Tecnológico de Antioquia
Institución Universitaria

Tecnológico de Antioquia
Institución Universitaria

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES

PRESENTADO POR:

COMITÉ DE INFORMÁTICA

Medellín

2016

Calle 78B Nº 72A 220 A.A. 011421 Medellín - Colombia
Conmutador: 444 37 00 Fax: 442 29 29
www.tdea.edu.co

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES

Actualmente, la información es considerada como el activo más importante de las organizaciones, lo que exige, entonces, un gran compromiso de la alta dirección para diseñar y aplicar políticas, cuyo objetivo sea el de proteger y salvaguardar este recurso y hacerlas más productivas. Dichas políticas son pensadas en la norma ISO 27001 de los Sistemas de Gestión de Seguridad de la Información.

Las políticas que se describen a continuación, deben ser parte fundamental del contrato y de estricto cumplimiento.

Las políticas que se proponen en este anexo, tienen presentes los cuatro pilares de la seguridad informática:

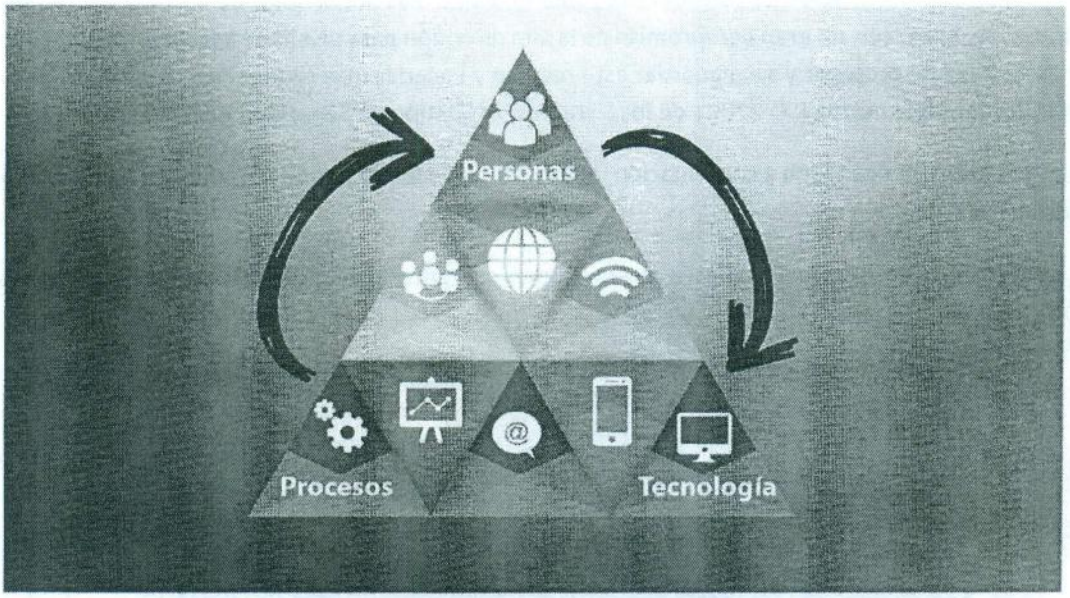
Disponibilidad: Que la información esté siempre disponible, teniendo en cuenta las variables de tiempo, lugar y oportunidad.

Confidencialidad: Que sólo sea accedida por las personas o sistemas autorizados, y que en su transmisión no sea interceptada ni vulnerada.

Integridad: Que no sea modificada, ni en su almacenamiento, ni en su transmisión.

No repudio: Garantizar que no se pueda negar algo que se hizo en los sistemas de información, archivos y demás información que está en medio digital.

De igual forma, tener en cuenta para todo proyecto de inversión, adecuación o asimilación de tecnología, que son importantes los tres pilares que se describen a continuación:



Es claro que, para que la política se cumpla a cabalidad, se requiere de compromiso de las personas, siendo éstas las más importantes en el proceso de asimilación de las mismas.

¿Por qué diseñar políticas de seguridad de la información y telecomunicaciones?

1. Para hacer cumplir normativas legales y cuidar el buen nombre de la Institución y de sus miembros.
2. Indicar qué se puede y qué no hacer con los recursos que la Institución asigna a las personas.
3. Clarificar responsabilidades y deberes con respecto a la información que se genera en la Institución.
4. Tener claro el concepto de propiedad intelectual de la información generada en la Institución.

