Universidad de los Andes

ANEXOS A LA DIRECTRIZ INSTITUCIONAL DE

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. DIRECTRIZ SOBRE ACTIVOS DE INFORMACIÓN

Los activos de información son datos creados o utilizados por procesos institucionales, en medio digital o papel y están almacenados en diversos formatos; para lograr su protección y mitigar riesgos se requiere realizar la valoración e implementar medidas de control para proteger nuestros activos, siendo necesario definir previamente la clasificación de la información, realizar su etiquetado, levantar inventario y gestionarlo, lo que permite definir propietarios, responsables y la gestión de los riesgos que puedan surgir en el proceso.

1.1. CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

Con el fin de dar cumplimiento normativo a la ley de protección de datos personales 1581 del 2012 y la ley de transparencia 1712 del 2014, es necesario establecer la clasificación de los activos, teniendo en cuenta el nivel de riesgo, su tratamiento, naturaleza y nivel de importancia, tanto para la Universidad como para cada uno de los procesos misionales y de apoyo que hacen uso de la misma.

Los niveles de clasificación de los activos de información institucional definidos por la Universidad de los Andes son:

Clasificación de Información	Descripción	Alienación con (Protección de Datos Personales) Ley 1581/2012- Ley 1266 de 2008
Pública	**Nivel 1. Información de uso público** Información que la Universidad por mera liberalidad o por exigencia legal explícitamente ha puesto a disposición o publicado para el uso de la opinión pública, que no requiere medidas de protección especiales y que puede ser publicada o divulgada a cualquier persona interna o externa a la Universidad. Ejemplos: Nombres y apellidos, Número de Cedula, Programas, Información de Interés Público para los estudiantes. Los usuarios con acceso a información pública deberán tener un nivel de seguridad bajo.	Es información que contiene datos personales tipo **Público:** Calificado como tal en la ley, dato que no es semiprivado, privado o sensible (Ej. datos relativos al estado civil de las personas, su profesión u oficio, su calidad de comerciante o servidor público y aquellos que pueden obtenerse sin reserva alguna). *(**Fuente**: Ley 1266 de 2018 artículo 3,literal f)*

Interno	**Nivel 2. Información de uso interno** Información de uso y acceso institucional para la comunidad Uniandina utilizada en el ejercicio de la actividad universitaria, la cual puede ser divulgada a cualquier miembro de la comunidad Uniandina sin que esto implique un riesgo significativo. Ejemplos: comportamiento financiero y crediticio de actividad comercial o de servicios y los datos sobre la seguridad social distintos. Los usuarios con acceso a información clasificada deberán tener un nivel de seguridad medio.	Es información que contiene datos personales **tipo Semiprivado:** Aquel que no tiene naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular, sino a cierto sector o grupo de personas o a la sociedad en general. Puede accederse a ellos por orden de autoridad judicial o administrativa y para los fines propios de sus funciones, o a través del cumplimiento de los principios de administración de datos personales antes analizados. (***Fuente:*** *Ley 1266 de 2008 artículo 3, literal g*)
Restringido	**Nivel 3. Información de uso restringido** Información cuyo uso o modificación no autorizada podría repercutir negativamente en la gestión académica, financiera o de operación de una o varias unidades o procesos, generando implicaciones legales, pérdidas financieras o afectaciones reputacionales. El acceso a esta información será restringido con base en la necesidad de conocer de cada una de las unidades, procesos o servicios que sean definidos. Ejemplo: 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. Datos Personales de menores niños y niñas. Toda la información que no ha sido explícitamente clasificada como información de uso público (nivel 1), como información de uso interno (nivel 2) o como información confidencial (nivel 4) debe ser considerada como información de uso restringido (nivel 3). Los usuarios con acceso a información reservada deberán tener un nivel de seguridad alto.	Es información que contiene datos personales **tipo Sensibles:** Se entiende por datos sensibles aquellos 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. *(**Fuente:** 1581 de 2012, Artículo 5o. Datos Sensibles)*

Confidencial	**Nivel 4. Información confidencial** Información cuyo uso o modificación no autorizada tenga grandes impactos de afectación reputacional, legal o financiera, los cuales puedan comprometer el cumplimiento de la misión y de los objetivos estratégicos de la Universidad. Esta información sólo debe ser conocida por el responsable de la misma o por las personas que él explícitamente autorice. Ejemplo: nivel de escolaridad, fotografías, videos, datos relacionados con su estilo de vida. Los usuarios con acceso a información confidencial deberán tener un nivel de seguridad alto.	Es información que contiene datos personales **tipo Privado**: Es un dato personal que por su naturaleza íntima o reservada solo interesa a su titular y para su tratamiento requiere de su autorización expresa. (Tomado de abc-ley-1581-de-2012-proteccion-de-datos-personales).

Para el caso que la información se clasifique en dos o más niveles, se le aplicara el nivel más alto de seguridad del etiquetado.

