corporación. Se deben restablecer las operaciones con el menor costo y pérdidas posibles y mantener canales de comunicación adecuados hacia funcionarios, estudiantes, proveedores, y otras terceras partes interesadas.

Normas de contingencia, administración de la crisis y recuperación de la normalidad

Normas Dirigidas a: COMITE DE SISTEMAS, UNIDADES ACADEMICAS Y ADMINISTRATIVAS Y DIRECCION DE SISTEMAS

- Se debe identificar los procesos críticos de negocio y determinar la dependencia e importancia que supone para la **Universidad Libre** en términos de disponibilidad.

- Las Unidades Académicas y Administrativas deben identificar procedimientos de contingencia que podrían ser utilizados en caso de un evento adverso y de la falta de disponibilidad de la plataforma tecnológica. Así mismo, estos procedimientos deben ser documentados y probados para garantizar su efectividad.

- Se deben designar responsables, asignarles responsabilidades y capacitarlos en las actividades a realizar y los procedimientos a seguir en caso de un evento catastrófico para la universidad.

- Se debe procurar minimizar los efectos adversos que pueda tener la ocurrencia de un evento catastrófico sobre la normalidad en la ejecución de las operaciones de la **Universidad Libre**, así como facilitar la recuperación del desastre.

- Se deben definir las estrategias de recuperación y procurar los mecanismos necesarios que garanticen una rápida respuesta, y reanudación de actividades frente a una situación crítica que impida la operación normal de la universidad.

- Utilizando los conductos establecidos, se debe mantener informados a funcionarios, estudiantes, proveedores y otras terceras partes de la situación y las expectativas de recuperación de la operación normal de la universidad.

Normas Dirigidas a: DIRECCION DE SISTEMAS Y ADMINISTRADORES DE LOS RECURSOS INFORMATICOS Y LOS SISTEMAS DE INFORMACION

- Los Centros de Cómputos deben contar con un Plan de recuperación ante desastres y un conjunto de procedimientos de contingencia para cada uno de los servicios y sistemas prestados.

- Los recursos informáticos deben contar con procedimientos de generación de copias de respaldo y recuperación que deben estar almacenados tanto internamente como en un centro externo de almacenamiento.

- Se deben realizar pruebas periódicas del Plan de recuperación ante desastres y documentar los resultados de dichas pruebas.

Documentos relacionados con ésta política

- Plan de Contingencia
- Procedimientos operativos para cada uno de los recursos informáticos y sistemas de información administrados (por ejemplo, soporte, mantenimiento, administración, operación y procesos especiales de cada uno de los recursos informáticos y sistemas de información)
- Procedimientos de contingencia y recuperación

16. Políticas de cumplimiento

16.1 Políticas de cumplimiento de requerimientos de licenciamiento y propiedad intelectual

La **Universidad Libre** debe velar porque el software instalado en los recursos informáticos cumpla con todos los requerimientos legales y de licenciamiento necesarios.

De igual manera, los funcionarios de la corporación tienen la obligación de respetar la legislación de la propiedad intelectual y los derechos de autor concernientes a los productos de software instalados en sus estaciones de trabajo o equipos portátiles.

Todo proceso de adquisición de software debe ser analizado y aprobado por el área responsable de la información y debidamente informado a la Dirección de Sistemas.

Normas de cumplimiento de requerimientos de licenciamiento y propiedad intelectual

Normas Dirigidas a TODOS LOS USUARIOS

- La modificación de los parámetros de configuración establecidos en las estaciones de trabajo o equipos portátiles, solo serán realizados por personal autorizado por la Dirección de Sistemas.

- La **Universidad Libre** debe tener establecida una lista estándar de software y sistemas de información permitidos en las estaciones de trabajo o equipos portátiles, para el desarrollo de las actividades laborales. Por lo tanto, los usuarios no deben instalar software o sistemas de información adicionales sin la previa autorización de la Dirección de Sistemas por medio de la asistencia del Soporte Técnico.

- Tanto los funcionarios de la universidad como los funcionarios provistos por terceras partes deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar o distribuir software o su documentación sin permiso del propietario de los derechos de autor y, su reproducción no autorizada es una violación de la ley. Sólo puede distribuirse el número especificado de copias bajo la licencia otorgada.

