1. De la política institucional de seguridad de la información

1.1. Declaración

Esta política es una declaración institucional que representa la posición de la Universidad de los Andes en lo relacionado con la protección de los activos de información y que debe ser aplicada en los procesos, los servicios y los recursos de tecnología, incluidos hardware y software. La presente política es de obligatorio y estricto cumplimiento por parte de las personas que hacen parte de los órganos de dirección y gobierno administrativa y académica de la Universidad, así como por profesoras (es), empleadas (os), estudiantes y terceros relacionados o vinculados con la Universidad. El incumplimiento de las mismas originará sanciones de tipo laboral, académica o responsabilidad contractual o extracontractual según el caso.

Todo aquel que tenga acceso y responsabilidad alguna con la información institucional, debe acatar esta política y la normatividad a esta asociada, para su gestión de acuerdo con las normas sobre el uso, transmisión, almacenamiento, la divulgación, el acceso, la clasificación y el tratamiento de la información, así como las demás normas de seguridad indicadas en este documento.

1.2. Razón de ser

La Universidad de los Andes es una institución autónoma, independiente e innovadora que propicia el pluralismo, la tolerancia y el respeto de las ideas; sus instalaciones, y sus recursos informáticos y de datos, son utilizados para el apoyo de su organización con fines académicos, educativos, de investigación y de servicio. La gestión académica y administrativa en la Universidad se apoya en el uso de recursos de tecnología para el procesamiento y transmisión de la información, proporcionando una mayor accesibilidad desde y hacia diferentes partes del mundo. Así mismo estos nuevos ambientes de interconexión y accesibilidad hoy día intensifican las amenazas y riesgos de acceso y uso no autorizado a la información institucional, como divulgaciones accidentales de datos sensibles, destrucción inesperada de información esencial y ataques a la infraestructura de tecnología, los cuales potencialmente pueden generar graves consecuencias para las personas y la Universidad como institución y uso inadecuado o por fuera de los objetivos para los cuales se han dispuesto los sistemas de información.

La evolución de esta interacción a través de la información por parte de la Comunidad Uniandina requiere de organización y fortalecimiento por parte del Gobierno de la Universidad en lo que tiene que ver con establecer los recursos para proteger la información y los elementos de tecnología que actúan como medio para el almacenamiento, procesamiento, comunicación y acceso de esa información.

Esta política es una iniciativa del Gobierno de la Universidad y liderada por el grupo de Seguridad de la Información, hoy día adscrito a la DSIT, y finalmente gestionada y aprobada por el Comité de Seguridad de la Información compuesto por la Oficina Jurídica, Auditoria Interna, Secretaria General y la DSIT, que se encargará de evaluar y aprobar los lineamientos de seguridad de la información a través del “Proceso de Desarrollo y Aprobación” descrito en la normatividad asociada a este documento.

1.3. A quienes se aplica el presente documento

Todos los órganos de dirección y gobierno administrativa y académica de la Universidad, así como las unidades académicas, administrativas, estudiantes y las personas naturales o jurídicas vinculadas con la Universidad de los Andes, que tengan algún vínculo contractual o cualquier otro tipo de interés y que tengan acceso y hagan uso de Información Institucional.

El uso de los servicios y recursos de tecnología de la Universidad de los Andes conlleva explícitamente a la aceptación de este documento y por ende su cumplimiento es obligatorio. La Universidad se reserva el derecho a modificar el presente documento sin previo aviso y a su entera discreción.

La versión vigente y actualizada de este documento será publicado en el sitio web de la Universidad y en http://dsit.uniandes.edu.co/segurinfo.

Para entender completamente esta política y la normatividad asociada, se recomienda ver la sección "Términos y Definiciones" de este documento en la página 11.

1.4. Roles y responsabilidades

Todo aquel que tenga acceso y responsabilidad con la información institucional, debe leer, aceptar de manera expresa y cumplir con las responsabilidades manifiestas en esta política, una vez entre a formar parte activa de la Comunidad Uniandina. Su actuar debe observar, entre otros, el principio de responsabilidad demostrada de manera que esté en capacidad de comprobar ante la Universidad o las autoridades el cumplimiento de las mismas.

Todos son responsables deben actuar diligentemente para evitar lo siguiente respecto de la información:

- Pérdida o destrucción.
- Modificación no permitida, manipulación, alteración o adulteración.
- Acceso no autorizado.
- Uso indebido.
- Revelación o difusión no autorizada.
- Circulación a personas no legitimadas.

Adicionalmente, a todos les corresponde garantizar la reserva y confidencialidad de la información que no sea de carácter público y por ende abstenerse de suministrarla a personas no autorizadas; así como a utilizarla sólo para los fines permitidos por la ley, la Universidad o los titulares de los datos personales según el caso.