1.2. ETIQUETADO DE LOS ARCHIVOS DE INFORMACIÓN

La Universidad de los Andes deberá etiquetar los activos de información mediante métodos manuales o, en la medida de lo posible, automatizados para facilitar el procesamiento adecuado de las medidas de seguridad que apliquen en cada caso.

Se deberán etiquetar los documentos con carácter institucional según los niveles de clasificación de la información definidos en el numeral 1.1 Clasificación de la Información.

Se deberá definir un proceso o procedimiento para el etiquetado de la información de acuerdo con los siguientes requisitos:

- ✓ Asegurar que el etiquetado de la información refleja el esquema de clasificación de la información adoptado.
- ✓ Asegurar que las etiquetas sean fácilmente reconocibles entre la Comunidad Uniandina.
- ✓ Orientar a la Comunidad Uniandina sobre dónde y cómo se colocarán o utilizarán las etiquetas, en función del proceso de acceso a los activos de información.
- ✓ Indicar las excepciones en los que se permite omitir el etiquetado, sin que suponga una omisión del deber de clasificar la información. Se deberá prestar especial atención y tratar con cuidado máximo el etiquetado de activos físicos que contengan información restringida o confidencial, para evitar su sustracción por ser fácilmente identificable. Se deberán establecer las medidas técnicas, si fueran necesarias, y viables de etiquetado automático de la información soportada en medios digitales. La Universidad de los Andes deberá asegurar la formación y capacitación de toda la comunidad Uniandina en el etiquetado de la información.

Para realizar el proceso de etiquetado de información tenga en cuenta:

- ✓ **Documentos en papel:** se asigna el nivel de clasificación de acuerdo con el tipo de información y el etiquetado se realizará por unidad de almacenamiento (Carpeta, AZ, Caja o demás utilizada como

unidad de almacenamiento físico) esta debe estar descrita en la parte superior derecha de la Unidad de almacenamiento.

- ✓ **Documentos electrónicos:** se asigna el nivel de clasificación de acuerdo con el tipo de información y el etiquetado se realizará de forma automática (metadatos).
- ✓ **Sistemas de información:** el nivel de confidencialidad en aplicaciones y bases de datos debe ser indicado en la pantalla de acceso al sistema, como también en la esquina superior derecha de cada pantalla consecutiva que muestra información confidencial.
- ✓ **Correo electrónico:** Establecer reglas que permitan asignar el nivel de clasificación de acuerdo con el tipo de información.
- ✓ **Información transmitida oralmente:** el nivel de confidencialidad de la información confidencial que se transmite a través de una comunicación cara a cara, por teléfono o por alguna otra vía de comunicación debe ser comunicado antes que la información propiamente dicha.

1.3. PROPIEDAD DE LOS ACTIVOS DE INFORMACIÓN

Todos los activos de información adquiridos de la Universidad de los Andes, por sus dependencias académicas o administrativas, con fines académicos y de admisión, administrativos o de investigación, son propiedad de la Universidad de los Andes, así como la información que en ellos se genere, almacene, procese o transmita, 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 o servicio entre la Universidad y otra entidad, ocasionando que la propiedad no sea exclusivamente de la Universidad, deberá existir previamente un documento legal firmado por las partes y aprobado por la Dirección Jurídica de la Universidad, en el cual se especifiquen claramente los términos, proporciones de propiedad y responsabilidades sobre los activos, información y demás productos o beneficios obtenidos en dicho proyecto.

1.4. RESPONSABILIDAD POR LOS ACTIVOS DE INFORMACIÓN

Todos los activos de información deben tener un responsable encargado de administrar, gestionar y hacer efectivos los riesgos y controles, realizar el inventario de activos de información y mantenerlo actualizado de acuerdo a lo que propietario es decir la Universidad haya definido; los principales controles a implementar serán copias de seguridad, asignación de controles de acceso y mantenerlos actualizados, modificación y borrado del mismos, también tendrá la función del etiquetado de los activos de información. El responsable de la información tiene la función de la implementación y mantenimiento de los controles requeridos y son quienes tienen la potestad de tomar decisiones sobre la información que se encuentre bajo su responsabilidad.

La implementación de los controles específicos puede ser delegada por el responsable del activo de información, pero no sus responsabilidades de custodia y protección.

Los responsables de los activos de información deberán cumplir con esta directriz, los lineamientos asociadas a ésta, los términos de uso y la legislación nacional vigente.

La Universidad de los Andes, en calidad de propietaria de los activos y servicios de información que ofrece a los miembros de la Comunidad Uniandina, es responsable de garantizar el adecuado cumplimiento de esta Directriz y de los datos que otros titulares le hayan autorizado para su tratamiento, bajo los términos y

condiciones de uso de cada una de las aplicaciones o servicios de información, del presente documento y de la legislación vigente en materia de tratamiento de datos. Todos los usuarios que utilicen los sistemas de información, servicios o información de la Universidad 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.