- Los funcionarios de **la Universidad Libre** y funcionarios provistos por terceros que hagan uso de la red de datos de la corporación deben cumplir con todos los términos y condiciones establecidos para obtener software e información de redes públicas.

Normas Dirigidas a: DIRECCION DE SISTEMAS Y ADMINISTRADORES DE LOS RECURSOS INFORMATICOS Y LOS SISTEMAS DE INFORMACION

- La Dirección de Sistemas es responsable de verificar que solo se instalen productos con licencia y software autorizado en los recursos informáticos. Además, es su deber establecer un procedimiento para el control de licencias.

- Es responsabilidad de la Dirección de Sistemas, mantener actualizados el sistema operativo y el software instalado en las estaciones de trabajo y equipos portátiles propiedad de la **Universidad Libre**, con el fin de prevenir problemas de seguridad relacionados con los mismos y que pongan en riesgo la información manejada en la estación de trabajo o el equipo portátil.

- Todo el software que se ejecute en la **Universidad Libre** debe estar protegido por derechos de autor y requerir licencia de uso.

Normas Dirigidas a: DIRECCION DE SISTEMAS, JEFES DE UNIDADES ACADEMICAS Y ADMINISTRADORES DE LOS RECURSOS INFORMATICOS Y LOS SISTEMAS DE INFORMACION

- Se deben implantar controles periódicos para evitar el uso de software sin licencia en la universidad.

Normas Dirigidas a: DIRECCIÓN JURÍDICA

- La Dirección Jurídica tiene la responsabilidad de identificar la legislación vigente que debe cumplir la **Universidad Libre** en función de la protección de la información y divulgar estos requerimientos tanto a los Jefes de Unidades Académicas y Administrativas como a la Dirección de Sistemas.

- De igual forma, debe servir de apoyo a las Unidades Académicas y Administrativas en la interpretación y manejo de dicha legislación.

Documentos relacionados con ésta política

- ❖ Procedimiento de verificación de uso de licencias de software.

16.2 Políticas de privacidad de la información

Toda la información que la **Universidad Libre** conozca y almacene de sus funcionarios, estudiantes, proveedores y entidades de control deberá ser utilizada para las funciones propias del negocio y no podrá ser publicada, revelada o entregada a funcionarios o a terceras partes sin autorización.

Normas de privacidad de la información

Norma Dirigida a: TODOS LOS USUARIOS

- ❖ Los funcionarios de la **Universidad Libre** deben observar fidelidad como producto de las tareas que les fueron asignadas y guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la corporación de la cual tengan conocimiento en el ejercicio de sus funciones.

- ❖ Los funcionarios tienen prohibido publicar potenciales difamaciones del personal, de la corporación, de los estudiantes y de la competencia.

- ❖ Es deber de los funcionarios de la **Universidad Libre** verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.

Documentos relacionados con ésta política

- ❖ Procedimientos para el acceso y divulgación, almacenamiento, generación de copias, transmisión, etiquetado y destrucción de la información por cada uno de los niveles de clasificación.
- ❖ Acuerdos de Confidencialidad

ORGANIZACION DE LA SEGURIDAD DE LA INFORMACION

ÍNDICE

17. Objetivo

La definición de la Organización de la Seguridad de la **Universidad Libre** se realiza con los propósitos de:

- ❖ Establecer los roles y responsabilidades relacionados con la seguridad de la información.

- ❖ Garantizar una adecuada segregación de funciones para la realización de las actividades de administración, operación y gestión de la información.

18. Definición de Roles y Responsabilidades

Esta definición de roles y responsabilidades está dirigida a todos los funcionarios relacionados con la Seguridad de la Información de la **Universidad Libre.**

18.1 Comité de Sistemas

Es responsable de:

- ❖ Aprobar y revisar periódicamente las políticas y normas de seguridad de la información definidas para los funcionarios administrativos y docentes, estudiantes y personal provisto por terceras partes que interactúen con los recursos informáticos de la **Universidad Libre** o que tengan acceso a su información.

- ❖ Propender por el cumplimiento de las políticas, normas y procedimientos de seguridad de la información.