A. Del Gobierno de la Universidad

Es responsabilidad del Gobierno de la Universidad:

- Apoyar y garantizar los recursos requeridos para la Gestión de la Seguridad de la Información en la Universidad de los Andes.
- Fomentar una cultura de seguridad de la información entre todas las personas a que se les aplica el presente documento.
- Aprobar y supervisar el cumplimiento de la Política Institucional de Seguridad de la Información.
- Asegurar que un plan estratégico de seguridad de la información sea desarrollado, documentado e implementado para todos los sistemas que soportan los procesos de la Universidad.
- Asegurar que los responsables del plan estratégico de seguridad de la Información tienen la autoridad necesaria para llevar a cabo su implementación y mejora continua.
- Evaluar anualmente la efectividad del plan implementado y su nivel de cumplimiento.
- Revisar periódicamente la presente política con miras a que se ajuste a las necesidades de seguridad según el estado de la técnica, los cambios tecnológicos o el surgimiento de nuevos riesgos.

- Implementar el principio de responsabilidad demostrada de conformidad con las instrucciones que emita la autoridad competente, las buenas prácticas, guías o estándares internacionales en dicha materia.

B. Del Comité de Seguridad de la Información

El Comité de Seguridad de la Información es el primer nivel de aprobación de las políticas y acuerdos sobre seguridad de la información. Además, son responsabilidades de este Comité:

- Monitorear el cumplimiento de las políticas y normatividad asociada.
- Definir el mecanismo para elegir o determinar sus integrantes.
- Identificar los roles y designar las responsabilidades de cada uno de sus integrantes.

C. De la DSIT

La Dirección de Servicios de Información y Tecnología, DSIT, ha sido delegada por la Vicerrectoría Administrativa y Financiera para:

- Direccionar y coordinar los recursos y esfuerzos para la implementación de esta política.
- Concientizar y educar a la Comunidad Uniandina en lo relacionado con la seguridad de la información y el debido tratamiento de la misma.
- Supervisar los avances tecnológicos y de información, cambios en la legislación vigente y regulaciones aplicables y objetivos de la Universidad, para con base en ello y obrando en coordinación con el Comité de Seguridad de la Información mantener la Política Institucional de Seguridad de la Información actualizada.
- Investigar los eventuales riesgos que podrían afectar la seguridad de información y definir las estrategias para mitigar dichos riesgos o tratarlos adecuadamente.

D. Del Grupo de Seguridad de la Información

Es el equipo al interior de la DSIT responsable de liderar el desarrollo, implementación, mantenimiento y cumplimiento de las políticas en lo relacionado con seguridad de la Información y es el encargado de la gestión de los Incidentes de seguridad de la información.

También tiene a su cargo recibir y tramitar las solicitudes de excepciones a los requisitos de seguridad, mantener una lista actualizada de dichas excepciones, revisar anualmente todas las excepciones a los requisitos de seguridad básicos, recibir y mantener un inventario de todos los sistemas que contienen información confidencial (según la sección 2.5 “Clasificación de Activos de Información” descrita en esta política, página 5).

E. De las unidades jefaturas y direcciones

Asumir la responsabilidad del cumplimiento de las políticas relacionadas con seguridad de la información y el debido tratamiento de la misma en su unidad. Solicitar o implementar procedimientos para cumplir con las normas institucionales sobre dichos aspectos.

F. De las unidades jefaturas y direcciones

Proteger y garantizar el debido tratamiento de la información institucional o personal, de profesores, estudiantes, egresados u otros empleados, a la cual tengan acceso dentro de sus labores, para evitar su pérdida, alteración, destrucción o uso indebido.

G. De las unidades jefaturas y direcciones

Proteger y garantizar el debido tratamiento de la información institucional o personal, de profesores, estudiantes, egresados u otros empleados, a la cual tengan acceso dentro de sus labores, para evitar su pérdida, alteración, destrucción o uso indebido.

H. De los usuarios

Los usuarios son los primeros responsables de evitar accesos no autorizados, robo, pérdida y uso indebido de la información institucional y de los servicios y procesos que hacen uso de ella. Por lo tanto, deben proteger y garantizar el debido tratamiento de la información propia o de terceros.

La aceptación y uso de los recursos, sistemas informáticos o información de la Universidad, establecen la obligación, como miembro de la Comunidad Uniandina o tercero relacionado, de comportase de acuerdo con la normatividad y los procedimientos establecidos en el presente documento por La Universidad de los Andes, así como con toda la legislación y regulaciones aplicables.

2. Normas generales

2.1. Gestión de activos físicos

Toda Con el objetivo de lograr y mantener la protección adecuada de los activos de la organización, debe existir un Inventario de Activos con toda la información de cada activo, los cuales estarán asignados a un usuario que desempeñará el rol de Designado y será el responsable de su custodia y protección.

La Universidad de los Andes requiere identificar todos los activos y documentar su importancia. Este inventario debe incluir toda la información necesaria para recuperarse de posibles desastres, incluyendo el tipo de activo, la ubicación, la información de soporte, la información sobre licencias y el valor para la Universidad entre otra información que se considere relevante para este fin.

El procedimiento para la adquisición, mantenimiento y desechado de los activos físicos, y la actualización periódica del inventario estará a cargo del Área de Activos Fijos de la Universidad.

