DOCUMENTOS
INSTITUCIONALES
CORPORACIÓN UNIVERSITARIA AMERICANA

POLÍTICA DE SEGURIDAD INFORMÁTICA

CORPORACIÓN UNIVERSITARIA AMERICANA
INSTITUCIÓN UNIVERSITARIA

Institución de Educación Superior sujeta a inspección y vigilancia por parte del Ministerio de Educación Nacional

Tabla de Contenido

1 OBJETIVO Y ALCANCE 3
2 GLOSARIO 5
3 PROTECCIÓN DE LA INFORMACIÓN GENERAL 5
4 CONTENIDO 6
4.1 ROLES Y RESPONSABILIDADES DE LA POLITICA DE SEGURIDAD INFORMATICA 6
4.1.1 De los Colaboradores 7
4.1.2 De los Estudiantes 8
4.1.3 De la Dirección de Sistemas de Información 8
4.1.4 Del Departamento de Virtualidad 9
4.2 DECLARACIÓN DE RESERVA DE DERECHOS 9
4.2.1 DERECHOS DE ACCESO 9
4.2.2 DERECHOS DE VIGILANCIA 9
4.2.3 Declaración de Propiedad Exclusiva 10
4.3 PROTOCOLOS DE SEGURIDAD INFORMATICA 10
4.3.1 CORREO ELECTRÓNICO 10
4.3.2 HOSPEDAJE DE PÁGINAS WEB 12
4.3.3 OTORGAMIENTO DE AVAL TÉCNICO 14
4.3.4 ANTIVIRUS CORPORATIVO 15
4.3.4.1. Administración y Operación 15
4.3.5 HOSPEDAJE DE APLICACIONES Y BASES DE DATOS 16
4.3.6 SERVICIO DE NOMBRE DE DOMINIO (DNS) 18
4.3.7 TELEFONÍA 19
4.3.8 SOPORTE TÉCNICO 21
5 NATURALEZA DEL CAMBIO 22

1 OBJETIVO Y ALCANCE

La CORPORACIÓN UNIVERSITARIA AMERICANA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los usuarios, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

El objetivo de la Política de Seguridad Informática de la Corporación Universitaria Americana consiste en establecer los criterios, directrices, estrategias y responsabilidades que le permitan a la Institución proteger su información a todos los niveles. Así como la tecnología para el procesamiento y administración de la misma.

La Política de Seguridad Informática proporciona la base para la aplicación de controles de seguridad que reduzcan los riesgos y las vulnerabilidades de los sistemas de información de la Institución, garantizando que los riesgos para la Seguridad Informática sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, eficiente y adaptada a los cambios que se produzcan en el entorno y las tecnologías de la Corporación Universitaria Americana para el funcionamiento de los programas académicos y los procesos definidos.

Este documento formaliza el compromiso de la Alta Dirección frente a la gestión de la seguridad informática y presenta de forma escrita a los usuarios de los sistemas de información el compendio normas institucionales para proteger de posibles riesgos de daño, pérdida y uso indebido de la información, los equipos y demás recursos informáticos, los cuales están en constante cambio y evolución de acuerdo con el avance de la tecnología y los requerimientos de las áreas.

Es aplicable tanto a la Dirección de sistemas de Información, la cual es el responsable designado por la Rectoría para la administración y control de los sistemas de información, por su parte este documento es extensivo a todos los colaboradores (Administrativos, Docentes, practicantes y OPS) y estudiantes que deberán comprometerse en el cumplimiento de los requisitos de la Política de Seguridad Informática y de los documentos asociados a la misma.

Esta Política aplica para todos los sistemas (Hardware y Software), entendiéndose como los computadores, redes, aplicaciones y sistemas operativos que son propiedad o son operados por la Corporación Universitaria Americana.

Con estas disposiciones la Corporación Universitaria Americana asegura y mantiene las infraestructuras de equipo, hardware, software y TIC relevantes para la gestión del conocimiento organizativo. El conocimiento existente en la Organización debe ser protegido y salvaguardado, aplicando reglas de confidencialidad y de propiedad intelectual, siempre que sea adecuado.

A continuación, se establecen 12 principios de seguridad que soportan el Sistema de Gestión de Seguridad de la Información - SGSI de LA CORPORACIÓN UNIVERSITARIA AMERICANA:

• Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.

• LA CORPORACIÓN UNIVERSITARIA AMERICANA protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

• LA CORPORACIÓN UNIVERSITARIA AMERICANA protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta.

Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

• LA CORPORACIÓN UNIVERSITARIA AMERICANA protegerá su información de las amenazas originadas por parte del personal.

• LA CORPORACIÓN UNIVERSITARIA AMERICANA protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

• LA CORPORACIÓN UNIVERSITARIA AMERICANA controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

• LA CORPORACIÓN UNIVERSITARIA AMERICANA implementará control de acceso a la información, sistemas y recursos de red.