- ❖ Establecer sanciones por el incumplimiento de las políticas, normas y procedimientos de seguridad de la información.

- ❖ Establecer los objetivos y estrategias de la seguridad de la información para la **Universidad Libre**.

- ❖ Avalar las asignaciones de los propietarios, responsables y custodios de los activos de información.

- ❖ Aprobar los Niveles de Aceptación del Riesgo para la gestión de los riesgos de seguridad de la información de la universidad y revisarlos de manera periódica.

- ❖ Aprobar las Guías de Clasificación de la Información.

- Revisar los resultados de las auditorías internas al Modelo de Seguridad de la Información.

- Contribuir en la coordinación del manejo de los incidentes de seguridad de la información y la asignación de las áreas participantes.

- Aprobar los procedimientos para el manejo de los incidentes de seguridad de la información.

- Evaluar el tipo de incidente para determinar el personal apropiado que se requiere para la respuesta.

- Realizar seguimiento de los incidentes de seguridad de la información en curso.

- Servir de interlocutor válido en caso que algún incidente haya tenido repercusiones públicas.

- Involucrar a las áreas que sean requeridas para prestar su asistencia en caso de ser necesario, como es el caso de Secretaría General, Dirección de Personal, Dirección Jurídica, Auditoría Interna, Seguridad y Servicios Generales.

- Contactar a los Presidentes y Rectores de las seccionales en caso de ser necesario.

- Validar que las áreas involucradas en el modelo de seguridad de la **Universidad Libre** cumplan a cabalidad con las responsabilidades asignadas para garantizar la seguridad de la información de la corporación.

- Validar los planes a ser ejecutados para el cumplimiento del Modelo de Seguridad de la Información en la universidad, cuando las tareas sean de alto impacto para la corporación.

18.2 Dirección de Sistemas (reuniendo sus funciones y las funciones del Oficial de Seguridad de la Información)

Es responsable de:

- Conocer y soportar las iniciativas de seguridad de la información que involucren a toda la universidad.

- Liderar la definición y mantenimiento de un Modelo de Seguridad de la información que refleje la necesidad real de la **Universidad Libre** en temas de seguridad de la información.

- Liderar la definición, actualización e implantación de las políticas, normas, procedimientos y estándares de seguridad de la información para toda la universidad, y someterlas a la aprobación del Comité de Sistemas.

- Asegurarse que las políticas, normas, estándares y procedimientos propuestos sean compatibles con las necesidades de tecnología de la universidad.

- Garantizar que la seguridad de la información sea parte del proceso de planeación en la adquisición de bienes y servicios.

- Generar un modelo de Acuerdos de Niveles de servicio para la **Universidad Libre** y divulgarlo a todas las Unidades Académicas y Administrativas que adquieran recursos tecnológicos o de software.

- Propender porque en los Acuerdos de Niveles de Servicio pactados con cada proveedor de servicios, se contemplen los requerimientos de seguridad de la información.

- Emitir concepto sobre la adquisición y/o arriendo de recursos informáticos o sistemas de información.

- Apoyar al Comité de Sistemas en los procesos de identificación de las necesidades tecnológicas y de seguridad de la información requeridas por la universidad.

- Participar en los procesos de implantación de nuevas soluciones de negocio que requieran el componente de seguridad de la información.

- Propender el acatamiento de los requerimientos de la **Universidad Libre** para proteger la información estableciendo controles en la plataforma tecnológica que permitan cumplir con las políticas, normas, procedimientos y estándares de seguridad de la información.

- Coordinar la implantación de las políticas, normas, procedimientos y estándares de seguridad de la información.

- Divulgar las políticas, normas, procedimientos y estándares a todos los funcionarios de la universidad y funcionarios provistos por terceras partes.

- Investigar sobre nuevas tecnologías y reportar periódicamente al Comité de Sistemas el estado de la seguridad en la universidad y la necesidad de nuevos proyectos.

- Generar las Guías para la Gestión de riesgos de Seguridad de la Información y someter los niveles de aceptación de riesgo a la aprobación del Comité de Sistemas.

- Realizar y/o actualizar periódicamente el Mapa de Riesgos de seguridad de los activos de información de la **Universidad Libre**, teniendo en cuenta tanto los activos de información existentes como aquellos asociados a los nuevos proyectos que se emprendan.

