El Consejo Universitario de la Universidad Centroccidental "Lisandro Alvarado", reunido en su sesión Nº 1647, Ordinaria, celebrada el día veintiuno de septiembre del dos mil cinco, en uso de las atribuciones que le confiere los artículos 21 y 22 de La Ley Orgánica de Hacienda Pública Nacional; el numeral 19 del artículo 26 de la Ley de Universidades y el numeral 21 del artículo 9º del Reglamento de la Universidad Centroccidental "Lisandro Alvarado", actuando de conformidad con lo establecido en el artículo 9ª, numeral 23 del Reglamento de la Universidad Centroccidental "Lisandro Alvarado", **APROBO: Las Normas de Seguridad Informática y de Telecomunicaciones de la Universidad Centroccidental "Lisandro Alvarado"**.

Preámbulo

"Las Instituciones Académicas existen para la transferencia de conocimiento, la persecución de la verdad, el desarrollo de los estudiantes y el bienestar general de la sociedad. La libre expresión y el discernimiento son indispensables para el logro de estas metas… La responsabilidad para afianzar y respetar las condiciones generales conducentes a la libertad de aprender es compartida por todos los miembros de la comunidad académica. Cada colegio y universidad tiene el deber de desarrollar las políticas y procedimientos que protejan y salvaguarden esta libertad."

Cita de la ***Asociación Americana de Profesores Universitarios*** (AAUP), Estados Unidos, en su ***Declaración Colectiva de Derechos y Libertades de los Estudiantes***.

Exposición de Motivo

Ante el esquema de globalización que las tecnologías de la información han originado, principalmente por el uso masivo y universal del Internet, como de los servicios involucrados con ellas, las instituciones se ven inmersas en amenazas y ambientes agresivos donde el delinquir, sabotear, robar se convierte en los retos para delincuentes informáticos universales conocidos como Hackers, Crakers, entre otros. Conforme las tecnologías aparecen, la severidad y frecuencia de estos ataques las han transformado en un continuo riesgo, que obliga a las instituciones a crear medidas de emergencia, normas y políticas definitivas para contrarrestar estos ataques, transgresiones y permita la protección de la privacidad, del derecho de autor y de la seguridad informática.

En nuestro país no existe una sola institución que no se haya visto sujeta a los ataques en sus infraestructuras informáticas o de telecomunicaciones. Ataques que pueden venir tanto desde el interior como del exterior de la institución.

La *Dirección de Telecomunicaciones* de la UCLA, consciente de este problema y preocupado por asegurar la integridad, privacidad y la seguridad de la información electrónica que circula en la Infraestructura de Red Digital de Voz y Dato de la UCLA (RedUCLA) esta implementando un sistema de gestión de acceso a páginas Web y protección antivirus de la Redes de Datos y Correo Electrónico para la Universidad Centroccidental "Lisandro Alvarado". Este sistema actualmente se encuentra en la etapa de entonación de sus cualidades y en espera de la definición de las políticas y normas que regirán su uso en la Institución.

Basándose por tanto en esto, la Universidad Centroccidental "Lisandro Alvarado", propone la legalización e incorporación de las ***Normas de Seguridad Informática y de Telecomunicaciones de la UCLA*** a los reglamentos de la Institución, y la aprobación por parte del Consejo Universitario de la reglas y procedimientos que son ejecutados actualmente por la Dirección de Telecomunicaciones para este propósito, esto con el fin de llenar un vacío existente, dado que para atender necesidades de índole de seguridad informática y de telecomunicaciones no se tiene un basamento legal que garantice la integridad, privacidad y disponibilidad de la información electrónica que circula en la RedUCLA.

Con la creación de estas Normas de Seguridad se protegerá a los usuarios, datos, redes y los dispositivos conectados a la RedUCLA con especificaciones tecnológicas, requerimientos administrativos y lineamientos que podrán limitar el uso no autorizado, virus, vandalismo y repeler ataques informáticos. Así como establecer basamentos que permitan incrementar la productividad administrativa y académica, privacidad y el derecho de autor en beneficio de la comunidad en general.

En ningún momento, la UCLA y las políticas de seguridad pretenden limitar la libertad de expresión y el derecho de nuestra comunidad a estar informados. Tampoco limita la información por religión, genero, ni tendencia política. Todo esto se realiza con el mejor interés de la Universidad en que los datos, redes

y los dispositivos conectados en la RedUCLA sean íntegros, protegidos y disponibles para los sistemas, servicios e información basados en estos. Así como, servir de herramienta organizacional para que cada uno de los miembros de la UCLA sea consciente sobre la importancia y sensibilidad de la información y servicios críticos que permitan a la Universidad desarrollarse, mantener su calidad y excelencia académica.

Objetivos de las Normas de Seguridad Informática y de Telecomunicaciones

General

Establecer las normas para el uso aceptable, la administración de todos los recursos tecnológicos y la información electrónica de la Universidad Centroccidental "Lisandro Alvarado", a través de procedimientos basados en estándares de protección con acceso equitativo de los recursos informáticos y pautas de seguridad que permitan el control de las actividades realizadas en la red.

Específicos

- Establecer los alcances y delimitaciones de las normas de seguridad informática y de telecomunicaciones.
- Definir las normas de seguridad informática y de telecomunicaciones.
- Establecer los niveles de responsabilidades para cada uno de los servicios y recursos informáticos y de telecomunicaciones de la Institución.
- Requerimientos mínimos que deben poseer las configuraciones de seguridad de los sistemas que cobijan el alcance de la política.
- Definición de las violaciones y las consecuencias del no cumplimiento de las normas de seguridad.
- Responsabilidades de los entes encargados de la seguridad y de los usuarios con respecto a la información a la que él o ella tiene acceso.

Concepto, Propósito y Alcance de las Normas de Seguridad Informática y de Telecomunicaciones

Concepto

Las políticas o normas de seguridad informática y de telecomunicaciones permiten regular la forma de comunicarse con los usuarios y el uso de los servicios que se prestan en la red. Las normas de seguridad informática y de telecomunicaciones establecen el canal formal de actuación del usuario, en relación con los recursos, servicios informáticos y de telecomunicaciones de la Universidad. Estas normas y políticas son capaces de crear consciencia y ser vigilantes del uso por la comunidad y fijar limitaciones de los recursos, servicios de informáticos y de telecomunicaciones de la UCLA.

Propósito

El propósito de estas normas es el proteger a los usuarios de la comunidad universitaria contra los virus, vandalismo, el uso informático no autorizado y cualquier otro ataques dirigido a sus datos, redes y los dispositivos conectados a la Infraestructura de telecomunicaciones de la UCLA (RedUCLA) a través de especificaciones tecnológicas, requerimientos administrativos y recomendaciones que serán gestionadas por la Dirección de Telecomunicaciones de la UCLA. Todo esto con el mejor interés de la Universidad en que los datos, redes y los dispositivos conectados en la RedUCLA sean íntegros, protegidos y disponibles para los usuarios, sistemas, servicios e información basados en estos. Estas normas y sus estándares asociados, por consiguiente, permitirán establecer configuraciones y administraciones de la red de forma segura para cualquier computadora provista con acceso a la RedUCLA.

Alcance

Los Dispositivos cubiertos por estas normas incluyen todos los equipos informáticos y de telecomunicaciones conectadas a la infraestructura de RedUCLA, tales como Computadores personales, Impresoras, Servidores, Switch, Concentradores, Instrumentos de Laboratorio o cualquier otro dispositivo que se conecte a la red. Así como la forma que debe ser usado por el personal para garantizar su seguridad de la información que fluye en esta Red.

Bases Legales

Estándares Internacionales

ISO/IEC 17799 – Estándar de Gestión de Seguridad de la Información en redes informáticas y otros medios donde fluye la información de la *Organización Internacional de Estándares* (ISO).