2.2. Homologación de cursos de libre elección

Con el objetivo de lograr y mantener la protección adecuada de los activos de la organización, debe existir un Inventario de Activos de Información, los cuales estarán asignados a un usuario que desempeñará el rol de Designado y será el responsable de su custodia y protección.

El procedimiento para la gestión de los activos de información y la actualización periódica del inventario, estará a cargo de la DSIT.

2.3. Propiedad de los activos

Todos los activos adquiridos por la Universidad de los Andes, por sus dependencias o centros adscritos, con fines académicos, administrativos y de investigación son propiedad de la Universidad de los Andes, así como la información que en ellos se genere, almacene o procese, exceptuando la información que por ser de carácter personal pertenece al titular de la misma.

En caso de que los activos o la información contenida en ellos sean de un proyecto especial entre la Universidad, sus dependencias o centros adscritos y otra entidad, ocasionando que la propiedad no sea exclusivamente de la Universidad, deberá existir previamente un acuerdo/contrato firmado por las partes y aprobado por la Oficina Jurídica de la Universidad, en el cual se especifiquen claramente los términos y proporciones de propiedad sobre los activos, información y demás productos o beneficios obtenidos en dicho proyecto.

2.4. Responsabilidad por los activos

Se deben identificar los Designados para todos los activos y asignar las responsabilidades de implementación y mantenimiento de los controles adecuados. La implementación de los controles específicos puede ser delegada por el designado, pero no sus responsabilidades de custodia y protección.

Los Designados deberán cumplir con esta política, la normatividad asociada a ella y demás normas, términos de uso y legislación nacional vigente.

2.5. Clasificación de los activos de información

Con el fin de determinar los diferentes niveles de protección y controles requeridos por la información institucional es necesario determinar la clasificación de la misma de acuerdo con el nivel de riesgos que entrañe el tratamiento y la naturaleza de la información, así como el nivel de importancia, tanto para la Universidad como para cada uno de los procesos misionales y de apoyo que hacen uso de la misma.

Toda la información tiene requerimientos implícitos de confidencialidad, integridad y disponibilidad, y los controles asociados para asegurar dichos requerimientos, son en primera instancia responsabilidad del responsable o encargado de la información. Para determinar posibles controles y su implementación, se puede solicitar ayuda a la DSIT a través del Grupo de Seguridad de la Información.

Con base en lo anterior se han determinado 3 niveles de clasificación de la información institucional según su nivel de Confidencialidad. La información de cada uno de los niveles no está exclusivamente limitada a los tipos que se describen a continuación, sino que puede extenderse a la información que según el Titular de la misma deba estar en cada uno de ellos.

Información confidencial (nivel 1)

La información confidencial es aquella que por su naturaleza y finalidad, sólo debe ser conocida por el Titular de la misma o por las personas que él explícitamente autorice. Es el nivel más alto de confidencialidad. El responsable o encargado del tratamiento de la información, únicamente en ejercicio de sus actividades para la Universidad y autorizado previamente por el Titular de la información, podrá utilizarla preservando su nivel de confidencialidad y evitando que esta pueda ser utilizada en contra de esta política y la legislación colombiana vigente.

Actualmente, toda la información que contiene cualquiera de los siguientes elementos de datos, se considera información confidencial (nivel 1):

- Número de cédula.
- Número de tarjeta de crédito.
- Número de licencia de conducir.
- Número de cuenta bancaria.
- Información médica de pacientes.
- Información financiera.
- Información académica.
- Religión.
- Orientación política.
- Estrato socioeconómico.
- O cualquier dato sensible del cual se pueda hacer uso para discriminar o a partir del cual se conozcan aspectos íntimos de las personas.

Información restringida (nivel 2)

Toda la información utilizada en el ejercicio de la actividad universitaria, y que no ha sido clasificada formalmente como información pública (nivel 3) o confidencial (nivel 1). Esta información estará restringida en su acceso a nivel particular y general; lo anterior con base a la necesidad de cada uno de los procesos y servicios, roles y perfiles que sean definidos en los sistemas de información y procedimientos.

Información pública (nivel 3)

La información que la Universidad ha puesto a disposición o publicado para el uso explícito de la opinión pública.

2.6. Responsabilidad por los activos de información

La Universidad de los Andes en calidad de propietaria de los activos, sistemas de información y de los servicios de información que ofrece a los miembros de la Comunidad Uniandina, es responsable de su propia información y de la información que otros Titulares le hayan autorizado para su tratamiento (ver la sección "Términos y Definiciones" de este documento, página 11), bajos los Términos y Condiciones de Uso de cada una de las aplicaciones o servicios de información y del presente documento.

Todos los usuarios que utilicen dichos activos, sistemas de información o servicios, aceptan expresamente, desde el primer uso, ser garantes de la información institucional y personal en ellos contenida y reconocen a la Universidad de los Andes como propietaria de dichos sistemas de información y recursos dispuestos para el cumplimiento de sus actividades.