• LA CORPORACIÓN UNIVERSITARIA AMERICANA garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

• LA CORPORACIÓN UNIVERSITARIA AMERICANA garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

• LA CORPORACIÓN UNIVERSITARIA AMERICANA garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

• LA CORPORACIÓN UNIVERSITARIA AMERICANA garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

2 GLOSARIO

TÉRMINO	DEFINICIÓN
SSL	Certificado de seguridad en la página corporativa para utilizar el protocolo de navegación seguro: https.
Derechos de Acceso	Controles de acceso y otras medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información manejada por computadores y sistemas de información de la CUA.
Derechos de Vigilancia	Restringir o revocar los privilegios de cualquier usuario. Inspeccionar, copiar, remover cualquier dato.
Dirección de Sistemas de Información – Dirección de Tecnologías de la información y las comunicaciones – TIC.	Área responsable de la plataforma tecnológica institucional: servidores, equipos, conectividad y demás componentes tecnológicos.
Firewall - cortafuegos	Genera el bloqueo al acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Los cortafuegos pueden ser implementados en hardware o software.
Usuario	Persona que tiene un vínculo con la Corporación desde diferentes roles en el sistema de información: Empleado administrativo, docente, estudiante o público en general.

3 PROTECCIÓN DE LA INFORMACIÓN GENERAL

La Corporación Universitaria Americana con la política de seguridad implementada garantiza la protección de los datos desde diferentes entornos como: utilizar la información en la red institucional o en la Internet, utilizando diferentes medios como: protocolos de seguridad de navegación, protocolos de acceso a la información con usuarios identificados y permitidos, seguridad perimetral de la red, copia de la información con la norma técnica definida y aplicando los principios en todos los entornos específicos.

3.1 REGISTRO Y AUDITORÍA

La responsabilidad del registro es del área de TIC y el seguimiento y auditoria se realiza por parte de la oficina de control interno, de la dirección de calidad con el seguimiento periódico a los procesos certificados con la norma ISO 9000 que tiene la corporación.

El almacenamiento de la información está definido en el capítulo específico, al igual que el funcionamiento de los sistemas de información y el almacenamiento de la información en las bases de datos definidas para ello.

3.2 DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN

Se tiene el procedimiento de soporte técnico que garantiza la continuidad o restablecimiento del servicio mediante la mesa de ayuda virtual o presencial garantizando los tiempos de respuesta en el servicio.

Niveles de disponibilidad: Está considerado entre 1 y 48 horas.

Plan de recuperación de la información: se tiene un modelo de copias en tres instancias: nube de cada usuario, servidor de backup local en cada sede y copia corporativa diaria.

Interrupciones: El mantenimiento preventivo de los equipos corporativos se realiza semestralmente en los horarios contrarios al uso de los equipos por parte de los usuarios

Acuerdos de Nivel de servicio: Acuerdo nivel de servicio 1: 30 minutos, Acuerdo nivel de servicio 2: 60 minutos, Acuerdo nivel de servicio 3: 48 horas.

Segregación de ambientes: se tienen los clientes o usuarios en entornos diferentes: Administrativos, docentes y estudiantes.

Gestión de Cambios: Control de cambios activo como lo define la norma ISO 9000.

4 CONTENIDO

4.1 ROLES Y RESPONSABILIDADES DE LA POLITICA DE SEGURIDAD INFORMATICA

Al aclarar las responsabilidades de los usuarios y las medidas que deben adoptar para proteger la información y los sistemas informáticos, la Corporación Universitaria Americana evita pérdidas graves o divulgación no autorizada. Por otra parte, el buen nombre de la Organización se debe en parte a la forma como protege su información y sus sistemas informáticos en todos los niveles (Directivos, Administrativos, Docentes, practicantes y terceros que tengan acceso a los sistemas informáticos institucionales), estas responsabilidades son:

4.1.1 De los Colaboradores

- Tomar conciencia de la importancia del establecimiento de la Política de Seguridad Informática, los procedimientos y la normatividad aplicable.
- Ser responsables de información Institucional, que demuestre la conformidad de sus obligaciones y trazabilidad de los procesos, deben establecer los medios que soporten la toma de decisiones (mantener, conservar, dar disposición final) con base en la información que se encuentre a su cargo.
- Ser responsables de la información, serán también los encargados de administrarla. En consonancia con lo anterior serán responsables todos aquellos que manejen información en los computadores asignados para llevar a cabo sus actividades o que tengan acceso a cualquier aplicación o sistema que sirva de apoyo a sus tareas.
- Ser responsables del correo Electrónico Institucional asignado y mantener la confidencialidad de su contraseña y la información de la cuenta, así como de todas las actividades que ocurran durante la utilización del correo. Notificar de manera inmediata si detecta el uso indebido o no autorizado de su cuenta por terceras personas.
- Son responsables por todas las actividades relacionadas con su identificación. La identificación no puede ser usada por otro individuo diferente a quien esta le fue otorgada.
- Los usuarios no deben permitir que otra persona realice labores bajo su identidad. De forma similar, los colaboradores y usuarios no deben realizar actividades bajo la identidad de alguien más. La utilización de los recursos informáticos por parte de terceras personas con conocimiento o consentimiento del usuario, o por su descuido o negligencia, lo hace responsable de los posibles daños que estas personas ocasionen a los equipos o a la propiedad de Corporación Universitaria Americana.
- Los colaboradores responsables de la información deberán almacenarla, implementar los controles de acceso (para prevenir la divulgación no autorizada) y periódicamente hacer copias de respaldo y así evitar la pérdida de información crítica utilizando los medios determinados por la Institución para tal fin.
- Los colaboradores con acceso a Internet, al acceder al servicio están aceptando que: 1. Serán sujetos de monitoreo de las actividades que realizan en Internet. 2. Existe la prohibición de acceso a páginas no autorizadas. 3. Se prohíbe la descarga de software sin la autorización del Departamento de Sistemas. 4. La utilización de Internet es para el desempeño de su función y no para propósitos personales.
- Cumplir con las responsabilidades de uso de correo electrónico definidas en el Ítem 2.3.1 del presento documento.