IEEE P1363 – Estándar de manejos de Claves de acceso y seguridad Informática del *Institute of Electrical and Eletronics Engineers* (IEEE)

Leyes Nacionales

Ley Especial Contra Delitos Informáticos promulgada en Gaceta Oficial N° 37.313 de fecha 30 de octubre de 2001 por la Asamblea Nacional

Ley Sobre Mensajes de Datos y Firmas Electrónicas promulgada en Gaceta Oficial N° 37.148 de fecha 28 de febrero de 2001, por Decreto N° 1.024 – 10 de febrero de 2001

Ley Orgánica de Telecomunicaciones, promulgada en Gaceta Oficial N° 37.148 de fecha 28 de febrero de 2001 por Decreto N° 1.024 - 10 de febrero de 2001

Normas y Procedimientos para la Seguridad Informática y de Telecomunicaciones de la Universidad Centroccidental "Lisandro Alvarado"

Capítulo I
Disposiciones Generales

Artículo 1

La Dirección de Telecomunicaciones es el ente que gestiona y da apoyo técnico en materia de Seguridad Informática y de Telecomunicación a las dependencias académicas, de investigación, y administrativas de la Universidad Centroccidental "Lisandro Alvarado". Sus atribuciones y deberes son las siguientes:

a Fijar las directrices de seguridad en informática y de telecomunicación de la Institución, dictando normas y políticas que serán estudiadas, consideradas y sometidas a aprobación en concordancia con los criterios generales por el Consejo Universitario de la Universidad Centroccidental "Lisandro Alvarado", y con los aportes y asesoría de la Dirección de Informática y la Dirección de Telecomunicaciones, además de velar por la ejecución del plan de seguridad establecido para cumplir con las normas de seguridad establecidas en este documento.

b Dictar criterios técnicos de interés común de las dependencias académicas, de investigación y administrativas de la Institución, en materia de seguridad en las tecnologías de información.

c Apoyar y asesorar a las Autoridades Universitarias en materia de seguridad en las áreas de informática y de telecomunicación.

d Apoyar a la Comisión de Informática con el estudio y aval de las solicitudes de adquisición de bienes informáticos y/o de telecomunicaciones en las dependencias académicas y administrativas de la Universidad Centroccidental "Lisandro Alvarado" que estén orientados al área de la seguridad informática o de telecomunicaciones.

e Promover, aprobar, sugerir, seguir y evaluar adquisiciones, planes y proyectos informáticos y de telecomunicaciones orientadas al área de la seguridad y protección antivirus en los centros y dependencias

académicas, de investigación y administrativas de la Universidad Centroccidental "Lisandro Alvarado".

f Actualizarse en cuanto a nuevas tecnologías del mercado para realizar propuestas y asesoramientos actualizados referentes a la seguridad informática y de las telecomunicaciones.

g Servir de ente de enlace entre la Institución y cualquier empresa que en materia de seguridad tecnológica de la información y las telecomunicaciones desee realizar convenios, en conjunto con la Dirección de Cooperación y Relaciones Interinstitucionales de la Universidad Centroccidental "Lisandro Alvarado".

h Adoptar medidas que garanticen la protección y seguridad tecnológica de las dependencias académicas y administrativas.

i Dar seguimiento de reubicaciones, donaciones y reutilización de los equipos que pudieran ser desincorporados al momento de aprobación de las solicitudes por sustitución de equipos informáticos y/o de telecomunicaciones.

j Los demás que le atribuya al Consejo Universitario expresamente o a través de sus reglamentos.

Artículo 2
Como conceptos básicos en este documento se define:

a. **Activos**. Los recursos del sistema de información o relacionados con éste, necesarios para que la Institución funcione correctamente y alcance los objetivos propuestos.

b. **RedUCLA**: Es toda la infraestructura de voz, dato y videoconferencias encargada de interconectar todos los activos de las dependencias académicas, de investigación y administrativa de la UCLA.

Artículo 3
Las normas presentadas en este documento se orientan con el propósito de garantizar los siguientes principios de la seguridad:

a. **Integridad**. Se define como las características que previene contra la modificación o destrucción no autorizadas de los activos.

b. **Disponibilidad**. Se define como la característica que previene contra la denegación no autorizada de acceso a los activos.

c. **Confidencialidad**. Se define como la característica que previene contra la divulgación no autorizada de los activos.

d. **Autenticación**. Se define como la característica de dar y reconocer la autenticidad de los activos (de tipo información) y/o la identidad de los actores y/o la autorización por parte de los autorizadores, así como la verificación de dichas tres cuestiones.

Artículo 4

Los sistemas informáticos de la UCLA, incluida su red de comunicaciones, están al servicio del cumplimiento de los fines propios de la institución universitaria en los ámbitos de la investigación, la docencia, la extensión y la gestión académica - administrativa. Cualesquiera otros usos estarán en todo momento subordinados a dichos fines. Se deberán extremar la atención sobre los siguientes puntos:

a. Cualquier equipo que tenga autorización para conectarse a la red de la UCLA, aunque no sea propiedad de la Universidad, quedará sujeto a las políticas contenidas en este documento y deberán tener un responsable designado. En el caso de equipos de uso personal el responsable será el usuario habitual o propietario de este equipo. En el resto de los equipos deberá existir un administrador que actuará como responsable del equipo.

b. La capacidad de transmisión de datos de la red es un recurso limitado, compartido por todo tipo de usuarios. Por ello no se permiten las transferencias de datos excesivas o muy voluminosas, es decir, que superen las limitantes que técnicamente establezca la Dirección de Telecomunicaciones en cada uno de sus servicios a fin de no comprometer la normal actividad de la Universidad.

Capítulo II
Obligaciones y Actividades del Usuario de la Infraestructura de Voz, Dato y Videoconferencia de la UCLA

Artículo 5
El sistema de seguridad que implemente la UCLA debe permitir a la Comunidad Universitaria el utilizar los equipos conectados a la RedUCLA para cumplir las siguientes metas:

- La modernización de la plataforma didáctica que promuevan la enseñanza en el uso de las nuevas tecnologías de información.

- Herramienta de apoyo, comunicación e información para los Estudiantes, Docentes, Investigadores y Administrativos.

- La automatización de los servicios administrativos y académicos de la Institución.

- Como apoyo a las actividades sin fines de lucro de fomento, extensión y cultura universitaria.

Artículo 6
El Personal Docente, de Investigación, de Extensión, Administrativo, Obrero, y los Estudiantes deben utilizar los Recursos Informáticos y la plataforma RedUCLA sólo para los fines enunciados en el Artículo 5.

Artículo 7
No se permite el uso de los recursos informáticos y la plataforma RedUCLA con fines de pasatiempo, comerciales o de divulgación de información cuyo contenido sea distinto al de investigación, académico, educacional o necesario para el desempeño de las funciones administrativas y gestión académica.

Artículo 8
La infraestructura y cualquier servicios que se ofrecen a través de la infraestructura de RedUCLA no deben usarse para:

a. Fines privados, personales o lúdicos.

b. La creación o transmisión de material que cause cualquier tipo de reclamo de otros usuarios de la UCLA.

c. La circulación de información difamatoria de cualquier tipo, ya sea contra entidades o personas.

d. Distribución de material que viole derechos de propiedad intelectual.

e. Desarrollo de actividades que persigan:

i. La congestión de la red de comunicaciones o sistemas informáticos mediante el envío de información o programas concebidos para tal fin.

ii. La destrucción o modificación premeditada de la información de otros usuarios.

iii. La violación de la privacidad e intimidad otros usuarios.

iv. El deterioro del trabajo de otros usuarios.

f. Destrucción, manipulación o apropiación indebida de la información que circula en la red.

g. Obtención y uso de cuentas o claves de acceso a computadores, correo electrónico, candados telefónicos y acceso remoto ajenas.

h. Proporcionar contraseñas a otros usuarios ajenos a la Institución para el ingreso a la RedUCLA.

i. La conexión de activos (hubs, switches, routers, modem, entre otros) que previsiblemente perturbe el correcto funcionamiento de la RedUCLA o que comprometa la seguridad, salvo expresa autorización de la Dirección de Telecomunicaciones.

j. Desconexión o reubicación de activos sin la autorización expresa de la Dirección de Telecomunicaciones.

k. El alojamiento en los servidores de la RedUCLA de dominios distintos a **ucla.edu.ve,** salvo expresa autorización de la Dirección de Telecomunicaciones.

i. Cualquier transmisión informática o acto que viole las legislaciones vigentes en la Republica Bolivariana de Venezuela y que comprometan a la Universidad en estos tipos de acciones ilícitas.

Artículo 9
Los miembros de la comunidad universitaria y demás beneficiarios que puedan acceder a su condición de usuario a la RedUCLA tiene los siguientes derechos:

a. A las prestaciones reconocidas en este documento para los servicios informáticos y de telecomunicaciones.

b. De tener una seguridad adecuada que garantice la integridad, disponibilidad y confidencialidad de su información digital dentro de las fronteras de la RedUCLA.

c. A ser informado con claridad de cualquier incidencia que sufra a causa de violaciones en la seguridad de la red.

Artículo 10
Los usuarios están obligados a cumplir con las restricciones acordadas para el uso del correo electrónico y en especial de no plagiar y copiar el software protegido por derecho de autor que se encuentre en los servicios de redes de telecomunicaciones, no violar la seguridad de las cuentas de correos electrónicos de los usuarios, de sus contraseñas de acceso a la red de datos y candados telefónicos electrónicos, que son secretos e individuales y a no forzar el acceso a servidores locales si no tiene la autorización respectiva.

Artículo 11
Bajo ninguna circunstancia de deberá tener acceso a las páginas WEB con contenido que atenten contra la moral y las buenas costumbres, así como el uso del correo electrónico y extensiones telefónicas para la difusión de prácticas

de violencia y hechos antisociales. La detección por parte de cualquier miembro de la Comunidad Universitaria esta en el deber de denunciarlo a fin de ser sancionada de acuerdo a lo establecido en estas normas.