Es responsabilidad de todos los usuarios, especialmente de los empleados de la Universidad, preservar y asegurar que todos los activos de información a los cuales tiene acceso o que dependan de él en el ejercicio de sus funciones, mantengan sus atributos y requerimientos de seguridad.

2.7. Seguridad de la información en el recurso humano

Todas las personas vinculadas a la Universidad de los Andes, en calidad de empleado, estudiante o egresado, deben leer, entender, aceptar y cumplir las disposiciones de esta política; poniendo especial atención a la sección 1.4 "Roles y Responsabilidades" en la página 2 de este documento.

Todas y cada una de las personas que administren, manejen, actualicen o tengan acceso a información de cualquier tipo que se encuentre en archivos, Bases o Bancos de Datos, físicos o digitales, se comprometen a conservarla y mantenerla de manera estrictamente confidencial y no revelarla a terceros. Todas las personas que trabajen en la administración y manejo de bases de datos, deberán suscribir un documento para efectos de asegurar tal compromiso. Esta obligación persiste y se mantiene inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento de la Información (ver la sección "Términos y Definiciones" de este documento, página 11).

2.8. Segregación de funciones

Con el objetivo de garantizar transparencia en su actuar, de evitar errores involuntarios o posiciones de poder que faciliten actuaciones indebidas, se debe garantizar que un único usuario no pueda llevar a cabo todas las fases de aprobación y ejecución asociadas a una actividad. De este modo, los miembros de la Comunidad Uniandina que tienen a su cargo la gestión de roles y permisos sobre aplicaciones, procesos y sistemas de La Universidad, deberán garantizar que cualquier acción se realice en etapas de aprobación, autorización, ejecución y mantenimiento de registros, cada una a cargo de diferentes personas.

2.9. Escritorio limpio

Los usuarios deberán adoptar y cumplir con la política de escritorio limpio, la cual establece que los espacios denominados como lugares de trabajo y/o escritorios, permanezcan despejados de documentación y medios extraíbles de almacenamiento de información durante su ausencia temporal o permanente de dicha área.

Es obligación de los usuarios el adoptar y/o solicitar medidas de protección apropiadas para la protección de la confidencialidad, integridad y disponibilidad de la información que reposa en sus escritorios o áreas de trabajo en cualquier medio que esta se encuentre allí.

Dentro de esta práctica segura es deber de los usuarios interesarse por conocer y orientar el personal flotante en dichas áreas que no pertenecen a la misma y que se encuentran en ella en calidad de invitado o transeúnte.

2.10. Controles criptográficos

La Universidad de los Andes permite la implementación de controles criptográficos con el objetivo de proteger la confidencialidad, autenticidad e integridad de la Información Confidencial o Restringida de acuerdo a la Clasificación de los Activos de Información descrita en esta política.

La DSIT o la dependencia que la Universidad disponga para tal fin, debe determinar la conveniencia y obligatoriedad del uso de cifrado, para la protección de la información transportada en medios móviles o removibles, en dispositivos o a través de las líneas de comunicación.

Estos controles criptográficos se pueden utilizar para lograr diferentes objetivos de seguridad, por ejemplo:

a. Confidencialidad: uso de cifrado de la información para proteger de accesos no autorizados y divulgación, la información sensible o crítica, bien sea almacenada o transmitida.
b. Integridad / autenticidad: uso de firmas digitales, firmas electrónicas o códigos de autenticación de mensajes para determinar el origen (autenticidad) y confirmar que la información sensible o crítica transmitida o almacenada no ha sido alterada (integridad).
c. No-repudio: uso de técnicas criptográficas para obtener prueba de la ocurrencia o no ocurrencia de un evento o acción sobre la información.

En los casos en los que se decida utilizar firmas digitales o electrónicas, se recomienda considerar toda la legislación pertinente, en particular la legislación que describe las condiciones bajo las cuales estos tipos de firma es obligatoria por mandato legal.

2.11. Acceso Físico

Todas las personas vinculadas a la Universidad de los Andes, en calidad de empleado, estudiante o egresado, podrán acceder al Campus de la Universidad y a las instalaciones que la Universidad disponga para el ejercicio de sus funciones, durante las horas y bajo las condiciones establecidas, a menos de que este acceso le sea derogado explícitamente por encontrarse en una situación particular contemplada en esta política o en la normatividad institucional.

Para el ingreso a zonas restringidas, como laboratorios especializados, cuartos técnicos, cuartos de mantenimiento, bodegas y centros de datos entre otros, los usuarios deberán contar con la debida autorización por parte del administrador o designado del área, y en caso de ser necesario, con la autorización de ingreso mediante los dispositivos dispuestos por parte del Área de Seguridad y Servicios Generales de la Universidad. Entre los posibles dispositivos de ingreso se encuentran los teclados numéricos y alfa-numéricos, controles biométricos, lectores de códigos de barras y lectores de carné entre otros.

Los usuarios al ingresar y hacer uso de las instalaciones de la Universidad, declaran haber leído los Términos y Condiciones, manuales y reglamentos relacionados, y se comprometen a cumplirlos, además de cumplir con las normas mínimas de cultura y convivencia y la legislación aplicable vigente.