- Tomar medidas para minimizar el riesgo por la pérdida o exposición de la información o los recursos informáticos bajo su responsabilidad.

- Reportar los incidentes relacionados con seguridad de la información al Comité de Sistemas, cuando sea necesario.

- Generar las directrices para reglamentar los lugares de ubicación, los controles de acceso físico y las condiciones ambientales requeridas para equipos de cómputo y utilidades de soporte del Centro de Computo así como de los Centros de Cableado.

- Gestionar las utilidades de soporte de los Centros de Cómputo y los Centros de Cableado.

- Coordinar los mantenimientos de los equipos de cómputo y las utilidades de soporte, como UPS y aires acondicionados con los proveedores.

- Generar las directrices para la aplicación de parches y actualizaciones en los equipos de cómputo administrados.

- Hacer el alistamiento de las estaciones de trabajo y equipos portátiles entregados a los funcionarios de la universidad y administrar el inventario del software instalado en el proceso de alistamiento.

- Generar las Guías para la Clasificación de la información según su importancia e impacto dentro de la universidad y, divulgarlas a todas las Unidades Académicas y Administrativas.

- Participar en cada una de las fases del ciclo de vida del desarrollo de sistemas de información y sugerir la incorporación de las medidas de seguridad requeridas.

- Realizar pruebas de vulnerabilidad para verificar la seguridad de los recursos informáticos y sistemas de información de la **Universidad Libre**.

- Identificar y satisfacer las necesidades de capacitación en temas de seguridad de la información para la Dirección de Sistemas.

- Crear y mantener un Programa de Concientización en Seguridad de la Información que involucre tanto a los funcionarios como a los terceros relacionados con la información de la **Universidad Libre**.

- Realizar campañas de entrenamiento y concientización para que, tanto los funcionarios de la corporación como los funcionarios provistos por terceras partes, conozcan los riesgos a los que está expuesta la universidad y su información.

- Desarrollar e implantar los procedimientos para el manejo de los incidentes de seguridad informática.

- Preparar indicadores de medición de la efectividad de la seguridad de la información en la universidad.

- Reportar e informar sobre el resultado del análisis de los incidentes de seguridad informática a las áreas usuarias involucradas.

- Contactar a los Directores de Sistemas de las seccionales en caso de ser necesario.

18.3 Auditoría Interna

Es responsable de:

- Verificar la efectividad de los mecanismos de control implantados para la mitigación de los riesgos identificados para los recursos informáticos.

- Presentar informes de auditoría al Comité de Sistemas en aras de que se tomen las medidas necesarias sobre las deficiencias que se hayan observado durante la realización de auditorías informáticas.

- Recomendar al Comité de Sistemas sobre posibles actualizaciones de políticas, normas, procedimientos y estándares de seguridad de la información, o la necesidad de emisión de nuevas políticas y normas.

- Participar en el análisis, investigación y evaluación de los incidentes de seguridad reportados.

- Verificar periódicamente que la Organización de la Seguridad de la Información definida en el Modelo de Seguridad de la Información realice las actividades de seguridad que les corresponden.

- Participar en la definición y mantenimiento del Modelo de Seguridad de la Información de la **Universidad Libre**.

- Formular y ejecutar el plan periódico de auditorías informáticas.

- Monitorear y evaluar el cumplimiento de las políticas, normas, procedimientos y estándares de seguridad de la información y recomendar los ajustes requeridos en función de proteger los intereses de la universidad.

- Inspeccionar la operación de los recursos informáticos y sistemas de información en producción.

- Verificar que las pruebas de funcionalidad y seguridad sobre los sistemas de información se realicen acorde con las metodologías definidas, contando con casos de prueba documentados.

- Monitorear y validar los controles efectuados sobre la calidad de los datos ingresados y generados por los sistemas de información.

- Participar en las revisiones periódicas del Mapa de Riesgos de seguridad de los activos de información de la **Universidad Libre**.

- Detectar fraudes, uso inadecuado o ineficiente de los recursos informáticos o sistemas de información de la **Universidad Libre**.