Artículo 12
No se permite la sintonización de emisoras de radio o de televisión a través de Internet, así como la descarga o distribución de materiales de audio y video de uso personal, sin fines académicos, de investigación, de extensión o de interés institucional. El requerimiento especial de este tipo de actividades debe solicitarse y justificarse por la dependencia ante la Dirección de Telecomunicaciones para su autorización.

Artículo 13
La UCLA se reserva el derecho de bloquear el acceso a toda página Web, Sistema de Mensajería Electrónica y Sistemas de transferencia de Archivos que atenten contra la ética de uso, el rendimiento y la calidad del servicio Internet, así como la seguridad en las redes de datos.

Capítulo III
Seguridad en Activos Conectados a la REDUCLA
Computadores Personales, Periféricos y otros Dispositivos Informáticos

Artículo 14
Los usuarios deberán mantener instaladas en sus equipos, y actualizadas periódicamente, las herramientas antivirus homologadas por la Universidad. Aun así, deben extremar las precauciones ante los mensajes de correo electrónico de procedencia desconocida. A los efectos de garantizar la integridad en la operatividad de sus equipos es recomendable que en caso de duda del remitente, no debe abrir los archivos electrónicos adjuntos y exponer el activo o la RedUCLA a virus informáticos.

Artículo 15
La asistencia técnica que presta la Dirección de Telecomunicaciones en materia de seguridad informática y de telecomunicaciones está exclusivamente dirigida a aquellos equipos que sean propiedad de la UCLA, inventariados y se encuentren ubicados en las Edificaciones de la Universidad.

Artículo 16
La responsabilidad del uso adecuado de las herramientas informáticas, como el computador personal y sus programas instalados, es del usuario del equipo. Los usuarios de equipos personales deberán realizar copias de seguridad de los datos que considere relevantes.

Artículo 17
Los responsables de los equipos conectados a la redes de la UCLA deben asegurarse de tener instalados los parches de seguridad y actualizaciones de los sistemas operativos.

Artículo 18
Los equipos no deben presentar configuraciones, ni operar con dispositivos que causen problemas en la red o a otros equipos conectados a ella, en concordancia con los lineamientos técnicos establecidos por la Dirección de Telecomunicaciones.

Servidores de Redes de Datos y Servidores de Aplicaciones

Artículo 19
Los responsables de los servidores de datos y servidores de aplicaciones están obligados a aplicar las normas de seguridad establecidas en este documento, así como los lineamientos relacionados al uso de servicios de directorio, de direccionamiento, nombres y dominios en la red, incluyendo el uso de DHCP, DNS y otros afines, que establezca la UCLA según propuesta de la Dirección de Telecomunicaciones. Además, deberán llevar a cabo una administración adecuada de sus equipos, manteniéndolos actualizados y protegidos contra las amenazas de seguridad conocidas para sus aplicaciones y sistema operativo del Servidor.

Artículo 20
En los servidores o computadores instalados en la Institución, no se pueden crear nuevos servicios que puedan entrar en conflicto con los servicios de red existentes sin la previa autorización de la Dirección de Telecomunicaciones, como servicios de asignación de direcciones, servicios Proxy, servicios DNS, servicios encaminadores de correo electrónico, entre otros, que puedan comprometer la seguridad de la red.

Laboratorios de Informática y Telecomunicación

Artículo 21

En los laboratorios orientados a informática y telecomunicaciones, sean de uso académico, de investigación, de extensión o gestiones administrativas, son de obligado cumplimiento las directivas generales sobre instalación, gestión y administración mencionadas en este documento así como cualesquiera otras específicas de los laboratorios de informática o telecomunicaciones y que se adecuen a las necesidades académicas de cada Decanato.

Artículo 22

Para la administración de un laboratorio de informática, la autoridad académica que la gestione debe mantener actualizado los aspectos más relevantes del equipamiento, aplicaciones a instalar, claves de acceso y uso de cada estación de trabajo.

Servicios o Aplicaciones Informáticas de Apoyo a la Gestión Académica y Administrativa

Artículo 23

Todo procedimiento para el desarrollo, adquisición o implantación de tecnología de información al servicio de la gestión académica o administrativa en la UCLA, deberá llevar el aval de la Dirección de Informática y la Dirección de Telecomunicaciones que certifique la seguridad necesaria para operar en la infraestructura de la RedUCLA. Asimismo, la Dirección de Informática y la Dirección de Telecomunicaciones en conjunto, deberán asesorar y supervisar todo tramite para la adquisición de equipamiento informático (hardware y software) destinado al uso académico o administrativo por parte de cualquier dependencia de la Institución.

Artículo 24

Debe ser indispensable el uso de herramientas que permitan la atención remota únicamente de los responsables de la gestión y soporte técnico en todos los equipos en el ámbito de la Universidad que estén ejecutando estos servicios o aplicaciones informáticas.

Artículo 25

En los computadores destinados a la gestión de aplicaciones académica o administrativa, se deberá desinstalar cualquier software que comprometa la seguridad o que entre en conflicto con la ejecución de estas aplicaciones. Así

como también, se limitara el acceso a Internet de considerarse necesario por parte de la dependencia que implemente la aplicación académica o administrativa.

Equipos para Extensiones Telefónicas

Artículo 26
La Dirección de Telecomunicaciones asignará los equipos telefónicos y la numeración de la extensión telefónica de la UCLA, a la coordinación, dependencia, unidad o departamento y deberá tener un responsable de su uso. En ningún momento el equipo telefónico o la numeración de la extensión telefónica será asignado para uso individual.

Artículo 27
La dependencia no podrá usar las líneas de las extensiones telefónicas de la UCLA como punto de conexión para sistemas de cobro electrónico o puntos de ventas que interactúen con entes externos (bancos, tiendas o entes similares).

Artículo 28
Todos los equipos telefónicos, líneas telefónicas y plan de numeración y componentes para las centrales digitales de la RedUCLA, así como aquellos equipos telefónicos adquiridos por las dependencias, forman parte de los activos de la red y serán gestionados por la Dirección de Telecomunicaciones así como su administración.

Artículo 29
Los usuarios asignados como responsables de la extensión telefónica velaran por el uso correcto del equipo y la línea telefónica.

Artículo 30
Los puntos de conexión para las extensiones telefónicas son para el uso de un solo equipo telefónico, se prohíbe la instalación de equipos auxiliares que comprometan la privacidad y garantías de operatividad técnica.

Artículo 31
No se permite la utilización de equipos y herramientas que interfieran los servicios telefónicos. Esta actividad solo puede ser utilizada por la Dirección de Telecomunicaciones en sus actividades de mantenimiento y detección de fallas.

Capítulo IV
Seguridad de las Claves de Correo Electrónico, Claves de Acceso Remoto y Clave de Acceso a la REDUCLA

Artículo 32
Todo usuario de los activos conectados a la RedUCLA deberá tener un nombre de usuario y clave de acceso para ingresar a su computador.

Artículo 33
La Dirección de Telecomunicaciones será la responsable de establecer los mecanismos y las categorías de usuarios para asignar las claves de accesos a todos los usuarios de la RedUCLA y su validación a nivel Institucional. La Dirección de Informática, los laboratorios Informáticos y Centros de Computación de pregrado y postgrado podrán suministrar claves de acceso a la RedUCLA, acogidos a los mecanismos y categorías que estandarice la Dirección de Telecomunicaciones para su control y registró.

Artículo 34
La Dirección de Telecomunicaciones será la única instancia autorizada para proveer el servicio de acceso remoto vía telefónica de la RedUCLA y las claves de acceso a este servicio.

Artículo 35
La Dirección de Telecomunicaciones asignará las claves de correo electrónico, de acceso remoto y acceso a la RedUCLA de acuerdo con el procedimiento establecido para tal efecto.

Artículo 36
La renovación de claves de correo electrónico, de acceso remoto y acceso a la RedUCLA se efectuará de acuerdo con el procedimiento establecido para tal efecto.

Artículo 37
Todas las claves de acceso remoto vía telefónica y de correo electrónico para acceso a RedUCLA son personales e intransferibles, por lo que únicamente podrán ser usadas por los propietarios de las mismas, siendo el poseedor de la clave el responsable de la confidencialidad de la contraseña correspondiente y su renovación periódica.

Artículo 38
La Dirección de Recursos Humanos y la Dirección del Personal Docente y de Investigación debe notificar a la Dirección de Telecomunicaciones cuando un Profesor, Investigador o empleado administrativo renuncia, es despedido o es jubilado con el propósito de eliminar su nombre de usuario y clave de acceso en los servicios que ya no requiera acceder como miembro activo de la comunidad universitaria. En el caso de que el usuario sea un estudiante, la Dirección de Control de Estudio debe notificar a la Dirección de Telecomunicaciones su egreso o retiro de la carrera a fin de eliminar su nombre de usuario y clave de acceso en los servicios que ya no requiera acceder como miembro activo de la comunidad universitaria.