Los procedimientos para el ingreso y salida del Campus, y de las demás instalaciones de la Universidad, es responsabilidad del Área de Seguridad y Servicios Generales de la Universidad.

3. Cuenta y contraseña institucional

La Universidad de los Andes ha dispuesto que todas las personas que tengan una vinculación con la Universidad como empleado, profesor o estudiante, tengan también una cuenta institucional asociada a los servicios que la Universidad considere pertinentes; es así como la cuenta institucional se establece como Identificador Único de cada usuario.

Los estudiantes retirados de la Universidad de los Andes por causas diferentes a la terminación de sus estudios, no continuarán con su cuenta institucional y perderán la posibilidad de acceder a las aplicaciones y servicios que la Universidad, o los terceros que ella disponga, provean.

Los estudiantes que hayan culminado sus estudios mantendrán su cuenta de correo electrónico institucional en calidad de egresados, pero será potestativo de la Universidad el mantener el acceso a las aplicaciones o servicios de información, incluido el correo electrónico, previa evaluación de capacidades, riesgos y conveniencia.

Los invitados, contratistas o terceros relacionados con la Universidad de los Andes podrán tener una cuenta institucional para acceder a los servicios que según sus propósitos, funciones o compromisos contractuales sean necesarios. Es potestativo de la Universidad de los Andes el autorizar o no la creación de la cuenta, previa evaluación de capacidades, riesgos y conveniencia.

Las personas que posean cuenta institucional están obligados a leer, entender y cumplir esta política y la normatividad asociada aplicable. Con el primer uso de las aplicaciones y los servicios prestados por la Universidad de los Andes o por los terceros que ella considere para tales fines, se genera manifestación expresa de conformidad y, aceptación de los términos y normativas asociadas y el compromiso de cumplirlos o de asumir las consecuencias de no cumplirlos.

La Universidad ofrece servicios de autenticación (LDAP y Directorio Activo) centralizados, y estos deben estar sincronizados con las cuentas y contraseñas institucionales. Algunos servicios o aplicaciones proporcionados por la Universidad, sus dependencias o proveedores dispuestos para tal fin, pueden tener otros métodos de autenticación y/o generar otras cuentas de usuario diferentes a la cuenta institucional, en cuyo caso el dueño o administrador de la aplicación o servicio deberá cumplir las disposiciones de la sección 5 “Acceso y Autorización” (página 9) y la normatividad asociada sobre “Uso de Contraseñas”.

La normatividad sobre la cuenta institucional asociada a esta política debe ser creada por el Grupo de Seguridad de la Información y aprobada por el Comité de Seguridad de la Información de la Universidad de los Andes.

4. Cuenta y contraseña institucional

El Comité de Seguridad de la Información será el encargado de aprobar la normatividad creada por el Grupo de Seguridad de la Información para la protección de los computadores, los dispositivos móviles y la información que en ellos se almacene o procese, o a la información que desde ellos se tenga acceso. Esta normatividad debe considerar como mínimo la seguridad física y lógica de los equipos, asignados a un usuario específico o de uso compartido, las consideraciones de movimiento, reasignación y eliminado de los equipos y las políticas de licenciamiento.

Las especificaciones operativas de esta normatividad en el término "computador" y “dispositivo móvil” incluyen, pero no se limitan a los computadores de escritorio o computadores portátiles, asistentes digitales personales (PDA), teléfonos celulares, tabletas, multifuncionales, unidades de almacenamiento flash USB, discos CD, discos DVD, discos Blu-ray o dispositivos similares.

Cada computador o dispositivo móvil de la Universidad tiene una finalidad académica, administrativa o de investigación específica, por lo cual sólo deberá ser utilizado por las personas que desempeñen esos roles dentro de la Universidad. El acceso físico y lógico a los computadores y dispositivos móviles debe ser concedido únicamente a los usuarios autorizados según su rol dentro de la Universidad.

Como mínimo, cada computador o dispositivo móvil de la Universidad, debe contar con la solución de software antivirus que la DSIT, o la dependencia que la Universidad disponga para tal fin, considere necesaria. Así mismo, esta solución sólo debe ser instalada, desinstalada, habilitada o inhabilitada por el personal de la DSIT o la dependencia que la Universidad disponga para tal fin. En ningún caso, los usuarios están autorizados a realizar dichas labores.

Todos los computadores y dispositivos móviles deben tener instalado únicamente software legalmente licenciado y respetar los acuerdos de licenciamiento, derechos de autor, la demás reglamentación de la Universidad y la legislación nacional vigente.

Ningún computador o dispositivo de la Universidad, o de propiedad de los usuarios haciendo uso de la infraestructura de redes de la Universidad, a pesar de tener asignada una dirección IP pública podrá ser utilizado como servidor web, de correo, de archivos o de cualquier otro tipo de servicio sin previa autorización de la DSIT y en cualquier caso deberá cumplir todos los requerimientos exigidos para tal fin por la DSIT.