- Verificar periódicamente que los usuarios privilegiados definidos dentro de los recursos informáticos y sistemas de información sean autorizados por la Dirección de Sistemas.

- Generar y hacer seguimiento a los planes de acción a ser ejecutados para el tratamiento de los riesgos de seguridad de los activos de información y todos los que se generen a partir de la implantación del modelo de seguridad de la información en la Universidad Libre.

18.4 Propietarios de los activos de información

Son responsables de:

- Velar por la información que genera o administra su área, la cual deber ser clasificada de acuerdo con las Guías de Clasificación de la Información.

- Definir los perfiles y los niveles de acceso que se otorgarán a los usuarios sobre sus activos de información, demostrando una adecuada segregación de funciones.

- Solicitar a los Administradores de los recursos informáticos y los sistemas de información que se establezcan los controles requeridos y se administren los perfiles definidos en dichos recursos informáticos y sistemas de información.

- Garantizar la aplicación y efectividad de los controles definidos para los activos de información de su propiedad de manera periódica.

- Autorizar la creación, modificación y eliminación de perfiles o cuentas de usuario en sus recursos informáticos o sistemas de información.

- Revisar periódicamente los niveles de acceso otorgados sobre sus activos de información.

- Solicitar los requerimientos de nuevas funcionalidades, servicios o modificaciones sobre sus recursos informáticos o sistemas de información, acogiéndose a las metodologías establecidas para éste propósito.

- Realizar pruebas de funcionalidad y documentar cada uno de sus casos de prueba sobre sus recursos informáticos o sistemas de información, acogiéndose a las metodologías establecidas para tal fin.

- Revisar de manera periódica la calidad de los datos ingresados y generados por los recursos informáticos y sistemas de información de su propiedad.

- Reportar los errores o las fallas de procesamiento en sus activos de información a las áreas encargadas dentro de la universidad o a los proveedores del servicio.

- Reportar a las áreas que pudieran tener responsabilidad en el manejo de incidentes como es el caso de la Dirección de Sistemas, Seguridad, Censoría y, cuando sea pertinente, al Comité de Sistemas los incidentes ocurridos con el manejo de la información que tienen bajo su responsabilidad, con el fin que se realicen las investigaciones necesarias.

- Solicitar concepto o informar a la Dirección de Sistemas de la adquisición o mantenimiento de sistemas de información o software.

18.5 Administradores de los recursos informáticos y los sistemas de información

Son responsables de:

- Participar en el análisis y evaluación de los aspectos de seguridad de cualquier nuevo recurso informático, sistema de información o software de la **Universidad Libre**, previo a la instalación del mismo.

- Implantar en los recursos informáticos, sistemas de información, software y herramientas de administración los controles, estándares y configuraciones recomendadas, acogiéndose a las políticas, normas, procedimientos y estándares de seguridad de la información.

- Documentar y mantener actualizados todos los procedimientos de operación y administración de los recursos informáticos, servicios o sistemas de información a su cargo.

- Reportar a la Dirección de Sistemas de la corporación la ocurrencia de situaciones que requieran cambios en la configuración de parámetros de seguridad de los recursos informáticos, servicios o sistemas de información a su cargo.

- Administrar los perfiles y cuentas de usuario definidos por los propietarios de los recursos informáticos, servicios o sistema de información.

- Efectuar proyecciones de crecimiento sobre los recursos informáticos administrados.

- Configurar las pistas de auditoría para el registro de los eventos requeridos, considerando evaluaciones de impacto en el desempeño de los recursos informáticos o sistemas de información administrados.

- Monitorear cada uno de los recursos informáticos y sistemas de información administrados, reportando los incidentes relacionados con seguridad de la información, a la Dirección de Sistemas o, cuando fuera necesario, al Comité de Sistemas.

- Asegurar el cumplimiento de todos los procedimientos de respaldo y recuperación de la información sobre los activos de información administrados.

- Asegurar el respaldo de los archivos de registro de auditoría (*logs o audit trails*) de acuerdo con los requerimientos de Auditoría Interna.

18.6 Desarrolladores (terceros proveedores de software)

Son responsables de:

- Diseñar, desarrollar e incorporar en los sistemas de información y software desarrollado para la **Universidad Libre** todos los controles adicionales definidos, producto de los requerimientos de seguridad de la información.