Capítulo V
Seguridad en el Servicio de Correo Electrónico Institucional

Artículo 39
La UCLA posee un único Servicio de Correo Electrónico Institucional, identificado con el dominio ***email.ucla.edu.ve*** y todos los mensajes electrónicos se encaminaran al uso exclusivo de este servicio. La Dirección de Telecomunicaciones es el ente encargado de Gestionar este Servicio.

Artículo 40
El uso del Servicio de Correo Electrónico Institucional estará regido por las "***Condiciones de Uso***" y "***Políticas de Privacidad***" elaboradas por la Dirección de Telecomunicaciones y aprobadas por el Consejo Universitario.

Artículo 41
En la RedUCLA no está permitido instalar ni usar servidores o encaminadores de correo que no cuenten con la autorización de la Dirección de Telecomunicaciones.

Artículo 42
Los usuarios son responsables de todas las actividades que realicen con sus cuentas y su buzón de correo electrónico que estén asociado con la UCLA. El uso indebido del correo electrónico puede acarrear responsabilidades civiles y penales, así como las establecidas en este documento y las previstas en las leyes del estado sobre esta materia.

Artículo 43
No está permitido facilitar u ofrecer las cuentas y buzones de correo electrónico Institucional a terceras personas o personal ajeno a la comunidad universitaria.

Artículo 44
No se permite la utilización abusiva del correo electrónico incluyendo la realización de prácticas tales como:

- Envío masivo por el usuario de mensajes o información que consuma injustificadamente los recursos del Servidor de Correo Electrónico Institucional e Internet.

- Actividades comerciales privadas.

- Propagación de cartas encadenadas o actividades similares.

Artículo 45
Los usuarios tendrán disponibles el acceso a servicios de correos electrónicos distintos al institucional únicamente vía Web y este será de uso personal únicamente. La UCLA no se hace responsable por soporte o daños que deriven del uso de estos servicios, el usuario será responsable de cualquier daño o perjuicio que derive del uso de estos servicios y afecten a la RedUCLA.

Artículo 46
La UCLA se reserva el derecho de bloquear y eliminar cualquier correo electrónico que intente ingresar al Servidor de Correo Electrónico con mensajes basura, comercial, virus y código malicioso, sin previo aviso al usuario. Sin embargo, la Dirección de Telecomunicaciones tendrá la potestad de notificar al usuario el bloqueo de alguna correspondencia electrónica, siempre y cuando las condiciones técnicas de la detección lo permita.

Artículo 47
Con el propósito de evitar potenciales virus y código malicioso, los siguientes tipos de archivos serán verificados por un sistema automatizado que permita filtrar y bloquear aquellos que se encuentren infectados, si son enviados por correos electrónicos:

a. Archivos ejecutables con extensión: *.bat, *.com y *.exe.

b. Archivos comprimidos con extensión: *.gz, .tar y .tgz

c. Librerías de enlaces dinámicos con extensión: *.dll

d. Archivo Visual Basic con extensión: *.vb?

e. Archivos Protectores de Pantalla con extensión: *.scr

f. Cualquier tipo de archivo que se considere sea portador de código malicioso o virus

Artículo 48
La Dirección de Telecomunicaciones establecerá el tamaño máximo que el archivo adjunto al Correo Electrónico puede tener. Esto estará determinado de acuerdo a las limitaciones técnicas y requerimientos de ancho de banda que exista en la RedUCLA.

Artículo 49
Es deber de la Dirección de Telecomunicaciones establecer los medios adecuados para el buen funcionamiento del servicio, los sistema de seguridad y protección antivirus necesarios para garantizar la integridad, confidencialidad y disponibilidad de los buzones de Correo Electrónico Institucionales.

Capítulo VI
Seguridad en el Acceso a la Red de Datos, Páginas WEB e INTERNET

Artículo 50
La Dirección de Telecomunicaciones será el único ente autorizado para:

a. Dar acceso a las Redes de Datos, servicios Web e Internet a las dependencias académicas y administrativas de la Institución.

b. Regular el uso y acceso a páginas Web e Internet en función de los intereses académicos, de investigación, extensión y gestión administrativa de la Institución.

Artículo 51
Cada punto de acceso a la red está diseñado para la conexión de un solo ordenador o periférico. No está permitida, por tanto, la conexión de equipos concentradores, puntos de acceso wireless, conmutadores o enrutadores, computadores o otros dispositivos que funciones como tales.

Artículo 52
La instalación de nuevos puntos de red se hará de conformidad con los criterios y estándares propuestos por la Dirección de Telecomunicaciones. Los trabajos correspondientes serán coordinados por la Dirección de Telecomunicaciones.

Artículo 53
Todos los equipos que se conectan a la red deben recibir una dirección IP y un nombre de red reservado por la Dirección de Telecomunicaciones, además de ser incluidos en el registro correspondiente, junto con la identidad y los datos de contacto del responsable del equipo. No está permitida la conexión de equipos con nombres o direcciones no registrados.

Artículo 54
No se permite el empleo de mecanismos para la manipulación de direcciones de red o cualquier otro uso que pueda afectar a la topología o a la estructura lógica de la red.

Artículo 55
Los equipos electrónicos de gestión e infraestructura de la RedUCLA serán instalados, configurados y mantenidos exclusivamente por la Dirección de Telecomunicaciones, según los estándares establecidos para esto.

Artículo 56
Ningún usuario está autorizado a utilizar analizadores del tráfico, analizadores de protocolo u otra herramienta que circulan por la red. Igualmente está prohibido utilizar herramientas de rastreo de puertos o que permitan detectar vulnerabilidades. Estas herramientas son de uso exclusivo de la Dirección de Telecomunicaciones. Se autoriza su utilización académica únicamente en la red local del Laboratorio de Redes del Decanato de Ciencias y Tecnología.

Artículo 57
La Dirección de Telecomunicaciones, deberá implementar un Sistema de Seguridad y Protección de la RedUCLA. Dicho sistema deberá aplicar el siguiente perfil de seguridad principal:

Para la protección de Virus y Código Malicioso. Por medio de este se deberá realizar el chequeo del flujo de información que entra y sale de la red de datos Institucional, manteniendo la confidencialidad al no necesitar la manipulación humana para este chequeo. Este rastreo se efectuara principalmente en:

a. Servicios Web para el acceso a direcciones de páginas URLs. Rastreo de virus y código malicioso que pudiesen contener las paginas Web que son solicitadas por los usuarios a través de los navegadores de Internet.

b. Servicios FTP para la transferencia de archivos en red. Rastreo de virus y código malicioso que pudiesen contener los documentos o cualquier otro archivo que sean transferido a través de Servidores con protocolo de transferencia de archivos (FTP) al computador del usuario que lo solicita.

c. Servicios IMAP, POP3 y SMTP para el acceso a correos electrónico. Rastreo de correos electrónicos y sus documentos adjunto a fin de bloquear cualquier virus o código malicioso que pudiese contener durante el envío o recepción en los buzones institucionales.

Para el Bloqueo de Archivos y Direcciones Web. Eliminación automática de archivos que contengan virus o código malicioso que no puedan ser rastreados por el Sistema de Seguridad y Protección de la RedUCLA y bloqueo de páginas Web que no cumplan con las condiciones establecidas en esta política. Este bloqueo se efectuara principalmente en:

a. Internet:

i. Bloqueo de Web URL. Bloqueo de direcciones a paginas Web y Sitios Web no deseados

ii. Bloqueo de Contenidos Web. Bloqueo de páginas Web que contengan palabras o frases no deseadas

iii. Filtrado de Script Web. Remueve códigos Scripts de las páginas Web consultadas que podrían ejecutar acciones maliciosas.

iv. Lista de Web exentas de bloqueo. Se establecerá una lista de aquellas paginas Web, Contenidos o Script exentos de bloqueos a través del sistema de seguridad.

b. Correo Electrónico:

i. Lista de Correos electrónicos Bloqueados. Se establece una lista de las direcciones de correos electrónicos etiquetados como no deseados o que generan molestias a los usuarios.

ii. Lista de Correos electrónicos exentos. Se establece una lista de las direcciones de correos electrónicos etiquetados como no deseados pero exentas del bloqueo.

iii. Bloqueo por Contenido del Correo Electrónico. Bloquear correos electrónicos que contengan contenido no acorde con el uso de esta herramienta en la Institución, con contenido tales como correo basura, publicidad con alto contenido sexual, entre otros.

iv. Tamaño del Corre Electrónico y FTP. Se bloquean correos electrónicos o transferencias de archivos cuyos tamaños en bytes sean superior al permitido por la Dirección de Telecomunicaciones.