Con la Política de Seguridad de la Información y las Telecomunicaciones se dan pautas para el buen manejo de la información institucional y el acceso a las telecomunicaciones, de tal forma que se minimicen los riesgos de: revelación, alteración, violación o borrado de la misma; de igual manera, se debe tener los recursos tecnológicos que la Institución disponga para el normal desarrollo de sus actividades académicas, administrativas, técnicas y legales.

Se considera información para efectos de la política, lo dicho o escrito, informes, conocimiento y datos, que se comunican o transmiten por medio de comunicación oral o escrita y por medios

LÍDER DE SEGURIDAD DE LA INFORMACIÓN Y DE LAS TELECOMUNICACIONES

Es la persona responsable de asegurar la implantación, mejora, mantenimiento, verificación y cumplimiento de la Política de Seguridad de la Información de la organización y los medios requeridos para lograrlo. Uno de estos medios es la realización de un Modelo de Seguridad de la Información Corporativo, del cual se debe velar por su correcto desarrollo, mantenimiento e implantación. También, apoyará a la Institución y la representará interna y externamente en todo lo referente al tema de Seguridad de la Información.

Es responsabilidad del líder de seguridad de la información definir las estrategias de capacitación en materia de seguridad de la información al interior de la Institución.

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Y DE LAS TELECOMUNICACIONES

Es el responsable de revisar y proponer a las directivas institucionales, para su aprobación, el texto de la Política de Seguridad de la Información, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejora del Sistema de Gestión de Seguridad de la Institución.

Las funciones de dicho comité serán asumidas por el Comité de Informática del Tecnológico de Antioquia, y un representante de la oficina Jurídica.

RESPONSABLE DE LA INFORMACIÓN

Es la persona que emite o recibe la información, propia de su cargo y que se constituye en un insumo para cumplir con el objetivo de sus funciones, y tiene la responsabilidad de administrarla y clasificarla, de acuerdo con su valor y criticidad. También, debe implantar la Política de Seguridad de la Información y de las telecomunicaciones dentro de su área.

USUARIOS

Son los responsables de proteger los activos de información de la Institución por medio del cumplimiento de la Política de Seguridad de Información y las Telecomunicaciones y estar alerta para identificar y reportar cualquier incumplimiento o falta de las normas o procedimientos establecidos.

CUMPLIMIENTO Y MANEJO DE VIOLACIONES A LA POLÍTICA

La Política de Seguridad de la Información y las Telecomunicaciones con sus respectivas normas es de cumplimiento obligatorio. Cada usuario debe entender su rol y asumir su responsabilidad respeto a los riesgos en seguridad de la información y la protección de los activos de información de la Institución. Cualquier incumplimiento de esta política que comprometa la integridad, confidencialidad, disponibilidad y/o privacidad de la información resultará en una acción

disciplinaria como al establecimiento de todas las acciones legales que sean pertinentes y establecidas para esas conductas.

La Política de Seguridad de la Información y de las Telecomunicaciones está basada en las mejores prácticas, y es acorde con la legislación nacional e internacional en los países que opere.

ADMINISTRACIÓN DE LA POLÍTICA Y PROCEDIMIENTO DE CAMBIO

La Política de Seguridad de la Información y las Telecomunicaciones se ha diseñado para que perdure en el tiempo, no obstante, debe revisarse semestralmente o frente a cambios estructurales que afecten a la Institución, para asegurar que cumple con la realidad. El Líder de Seguridad de la Información de la organización es responsable por esta tarea.

Cualquier usuario puede identificar la necesidad de modificar la política. Para hacer efectivo este requerimiento debe comunicar sus inquietudes al Líder de Seguridad de la Información de la Institución, responsable por el mantenimiento de la misma.

Ante la necesidad de una adición o cambio a la política, el Líder de Seguridad de la Información y las Telecomunicaciones de la Institución la procesará y enviará para el correspondiente estudio y de ser pertinente para la aprobación por parte del Comité de Informática con un representando de la coordinación Jurídica de la Institución. La formalización de la nueva política de Seguridad de la Información y las Telecomunicaciones será realizada mediante la aprobación en el Sistema Integrado de Calidad, con acto administrativo por parte de la Rectoria.