- Proponer y presentar la arquitectura de seguridad de los sistemas de información y software desarrollado tanto a los Propietarios de dichos sistemas de información como a la Dirección de Sistemas.

- Acogerse a las metodologías de definición de requerimientos de nuevas funcionalidades, servicios o modificaciones a los sistemas de información o al software desarrollados.

- Implantar controles que permitan la recuperación de la información y la continuidad de las funciones de los sistemas de información y software que diseñen y desarrollen.

- Generar la documentación para la instalación, administración y operación de los sistemas de información o software desarrollados para la corporación.

18.7 Jefes de Unidades Académicas y Administrativas

- Realizar un análisis de riesgos antes de conceder acceso a terceras partes a la información o los recursos de procesamiento de la misma en sus áreas y establecer una periodicidad para su realización.

- Recibir los recursos informáticos asignados a sus funcionarios cuando éstos se retiran de la universidad o son trasladados entre áreas, sedes o seccionales.

- Solicitar el borrado de información de las estaciones de trabajo de funcionarios retirados o trasladados entre áreas, sedes o seccionales a la Dirección de Sistemas.

- Solicitar a la Dirección de Sistemas y a los Administradores de los sistemas de información la creación de usuarios y la activación de cuentas, para sus funcionarios y los provistos por terceras partes, en la red y los sistemas de información de acuerdo con los perfiles requeridos, adjuntando los soportes necesarios.

- Establecer los acuerdos de cumplimiento de las Políticas de Seguridad de la Información con todos los funcionarios provistos por terceras partes que realizan labores para sus áreas y administrar dichos acuerdos como parte de los contratos efectuados con los terceros.

- Informar a la Dirección de Sistemas del retiro o cambio de labores de funcionarios suministrados por terceros para la remoción o reasignación de derechos de acceso sobre los recursos informáticos y sistemas de información.

- Informar a Seguridad del retiro de funcionarios provistos por terceras partes para prevenir accesos no autorizados a las instalaciones de la corporación.

- Fortalecer la seguridad física de sus oficinas, por medio de la instalación de sistemas de control de acceso físico y sistemas de monitoreo, cuando sea necesario.

- Identificar las estaciones de trabajo críticas de sus áreas e informarlo a la Dirección de Sistemas.

- Establecer Acuerdos con Intercambio con terceras partes con las cuales se requiere intercambio de información de la **Universidad Libre**.

- Dar cumplimiento a las actividades de los planes de acción generados a partir de la implantación del Modelo de Seguridad de la Información.

18.8 Dirección Jurídica

Es responsable de:

- Identificar e informar la normatividad y legislación vigente que debe cumplir la **Universidad Libre** en función de la protección de la información, como es el caso del uso de mensajes de datos, firmas digitales y delitos informáticos, entre otros y verificar el cumplimiento de dichas regulaciones.

- Servir de apoyo a las Unidades Académicas y Administrativas en el análisis y la interpretación de la normatividad y legislación aplicables a la corporación.

- Revisar la validez de las condiciones establecidas en los contratos suscritos con terceras partes proveedoras de servicios, los Acuerdos de Niveles de Servicio y los requisitos de seguridad a los que los terceros deben acogerse, como es el caso de la constitución de pólizas y el establecimiento de acuerdos de confidencialidad, por mencionar algunos.

- Generar modelos de Acuerdos de Confidencialidad para terceros que prestan servicios a la universidad y divulgarlos a todas las Unidades Académicas y Administrativas, teniendo en cuenta los diferentes esquemas de contratación como son contratos y órdenes de compra.

- Establecer los acuerdos de Confidencialidad con todos los funcionarios provistos por terceras partes que realizan labores para las Unidades Académicas y Administrativas.

- Establecer los requerimientos legales para el intercambio de información con terceras partes que prestan servicios a la universidad.

- Generar modelos de Acuerdos de Intercambio de información y divulgarlos a todas las Unidades Académicas y Administrativas.

- Establecer los Acuerdos de Intercambio de información con todas las terceras partes que requieren información o realizan labores para la Universidad Libre.