Artículo 58

La Dirección de Telecomunicaciones establecerá el tamaño máximo que los archivos transferidos vía FTP o por Correo Electrónico puede tener. Esto estará determinado de acuerdo a las limitaciones técnicas y requerimientos de ancho de banda que exista.

Artículo 59
El Sistema de Seguridad y Protección Antivirus podrá rastrear todos los archivos que circulan en la red, excepto los siguientes formatos: Imagen CD, .ace, .bzip2, .Tar, .Gzip. Por lo cual es responsabilidad del usuario el chequear con un software antivirus este tipo de archivos antes de abrirlos.

Capítulo VII
Perfiles de Protección y Seguridad en la Red de Dato y Categorías Páginas WEB

Artículo 60
Es responsabilidad de la Dirección de Telecomunicaciones establecer Perfiles de Protección adecuados para cada grupo de usuarios que se encuentren en la RedUCLA, estas se definirán de la siguiente manera:

a. Los Perfiles de Protección son las agrupaciones virtuales según los tipos de usuarios existentes en la RedUCLA. Estos usuarios será definidos como:

   i. Autoridades Rectorales: Comprende los miembros del Consejo Universitario.

   ii. Docentes.

   iii. Investigadores.

   iv. Estudiantes.

   v. Directores, Jefes de Departamento y Coordinadores de las dependencias académica.

   vi. Directores, Jefes de Departamento y Coordinadores de las dependencias administrativas.

   vii. Usuarios de Aplicaciones Administrativas

   viii. Usuarios de Aplicaciones Académicas

ix. Supervisores y Administradores de la RedUCLA

x. Usuarios Especiales. Son todos aquellos usuarios que según su uso de la RedUCLA requieren configuraciones con perfil de protección especiales.

b. Para cada Perfil de Protección, la Dirección de Telecomunicaciones propondrá ante el Consejo Universitario el tipo de medidas y restricciones, las cuales serán sometida a su autorización y posterior aplicación. Estos Perfiles de Protección serán elaborados bajo los siguientes criterios de elaboración y aplicación:

i. La Dirección de Telecomunicaciones consultará y recibirá de cada Consejo de Decanato las propuestas de restricciones y medidas de seguridad a ser aplicadas a los usuarios en el Decanato con su respectiva justificación.

ii. La Dirección de Telecomunicaciones elaborará restricciones y medidas de seguridad que sean propuestas por el Consejo Universitario y tengan carácter de aplicación general o particular en la Institución.

iii. La Dirección de Telecomunicaciones elaborará restricciones y medidas de seguridad que sean necesarias para proteger la integridad y seguridad de la RedUCLA con su respectiva justificación.

Artículo 61

Para la aplicación de filtros de páginas Web que se definan en las restricciones de los Perfiles de Protección, se aplicará Categorías de Web de la siguiente manera:

a. **Con Riesgos Potenciales**: Sobre temas de Abuso de Droga, Cultos Oscuros, Hacker (Delincuencias en las Redes), Racismo y Odio, Violencia.

b. **Controversiales y Acciones Objetables**: Aborto, Adulterio, Materiales de adulto, Alcohol y Tabaco, Armas, Extremistas y Terroristas, Nudismo, Pornografía, Acciones de Mal Gusto.

c. **Potencialmente no productivos**: Publicidad y Mercadeo, Agencia de negocios, Bolsa de valores, Transacciones Bancarias, Software no productivo, Juegos, Comunicación vía Internet, Navegación prepagada, Correo Electrónico vía Web.

d. **Potencialmente Consumidores de Ancho de Banda**: Almacenamiento y Compartidores de Archivos, Video por demanda para películas.

e. **Potencialmente Violadores de Seguridad**: Sitios Web Malicioso, Spyware.

f. **Interés General**: Arte y Entretenimiento, Institutos Culturales, Educación, Servicios y Datos Financieros, De Interés Homosexuales o Lesbianismo o Bisexuales, Salud, Bolsas de Trabajos, Medicina, Noticias y Medios de Comunicación, Agendas Personales, Organización Políticas, Materiales Referenciales, Religión, Portales y Motores de Búsqueda, Compras Virtuales, Organizaciones Sexuales, Estilos de Vida y Sociedad, Eventos especiales, Deporte, Viajes, Vehículos.

g. **Investigación y Educación**: Cursos en Línea, Universidades, Escuelas, Investigación y Desarrollo, Institutos de Estándares, Biomedicina, Foros de Investigación, Ciencias y Tecnología.

h. **Orientadas a Negocio**: Economía y Negocios, Seguridad en Computadoras, Organizaciones Legales y Gubernamentales, Tecnología de Información, Organizaciones Militares.

i. **Otras**: Contenido Dinámico, Hospedajes de Web.

En los Perfiles de Protección, se podrán contener el filtro de una categoría o individualmente por cada uno de los ítems que conforman dicha categoría.

Artículo 62
La Dirección de Telecomunicaciones podrá aplicar restricciones y medidas de seguridad bajo el carácter de emergencia o por violación de la seguridad informática, en cuyo caso tendrá un lapso de 30 días hábiles para someter al Consejo Universitario su autorización definitiva o temporal. Esta restricción o medida de seguridad se dejara sin efecto al cumplirse el lapso de sometimiento ante el Consejo Universitario o de culminar la emergencia o la violación de la seguridad.

Artículo 63
Para cada Perfil de Protección, la Dirección de Telecomunicaciones podrá determinar la necesidad de aplicar detección y eliminación de virus en paginas Web, FTP y Correo Electrónico.

Artículo 64
Para cada Perfil de Protección, la Dirección de Telecomunicaciones podrá determinar la necesidad de aplicar tamaños límites en los archivos transferidos vía Web, FTP o Correo Electrónico.

Capítulo VIII
Responsabilidad Disciplinaria

Artículo 65
Todo miembro de la comunidad universitaria al cual se hace referencia en esta normativa estarán sujetos a responsabilidad disciplinaria y serán sancionados en los supuestos y de acuerdo con los principios establecidos en esta normativa y en las leyes definidas por la Republica Bolivariana de Venezuela para este fin.

Artículo 66
Las Faltas podrán ser muy graves, graves y leves

a. Se consideran faltas muy graves:

    i. El incumplimiento del Artículo 8 en sus numerales *c*, *d*, *e* y *l*.

    ii. Cuando la misma persona incurra en tres (3) faltas grave, le será imputada una falta muy grave, aplicándosele las sanciones disciplinarias corresponden a estos casos.

iii. El cobro indebido a los usuarios por utilizar algún servicio de Telecomunicaciones de la UCLA, sin previa autorización de la Dirección de Telecomunicaciones.

iv. Usurpar el nombre de usuario y clave de acceso sin el consentimiento del verdadero usuario.

v. La violación de los mecanismos de seguridad informática y de telecomunicaciones.

b. Se consideran faltas graves:

i. El incumplimiento del Artículo 8 en sus numerales *a*, *b*, *f*, *g* y *h*.

ii. Cuando la misma persona incurra en tres (3) faltas leves, le será imputada una falta grave, aplicándosele las sanciones disciplinarias corresponden a estos casos.

iii. El uso del correo electrónico y extensiones telefónicas para la difusión de prácticas de violencia y hechos antisociales.

iv. Realizar actividades indebidas sin la previa autorización de la Dirección de Telecomunicaciones.

v. La asignación no autorizada de Direcciones IP Certificadas y No Certificadas de la Institución.

v. La implementación de servicios o aplicaciones que entren en conflicto con los servicios de red existentes y sin la previa autorización de la Dirección de Telecomunicaciones.

c. Se consideran faltas leves:

i. El incumplimiento del Artículo 8 en sus numerales *i*, *j* y *k*.

ii. El incumplimiento del Artículo 44.

iii Acceder a páginas WEB cuyo contenido atente contra la moral y las buenas costumbres.

iv. La utilización indebida de las extensiones telefónicas de la UCLA.

Artículo 67
Cuando se demuestre un uso incorrecto o no aceptable con respecto a lo especificado en este documento, la UCLA autoriza a la Dirección de Telecomunicaciones proceder a la suspensión del servicio al usuario y de ser necesario al computador o dispositivo de red. Dependiendo de la gravedad y reiteración del incidente efectuara los siguientes tipos de suspensión:

a. Suspensión temporal o de emergencia del servicio: esta medida se aplicará cuando se produzca la violación de los términos de este documento de forma premeditada o cuando se este causando una degradación de los recursos de la red y/o implique a la UCLA en algún tipo de responsabilidad. La acción consistirá en filtrar el tráfico relacionado con el computador o dispositivo de red causante del incidente o Bloqueo de la Clave de Acceso del Usuario. Filtrar el tráfico consiste en bloquear el tráfico de ese equipo, con lo que dicho equipo estará conectado a la Red de Datos pero desconectado del Internet. Bloquear la Clave de Acceso consiste en no permitir al usuario el ingreso a la Red de Datos con su nombre de usuario y clave de seguridad. En caso que el incidente este afectando al resto de los activos de la RedUCLA, se procedería a la desconexión física quedando el equipo sin acceso alguno a la RedUCLA.

b. Suspensión indefinida del equipo: Esta medida se aplicará cuando se incurra en infracciones del tipo muy grave, grave o una reiterada violación de las condiciones de este documento, después de los correspondientes avisos por parte de la Dirección de Telecomunicaciones. El servicio podrá restablecerse cuando se considere que las medidas adoptadas por el responsable del activo causante del incidente garantiza un uso aceptable en el futuro.