Serán la Rectoría y la alta Dirección las que decidan las acciones a tomar en el caso de incumplimiento de la presente política una vez establecidas las repercusiones que sobre los recursos y servicios informáticos haya podido tener la violación de la misma. Todo ello, sin perjuicio de las acciones disciplinarias, administrativas, civiles o penales que en su caso correspondan, a las personas presuntamente implicadas en dicho incumplimiento.

1. SEGURIDAD DE LA INFORMACIÓN

ALCANCE

La Política de Seguridad de la Información y las Telecomunicaciones para el Tecnológico de Antioquia presenta las orientaciones generales para implementar un modelo de seguridad de la información confiable y flexible; define el marco básico de cualquier norma, proceso, procedimiento, estándar y/o acción, relacionados con el manejo de la seguridad de la información.

Esta política aplica para todos los niveles de la Institución: empleados, docentes, estudiantes, egresados, terceros y proveedores, que acceden, ya sea interna o externamente, a cualquier activo de información, independiente de su ubicación. Adicionalmente, la presente política aplica para

toda la información creada, procesada o utilizada como soporte a las actividades académicas y administrativas, cualquiera sea el medio, formato, presentación o lugar en el cual se encuentre.

La Política de Seguridad de la Información del Tecnológico de Antioquia, se constituye en una serie de mejores prácticas para el manejo de la información generada y trasmitida en la Institución, para la cual la información es considerada uno de sus activos más importantes.

OBJETIVO GENERAL

Brindar orientaciones generales en cuanto al manejo de la información generada en el Tecnológico de Antioquia, con el fin de prevenir modificaciones no planeadas, realizadas con o sin intención, que sea accedida sólo por las personas dueñas y para fines exclusivos de la actividad propia de la misma Institución, y que esté disponible siempre, sin importar tiempo y lugar.

OBJETIVOS ESPECÍFICOS

a. Orientar a las personas vinculadas con el Tecnológico de Antioquia, sobre el uso de la información generada en la Institución.

b. Comunicar a las personas vinculadas con el Tecnológico de Antioquia, los cuidados, y formas de *backups* de la información de sus equipos en la Institución.

c. Definir la conducta a seguir en lo relacionado con el acceso, uso, manejo y administración de los recursos tecnológicos suministrados por el Tecnológico de Antioquia para el normal desarrollo de sus actividades académicas y administrativas.

d. Establecer y comunicar la responsabilidad en el uso de los activos de información, que soportan el conocimiento, procesos y sistemas del Tecnológico de Antioquia.

e. Establecer los canales de comunicación que le permitan a la Rectoría y a la comunidad mantenerse informados de los riesgos y uso inadecuado de los activos de información, así como las acciones tomadas para su mitigación y corrección.

f. Mantener el buen nombre del Tecnológico de Antioquia.

LINEAMIENTOS

a. La información de la Institución, de los clientes, proveedores y contratistas es un activo muy importante para el Tecnológico de Antioquia, por lo tanto, debe ser protegida permanentemente, garantizando su disponibilidad y confidencialidad.

b. Cada persona que tenga acceso a un sistema de información o que manipule información institucional local en los equipos dispuestos para tal fin, debe contar con un acuerdo de confidencialidad firmado.

c. Cada líder de proceso tendrá un espacio en los servidores del Tecnológico de Antioquia donde debe guardar periódicamente la información generada en su proceso.

d. No se permite información de tipo personal en los recursos dispuestos por el Tecnológico de Antioquia; ésta es para las funciones propias del cargo que desempeña.

e. Los riesgos a que está expuesta la información deben ser identificados, evaluados y mitigados para garantizar la continuidad de sus actividades sustanciales.

f. El Tecnológico de Antioquia implementará un plan permanente de capacitación y transformación de la cultura de seguridad de la información.

g. Los empleados, docentes, egresados, estudiantes, clientes y usuarios que utilizan local o remotamente recursos de información del Tecnológico de Antioquia deben cumplir con la Política de Seguridad de la Información.

h. La información del Tecnológico de Antioquia será utilizada únicamente para los fines que fue obtenida.

i. Los planes de continuidad deben contemplar mecanismos de contingencia y acciones de recuperación ante desastres, para mantener los niveles de disponibilidad exigidos por el Tecnológico de Antioquia.

j. La información debe preservarse, de tal forma que se garantice disponibilidad y confidencialidad, a través de mecanismos de replicación y previa valoración de la importancia de la misma.

k. Cada empleado de la Institución, debe suministrar la información propia de su cargo a quien sea necesario, en caso de un traslado o desvinculación de la misma.

l. El Tecnológico de Antioquia debe vigilar el cumplimiento de la presente política y cuando exista una violación informarla de inmediato al Líder de Seguridad de la Información.