Todos los usuarios que terminen su vínculo laboral con la Universidad, se comprometen a hacer entrega a su supervisor o jefe inmediato de los activos de información que se encuentren a su cargo o a los que hayan tenido acceso, comprometiéndose a no conservar ningún tipo de copia en medios físicos o digitales.

1.5. Inventario de activos de información

Con el objetivo de mantener la protección adecuada de los activos de información de la Universidad, y crear un punto de referencia para evaluar el nivel de permisos de acceso a sistemas, reportes o bases de datos, que se brinda a un usuario según su vínculo contractual, debe existir un inventario de activos de información.

Se deberá realizar la metodología del inventario de los activos de información, como la asignación del responsable y la definición de los lineamientos, normas y/o procedimientos para la gestión del inventario de los activos de información y la actualización periódica del mismo.

El Comité de Gobierno de Información deberá asignar, revisar, validar y aprobar los lineamientos sobre el inventario de activos, la gestión y responsabilidad de los mismos.

2. DIRECTRIZ SOBRE LA SEGURIDAD FÍSICA

Todas las personas vinculadas a la Universidad de los Andes, en calidad de empleado, estudiante, egresado, proveedor o tercero 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 por la Dirección de Gerencia del Campus, a menos de que este acceso le sea negado explícitamente por encontrarse en una situación particular contemplada en esta o en otras Directrices.

La Gerencia del Campus de la Universidad debe realizar el proceso divulgación a los usuarios sobre la responsabilidad del uso de las instalaciones de la Universidad, a través de la previa lectura de los términos y condiciones, manuales y reglamentos relacionados, y se comprometan a cumplirlos. Además, todos los usuarios deben cumplir con las normas mínimas de cultura y convivencia y la legislación aplicable vigente.

La Gerencia del Campus en conjunto con la DSIT, deben crear las normas y lineamientos asociados con el control de acceso físico a las diferentes áreas restringidas de tecnología de la Universidad y con la protección de la infraestructura e información que en ellas se encuentra. El Comité de Gobierno de Información debe revisar y aprobar dichas normas.

Las unidades encargadas de otras áreas restringidas deberán documentar los procesos explícitos para el acceso a dichas áreas, respetando siempre la Directriz Institucional de Seguridad y Privacidad de la Información y los lineamientos establecidos por el Comité de Gobierno de Información.

2.1. ESCRITORIO LIMPIO

Los usuarios deben adoptar o solicitar acompañamiento para salvaguardar la confidencialidad, integridad y disponibilidad de la información que reposa en sus escritorios o áreas de trabajo, establecidos de acuerdo a los lineamientos definidos por la Universidad.

Los usuarios deberán seguir las recomendaciones y buenas prácticas generadas de escritorio limpio para los documentos y medios de almacenamiento removibles, impartidas por la Universidad, las cuales establecen que los espacios designados como lugares de trabajo o escritorios, deben permanecer despejados de documentación y medios extraíbles de almacenamiento de información durante su ausencia temporal o permanente de dicha área.

Dentro de las buenas prácticas de escritorio limpio también está considerado el bloqueo de las sesiones de trabajo en los computadores personales en el momento en que los mismos se encuentren desatendidos.

Dentro de esta práctica segura, los usuarios deben interesarse por conocer y orientar al personal flotante que se encuentra en calidad de invitado o transeúnte en dichas áreas de trabajo, para el cumplimiento de la normatividad sobre seguridad de la información.

3. DIRECTRIZ SOBRE EL CONTROL DE ACCESOS Y LA AUTORIZACIÓN

Con el objetivo de controlar el acceso a la información, a los servicios de procesamiento de información y a los procesos institucionales, se deben implementar controles de acceso fundamentándose en los requisitos establecidos en las normas y lineamientos asociados a esta Directriz Institucional de Seguridad y Privacidad de la Información. Dicha normatividad debe ser aprobada por el Comité de Gobierno de Información y el Comité de Gestión Documental de la Universidad de los Andes o por quien este designe.

Las reglas y los derechos para el control del acceso deben estar definidos de tal manera que se contribuya con la adecuada segregación de funciones, velando por el cumplimiento del principio de, menor privilegio y minimizando la convergencia de conflictos asociados al acceso de la información.

Los accesos de cada usuario o grupo de usuarios se deben documentar y establecer con claridad en los documentos técnicos y de seguridad de los servicios y aplicaciones, tanto a nivel lógico como a nivel físico y se deben considerar en conjunto. Estos documentos son responsabilidad de los administradores técnicos y funcionales de cada servicio o aplicación. Dentro de la documentación relacionada se deben tener en cuenta los procedimientos formales que guíen las actividades de asignación, modificación y revocación de privilegios asignados para cada uno de los usuarios.

Los usuarios y los proveedores de servicios deben ser informados por parte de los encargados de los servicios sobre los requisitos y disposiciones establecidos por la Universidad en relación con los controles de acceso y ellos deberán expresar formal y explícitamente su aceptación y compromiso de cumplimiento. Con el solo hecho de realizar la activación de la cuenta y la autenticación en los sistemas de información de la Universidad,

el usuario está aceptando y se compromete a cumplir con las normas de uso de las cuentas, con esta Directriz Institucional de Seguridad y Privacidad de la Información y con todos los lineamientos y normas asociadas.