Artículo 68
De aplicarse algunas de las suspensiones descritas en el articulo anterior, serán presentadas por la Dirección de Telecomunicaciones a través de un

informe escrito ante el Consejo Universitario a fin de aperturar un expediente disciplinario por los mismos hechos, dictar resolución de acuerdo al tipo de falta cometida y sancionar al responsable de dicha falta.

Artículo 69
En caso del incumplimiento a las normas descritas y la violación de las reglas establecidas serán sancionado con la suspensión de uso durante un semestre para toda dependencia o todo aquel personal académico o administrativo de la Institución que sean consideradas faltas muy graves, según resolución dictada por el Consejo Universitario.

Artículo 70
El incumplimiento de las normas descritas y la violación de las reglas establecidas serán sancionado con la suspensión de uso durante un mes hasta un semestre para todo aquel usuario de la Institución, que sean consideradas faltas graves, según resolución dictada por el Consejo Universitario.

Artículo 71
El incumplimiento de las normas descritas y la violación de las reglas establecidas serán sancionado con la suspensión de uso durante una semana hasta un mes para todo aquel usuario de la Institución, que sean consideradas faltas leves, según resolución dictada por el Consejo Universitario.

Artículo 72
Cualquier costo generado por el daño a la infraestructura de la RedUCLA, será pagado por los responsables de este hecho.

Artículo 73
El incumplimiento o falta muy grave que atente contra el articulado de las leyes nacionales relacionados con delito informático, serán presentado ante el Consejo Universitario a fin de formalizar la denuncia del responsable y someter la autorización para elevar el caso a las autoridades nacionales que les competa resolver estos ilícitos.

Artículo 74
Lo no previsto será resuelto por la Dirección de Telecomunicaciones y aprobado por el Consejo Universitario de la Universidad Centroccidental "Lisandro Alvarado".

Capítulo IX
Disposiciones Finales

Artículo 75
Estas normas entraran en vigencia a partir de la fecha de la aprobación por el Consejo Universitario.

Artículo 76
La Dirección de Telecomunicaciones procederá a tomar las medidas necesarias para la reestructuración de la Infraestructura Tecnológica, que le permitan modificar sus servicios e introducir los cambios que en materia de seguridad informática y de telecomunicaciones sean necesarios para asumir las atribuciones fijadas en estas normas de Seguridad.

Artículo 77
Todas las dependencias de la UCLA darán a conocer y harán cumplir a los usuarios las disposiciones establecidas en el presente documento.

Artículo 78
Lo no previsto en el presente reglamento será resuelto por el Consejo Universitario.

Procedimientos

Asignación de Nombre de Usuario y Claves para el Acceso al Correo Electrónico, Acceso al Servicio Remoto y Acceso a la REDUCLA

Objetivo

La Dirección de Telecomunicaciones proporcionará a las dependencias, al personal académico, al personal administrativo y a los estudiantes universitarios que lo soliciten, claves de correo electrónico, de acceso remoto y acceso a la RedUCLA.

Descripción Narrativa

Responsable	Actividad
El Interesado	1) Entrega la "Solicitud de inscripción a RedUCLA" en el departamento de Atención a Usuarios de la Dirección de Telecomunicaciones, presentando la siguiente información: a) Personal académico y administrativo de la UCLA: presenta el original de la Cédula de Identidad, y del Carnet de Identificación de la UCLA. b) Estudiantes: presenta el original de la Cédula de Identidad y del Carnet de estudiante de la UCLA.
Dirección de Telecomunicaciones	2) Analiza si la solicitud cubre los requisitos. Si no los cubre, se rechaza la solicitud. 3) Activa la(s) clave(s) dentro del sistema. 4) Entrega al usuario su(s) clave(s). 5) Se le solicita al usuario leer y firmar los contratos y condiciones de uso, se le entrega una copia de no estar publicadas en la página Web del servicio solicitado.

Renovación de Claves de Correo Electrónico y de Acceso Remoto o Acceso a la REDUCLA

Objetivo

La Dirección de Telecomunicaciones proporcionará a las dependencias, al personal académico, administrativo y estudiantes universitarios la renovación de las claves de correo electrónico, acceso remoto y/o acceso a RedUCLA.

Descripción Narrativa

Responsable	Actividad
Dirección de Telecomunicaciones	1) Si la clave fue asignada por un lapso de tiempo, se envía por correo electrónico la notificación de que su(s) clave(s) está(n) próxima(s) a vencer.
Interesado	2) Solicita la renovación en el Departamento de Atención a Usuarios de la Dirección de Telecomunicaciones. a) Si el interesado es personal académico o administrativo, llena la "Solicitud de renovación de claves de RedUCLA" y presenta original de la cedula de identidad y carnet de la UCLA. b) Si la renovación es solicitada por un estudiante, llena el formato de "solicitud de renovación del servicio" y presenta original de la cedula de identidad y del Carnet de Estudiante de la UCLA.
Dirección de Telecomunicaciones	3) Analiza si la solicitud cubre los requisitos. Si no los cubre, se rechaza la solicitud. 4) Renueva la(s) clave(s) dentro del sistema. 5) Entrega la información al interesado.

Condiciones de uso y Políticas de Privacidad del Servicio de Correo Electrónico Institucional (email.ucla.edu.ve) de la Universidad Centroccidental "Lisandro Alvarado"

En apoyo de los objetivos fundamentales de nuestra institución, educación e investigación, y respetando los principios de libertad de expresión y privacidad de información, se ofrece un serie de recursos y servicios de información a nuestros usuarios de la RedUCLA. Se debe reconocer que la calidad de estos servicios depende en gran medida de la responsabilidad individual de los usuarios.

Al usar la cuenta de correo email.ucla.edu.ve queda implícito que el usuario esta de acuerdo con las siguientes condiciones y políticas:

Condiciones de uso del Servicio de Correo Electrónico Institucional

I. Conocimiento y Aceptación de los Términos de Servicio

1. El Servicio de Correo Electrónico Institucional, en adelante "SERVICIO", perteneciente a la Universidad Centroccidental "Lisandro Alvarado" (UCLA) y gestionado por la Dirección de Telecomunicaciones de la UCLA, le será prestado a los Empleados Administrativos, Docentes, Investigadores y Estudiantes, en adelante "USUARIO", bajo los términos y condiciones descritos en este documento y bajo cualquier regla o política que sea presentada por la Dirección de Telecomunicaciones y aprobadas por el Consejo Universitario.

II. Descripción del Servicio:

3. La UCLA proveerá al USUARIO la capacidad de enviar y recibir correo electrónico a través de Internet por medio de su Sistema de Correo Institucional. Para el uso del Servicio, el USUARIO puede utilizar los equipos que la UCLA decida asignar para el acceso a través de la RedUCLA, o bien accederlo remotamente por medio de una conexión de algún proveedor de Servicios de Internet o por el servicio de acceso remoto que la UCLA implante. Para utilizar El SERVICIO, el USUARIO debe:
    a. Disponer del equipo necesario para establecer una conexión con Internet.

b. Disponer de acceso a Internet.

4. Esté Servicio es de uso Individual, Institucional y por ende intransferible. Es una falta grave facilitar y/o ofrecer nuestra cuenta y buzón a personas no autorizadas.

III. Obligaciones Acerca del Registro de Información del Usuario

5. Para el uso del Servicio, el USUARIO debe:

    a. Suministrar información real en la planilla de registro que se puede acceder en las opciones de email.ucla.edu.ve.

    b. Mantener actualizada dicha información anualmente.

6. Sí la información suministrada es falsa, inexacta, inapropiada o no es actualizada, la Dirección de Telecomunicaciones está en el derecho de finalizar el uso del SERVICIO por parte del USUARIO.

7. La Dirección de Telecomunicaciones se reserva el derecho de aceptar las solicitudes para usar el servicio y mantendrá la privacidad de los datos suministrados.

V. Modificaciones a los Términos de Servicio

8. La Dirección de Telecomunicaciones puede cambiar los términos y condiciones de este DOCUMENTO en cualquier momento y sometido al Consejo Universitario para su aprobación. EL USUARIO será notificado según el procedimiento que se establezca para tal caso, con la descripción de los cambios. En caso que el USUARIO este inconforme con los cambios en el DOCUMENTO, podrá prescindir del Servicio notificando a la Dirección de Telecomunicaciones usando el procedimiento diseñado para tal fin.