4.1.2 De los Estudiantes

Los estudiantes

- El uso indebido de los sistemas de información de la Universidad está prohibido
- Intentar modificar, reubicar o sustraer equipos de cómputo, software, información o periféricos sin la debida autorización.
- Transgredir o burlar las verificaciones de identidad u otros sistemas de seguridad.
- No se debe ingresar alimentos a las salas de sistemas.
- Utilizar los sistemas de información para propósitos ilegales o no autorizados.
- Descargar o publicar material ilegal, con derechos de propiedad o material nocivo usando un computador de la Institución.

El Estudiante debe dar un buen uso a los dispositivos, por lo tanto no debe:

- Propinarle golpes, rayones, etc.
- Derramarle líquidos.
- Instalar software diferente al asignado.
- Instalar o configurar dispositivos de hardware diferentes a los asignados.
- Dejarlo sin seguridad en un lugar no vigilado.
- Entre otros que deterioren la integridad del dispositivo.

4.1.3 De la Dirección de Sistemas de Información

La dirección de Sistemas de Información asegurará la integridad de la plataforma tecnológica de la Institución:

- El acceso a Internet será monitoreado por la Dirección de Sistemas de Información para asegurar el uso apropiado y el cumplimiento de las Políticas de Seguridad, las restricciones de accesibilidad a internet o a contenidos específicos serán ejecutadas por la solicitud del jefe de área o por directriz institucional. De necesitarse el acceso a una página bloqueada deberá ser autorizado por el Jefe de Área.
- Si fuera necesario leer el correo de alguien más (mientras un empleado se encuentre fuera o de vacaciones) el jefe de la respectiva área determinará a qué buzón deben ser redireccionados sus correos en su ausencia o por su parte solicitar las credenciales para la recuperación de información para los fines definidos en los procesos al área de sistemas.
- La información de los computadores debe ser periódicamente respaldada en dispositivos destinados para tal fin, para lo cual el Colaborador o Usuario que requiera según criticidad de la información realizar respaldos con apoyo del área de Sistemas deberá solicitarlo, para que este sea resguardado en los Servidores de la institución o medios magnéticos según se requiera.

- El Departamento de Sistemas es el responsable de respaldar la información contenida en los servidores de la Institución.
- El Departamento de Sistemas brindará apoyo y asistencia técnica para la instalación de software o hardware.

4.1.4 Del Departamento de Virtualidad

La dirección de Virtualidad a través de los administradores AVA o EVA asegurará la integridad de este espacio virtual de la Institución, donde los docentes pueden interactuar con los estudiantes a través de diferentes actividades, como lo son: fotos, tareas, exámenes, URL, videos, etc. como parte del proceso formativo en programas presenciales y virtuales.

El acceso a la red (AVA) será administrado por el departamento de Virtualidad a través del proveedor del servicio. En función de las necesidades y prioridades de la Institución y de la disponibilidad de recursos.

4.2 DECLARACIÓN DE RESERVA DE DERECHOS

4.2.1 DERECHOS DE ACCESO

La Corporación Universitaria Americana usa controles de acceso y otras medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información manejada por computadores y sistemas de información. Para mantener estos objetivos la Corporación Universitaria Americana se reserva el derecho y la autoridad de:

1. Restringir o revocar los privilegios de cualquier usuario;

2. Inspeccionar, copiar, remover cualquier dato, programa u otro recurso que vaya en contra de los objetivos antes planteados;

3. Tomar cualquier medida necesaria para manejar y proteger los sistemas de información de La Cámara. Esta autoridad se puede ejercer con o sin conocimiento de los usuarios, bajo la responsabilidad del comité de seguridad siempre con el concurso de la Presidencia o de quién él delegue esta función.

4.2.2 DERECHOS DE VIGILANCIA

La Dirección de Sistemas de Información, previa autorización de la Rectoría, Vicerrectorías o Jefe de área, se reservará el derecho de supervisar, monitorear e inspeccionar en cualquier momento los sistemas de información utilizados por los Colaboradores, cuando se detecte posibles

irregularidades en el manejo de la información o se requiera la realización de respaldos de la misma. Las inspecciones pueden llevarse a cabo con o sin el consentimiento y presencia del empleado involucrado.

Los Sistemas de Información sujetos a dicha inspección incluyen los registros de la actividad de los empleados: archivos y correos electrónicos institucionales y soportes físicos de la información auditada pueden ser sujetos de la misma inspección en cualquier momento. Lo anterior, sin perjuicio del respeto a la intimidad personal y a la inviolabilidad de la correspondencia y demás formas de comunicación privada en los términos del mandato constitucional.