RECOMENDACIONES

a. Guardar con regularidad la información institucional en los servidores dispuesto para tal fin, con el objetivo de mantener actualizada su información.

EXCEPCIONES A LA POLÍTICA

No se aceptan excepciones a la definición de la Política de Seguridad de la Información.

2. GESTIÓN DE USUARIOS Y CONTRASEÑAS

ALCANCE

Las contraseñas son un aspecto fundamental de la seguridad para el acceso a los recursos informáticos de información y telecomunicaciones; es la primera línea de protección. Una contraseña mal elegida o protegida puede resultar en un riesgo de seguridad para todo el

Tecnológico de Antioquia. Por ello, todos los usuarios de la red del Tecnológico de Antioquia son responsables de velar por la seguridad de las contraseñas seleccionadas por ellos mismos con las recomendaciones dadas en la política para el uso de los distintos servicios ofrecidos a la comunidad universitaria.

La seguridad provista por una contraseña depende de que la misma se mantenga siempre en secreto; todas las directrices suministradas por esta política tienen por objetivo mantener esta característica fundamental en las contraseñas de los recursos de tecnología.

El ámbito de esta política incluye a todos aquellos usuarios de los servicios y recursos informáticos del Tecnológico de Antioquia que tienen o son responsables de una cuenta de usuario o cualquier otro tipo de acceso que requiera una contraseña en cualquiera de los sistemas del Tecnológico de Antioquia.

OBJETIVO GENERAL

Establecer un estándar para la creación de contraseñas seguras y la protección de dichas contraseñas, y el cambio frecuente de las mismas.

OBEJETIVOS ESPECÍFICOS

a. Brindar orientaciones generales sobre cómo crear una contraseña segura y cómo cambiarla periódicamente.

b. Dar recomendaciones en la forma cómo se debe proteger las contraseñas y la frecuencia de cambio de las mismas.

LINEAMIENTOS

a. Todas las contraseñas de sistema (*root*, administradores de servidores, cuentas de administración de aplicaciones, etc.) deben ser cambiadas al menos una vez cada dos mes.

b. Todas las contraseñas de usuario (cuentas de usuarios del dominio, cuentas de email, cuentas de servicios web, etc.) deben ser cambiadas al menos una vez cada dos meses y cumplir con el mínimo de complejidad

c. Las contraseñas no deben ser incluidas en mensajes de correo electrónico, ni ningún otro medio de comunicación electrónica.

d. Tampoco deben ser comunicadas las contraseñas en conversaciones telefónicas.

e. Las contraseñas serán generadas automáticamente con las características recomendadas en esta política y se les comunicará a los usuarios su contraseña siempre en estado "Cambio en el próximo inicio de sección" para obligar al usuario a cambiarla en el primer uso que haga de la cuenta o servicio.

f. No se deben utilizar contraseñas que sean palabras (aunque sean extranjeras), o nombres (el del usuario, personajes de ficción, miembros de la familia, mascotas, marcas, ciudades, lugares, u otro relacionado).

g. No se deben usar contraseñas completamente numéricas con algún significado (teléfono, D.N.I., fecha de nacimiento, placa del automóvil, etc.).

h. Se debe elegir una contraseña que mezcle caracteres alfabéticos (mayúsculas y minúsculas), numéricos y caracteres especiales (/ * @ etc).

i. Deben contener como mínimo 8 caracteres con las combinaciones descritas anteriormente.

j. Se debe tener contraseñas diferentes en máquinas diferentes. Es posible usar una contraseña base y ciertas variaciones lógicas de la misma para distintas máquinas.

k. Por ninguna razón la contraseña debe compartirse con otro usuario.

l. No se permite ninguna cuenta sin contraseña.

m. No se mantienen contraseñas por defecto de ningún sistema de información o telecomunicaciones.

n. No se debe teclear la contraseña si hay alguien mirando. Es una norma tácita de buen usuario no mirar el teclado mientras alguien teclea su contraseña.

o. El sistema restringirá a 10 el uso de contraseñas repetidas.