9. El uso continuado del SERVICIO por parte del USUARIO implica que:

    a. Conoce estas condiciones y sus modificaciones

b. Acepta estas condiciones y sus modificaciones

VI. Modificaciones al Servicio

10. La Dirección de Telecomunicaciones se reserva el derecho de modificar o descontinuar el Servicio temporal o permanentemente con o sin notificación al USUARIO. El USUARIO acepta que la Dirección de Telecomunicaciones no será responsable ante él o terceros por las modificaciones o finalización del SERVICIO y no deberá ejercer acción alguna al respecto.

VII. Política de Privacidad

11. Los servicios de correo electrónico suministrados por nuestra organización pueden ser usados de forma incidental para temas personales excepto si:

    a. Interfieren con el rendimiento del propio servicio,

    b. Interfieren en las labores propias de los gestores del servicio

    c. Suponen un alto coste para nuestra organización.

    d. Los mensajes de tipo personal están sujetas a los términos y condiciones de este documento.
    e. Comprometa las políticas de seguridad informática y de telecomunicaciones de la UCLA.

VIII. Conducta de los USUARIOS

17. El USUARIO acepta cumplir con todas las políticas internas, leyes locales, estatales, nacionales e internacionales que regulan el uso del correo electrónico y acepta no interferir con el uso y disfrute de otro USUARIO, siendo el único responsable por el contenido de sus mensajes transmitidos por medio de nuestro SERVICIO.

18. El USUARIO no usará el servicio para propósitos ilegales, interferir o destruir el servicio, servidores o redes conectadas con este SERVICIO.

19. El USUARIO no transmitirá por medio de nuestro servicio:

    a Algún material de índole inmoral, vulgar, obsceno o que de alguna forma viole las normas de la moral y las buenas costumbres.

    b Mensajes que violen la privacidad, la integridad o los derechos de persona o institución alguna. De la misma forma no podrá atacar, en forma directa o indirecta, a otro usuario de nuestro servicio.

    c Material no solicitado a nuestros usuarios o que viole alguna ley local, estatal, nacional o internacional.

    d Mensajes en forma anónima

20. La Dirección de Telecomunicaciones no se hace responsable por la transmisión y recepción de los mensajes a los usuarios fuera de nuestros servidores y SERVICIO.

21. Este SERVICIO hace uso de Internet para enviar y recibir ciertos mensajes, la conducta del USUARIO está sujeta a la regulación, políticas y procedimientos de Internet y de la Republica Bolivariana de Venezuela.

22. El Correo Electrónico es una herramienta para el intercambio de información entre personas no es un herramienta de difusión de información. Para ello existen otros canales más adecuados y efectivos, para lo que debe de ponerse en contacto con los responsables del servicio.

IX. Abuso en el Correo Electrónico

23. El USUARIO debe de ser consciente de los términos, prohibiciones y perjuicios englobados en ***Abuso en el Correo Electrónico***.

24. No es correcto enviar correo a personas que no desean recibirlo. Si le solicitan detener ésta práctica, deberá de hacerlo inmediatamente. Si la Dirección de Telecomunicaciones recibe quejas, denuncias o reclamaciones por estas prácticas se tomarán las medidas sancionadoras adecuadas.

25. Está completamente prohibido realizar cualquier abuso de los tipos definidos en el ***Abuso de Correo Electrónico***, además de cualquiera de las siguientes actividades:

    a. Utilizar el correo electrónico para cualquier propósito comercial o financiero.

    b. No se debe participar en la propagación de cartas encadenadas o participar en esquemas piramidales o temas similares.

    c. Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados para nuestra Universidad.

    d. Está prohibido falsificar las cabeceras de correo electrónico.

    e. Las cuentas de la Universidad no deben ser usadas para recoger correo de buzones de otro Proveedor Internet.

26. Estará penalizado con la cancelación del buzón, el envío a las listas de distribución masiva de mensajes que posea la Institución y que comprometan la reputación de la Universidad y cualquiera de sus dependencias o violen cualquier ley de la Republica.

X. Indemnización

27. La Dirección de Telecomunicaciones declina cualquier responsabilidad de falta de servicio por parte de terceros, por problemas técnicos, o cualquier otra causa que afecten al SERVICIO. La Dirección de

Telecomunicaciones declina cualquier responsabilidad sobre errores que se comentan en el SERVICIO ya sea de recepción, envío, fallas técnicas, de forma parcial o general.

XI. Re-venta del Servicio

28. El USUARIO no podrá revender, arrendar, u obtener lucro por el uso o el acceso de nuestro SERVICIO

XII. Almacenamiento de Mensajes

29. La Dirección de Telecomunicaciones no asume responsabilidad alguna por la eliminación, pérdida o cualquier falla o problema con los mensajes almacenados en el sistema. El USUARIO acata el establecimiento por parte de la Dirección de Telecomunicaciones, de un límite o cuotas de disco para el tamaño de la carpeta de mensajes recibidos (Inbox) y/o alguna otra carpeta creada para el almacenamiento de sus mensajes.

30. Así mismo, acepta que, los mensajes almacenados tienen un periodo de permanencia dentro del sistema establecido por la Dirección de Telecomunicaciones, el cual no será mayor a treinta (30) días, por lo tanto se recomienda tomar las previsiones del caso y realizar respaldos de la información contenida en el Servicio, hacia su computador personal u otros medios que tenga para esto.

XIII. Finalización del Servicio

31. El USUARIO acepta que la Dirección de Telecomunicaciones lo retire del SERVICIO por:

    a. Renuncia voluntaria al uso del servicio de Correo Electrónico Institucional.

    b. Si el USUARIO viola o actúa en contra de las condiciones de este DOCUMENTO

    c. Si el USUARIO viola los derechos de la Dirección de Telecomunicaciones o de algún otro USUARIO del SERVICIO.

b. Si EL USUARIO por alguna razón deja de pertenecer a la comunidad universitaria de la UCLA.

32. El USUARIO conoce y acepta que al darse por terminado el SERVICIO, la Dirección de Telecomunicaciones eliminará inmediatamente del sistema todos los archivos asociados a la cuenta del USUARIO almacenados en el SERVICIO.

XIV. Propiedad y Derechos de Contenidos

33. El USUARIO conoce y acepta que no puede reproducir, transmitir, o distribuir por medio de este SERVICIO material que este protegido por derechos de autor, registro de marca, patente o alguna ley sin la autorización expresa de su(s) autor(es). Cualquier acción que viole las normas de derecho de autor será bajo la responsabilidad del USUARIO.

XV. Términos de Garantías

34. El USUARIO acepta que el uso del SERVICIO o de algún material obtenido por medio de él, es a su propio riesgo. El SERVICIO es suministrado bajo la filosofía de "como es" y "cuando este disponible".

35. Debido a que este SERVICIO depende de factores ajenos a los administrados por la Dirección de Telecomunicaciones, tales como Acceso a Internet, Proveedores, Condiciones Técnicas, entre otros. La Dirección de Telecomunicaciones no garantiza que el SERVICIO satisfaga totalmente los requerimientos del USUARIO, que el servicio sea ininterrumpido, oportuno, seguro o libre de error, que la información obtenida por medio de él sea veraz. Así como tampoco garantiza que las transacciones de cualquier tipo serán efectivamente realizadas, ni se podrá culpar a la Dirección de Telecomunicaciones de este hecho. La Dirección de Telecomunicaciones hará sus mejores esfuerzos de gestión administrativa y técnica para mantener operativo el SERVICIO.

XVI. Límites de Responsabilidad

36. El USUARIO acepta que la Dirección de Telecomunicaciones no es responsable por algún daño accidental, directo, indirecto, o especial, como resultado del uso del SERVICIO o la imposibilidad de su uso, o por algún costo que esta situación acarree en forma directa o indirecta.

Tampoco es responsable por los costos o pagos que se deban realizar por alguna transacción o por algún servicio u operación comercial contactado a través del SERVICIO

37. La Dirección de Telecomunicaciones no se responsabiliza por los daños ocasionados, imputados o imputables a la interrupción, suspensión y/o finalización el SERVICIO.

XVIII. Notificaciones

38. Alguna notificación al USUARIO o al SERVICIO puede ser realizada por correo electrónico o por los mecanismos de comunicación regulares que proporciona la Universidad.

XIX. General

39. Los usuarios deben ser conscientes de la diferencia entre utilizar direcciones de correo electrónico suministradas por nuestra institución o las privadas ofrecidas por cualquier otro proveedor de Internet. El campo "remitente" de las cabeceras de correo indica el origen al que pertenece el emisor de un mensaje, por lo que hay que tener en cuenta las repercusiones. Las direcciones de la universidad (del tipo **<NombreUsuario>@ucla.edu.ve**) no pueden usarse para actividades privadas o actividades no relacionadas con la educación e investigación.