3.1. CUENTA Y CONTRASEÑA INSTITUCIONAL

La Universidad de los Andes ha dispuesto que las personas que tengan una vinculación con la Universidad como empleado, profesor, estudiante o egresado, tengan también una cuenta institucional asociada a los servicios que la Universidad considere pertinentes.

El usuario entiende y acepta que la cuenta que le asigna la Universidad de los Andes es personal e intransferible y podrá hacer uso de ella mientras conserve y mantenga la calidad de miembro de la Comunidad Uniandina y su uso debe estar limitado a las funciones desarrolladas según el rol o cargo desempeñado, evitando en todo caso el uso para fines personales. De igual forma se compromete a salvaguardar la clave que el usuario asigna para utilizar el servicio, a cambiarla frecuentemente, cada vez que el sistema se lo solicite o cada vez que las circunstancias lo requieran y a no compartirla con otros usuarios y se compromete al uso y adopción obligatorio de las medidas de control de acceso definidas o establecidas para cada sistema y por la Universidad. El usuario acepta la responsabilidad directa e indirecta, por todas las acciones resultantes por el uso de su cuenta institucional.

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 o provea.

Los estudiantes que hayan culminado sus estudios mantendrán su cuenta de correo electrónico institucional en calidad de egresados, es responsabilidad de cada egresado activar su cuenta de correo de acuerdo a los mecanismos definidos institucionalmente para tal fin, 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 y riesgos.

Los invitados, contratistas o terceros relacionados con la Universidad de los Andes podrán tener una cuenta institucional provisional 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. Los periodos de disponibilidad de dichas cuentas se establecerán de acuerdo con los requerimientos contractuales y será responsabilidad del jefe de área o supervisor del contrato velar por que se cumplan.

En caso de presentarse un incidente de seguridad en el que se identifique un uso inadecuado de la cuenta institucional, la Universidad de los Andes está en plena potestad de realizar los procesos pertinentes de investigación, recopilando la información necesaria para aclarar los hechos y si es el caso cancelar la cuenta.

La responsabilidad de solicitar la creación y la cancelación de las cuentas será de la unidad que corresponda, así:

- ✓ Estudiantes – Dirección de Admisiones y Registro.
- ✓ Estudiantes EDCO - Dirección Educación Continua.

- ✓ Empleados (profesores y administrativos) – GHDO.
- ✓ Egresados – Dirección de Relacionamiento.
- ✓ Contratistas / proveedores – Supervisor del contrato.
- ✓ Invitados o terceros - Unidad solicitante.
- ✓ Cuentas impersonales, listas manuales, listas de cursos y grupos de seguridad – Director de la unidad responsable de la solicitud.

Las personas que posean cuenta institucional están obligadas a leer, entender y cumplir esta directriz 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 autorizados, 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 DSIT ofrece servicios de autenticación federada y Directorio Activo centralizados y sincronizados con las cuentas y contraseñas institucionales. Los servicios o aplicaciones proporcionados por la Universidad, sus dependencias o proveedores, preferentemente deben realizar la autenticación con los servicios de autenticación federada ofrecidos, aun cuando la gestión de la autorización se haga en cada sistema o aplicación. En casos excepcionales que deben ser analizados y autorizados por la DSIT, pueden existir otros métodos de autenticación o generar otras cuentas de usuario diferentes a la cuenta institucional, en cuyo caso el encargado o administrador de la aplicación o servicio deberá cumplir con las normas establecidas para el uso de cuentas y contraseñas.

Los lineamientos, requisitos y controles sobre el control de acceso y uso de la cuenta institucional deben ser definidos por la DSIT, aprobados por el Comité de Gobierno de Información y cumplidos por todos los usuarios.

3.2. CUENTAS IMPERSONALES

Para mantener un contacto continuo y permanente con los miembros de la comunidad Uniandina y con terceros, algunos de los roles existentes en la Universidad deben tener asociado un nombre de cuenta genérico relacionado con el rol especifico. Estas cuentas impersonales de uso institucional se asocian con la función o proceso que desempeña el usuario y por lo tanto son personales e intransferibles, mientras el usuario desempeñe el cargo al que están asociadas.

En el momento en el que un rol relacionado con una cuenta impersonal ya no sea desempeñado por el usuario, por cambio de cargo o desvinculación, el usuario debe realizar la entrega formal de la cuenta a quien vaya a asumir el rol o en su defecto a su jefe inmediato.

Los usuarios que por sus funciones requieran administrar cuentas de correo impersonales, deberán seguir las reglas descritas en la sección 3.1. Cuenta y contraseña institucional y las demás normas descritas en la Directriz Institucional de Seguridad y Privacidad de la Información.