La Corporación Universitaria Americana se reserva el derecho de retirar cualquier material o recurso que sea considerado lesivo para los intereses de la Institución o que contenga información ilegal.

4.2.3 Declaración de Propiedad Exclusiva

La Corporación Universitaria Americana tiene propiedad y derechos exclusivos sobre las patentes, derechos de autor, invenciones, programas o cualquier otra propiedad intelectual desarrollada por sus empleados en la plataforma tecnológica de la Institución.

4.3 PROTOCOLOS DE SEGURIDAD INFORMATICA

4.3.1 CORREO ELECTRÓNICO

El servicio se otorgará mediante la asignación de una dirección de correo electrónico institucional la cual se podrá acceder mediante un nombre de usuario y una contraseña asociada. Este servicio tiene como función ofrecer una herramienta de comunicación digital para la transferencia de información y documentos entre los miembros de la Comunidad Estudiantil; y con el entorno, en función a las actividades que realiza en la Institución, dentro de los lineamientos se destaca:

4.3.1.1 Administración y operación

- Se podrán otorgar cuentas de correo individuales o genéricas, según las necesidades del área.
- Para correos electrónicos de Colaboradores (Administrativos, Docentes, practicantes y OPS), el área de Talento Humano será el encargado de solicitar al Departamento de

Sistemas, tras la contratación de la persona, la creación y/o acceso al correo institucional correspondiente.

- Las cuentas de correo asignadas a los miembros de la corporación universitaria deberán ser eliminadas en caso de que la misma no haya sido utilizada en un lapso de 6 meses o más sin ningún tipo de notificación; o por requerimiento de su supervisor inmediato siguiendo los procedimientos establecidos para tal fin.
- Para los correos electrónicos de estudiantes nuevos, el área de admisiones envía listado al área de virtualidad, quien se encarga de la creación de usuarios, posteriormente es transferidos al área de sistemas quien oficializa la creación de correo y respectivas contraseñas. El estudiante visualizará a través del primer ingreso a AVA los pasos básicos de ingreso al correo.
- Para las dificultades de accesibilidad en correos electrónicos por parte del estudiante se ha dispuesto por la institución el "Servicio en línea" a través de la página web o servicio telefónico, donde el área de sistemas o a quien se delegue, da solución a los requerimientos del estudiante frente al uso correos.
- La Dirección de sistemas de información deberá notificar a los usuarios de la suspensión del servicio por razones de mantenimiento o por fallas ocurridas en la operatividad de este.

4.3.1.2 Del Usuario

- El usuario del correo Electrónico será responsable de mantener la confidencialidad de su contraseña y la información de la cuenta, así como de todas las actividades que ocurran durante la utilización del correo.
- La cuenta de correo electrónico y la clave asociada asignada es personal, intransferible y por razones de seguridad deberá ser cambiada periódicamente, se recomienda una periodicidad de 3 meses.
- Responsabilidades del Usuario: el uso del correo electrónico por parte de los usuarios deberá estar orientado a la transferencia de información de tipo Institucional, evitando:

  a) Difundir información confidencial de la Institución; b) Retransmitir o leer correos, donde se desconozca la procedencia del mismo; c) Transmitir información pornográfica o de carácter sexista; d) Enviar información referida a cualquier forma discriminatoria por razones de sexo, raza, filiación política o religiosa, minusvalía física o condición social; E) Mantener la confidencialidad de su contraseña y la información de la cuenta; f) Notificar de manera inmediata si detecta el uso indebido o no autorizado de su cuenta por terceras personas; g) Revisar y depurar su buzón de correo periódicamente, a fin de evitar que el mismo se sature.

4.3.1.3 Requisitos para optar al Servicio:

El usuario solicitante (docente Virtual, administrativo,) que no esté adscrito a la nómina de la Corporación, deberá presentar anexo a la solicitud, su constancia de trabajo o cualquier otro documento que acredite su vinculación con esta casa de estudios, avalado por su supervisor inmediato o autoridad competente, de lo contrario no será procesada la solicitud. Para procesar solicitudes de cuentas genéricas, será necesario que el oficio de solicitud venga acompañado de una exposición de motivos que justifique la utilización de la misma. El usuario deberá aceptar los acuerdos y/o compromisos asociados al servicio.

El estudiante virtual solicitante deberá indicar en la solicitud sus datos personales, el nombre de la lista y las cuentas de correo electrónicas de los integrantes que harán uso de la lista. También deberá indicar el objetivo de la lista, el tipo de lista y el tiempo de duración de la misma.

Las constancias o documentos probatorios podrán ser enviados de manera digital a través del correo electrónico o presentados de manera física en la recepción de la Dirección de sistemas de información. El estudiante virtual deberá aceptar los acuerdos y/o compromisos asociados al servicio.

4.3.2 HOSPEDAJE DE PÁGINAS WEB

Este servicio tendrá como objetivo ofrecer en servidores de la Corporación Universitaria Americana, espacio de almacenamiento y perisologías de acceso para alojar páginas web institucionales que requieran ser vistas desde la Intranet o desde Internet.