41. Lo no contemplado en este DOCUMENTO estará sujeto a decisión por parte de la Dirección de Telecomunicaciones.

Políticas de Privacidad del Servicio de Correo Electrónico Institucional

1. La UCLA considera que los mensajes enviados por correo electrónico vía nuestro SERVICIO será una correspondencia privada entre el emisor y el destinatario. La Dirección de Telecomunicaciones no editará o desechará el contenido de una comunicación privada del USUARIO, a menos que éste lo autorice o cumpla las siguientes condiciones:
    a. Sí es exigido por algún trámite de averiguación interna del Consejo Universitario o una solicitud judicial de la nación.

    b. Para cumplir con un proceso legal.

c. Si se presenta una violación a las políticas de seguridad del SERVICIO.

d. Para responder a reclamos sobre contenidos que infrinjan los derechos de terceros.

e. Para proteger los derechos o propiedades del Usuario o Terceros.

f. Cuando se sospeche que porta un virus informático o correo basura.

2. El USUARIO conoce y aprueba que ciertos procesos técnicos de la comunicación por correo electrónico son y pueden ser requeridos para:

   a. Enviar y recibir mensajes.

   b. Requerimientos técnicos de conectividad de la Red.

   c. Por limitación del Servicio.

   d. Por otros requerimientos técnicos.

3. El USUARIO conoce y aprueba que la Dirección de Telecomunicaciones no se responsabiliza por el contenido del o los mensajes enviados por algún USUARIO del SERVICIO, esto incluye entre otros: Mensajes obscenos, acusadores, difamatorios o amenazantes, material ofensivo, invasión de privacidad, violación de los derechos de autor o de la propiedad intelectual, portadores de virus informáticos. El USUARIO podrá realizar el reclamo correspondiente a fin de que la Dirección de Telecomunicaciones realice su mejor esfuerzo por evitar esta situación.

Cuenta, Password y Seguridad

4. El USUARIO recibe al momento de ser registrado en el sistema una cuenta (login) y una clave (password) que será usado por él para mantener la seguridad de su cuenta, siendo el único responsable de la misma. Se advierte que la clave debe ser cambiada periódicamente y que

los administradores del sistema podrán en cualquier momento monitorear dicha clave con la finalidad de advertir o notificar la simplicidad de la misma, lo cual puede facilitar la violación de la cuenta por parte de otro usuario perteneciente o no a nuestro SERVICIO. En ningún caso la Dirección de Telecomunicaciones se hace responsable por daños ocurridos en una cuenta por mal uso de la clave. El USUARIO acepta en notificar por correo electrónico inmediatamente a la Dirección de Telecomunicaciones de cualquier uso no autorizado a su cuenta, o cualquier instrucción de seguridad conocida por el USUARIO.

5. El USUARIO es el único responsable de las actividades realizadas con su cuenta.

Abuso en el Correo Electrónico

Introducción

Definimos al Abuso en Correo Electrónico como las diversas actividades que trascienden los objetivos habituales del servicio de correo y perjudican directa o indirectamente a los usuarios. Algunos de los términos habitualmente asociados en Internet a estos tipos de abuso son spamming, mail bombing, unsolicited bulk email (UBE), unsolicited commercial email (UCE), junk mail, etc., abarcando un amplio abanico de formas de difusión.

De los tipos de abuso, el que más destaca es el conocido como spam que es un término aplicado a mensajes distribuidos a una gran cantidad de destinatarios de forma indiscriminada. En la mayoría de los casos el emisor de estos mensajes es desconocido y generalmente es imposible responderlo (reply) de la forma habitual o incluso llegar a identificar una dirección de retorno correcta.

Definición de términos

El correo en Internet es procesado por máquinas o servidores de origen, de encaminamiento y de destino utilizando el estándar de correo SMTP. Los agentes implicados en la transferencia de correo son:

Operador de Origen: Es la organización responsable de la máquina que encamina el mensaje de correo hacia Internet.

Operador de Encaminamiento: Es la organización responsable de las máquinas que encaminan el mensaje de correo entre el operador de origen y el operador de destino).

Operador de Destino: Es la organización o responsable de la máquina que mantiene el control de los buzones de los destinatarios.

Emisor: Es la persona origen del mensaje. Incluso cuando el emisor es un programa o sistema operativo, habrá una o más personas que sea(n) responsable(s) del mismo.

Receptor: Es la persona que recibe el mensaje. Al igual que en el caso del receptor, puede no tratarse de una persona física, pero siempre habrá al menos un responsable más o menos directo de cada dirección de destino.

Listas de correo: Son receptores de correo que actúan distribuyendo el mensaje a un número de destinatarios. Se las puede considerar como una especie de encaminadoras de correo. Estas listas pueden ser gestionadas por una persona o por un proceso automático.

No se les considera emisores ni receptores propiamente dichos, ya que la lista no es ni el origen ni el destinatario final de los mensajes. Sin embargo, pueden considerarse como tal en algunos casos: por ejemplo, los mensajes de control enviados para darse de alta o baja de una lista, y las respuestas del servidor a dichas acciones. Incluso en esos casos hay una persona detrás del servidor: el administrador del mismo.

Tipos de abuso

Las actividades catalogadas como Abuso en Correo Electrónico se pueden clasificar en cuatro grandes grupos:

Difusión de contenido inadecuado. Contenido ilegal por naturaleza (todo el que constituya complicidad con hechos delictivos). Ejemplos: apología del terrorismo, programas piratas, pornografía infantil, amenazas, estafas, esquemas de enriquecimiento piramidal, virus o código hostil en general.

Contenido fuera de contexto en un foro temático. Pueden definir lo que es admisible: el moderador del foro, si existe; su administrador o

propietario, en caso contrario, o los usuarios del mismo en condiciones definidas previamente al establecerlo (por ejemplo, mayoría simple en una lista de correo).

Difusión a través de canales no autorizados. Uso no autorizado de una estafeta ajena para reenviar correo propio. Aunque el mensaje en sí sea legítimo, se están utilizando recursos ajenos sin su consentimiento (nada que objetar cuando se trata de una estafeta de uso público, declarada como tal).

Difusión masiva no autorizada. El uso de estafetas propias o ajenas para enviar de forma masiva publicidad o cualquier otro tipo de correo no solicitado se considera inadecuado por varios motivos, pero principalmente éste: el anunciante descarga en transmisores y destinatarios el coste de sus operaciones publicitarias, tanto si quieren como si no.

Ataques con objeto de imposibilitar o dificultar el servicio.

Dirigido a un usuario o al propio sistema de correo. En ambos casos el ataque consiste en el envío de un número alto de mensajes por segundo, o cualquier variante, que tenga el objetivo neto de paralizar el servicio por saturación de las líneas, de la capacidad de CPU del servidor, o del espacio en disco de servidor o usuario. Se puede considerar como una inversión del concepto de difusión masiva (1->n), en el sentido de que es un ataque (n->1).

En inglés estos ataques se conocen como mail bombing, y son un caso particular de denial of service (DoS). En castellano podemos llamarlos bomba de correo o saturación, siendo un caso particular de denegación de servicio.

Suscripción indiscriminada a listas de correo. Es una versión del ataque anterior, en la que de forma automatizada se suscribe a la víctima a miles de listas de correo. Dado que en este caso los ataques no vienen de una sola dirección, sino varias, son mucho más difíciles de atajar.

Problemas ocasionados

Efectos en los receptores. Los usuarios afectados por el Abuso en Correo Electrónico lo son en dos aspectos: costes económicos y costes sociales. También se debe considerar la pérdida de tiempo que suponen, y que puede entenderse como un coste económico indirecto.

Si se multiplica el coste de un mensaje a un receptor por los millones de mensajes distribuidos puede hacerse una idea de la magnitud económica, y del porcentaje mínimo de la misma que es asumido por el emisor. En lo que respecta a los costes sociales del ACE debe considerarse, aparte de la molestia u ofensa asociada a determinados contenidos, la inhibición del derecho a publicar la propia dirección en medios como News o Web por miedo a que sea capturada.

Efectos en los operadores. Los operadores de destino y encaminamiento acarrean su parte del coste: tiempo de proceso, espacio en disco, ancho de banda, y sobre todo tiempo adicional de personal dedicado a solucionar estos problemas en situaciones de saturación.

Dado, sellado y firmado en la sala de Sesiones del Consejo Universitario de la Universidad Centroccidental "Lisandro Alvarado", en su Sesión N° 1647, Ordinaria, celebrada el día veintiuno de septiembre de dos mil cinco .

Dr. Francesco Leone Durante
Rector

Prof. Nelly Velásquez Velásquez
Secretaria General