RECOMENDACIONES

a. Cambiar la contraseña con mayor frecuencia y también siempre que el usuario sospeche que la seguridad de su contraseña pueda haber sido comprometida.

b. Combinar palabras cortas con algún número o carácter de puntuación: soy2_yo3

c. Usar un acrónimo de alguna frase fácil de recordar: A r io R evuelto G anancia d e P escadores -> ArRGdP

d. Añadir un número al acrónimo para mayor seguridad: A9r7R5G3d1P

e. Mejor incluso si la frase no es conocida: H a sta A h ora n o h e O l vidado m i C o ntraseña -> aHoello

f. Elegir una palabra sin sentido, aunque pronunciable: taChunda72, AtajulH, Wen2Mar

g. No utilice la característica de "Recordar Contraseña" existente en algunas aplicaciones (Outlook, Netscape, Internet Explorer).

h. Si alguien le pide la contraseña, refiérale a este documento o pídale que se comunique con la Unidad de Tecnología del Tecnológico de Antioquia.

i. Si sospecha que una cuenta o su contraseña pueden haber sido comprometida, cámbiela inmediatamente o comuníquese con la Unidad de Tecnología del Tecnológico de Antioquia.

EXCEPCIONES A LA POLÍTICA

No se aceptan excepciones a la definición de la Política de Gestión de Usuarios y Contraseñas.

3. USO DE INTERNET, CORREO ELECTRÓNICO Y MENSAJERÍA INSTANTÁNEA

ALCANCE

Hoy en día, es una necesidad la utilización de internet y el correo electrónico, junto con la mensajería instantánea, ya que acorta caminos, propicia la agilidad en las respuestas y en las comunicaciones, y ayuda a las instituciones a proyectarse en el medio. Internet es una excelente herramienta para mejorar la operatividad de todo negocio, crear nuevos productos o servicios, abrir nuevos mercados, sobre todo y, en definitiva, mejorar los procesos de comunicación institucional. Pero como tal, es un medio que como puede ayudar a proyectar un negocio puede llevar a las personas a incurrir en el desaprovechamiento de tiempo y recursos, lo que implica que se deben implementar controles que propicien un mejor uso de esta tecnología.

OBJETIVO GENERAL

Brindar orientaciones generales sobre lo que se puede o no hacer en internet con los recursos que entrega la Institución a sus funcionarios.

OBJETIVOS ESPECÍFICOS

a. Recomendar las mejores prácticas sobre el uso de Internet.
b. Dar directrices sobre la utilización del correo electrónico.
c. Orientar sobre la utilización de la mensajería instantánea.

LINEAMIENTOS

a. El uso de la información electrónica contenida en la mensajería debe cumplir con las Políticas de Seguridad de la Información y las Telecomunicaciones. Por lo anterior, los usuarios de los servicios de mensajería electrónica son los responsables del contenido de las comunicaciones enviadas y recibidas.
b. Está prohibido el envío de información confidencial al exterior sin previa autorización del dueño.
c. Está prohibido utilizar el servicio de correo electrónico o mensajerías instantánea para algún [illegible] acoso, difamación, calumnia, burlas, sátiras, epígrafes, sarcasmos, ultrajes,

amenazas con intención de intimidar, insultar o cualquier otra forma de actividad hostil para deshonrar a una persona.

d. Está prohibida la suplantación, el enmascaramiento o la firma de otro usuario en el uso de cualquier recurso de información.

e. Está prohibida la replicación de mensajes que son exclusivos para una persona en particular o de advertencias públicas hacia otros usuarios.

f. Está prohibido el envío de mensajes cadena, pornografía, mensajes no solicitados y bromas.

g. Los mensajes que son dirigidos a toda la organización con un fin específico solo podrán ser enviados por Comunicaciones, Talento Humano, Vicerrectoria y Rectoria.

h. Las personas no tendrán autorización para ingresar a páginas de ocio y pornografía o cualquier otra página prohibida por la ley.

i. Los líderes de procesos, podrán determinar quiénes tendrán o no acceso a internet en horarios laborales.

j. La Institución contará con un sistema de protección perimetral, que proteja la navegación en internet y los mensajes de correo electrónico entrantes y salientes, contra virus, *malware*, *spam* y otros medios de ataque a los sistemas de cómputo y de información.