5. Acceso y autorización

Con el objetivo de controlar el acceso a la información, a los servicios de procesamiento de información y a los procesos de negocio, se deben implementar controles de acceso con base en los requisitos establecidos en la normatividad asociada a esta política institucional de seguridad. Dicha normatividad debe ser creada por **el Grupo de Seguridad de la Información** y aprobada por el Comité de Seguridad de la Información de la Universidad de los Andes.

Las reglas y los derechos para el control del acceso para cada usuario o grupo de usuarios se deben documentar y establecer con claridad a través de los documentos técnicos y de seguridad de los servicios y aplicaciones a nivel tanto lógico como físico y se deben considerar en conjunto. Estos documentos técnicos son responsabilidad de los **dueños de servicio o aplicación**.

Los usuarios y los proveedores de servicios deben ser informados sobre los requisitos y disposiciones establecidas por la Universidad relacionados con los controles de acceso y ellos deberán aceptar formal y explícitamente su aprobación y compromiso de cumplimiento.

Preferiblemente, los servicios y aplicaciones deben utilizar los servicios centralizados de autenticación de la Universidad (LDAP y Directorio Activo) aun cuando la gestión de la autorización se haga en cada sistema o aplicación. En los casos en que se necesite crear otras cuentas, las contraseñas deberán seguir la normatividad sobre “Uso de Contraseñas”.

6. Colaboración y mensajería

El servicio de correo electrónico de la Universidad de los Andes es un servicio que ofrece la Universidad a sus estudiantes, egresados, profesores y empleados como herramienta esencial para el desarrollo de sus actividades. Este servicio solo se provee a usuarios con una cuenta institucional de Uniandes y es accesible vía un computador, portátil o dispositivo móvil que tenga conexión a Internet. Como complemento al servicio de correo electrónico institucional, la Universidad provee otras herramientas de colaboración como Calendario de actividades, cliente de mensajería web, conferencia web y almacenamiento de datos.

La Universidad de los Andes podrá ofrecer este servicio a terceros relacionados si se considera que estos lo requieren para el desarrollo de sus actividades relacionadas con la Universidad. En ningún caso podrá utilizarse el servicio para otros fines que no se encuentren expresamente definido en los Términos y Condiciones.

El usuario entiende y acepta que esta cuenta es un privilegio personal e intransferible que le asigna la Universidad de los Andes mientras conserve y mantenga la calidad de miembro de la Comunidad Uniandina como empleado, estudiante, contratista, egresado, etc., y se compromete a salvaguardar la clave que el usuario asigna para poder usar el servicio, a cambiarla frecuentemente o cada vez que el sistema se lo solicite y a no compartirla con otros usuarios. El usuario acepta la responsabilidad directa e indirecta, por todas las acciones resultantes por el uso del servicio de correo electrónico de la Universidad de los Andes.

La Universidad de los Andes se reserva el derecho de proveer este servicio directamente o de prestarlo mediante un proveedor, de establecer la ubicación física de la información o de acordar dicha ubicación directamente con el proveedor, y de cambiar en cualquier momento el proveedor del servicio y/o la ubicación física de la información según lo considere pertinente. Para el efecto de esta política y de los Términos y Condiciones, se entiende como servicio de correo electrónico de la Universidad de los Andes, al prestado directamente por la Universidad o por el proveedor que ella haya escogido para tal fin.

Es responsabilidad del **Grupo de Seguridad de la Información** el crear la normatividad, de las herramientas de colaboración y mensajería asociada a esta política; del **Comité de Seguridad de la Información**, aprobarla; y de los usuarios, leerla y cumplirla.

7. Sistemas de información académicos y administrativos

La Universidad de los Andes, para el cumplimiento de sus objetivos misionales y el desarrollo de sus actividades cotidianas administrativas, académicas y de investigación, utiliza Aplicaciones y Sistemas de Información de terceros y desarrollados in-House. El **Grupo de Seguridad de la Información** debe crear la normatividad relacionada con la utilización de estos Sistemas de Información, el acceso y gestión de los usuarios, los roles y responsabilidades de los usuarios al utilizarlos y con todo el ciclo de vida de desarrollo. Esta normatividad debe ser aprobada por el **Comité de Seguridad de la Información**.

De manera preferente, las aplicaciones y los Sistemas de Información deben utilizar los servicios de autenticación que provee la Universidad (LDAP y Directorio Activo); en caso contrario, las cuentas de usuario y clave usadas para el acceso a dichas aplicaciones y servicios deben cumplir con la normatividad asociada con las "Normas Generales", el "Uso de Contraseñas" y el "Acceso y Autorización"; teniendo especial cuidado con la Segregación de Funciones.

Para cada uno de los sistemas de información se debe establecer el rol de propietario de la aplicación, quien será el responsable de la verificación de conformidad con estándares de desarrollo, la definición de requerimientos funcionales, el análisis del riesgo, el cumplimiento de los estándares de prueba y puesta en producción de los sistemas de información.