El usuario que tenga a su cargo el uso de una cuenta impersonal es responsable por todas las acciones realizadas desde esta cuenta mientras la tenga asignada.

En caso de existir cuentas genéricas, que debe ser la excepción y debemos propender a evitar su uso, como las cuentas de administración de sistemas operativos o cuentas de altos privilegios, para dichas cuentas se deben establecer los controles necesarios para poder monitorear su actividad y asignar en todo momento la responsabilidad de las acciones que sean realizadas con dicha cuenta.

3.3. 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 dueños de los procesos o quienes hagan sus veces al interior de las unidades son los responsables de realizar la asignación de roles garantizando que las acciones realizadas en etapas de aprobación, autorización, ejecución y mantenimiento de registros estén a cargo de diferentes personas, cuidando que los roles, permisos y atribuciones están asignados de acuerdo a las funciones o responsabilidades de la persona a la cual se le va a asignar el permiso. Estos requerimientos de segregación de funciones deben ser tenidos en cuenta para la adquisición o desarrollo de todas las plataformas y sistemas de información de la Universidad.

3.4. Gestión de acceso remoto

Cualquier computador o dispositivo móvil utilizado para acceder a los recursos de tecnología y servicios de la Universidad de los Andes debe cumplir con los lineamientos establecidos en la Universidad por la DSIT para el acceso remoto.

La Mesa de Servicio de la DSIT en cumplimiento de sus funciones y en gestión de soporte y mantenimiento de equipos en modalidad de Teletrabajo o Trabajo Remoto, podrá realizar la conexión remota a los equipos administrados por la Universidad de los Andes con herramientas o Software Licenciado previamente aprobado e instalado con las validaciones correspondientes a los protocolos establecido por Seguridad de la Información y administrado por esta Dirección. En los casos que el usuario pueda realizar uso de herramientas de acceso remoto la Mesa de Servicios deberá proveer a los usuarios toda la información sobre cómo acceder y utilizar las tecnologías de acceso remoto disponibles en la Universidad, de acuerdo con el sistema operativo y a las políticas de directorio activo. Este acceso podrá ser admitido con base en la clasificación de la información a la que requiere acceso y al computador o dispositivo móvil desde el cual se va a realizar el acceso. En caso de solicitar acceso remoto a estaciones de trabajo se debe contar con la aprobación del jefe inmediato de la persona que lo solicita y cuando el acceso remoto solicitado sea a servidores, bases de datos o aplicaciones se debe contar con las aprobaciones adicionales del encargado de la información y del administrador de la aplicación en cuestión.

Se debe prestar especial atención a la configuración de las opciones de acceso remoto en el sistema operativo, hardware y servicios, para asegurarse de que no presentan un riesgo para la seguridad del computador o dispositivo móvil y para la Universidad de los Andes.

El acceso remoto fuera de la red institucional de la Universidad de los Andes solamente se podrá realizar a través de una red de acceso privada virtual (VPN), previamente configurada y aprobada por la DSIT de acuerdo con la finalidad declarada en la solicitud de acceso.

4. DIRECTRIZ SOBRE LOS SISTEMAS DE COLABORACIÓN Y MENSAJERÍA

El servicio de correo electrónico y las herramientas de colaboración de la Universidad de los Andes son herramientas con fines académicos o administrativos que la Universidad pone a disposición de sus estudiantes, profesores, egresados, administrativos o terceros como medio esencial para el desarrollo de sus actividades, por este motivo no debe ser usado para fines personales, políticos, comerciales o publicitarios a título propio, y los mensajes enviados deben respetar la normas mínimas de cultura y convivencia evitando el envío de mensajes ofensivos o mensajes masivos de cualquier tipo que puedan ser considerados como spam o correo basura. Este servicio solo se provee a usuarios con una cuenta institucional y es accesible por medio de un computador, portátil o dispositivo móvil que tenga conexión a Internet. La Universidad de los Andes podrá ofrecer este servicio a terceros 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 definidos en los Términos y Condiciones de los servicios de colaboración y mensajería.

La Universidad de los Andes se reserva el derecho unilateral 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 o la ubicación física de la información según lo considere pertinente. Para el efecto de esta directriz y de los Términos y Condiciones de los servicios de colaboración y mensajería, 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.

Como complemento al servicio de correo electrónico institucional, la Universidad puede proveer otras herramientas de colaboración como calendario de actividades, cliente de mensajería web, conferencia web, almacenamiento de datos, entre otros. Es responsabilidad de la DSIT definir la normatividad y los Términos y condiciones para el uso de cada uno de estos servicios.

5. DIRECTRIZ SOBRE LA SEGURIDAD EN DISPOSITIVOS MÓVILES Y COMPUTADORES

La DSIT debe establecer la normatividad para la protección de los computadores, los dispositivos móviles y la información que en ellos se almacene o procese, o a la 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 normas de licenciamiento, los controles de seguridad necesarios, el cumplimiento de disposiciones normativas y las consideraciones de movimiento, reasignación y disposición de los equipos. El Comité de Gobierno de Información será el encargado de aprobar dicha normatividad.