En el caso de la Dirección de Sistemas de Información, el servicio de hospedaje de páginas Web será exclusivamente para los usuarios cuya Facultad o Dependencia Central no cuentan con un servidor de páginas Web. Este servicio se brindará de acuerdo con la disponibilidad de los recursos de hardware y software en sus servidores.

4.3.2.1 Administración y operación

- La Dirección de Sistemas de Información o el Departamento de Sistemas de Información serán responsables de mantener la operatividad del servidor y atenderán las fallas que el mismo presente tanto a nivel del sistema operativo como a nivel de hardware.
- Los acuerdos o compromisos asociados al servicio deberán estar definidos, ser divulgados a la comunidad estudiantil y serán respetados para dar cumplimiento a la prestación de este de forma oportuna y correcta.
- La Dirección de Sistemas de Información o el Departamento de Sistemas de Información deberán mantener en el servidor una solución de antivirus corporativo actualizada con el fin de detectar la presencia de virus.

- La Dirección de Sistemas de Información o el Departamento de Sistemas de Información deberán asegurar a los usuarios del servicio los recursos de almacenamiento comprometidos y los respaldos de la información allí contenida.
- La Dirección de Sistemas de Información o el Departamento de Sistemas de Información, será responsable de monitorear la utilización de los recursos de hardware en el servidor. Esto con el fin de proceder a la actualización de este en el caso de ser requerido para garantizar la continuidad de los servicios.
- La Dirección de Sistemas de Información o el Departamento de Sistemas de Información notificará a los usuarios de la suspensión del servicio por razones de mantenimiento o por fallas ocurridas en la operatividad de este.

4.3.2.2 Del Usuario

- El espacio en disco asignado para el hospedaje de las páginas Web, se utilizará solo para el fin que se haya creado, por lo cual en el mismo no se podrá almacenar archivos de índole personal ni de entretenimiento como música, videos, juegos, etc.
- El usuario una vez que no requiera del servicio de hospedaje de páginas Web, deberá formalizar su retiro a través de la Dirección de Sistemas de Información o el Departamento de Sistemas de Información que provee el servicio. El usuario será responsable de verificar el buen funcionamiento de su página Web una vez que transfieran la información al servidor.
- El código de usuario y la clave de acceso asignado al administrador de la página Web será personal, confidencial e intransferible.
- El usuario deberá notificar de manera inmediata a la Dirección de Sistemas de Información o al Departamento de Sistemas de Información, si detecta el uso indebido o no autorizado de su cuenta por terceras personas.
- La Facultad o Dependencia Central notificará ante la Dirección de Sistemas de Información o al Departamento de Sistemas de Información, de cualquier cambio ocurrido con la persona responsable de la administración de su respectiva página Web, a fin de hacer los cambios correspondientes a nivel del código de usuario.
- Los usuarios del servicio deberán asegurarse de que la información a hospedar en el servidor esté libre de virus.
- Los usuarios de la Comunidad Estudiantil no podrán instalar servicios de hospedaje de página web de forma autónoma.

4.3.2.3 Requisitos para optar al Servicio:

- El usuario solicitante (docente virtual, administrativo) que no esté adscrito a la nómina de la Corporación Universitaria Americana, deberá presentar anexo a la solicitud, su constancia de trabajo o cualquier otro documento que acredite su vinculación con esta casa de estudios, de lo contrario no será procesada la solicitud. El contenido de las páginas Web objeto de la solicitud deberá ser de carácter institucional.
- La solicitud de hospedaje de una página WEB deberá venir acompañada de una justificación Institucional y debe estar avalada por la autoridad competente.
- El usuario deberá aceptar los acuerdos y/o compromisos asociados al servicio.

4.3.3 OTORGAMIENTO DE AVAL TÉCNICO

Este servicio contemplará la evaluación técnica para las adquisiciones de equipos tales como: computadores de escritorio, servidores, laptops, impresoras, scanners, video beams, entre otros; así como software y servicios TIC.

4.3.3.1 Administración y Operación

- El Departamento de Sistemas de Información deberán realizar la evaluación técnica para las adquisiciones de Equipos y Servicios de TIC de la Facultad o Dependencia Central a la cual esté adscrita.
- La Dirección de Sistemas de información a través de la División de Atención a Usuarios, deberá efectuar la evaluación técnica para las adquisiciones de Equipos y Servicios de TIC de las Dependencias Centrales que no posea el Departamento de Sistemas de Información.
- La Dirección de Sistemas de Información o el Departamento de Sistemas de Información, deberá evaluar y llevará el control de las solicitudes de acuerdo con los estándares vigentes establecidos por la Institución, a través de los organismos competentes; y seguirá las normativas del procedimiento asociado al servicio.
- El responsable de la administración del servicio deberá definir los acuerdos de servicio, divulgarlos a su comunidad y respetarlos para dar cumplimiento a la prestación de dicho servicio de forma oportuna y correcta.

4.3.3.2 Del Usuario

- Deberá tramitar toda solicitud del aval técnico para la adquisición de equipos y servicios de TIC
- Deberá tramitar el aval técnico emitido por el Departamento de Sistemas de Información, para la adquisición de Equipos y Servicios de TIC, independientemente del tipo de financiamiento que se maneje.