Para la puesta en producción de una aplicación, se debe contar con la autorización del grupo de soporte y del propietario, previa validación de todos los entregables y pruebas en los otros ambientes. La puesta en producción debe estar acompañada de las respectivas garantías, compromiso de corrección de errores por parte de los proveedores y manuales de usuario y de operación.

Las sanciones por incumplimiento de estas normas deben aplicarse según corresponda a los términos y cláusulas estipulados en los contratos con funcionarios y terceros.

En el caso de los sitios web, así sean de contenido estático, deberán cumplir con los lineamientos que la DSIT disponga para su publicación, mantenimiento y administración, así como los requisitos de construcción, diseño y diagramación, con el objetivo de mantener la imagen institucional y asegurar su disponibilidad y correcto funcionamiento. En el caso en que estos sitios vayan a estar alojados en computadores, servidores o dispositivos que no se encuentren ubicados dentro de los Centros de Cómputo de la DSIT, se deberá contar con aprobación expresa de la DSIT.

8. Seguridad de la infraestructura y respaldo de la información

Los usuarios que requieran tener acceso a áreas restringidas de tecnología para el desarrollo de sus actividades, deben poder hacerlo mientras cumplan con los lineamientos descritos en la normatividad asociada. Está prohibido el libre ingreso y tránsito dentro de estas áreas por parte de usuarios no autorizados expresamente por el personal encargado de dichas áreas.

Por la seguridad de las instalaciones, los equipos y la información en ellos contenidos, queda expresamente prohibido fumar y el almacenamiento o consumo de bebidas y alimentos dentro de las áreas técnicas restringidas.

La DSIT o la dependencia que la Universidad designe para tal fin, debe establecer los procedimientos de rutina para implementar la política y la estrategia de respaldo acordada, para hacer copias de seguridad de los datos y probar sus tiempos de restauración e integridad.

El **Grupo de Seguridad de la Información** debe crear la normatividad asociada con el control de acceso físico a las diferentes áreas restringidas de tecnología de la Universidad y la protección de la infraestructura e información que en ellos se encuentra y el **Comité de Seguridad de la Información** debe revisarla y aprobarla.

Los grupos al interior de la DSIT y de otras áreas restringidas deberán documentar los procesos explícitos para el acceso a dichas áreas, respetando siempre esta **Política Institucional de Seguridad de la Información** y alineados a la normatividad asociada aprobada por el **Comité de Seguridad de la Información**.

9. Incidentes de seguridad de la información

Para la Universidad es importante detectar, tratar y evitar incidentes de Seguridad de la Información que pongan en riesgo los activos de información de su operación, su personal, sus estudiantes y egresados y los terceros asociados. Por este motivo, se deben definir, implementar y monitorear sistemas de monitoreo y detección temprana y políticas de control, erradicación y comunicación de incidentes. Dichas tareas deben ser definidas por el **Grupo de Seguridad de la Información** y aprobadas por el **Comité de Seguridad de la Información**.

Para la gestión de los incidentes de seguridad de la información es necesario contar con una categorización de incidentes, un proceso formal de gestión y las directrices generales de comunicación, los cuales estarán definidos en la normatividad asociada a esta política.

10. Términos y definiciones de la normatividad

Los siguientes términos y definiciones son utilizados en este documento y en todos los demás relacionados con la Gestión de la Seguridad de la Información de la Universidad de los Andes.

Terminología general

Política	Declaración de intención y lineamiento de un objetivo expresado formalmente para el cumplimiento a nivel institucional, organizacional y de equipo con relación al uso y su objetivo.
Activos de información	Información vista o almacenada en documentos y registros de tipo físico o digital que tiene valor para la organización dentro de los procesos y servicios.
Seguridad de la información	Gestión realizada a través de políticas, lineamientos y procedimientos para el control y establecimiento de los atributos de disponibilidad, integridad y confidencialidad en la información.
Seguridad informática	Gestión de la implementación y mantenimiento de las herramientas y controles establecidos a nivel de hardware, software y organizacional para la seguridad de la información.
Confidencialidad	Es la propiedad o atributo de la información que hace referencia a que la información debe ser conocida y divulgada únicamente por las personas, procesos o sistemas debidamente autorizados para tal fin.
Integridad de la información	Es la propiedad o atributo de la información que hace referencia a que la información debe estar libre de modificaciones por parte de personas, procesos o sistemas que no cuenten con la debida autorización.
Disponibilidad de la información	Es la propiedad o atributo de la información que hace referencia a que la información debe estar a disposición de las personas, procesos o sistemas debidamente autorizados en el momento en que la necesiten.
Autenticidad de la información	Es la propiedad o atributo de la información que hace referencia a que el origen de esta es determinable y que su integridad no ha sido alterada.
SGS	Sistema o Metodología planeada y establecida para le gestión óptima de los servicios de información y tecnología.
Inventario de activos de información	Listado de activos de información clasificados de acuerdo con su nivel de importancia, confidencialidad y valor para la Universidad.
Cifrar / Descifrar	Procedimiento utilizado para transformar, mediante la utilización de un algoritmo de cifrado y una clave o contraseña, una información en otra incomprensible. La información inicial debe poderse recuperar a partir de la información incomprensible y una clave o contraseña, proceso que se denomina descifrar. De manera equivocada se utilizan los términos **Encriptar y Desencriptar** como sinónimos de Cifrar y Descifrar sin estar aún reconocidos por la Real Academia de la Lengua Española.
Ingeniería Social	Se denomina así a los métodos utilizados para obtener información a través de la manipulación de los usuarios legítimos. Algunos de los métodos más comunes son la suplantación telefónica, recolección de información de medios y documentos desechados y phishing.