Las especificaciones operativas de esta directriz 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 propiedad 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.

Dependiendo del nivel de acceso y de clasificación de la información que se almacene, procese o sea accedida desde el dispositivo o por el usuario que haga uso de este, la DSIT debe establecer las normas, lineamientos y controles necesarios a ser aplicados para cada nivel de clasificación de la información, la clasificación dada a cada uno de los dispositivos móviles o computadores se debe ver reflejada en el inventario de activos de información digital. Como mínimo, cada computador de la Universidad debe encontrarse adherido al dominio institucional, el cual es administrado por la DSIT, debe contar con las actualizaciones de seguridad recomendadas por el fabricante y debe contar con la solución de software antivirus que la DSIT considere necesaria. Así mismo, estas soluciones sólo deben ser instaladas, desinstaladas, habilitadas o inhabilitadas 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.

Los privilegios de administración sobre las máquinas de la Universidad están reservados a los usuarios encargados de su configuración; en caso de que otro tipo de usuario requiera este permiso, debe realizar a la mesa de servicio una solicitud justificada y previamente aprobada por su jefe inmediato. La DSIT se reservará el derecho de aceptar o rechazar la solicitud y, en caso de que esta sea aprobada, el usuario deberá aceptar explícitamente los riesgos y responsabilidades asociados con el otorgamiento de estos permisos.

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 del Director de la unidad académica o administrativa responsable de dicho dispositivo. En caso de que la DSIT otorgue la autorización requerida para este uso, el usuario se obliga a cumplir todos los requerimientos exigidos para este fin.

De la misma manera, se prohíbe el uso de computadores o dispositivos móviles para acciones que interfieran o afecten la seguridad, el desempeño o el rendimiento de los sistemas, las aplicaciones o la red institucional. En los casos en los que se presente este tipo de afectación por parte de uno o varios computadores o dispositivos móviles, la Universidad de los Andes desconectará de forma inmediata de la red dichos equipos y dará posterior aviso a los responsables o a quienes estén a cargo de estos, con el fin de proteger la infraestructura y demás recursos y servicios que se están viendo afectados.

En el caso de computadores y dispositivos móviles de propiedad de los usuarios, la Universidad no ofrece ningún tipo de soporte o servicio sobre los mismos y se reserva el derecho de establecer los controles y permitir el acceso a los sistemas de información o información de la Universidad. En ningún caso información clasificada como interna, restringida y/o confidencial debe ser almacenada en computadores o dispositivos móviles que no sean administrados por la Universidad, para ello se ofrecen mecanismos de almacenamiento en nube asociados a las cuentas institucionales.

6. DIRECTRIZ SOBRE LA SEGURIDAD DE LA INFRAESTRUCTURA DE TI

La Universidad de los Andes propende por minimizar los riesgos de alteración de los sistemas de información mediante controles de implementación de cambios y procedimientos formales de seguridad y control.

6.1. GESTIÓN DE LA VULNERABILIDAD

Los administradores de las aplicaciones y del software institucional deben velar por que en la infraestructura que compone las aplicaciones, se realicen las actualizaciones críticas o de seguridad oportunamente; los ambientes de producción no deben contar con versiones obsoletas o que no cuenten con soporte por parte del fabricante.

En caso de que un sistema presente vulnerabilidades críticas para las que aún no existan actualizaciones adecuadas, la DSIT se reserva el derecho de desactivar o dejar de utilizar el sistema afectado hasta tanto no se cuente con una solución que minimice los riesgos de seguridad para la Universidad.

La actualización de los sistemas debe ser llevada a cabo mediante el proceso de cambios definido y liderado por la DSIT, contemplando la documentación, el análisis de riesgos, la ejecución de pruebas previas, la gestión de ambientes y la generación de una copia de seguridad de la versión anterior, por si fuera necesaria una restauración. La instalación debe ser realizada por un administrador de sistemas que se encuentre cualificado, quien debe dejar un registro con todas las acciones que haya realizado.

En el caso de los sistemas administrados por terceros, el proveedor debe proporcionar el servicio técnico y ejecutar las actualizaciones siguiendo el procedimiento de control de cambios definido e informando a la DSIT los detalles de la actividad a ser ejecutada. La unidad responsable del contrato debe supervisar todas las actividades del proveedor cuando éste se encuentre prestando sus servicios, otorgándole acceso únicamente a los sistemas necesarios para realizar su labor de una forma correcta.

Para aumentar la fiabilidad de las pruebas realizadas sobre los sistemas, se deben utilizar datos cercanos a los manejados en ambientes de producción, tanto en calidad como en volumen. Teniendo en cuenta que los datos de prueba también deben ser protegidos, se deben implantar controles muy similares a los que se encuentran implantados en producción y, en cumplimiento de la Ley de protección de datos, los datos personales reales deben ser enmascarados y anonimizados para su utilización en ambientes de prueba.