4.3.4 ANTIVIRUS CORPORATIVO

Este servicio ofrece una moderna tecnología con los más altos niveles de seguridad informática de última generación, que integra controles avanzados de red, protección de usuarios, aplicaciones, tráfico interno, accesos. Mejor rendimiento, seguridad y control en las estaciones de trabajo conectadas a la red de la Institución.

4.3.4.1. Administración y Operación

- Implementará mecanismos de alerta ante la presencia de virus o riesgos de seguridad y centralizar en el Departamento de Sistemas de Información la generación de informes dentro de cada Facultad y/o dependencias.
- Determina comportamientos sospechosos, lo que permite la detección de malware especialmente diseñado para esquivar las soluciones tradicionales.
- Prefiltra todo el tráfico HTTP y hace un seguimiento del tráfico sospechoso, así como de la ruta del archivo del proceso que está enviando tráfico malicioso.
- El administrador tiene la facultad de aplicar sus políticas de datos, dispositivo, aplicación y web con facilidad, gracias a la perfecta integración en el agente para estaciones y en la consola de administración.
- Elimina virus, troyanos, rootkits, programas espía y otro tipo de malware
- bloquear programas maliciosos e infecciones al identificar e impedir el puñado de técnicas y comportamientos utilizados en casi todas las vulnerabilidades.
- La comunicación instantánea y automática entre la estación de trabajo y la red advierte al sistema de lo que está detectando el firewall exactamente, lo que permite que el agente de protección de la estación utilice esa información inmediatamente para descubrir el proceso detrás de la amenaza.
- Instalará una solución de antivirus corporativo debidamente licenciada, en un servidor que permita la administración y distribución remota de las actualizaciones a todos los computadores.

- Para aquellas Facultades y/o Dependencias Centrales que brinden el servicio de correo electrónico a sus usuarios, deberán disponer de una solución de antivirus para la verificación de los correos electrónicos.
- Mantendrá a los usuarios informados mediante boletines informativos periódicos donde se alerta sobre nuevos virus y se emitirán recomendaciones para ser aplicadas en los computadores.

4.3.4.2 Del Usuario

- Estará alerta y no abrirá archivos o ejecutará programas de procedencia dudosa, tanto en anexos de correo, mensajería instantánea o Internet (ya sean vía Web o FTP). En caso de que lo descarguen, éstos no deberán ejecutarse, a menos que hayan sido analizados previamente por un software antivirus.
- Estará alerta de los correos electrónicos que reciba y desconfiará de aquellos correos de procedencia desconocida, o de un conocido con un 'Asunto' poco habitual en él, se debe comprobar su procedencia real antes de abrirlo.
- No contestará mensajes spam (publicidad no deseada), ya que al hacerlo reconfirmará su dirección de correo. De igual modo, no distribuirá cartas en cadena, ya que esto puede causar diversos efectos como la sobrecarga de la red, del servidor de correo y además la molestia de los usuarios al inundarle su buzón con muchos correos no deseados.
- En caso de presentar dudas sobre un servicio, aplicación o archivo, entre otros, se recomendará contactar al administrador de red de su Facultad y/o Dependencia Central para que tome las acciones debidas.

4.3.4.3 Requisitos para optar al servicio:

- El usuario deberá aceptar los acuerdos y/o compromisos asociados al servicio.
- Dispondrá de un servidor de Antivirus Corporativo que sea el principal de la Facultad. En el caso de las Dependencia Centrales, la Dirección de Sistemas de Información ofrecerá este servicio.

4.3.5 HOSPEDAJE DE APLICACIONES Y BASES DE DATOS

Este servicio tendrá como objetivo ofrecer espacio de almacenamiento, capacidad de procesamiento y permiso para alojar las Aplicaciones y Bases de Datos institucionales en el hosting de GO Daddy infinito o en el que la Dirección de Sistemas de Información recomiende.

Exclusivamente para las Dependencias Centrales que no cuentan con servidores para tal fin. Este servicio se brindará de acuerdo a la disponibilidad de los recursos de hardware y software en sus servidores.

4.3.5.1 Administración y operación

- La Dirección de Sistemas de Información o el Departamento de Sistemas de Información será responsable de mantener la operatividad del servidor donde se aloje las aplicaciones y bases de datos y atenderá las fallas que el mismo presente tanto a nivel del sistema operativo como a nivel de hardware.
- Se creará una cuenta de usuario para la administración de la aplicación y otra para la administración de la Base de Datos o sus equivalentes en el Departamento de Sistemas de Información.
- La Dirección de Sistemas de Información o el Departamento de Sistemas de Información informará al solicitante, en el caso de que la instalación sea satisfactoria, de la operatividad del servicio y de las responsabilidades asociadas.
- La Dirección de Sistemas de Información y/o el Departamento de Sistemas de Información serán responsables de monitorear la utilización de los recursos de hardware en los servidores. Esto con el fin de proceder a la actualización de los servidores en el caso de ser requerido para garantizar la continuidad de los servicios.
- Los acuerdos o compromisos asociados al servicio deberán estar definidos, ser divulgados a la comunidad universitaria y ser respetados para dar cumplimiento a la prestación del mismo de forma oportuna y correcta.
- La Dirección de Sistemas de Información o el Departamento de Sistemas de Información notificará a los usuarios de la suspensión de los servicios por razones de mantenimiento o por fallas ocurridas en la operatividad de los mismos.