18.9 Dirección de Personal

Es responsable de:

- Revisar y actualizar los manuales de funciones de los cargos de la universidad y entregar copia de ellos a los funcionarios en el momento del ingreso o cambio de cargo.

- Asegurar que todos los funcionarios de la **Universidad Libre** conozcan sus responsabilidades legales con respecto al uso de los recursos informáticos, sistemas de información y cualquier otra forma de almacenamiento o procesamiento de la información de la universidad.

- Generar un modelo de Acuerdo de Confidencialidad y divulgarlo a todos los funcionarios de la corporación.

- Velar por la aceptación de los acuerdos de Confidencialidad y de cumplimiento de la Políticas de Seguridad de la Información por parte de todos los funcionarios de la **Universidad Libre** y administrar dichos acuerdos como parte de las hojas de vida de éstos funcionarios.

- Proveer la logística y facilitar los recursos necesarios para la realización de la campaña de concientización y los cursos de entrenamiento en temas de seguridad de la información.

- Convocar a los funcionarios a las charlas y eventos del programa de concientización en seguridad de la información, controlar la asistencia a dichas charlas y eventos y aplicar las sanciones pertinentes por la falta de asistencia no justificada.

- Informar a la Dirección de Sistemas y a los Administradores de los sistemas de información del retiro o cambio de labores de funcionarios de la universidad

para la remoción o reasignación de derechos de acceso sobre los recursos informáticos y sistemas de información.

- Informar a Seguridad del retiro de funcionarios de la universidad para prevenir accesos no autorizados a las instalaciones de la corporación.

18.10 Secretaría General

Es responsable de:

- Generar y establecer las directrices de archivística para la **Universidad Libre** y divulgarlas a todas las Unidades Académicas y Administrativas.

- Evaluar la capacidad de almacenamiento documental de la universidad y proveer los recursos y condiciones físicas y ambientales adecuadas de almacenamiento de documentos y/o medios de almacenamiento a todas las Unidades Académicas y Administrativas.

- Velar porque la destrucción de la documentación física de la universidad se efectué acogiéndose a las tablas de retención definidas y al procedimiento establecido para tal fin.

18.11 Seguridad

Es responsable de:

- Controlar el ingreso y salida de recursos informáticos de las instalaciones de la **Universidad Libre**.

- Brindar asesoría y apoyo a las Unidades Académicas y Administrativas para la instalación de cámaras, sistemas de alarmas u otros sistemas de monitoreo.

- Revisar de manera periódica y continua los sistemas de monitoreo implantados en las oficinas de la corporación y administrar los registros generados por dichos sistemas.

- Controlar el ingreso y salida de los funcionarios y estudiantes de la universidad en todas las entradas de la universidad.

- Velar porque todos los visitantes de la **Universidad Libre** sean debidamente registrados y asignar la identificación que los acredita.

- Revisar los maletines, bolsos o carteras, tanto cuando se ingresa como cuando se dejan las instalaciones de la universidad.

- ❖ Desarrollar e implantar los procedimientos para el manejo de los incidentes de seguridad física.

- ❖ Participar en el análisis, investigación y evaluación de los incidentes de seguridad reportados cuando sea requerido.

- ❖ Generar estudios referentes a los lugares susceptibles a terrorismo y/o asonada en la universidad y llevar a cabo la divulgación de las acciones a tomar ante eventos de éstas características.

- ❖ Facilitar el transporte y las condiciones adecuadas para el traslado de recursos informáticos, documentos y medios de almacenamiento entre sedes acogiéndose al procedimiento para el traslado de información física.

18.12 Servicios Generales

Es responsable de:

- ❖ Mantener un inventario actualizado de los recursos informáticos que son propiedad de la **Universidad Libre** y verificar periódicamente dicho inventario.

- ❖ Generar los procedimientos para el traslado de los medios de almacenamiento y documentos de la corporación.

- ❖ Implantar mecanismos de control para la protección de la información enviada entre áreas de la universidad utilizando la mensajería interna.

COMUNIQUESE Y CUMPLASE

Dado en Bogotá, D.C., a los diecisiete (17) días del mes de noviembre de dos mil nueve (2009).

LUIS FRANCISCO SIERRA REYES
Presidente Nacional

PABLO EMILIO CRUZ SAMBONI
Secretario General