Para las aplicaciones o sistemas desarrollados internamente, el responsable del desarrollo debe implementar los mecanismos para proteger el código fuente contra los accesos no autorizados que puedan manipularlo de forma maliciosa o modificarlo por error.

6.2. SEGURIDAD EN LAS REDES

Los controles necesarios para garantizar una adecuada seguridad en las redes de la Universidad deben ser diseñados, implementados y mantenidos por la DSIT y deben estar encaminados a identificar, autenticar,

autorizar y controlar el uso de los recursos de red que están a disposición de los diferentes usuarios de acuerdo a su rol y al tipo de información o servicio que deseen acceder.

Se debe establecer una separación de redes de acuerdo a las funciones desempeñadas por los dispositivos presentes en la red, estableciendo una segregación lógica de las redes en distintos dominios, dependiendo de la función que desarrollen o el tipo de usuarios, servicios o datos que puedan contener. Dentro de cada dominio se deben establecer los controles y autorizaciones de acceso necesarios para garantizar la seguridad de los dispositivos e información en ellos contenida, limitando siempre las conexiones al mínimo necesario para garantizar la operación de los servicios ofrecidos.

Debe existir una segregación de funciones en la asignación de las responsabilidades y los procedimientos para la gestión de los equipos e infraestructura de red y las responsabilidades de administración de la infraestructura de cómputo y de sistemas de información.

Para la protección de los datos en tránsito y la interconexión entre sistemas de información se deben emplear soluciones de cifrado y autenticación según la clasificación de la información a ser transmitida o intercambiada buscando proteger la confidencialidad e integridad de los datos, teniendo en cuenta la legislación vigente sobre transmisión y transferencia internacional de datos personales.

7. DIRECTRIZ SOBRE LA SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

Para el cumplimiento de sus objetivos misionales y el desarrollo de sus actividades cotidianas administrativas, académicas y de investigación, la Universidad de los Andes utiliza aplicaciones y sistemas de Información de terceros y desarrollados internamente. La DSIT debe crear las normas y lineamientos relacionados 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 el ciclo de vida de desarrollo.

Para cada uno de los sistemas de información se debe establecer el rol de encargado de la aplicación, quien será el responsable de que se realice la verificación de conformidad con estándares de desarrollo, la definición de requerimientos funcionales, requerimientos no funcionales, de calidad y de seguridad, el análisis de riesgos y 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 aprobación del dueño del servicio y/o aplicación y cumplir con los prerrequisitos definidos en el proceso de puesta en servicio.

En el caso de los sitios web, aunque su contenido sea estático, deberán cumplir con las normas definidas por la DSIT y aprobadas por el Comité de Gobierno de Información, para su publicación, mantenimiento y administración, así como con los requisitos de construcción, diseño y diagramación descritos en los manuales y directrices institucionales definidos por la Dirección de Posicionamiento, 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 y tener en cuenta las disposiciones de la SIC y el listado de países seguros para gestionar datos.

8. DIRECTRIZ SOBRE LA SEGURIDAD EN LOS SERVICIOS EN LA NUBE

La seguridad en la nube es un subdominio de la seguridad en redes y la seguridad de la información. Se refiere a una amplia gama de normas, tecnologías y formas de control destinadas a proteger datos, aplicaciones e infraestructura asociada a la computación en la nube.

Los servicios que se ofrecen en la nube a través de Internet están orientados a solucionar de forma simple los requerimientos que tienen los usuarios finales, por lo cual la nube constituye un modelo diferente de prestación de servicios y tecnología en el que los usuarios acceden a un conjunto de recursos compartidos, escalables y elásticos, con un autoservicio de administración y aprovisionamiento bajo demanda, en el cual se paga por los recursos consumidos, de acuerdo con escenarios de demanda variable.

Dependiendo del modelo de servicio definido por el proveedor de servicios en la nube, la administración de los controles de seguridad implementados será compartida entre el proveedor del servicio y la Universidad; estos acuerdos deben quedar claramente especificados en los contratos con los proveedores, en la definición del servicio y en las responsabilidades sobre el servicio. Aunque la administración de los controles de seguridad sea compartida con el proveedor del servicio, la responsabilidad de la Universidad sobre la información que sea creada, almacenada, consultada, procesada o transmitida no puede ser delegada y será asignada al responsable de la aplicación, según sea el caso. En todos los casos se debe garantizar el cumplimiento del Manual de Políticas de tratamiento de datos personales por parte del proveedor del servicio de nube, prestando especial atención a lo referente a las disposiciones normativas relacionadas a la transmisión y transferencias internacionales de datos.