Universidad de los Andes | Vigilada Mineducación
Reconocimiento como Universidad: Decreto 1297 del 30 de mayo de 1964.
Reconocimiento personería jurídica: Resolución 28 del 23 de febrero de 1949 Minjusticia.
La versión actualizada de los reglamentos y demás normatividad se debe consultar en: https://secretariageneral.uniandes.edu.co

Terminología institucional

Información institucional	Información que es insumo y/o resultado para cada uno de los procesos, servicios, procedimientos y actividades ejercidas en la Universidad de los Andes.
Información institucional sensible	Se refieren a, la información relacionada con los profesores, estudiantes, usuarios, procesos, servicios e investigaciones que por su nivel de importancia tiene un valor significativo para la Universidad.
Gobierno de la Universidad	Consejo Superior, Comité Directivo, Consejo Académico, Consejos de Facultad.
DSIT	Dirección de Servicios de Información y Tecnología.
Comunidad Uniandina	Grupo de personas conformado por los profesores, empleados, estudiantes y egresados de la Universidad de los Andes.
Terceros relacionados	Se refiere a personas o instituciones que tienen relaciones contractuales o de otro tipo con la Universidad y que no son empleados, profesores, estudiantes o egresados.
Usuarios	Se refiere a todo miembro activo de la Comunidad Uniandina que posee acceso controlado o no a información y a recursos o servicios de información institucionales en la Universidad de los Andes.
Designado	Miembro de la Comunidad Uniandina que para el desarrollo de sus actividades relacionadas con la Universidad tiene a su cargo uno o más activos y es responsable de su protección y custodia.
Actividades institucionales	Se refiere a toda aquella actividad o acción ejecutada por los miembros de la Comunidad Uniandina, de forma autónoma o delegada y que se hace con propósitos administrativos, académicos y/o de investigación.
Dueños del servicio	Se refiere a aquellas personas que se encargan de la toma de decisiones en cuanto al diseño y soporte de un servicio, independientemente de que este sea usado por diferentes dueños de proceso o de otros servicios.
Dueños del proceso	Se refiere a aquellos roles o personas que definen y gestionan cada una de las instancias de un proceso, independientemente de que este sea ejecutado por diferentes dueños de otros procesos.
Administrador de Aplicación	Se refiere a aquellos roles o personas que se encargan de la gestión de una aplicación.

Terminología legal

Autorización	Consentimiento previo y expreso, informado por parte del titular al responsable para llevar a cabo el Tratamiento de datos personales.
Archivo	Conjunto de documentos, sea cual fuere su fecha, forma y soporte material o inmaterial, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia (Artículo 3 de la ley 594 de 2000 "por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones"
Base de Datos	Conjunto organizado de datos personales que sea objeto de Tratamiento. Ley 1581 de 2012. Para efectos de la documentación de la Universidad de los Andes, se extenderá esta definición al conjunto organizado de datos personales, información institucional y en general cualquier tipo de información que sea almacenada sistemáticamente.
Dato personal	Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Ley 1581 de 2012.
Dato sensible	Información que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos (Decreto 1377 de 2013), entre otros, la captura de imagen fija o en movimiento, huellas digitales, fotografías, iris, reconocimiento de voz, facial o de palma de mano, etc.
Tratamiento de la información	Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. Ley 1581 de 2012.

Encargado del Tratamiento de la información	Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento. Ley 1581 de 2012.
Responsable del Tratamiento de la información	Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.
Titular	Persona natural cuyos datos personales sean objeto de tratamiento. Ley 1581 de 2012.
Autorizado	Se refiere a la gestión de acceso y/o a la gestión de conceder un permiso a un individuo para el uso de un recurso de tecnología o de información institucional.
Computador o dispositivo móvil	Se refiere a cualquier recurso de tecnología que sea o no propiedad de la Universidad de los Andes, en forma temporal o permanente y sobre la cual se ha asignado una responsabilidad de tenencia y uso.
Recursos de tecnología	Se refiere a todos los recursos de infraestructura dispuestos por la Universidad para la recolección, generación, almacenamiento, trasferencia y otros usos de la información.

Universidad de los Andes | Vigilada Mineducación
Reconocimiento como Universidad: Decreto 1297 del 30 de mayo de 1964.
Reconocimiento personería jurídica: Resolución 28 del 23 de febrero de 1949 Minjusticia.
La versión actualizada de los reglamentos y demás normatividad se debe consultar en: https://secretariageneral.uniandes.edu.co