4.3.5.2 Del Usuario

- Deberán hacer uso de este servicio para realizar actividades propias o directamente relacionadas con las funciones de la Institución: Docencia, Investigación y Extensión. En caso de hacer uso del mismo por razones personales, una vez autorizado por su supervisor inmediato, deberá hacerlo fuera de su horario de trabajo.
- Respetará las restricciones de acceso a páginas Web que indique el Departamento de Sistemas de Información o la Dirección de Sistemas de Información.

- En caso de requerir el acceso a alguna página bloqueada, deberá justificarlo y solicitar el desbloqueo al Departamento de Sistemas de Información o la Dirección de Sistemas de Información.

4.3.5.3 Requisitos para optar al Servicio:

- Los usuarios tendrán acceso a este servicio siempre y cuando sea aprobado por la autoridad competente de la Dependencia Central o Facultad, a través de un equipo con características óptimas y con conexión a la red, para su buen uso y funcionamiento.
- Tramitará la aprobación de casos excepcionales a las normas, debidamente justificados para su posterior autorización por parte de la Dirección de Sistemas de Información o la autoridad competente.

4.3.6 SERVICIO DE NOMBRE DE DOMINIO (DNS)

El servicio de nombres DNS de nuestra Institución permite asociar direcciones IP en el rango asignado a cada sede de la Corporación Universitaria Americana.

El correcto funcionamiento del servicio de nombres es fundamental en el funcionamiento de la redes, siendo necesario seguir unas reglas a la hora de asignar nombres para conseguir este fin.

Este servicio será exclusivamente para los usuarios de las Dependencias Centrales que no cuentan con un servidor de DNS. En las Facultades esté servicio será administrado por el Departamento de Sistemas de Información respectivamente.

4.3.6.1 Administración y Operación

- La Dirección de Sistemas de Información será la responsable de administrar este servicio de DNS.
- La Dirección de Sistemas de Información o el Departamento de Sistemas de Información será responsable de mantener la operatividad del servidor donde se aloje el servicio de DNS y atenderá las fallas que el mismo presente tanto a nivel del sistema operativo como a nivel de hardware.
- La Dirección de Sistemas de Información o el Departamento de Sistemas de Información verificara que la dirección IP correspondiente para cada facultad, Dpto. y sede pertenezca al espacio de direcciones reservado por los servidores.

- Los acuerdos o compromisos asociados al servicio deberán estar definidos y ser respetados para dar cumplimiento a la prestación del mismo de forma oportuna y correcta por los usuarios del servicio.
- La Dirección de Sistemas de Información o el Departamento de Sistemas de Información, será responsable de monitorear la utilización de los recursos de hardware en el servidor. Esto con el fin de proceder a la actualización del mismo en el caso de ser requerido para garantizar la continuidad de los servicios.
- La Dirección de Sistemas de Información y/o el Departamento de Sistemas de Información notificará a los usuarios de la suspensión del servicio por razones de mantenimiento o por fallas ocurridas en la operatividad del mismo.

4.3.7 TELEFONÍA

Este servicio tendrá como función ofrecer a los miembros de la comunidad estudiantil la posibilidad de comunicarse interna o externamente mediante el sistema de telefonía de la Corporación Universitaria Americana que es basado bajo la plataforma Asterisk (open source) el cual incluye:

1. La asignación / configuración de extensiones telefónicas IP o Softphone.
2. La asignación, traslado o mudanza de aparatos telefónicos,
3. La eliminación de extensiones telefónicas análogas.

Este servicio se ofrecerá de acuerdo a perfiles predefinidos que permiten realizar llamadas:

1. Internas
2. Locales
3. Nacionales

La asignación de aparato telefónico dependerá de la disponibilidad de estos equipos que tenga la Dirección de Tecnología de Información y Comunicaciones (Dirección de Sistemas de Información) al momento de la solicitud. En caso contrario, si el Dpto. de Sistemas no dispone de este recurso, el solicitante (Administrativo, Docente o Portería), debe remitirle a su jefe de Área o Facultad para dicho procedimiento, siempre y cuando este dentro del presupuesto asignado.

Los aparatos telefónicos serán un recurso que la Institución pone a disposición de los usuarios para facilitar el desarrollo de sus funciones. En este sentido como se indica en las Políticas Generales descritas en este documento, los recursos son propiedad de la institución y no de la persona a quién fue asignada para su uso.

4.3.7.1 Administración y Operación

- Velará por el uso racional del servicio telefónico.
- Divulgará y velará por el cumplimiento de las presentes normativas.
- Proveerá y mantendrá la infraestructura necesaria para la disponibilidad del servicio, en ocasiones en conjunto con las Facultades y Dependencias Centrales.
- Administrará y gestionará el uso de las extensiones telefónicas y las configuraciones asociadas para planificar el crecimiento futuro, así como para atender oportunamente las averías y/o cambio de perfil de usuario.
- Brindará soporte técnico a los usuarios del servicio telefónico.
- Mantendrá un inventario de los aparatos telefónicos para la administración, reposición, detección de necesidades y resguardo de los bienes de la Institución.