RECOMENDACIONES

a. No ingrese a sitios de ocio y pornografía, son estos los que más virus y *malware* propagan en equipos de cómputo y redes, poniendo en riesgo la seguridad del sistema.

b. No abra mensajes de correo electrónico de personas extrañas y con archivos adjuntos de dudosa procedencia.

c. No responda a mensajes de correo electrónico que solicitan datos personales.

d. Utilice contraseñas complejas.

EXCEPCIONES A LA POLÍTICA

No se aceptan excepciones a la definición de la política.

4. USO DE LOS RECURSOS TECNOLÓGICOS

ALCANCE

Los equipos de cómputo y recursos de información, son de vital importancia para la operación de los diferentes procesos de la institución. La Entidad, dentro de sus políticas de inversión, se ha propuesto entregar los mejores recursos a sus empleados, estudiantes y docentes, para ayudar a

que sus funciones y procesos sean llevados a cabo eficiente y eficazmente. Esto implica, además, controles para que su utilización sea acorde con las necesidades y políticas anteriormente descritas.

OBJETIVO GENERAL

Brindar orientaciones generales sobre la utilización de los recursos de cómputo y de información, para lograr su máximo aprovechamiento y cuidar el buen nombre de la Institución.

OBJETIVOS ESPECÍFICOS

a. Dar directrices sobre la utilización de los equipos de cómputo, y sistemas de información.
b. Orientar sobre lo que se debe o no instalar en los equipos de computo

LINEAMIENTOS

a. Los recursos de cómputo y de información son provistos a sus funcionarios y proveedores para el uso exclusivo del Tecnológico de Antioquia.
b. La propiedad intelectual sobre patentes, derechos de autor, invenciones o información, permanecerá en el Tecnológico de Antioquia; de igual forma, la Institución respetará los derechos de autor y licencias de uso, para lo cual solamente software aprobado, probado y autorizado debe ser instalado en los equipos y sistemas del Tecnológico de Antioquia.
c. El área técnica será la encargada de instalar o desinstalar software, y de revisar periódicamente el software instalado en los equipos de cómputo y reportando el software instalado no autorizado al líder del proceso de las TIC, quien llevará el informe al comité de informática con un representante de la oficina Jurídica.
d. Con el fin de cuidar el buen nombre de la Institución, y siendo respetuosos de las leyes sobre derechos de autor y demás temas legales y de licenciamiento, se prohíbe la instalación y la utilización de software ilegal o no licenciado.
e. No se permite la utilización de los recursos de cómputo o información dispuestos por la Institución, para trabajos o asuntos personales.
f. Se prohíbe copiar por la red de la Institución y almacenar información personal en los equipos de cómputo o recursos de información, tales como música, videos, fotos, documentos, entre otros.
g. No está permitido la conexión de equipos y software diferentes a los dispuestos por la Institución como son: Access Point, software de escaneo de red y de vulnerabilidades, scanner, impresoras, entre otros.
h. Se prohíbe la desconexión de la red de un equipo institucional para conectar un equipo personal.

RECOMENDACIONES

a. Desconecte los equipos de cómputo cuando no vaya a trabajar en ellos por largos períodos de tiempo. Con esto se evita que el equipo se dañe por alguna descarga eléctrica y se aporta a la protección con el medio ambiente.
b. Apague los equipos o pantallas cuando salga a almorzar o a reuniones.
c. No permita que personas ajenas a la Institución, utilice sus recursos tecnológicos.

EXCEPCIONES A LA POLÍTICA

No se aceptan excepciones a la definición de la política de Seguridad de la Información.

Integrantes Comité de Informática

CARLOS ALBERTO CORTES LOPEZ
Lider Proceso de las TICs

BEATRIZ EUGENIA MUÑOZ CAICEDO
Directora Administrativa y Financiera

DARIO ENRIQUE SOTO DURAN
Decano Facultad de Ingenierias

RICARDO ANDRES SUAZA GONZALEZ
Director de Planeación

SEBASTIAN GOMEZ JARAMILLO
Docente de Planta

JONATHAN BEAN MOSQUERA
Profesional Universitario