4.3.7.2 Del Usuario

- El usuario será responsable del uso que se le dé a la extensión telefónica que le fue asignada, independientemente de que terceras personas hagan uso indebido de su extensión.
- El usuario será responsable del equipamiento telefónico que le ha sido asignado.
- Notificará a la Dirección de Sistemas de Información cualquier anomalía en el servicio telefónico.
- Notificará a la Dirección de Sistemas de Información la desincorporación o cambio de personal en sus funciones a fin de actualizar la Base de Datos de usuarios del servicio telefónico y poder eliminar el servicio o modificar el perfil.

4.3.7.3 Requisitos para optar al Servicio:

- El usuario solicitante (Docente, Administrativo, o Portería) que no esté adscrito a la nómina de la Corporación Universitaria Americana y avalado por su supervisor inmediato o autoridad competente, no será procesada la solicitud.
- En el caso de una instalación o modificación, la solicitud deberá incluir el perfil que será asignado al usuario/extensión y deberá contar con la aprobación de la autoridad de la Facultad o Dependencia Central o en quién ésta delegue para estas funciones.
- El Usuario para obtener este servicio debe tener un puesto de trabajo con conexión a la red de la Institución, ya que esta nueva tecnología funciona con configuración IP.
- Si el usuario requiere servicios como: hacer llamadas Nacionales, llamadas a celulares; el jefe de área o facultad debe solicitar a Dpto. de Talento Humano este servicio, y una vez aprobado, La Dirección de Sistemas de Información o el Departamento de Sistemas de

Información se encargara de la configuración de la Extensión a través de la plataforma Asterisk para habilitar el servicio.

4.3.8 SOPORTE TÉCNICO

Este servicio tiene como objetivo la prevención y/o solución de problemas técnicos de:

- Hardware: Impresoras, teléfonos, portátiles, computadores, videobeam, entre otros.
- Software: Aplicaciones institucionales, sistemas operativos, software ofimáticos, entre otros.
- Redes: cableado estructurado e interconectividad de redes.

4.3.8.1 Administración y Operación

- El Departamento de Sistemas de Información o la Dirección de Sistemas de Información a través del personal de soporte técnico atenderá cada solicitud de servicio a su comunidad de usuarios finales. Cada soporte que se realice, se registrará como evidencia en un formato o documento con la finalidad de registrar, documentar y gestionar cada uno de los casos que requieran atención, lo cual contribuirá a controlar y mejorar la prestación de este tipo de servicios.
- Se deberá trabajar con la Planilla de Atención a Usuarios donde se documentará brevemente el caso y las acciones que se realizaron para atenderlo, y la misma deberá ser firmada como señal de conformidad en relación al soporte técnico prestado.
- El Departamento de Sistemas de Información o la Dirección de Sistemas de Información prestará soporte técnico a nivel de aplicaciones que sean consideradas como herramientas estrictamente institucionales o que se requieran para el desarrollo de sus funciones, debidamente justificadas por el supervisor inmediato. Es bueno acotar que el soporte técnico de estas aplicaciones estará sujeto a la experticia que posea el personal del Departamento de Sistemas de Información o de la Dirección de Sistemas de Información.

4.3.8.2 Del Usuario

- El usuario deberá formalizar su solicitud de servicio a través de correo electrónico, vía telefónica o dirigirse personalmente al Departamento de Sistemas.
- Cualquier solicitud de traslado de equipo o préstamo del mismo a otro lugar que no sea la institución, deberá ser diligenciado y firmado por el usuario (Docente, Administrativo) por

medio de un acta de entrega diligenciada por el Departamento de Sistemas donde evidenciara que este equipo le pertenece a la Institución.

4.3.8.3 Requisitos para optar al Servicio:

- El usuario solicitante podrá ser cualquier miembro de la Comunidad Estudiantil, ya sea personal docente, administrativo, que tenga asignado un equipo por la Facultad o Dependencia Central, para realizar sus actividades de carácter estrictamente institucional.

5 NATURALEZA DEL CAMBIO

Versión	Naturaleza del Cambio	Fecha
1.0	Creación del procedimiento para Sede Barranquilla	30/03/2016
2.0	Actualización de política, cambio de plantilla a partir de recomendaciones de auditoria interna.	29/09/2019
3.0	**En el ítem 1. Objetivo y Alcance** se adiciona: La CORPORACIÓN UNIVERSITARIA AMERICANA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los usuarios, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad. Se establecen 12 principios de seguridad que soportan el Sistema de Gestión de Seguridad de la Información - SGSI de La Corporación Universitaria Americana, pág. **Se adiciona el ítem 2**. Glosario **Se adiciona el ítem 3**. Protección de la información general – 3.1 Registro y Auditoría – Disponibilidad del Servicio e información	4/11/2020

Elaboró	Revisó	Aprobó
Coordinador Soporte Técnico	Director de Planeación	Rectora