Los modelos de servicio en la nube más utilizados y comúnmente aceptados se clasifican de acuerdo con el nivel de administración de las capas de tecnología asignado al proveedor; si bien en cualquiera de estos modelos se deben aplicar todos los controles de seguridad necesarios para cumplir con las directrices, normas y lineamientos de seguridad de la información definidos, la administración de algunos controles será delegada al proveedor del servicio, de manera general:

- Infraestructura como Servicio (IaaS): el proveedor del servicio debe garantizar todos los controles de seguridad relacionados con el plano de gestión de su infraestructura, con la consola de aprovisionamiento y administración de los servicios, con la infraestructura de virtualización y orquestación, con las APIs de integración y con el almacenamiento de las máquinas virtuales.

- Plataforma como Servicio (PaaS): adicionalmente a los controles establecidos para IaaS, el proveedor del servicio debe garantizar los controles de seguridad relacionados con el sistema operativo, software base y software aplicativo, actualización de versiones y parches de seguridad, almacenamiento de información y conectividad de red.

- Software como Servicio (SaaS): adicionalmente a los controles establecidos para IaaS y PaaS, el proveedor del servicio debe garantizar los controles de seguridad relacionados con el software aplicativo, la gestión de vulnerabilidades y brindar los mecanismos para establecer una adecuada segregación de funciones.

El administrador técnico de la aplicación será el responsable de verificar que el proveedor de servicios en la nube realice la correcta aplicación de los controles de seguridad que se encuentran a su cargo y también será responsable por que sean configuradas adecuadamente las opciones de seguridad que el proveedor de servicios en la nube pone a disposición del administrador del servicio del lado del cliente.

Todos los servicios en la nube o administrados por terceros que sean utilizados para crear, almacenar, consultar, procesar, transmitir o publicar información de la Universidad deberán ser aprobados por la DSIT, quien verificará que los mismos cumplan con los requisitos mínimos de seguridad y que cuentan con los acuerdos correspondientes para garantizar la seguridad de la información entregada al tercero.

9. DIRECTRIZ SOBRE LA SEGURIDAD CON PROVEEDORES Y TERCEROS

Todo proveedor o tercero que tenga o desee tener acuerdos o relaciones con la Universidad de los Andes debe cumplir con la normatividad institucional y con los términos pactados en el marco del acuerdo o relación contractual establecida; en este sentido, los proveedores o terceros deben velar por la correcta gestión y protección de la información y de los activos de información de la Universidad que como parte del desarrollo del objeto contractual se puedan tener, evitando que se produzcan accesos no autorizados, fugas, destrucciones o alteraciones que puedan afectar el funcionamiento o la reputación de la Universidad.

Todo proveedor o tercero que tenga acceso a los activos de información y preste servicios a la Universidad de los Andes debe contar con políticas, normas y estándares de seguridad de la información en su organización.

Todo proveedor o tercero debe hacer extensivo el acuerdo de confidencialidad y las directrices relacionadas a los empleados y terceros involucrados en el desarrollo de la relación contractual o precontractual con la Universidad de los Andes.

Todo proveedor o tercero debe informar a la Universidad de los Andes sobre los cambios o la instalación de nueva infraestructura tecnológica o física que haga parte del procesamiento de información de propiedad de la Universidad.

En el momento de realizar la firma del acuerdo o relación contractual, el proveedor o tercero se compromete a que, una vez finalizado el contrato, realizará la destrucción o borrado seguro de la información propiedad de la Universidad y la adecuada transferencia de la información.

Todo proveedor debe colaborar y permitir a la Universidad de los Andes realizar auditorías sobre la infraestructura tecnológica, procesos, políticas y demás aspectos relacionados con el soporte y la prestación de los servicios que hacen parte de la relación contractual.

Los activos desarrollados por la Universidad y licenciados a un tercero están cobijados por la presente Directriz y por lo tanto deben cumplir todas sus normas.

9.1. PROYECTOS CON TERCEROS

En los proyectos con terceros se debe establecer claramente la propiedad sobre los activos de información y, en particular, en el caso del desarrollo de aplicaciones o sistemas, se debe garantizar la entrega del código fuente estable a la Universidad una vez finalice el proyecto

Todo proveedor o tercero que preste el servicio de desarrollo de aplicaciones o sistemas a la Universidad de los Andes debe implementar las normas y buenas prácticas de la industria; adicionalmente, debe cumplir con los lineamientos correspondientes al desarrollo seguro y despliegue de aplicaciones definidos por la DSIT.

Es responsabilidad del proveedor o tercero utilizar software legalmente licenciado para el desarrollo de los proyectos con la Universidad. En caso de que la Universidad de los Andes se vea obligada a enfrentar reclamaciones o a pagar cualquier tipo de sanción por esta violación, el proveedor o tercero deberá reembolsar a la Universidad la totalidad de los gastos en que haya incurrido.

9.2. ENTREGA DE INFORMACIÓN A TERCEROS

Los proveedores o terceros solo podrán desarrollar para la Universidad de los Andes aquellas actividades cubiertas por el correspondiente acuerdo o contrato; en este sentido, los proveedores o terceros no podrán hacer uso de la información entregada por la Universidad de los Andes con fines diferentes a los especificados en los acuerdos firmados por las partes.

La disponibilidad de la información se rige por los acuerdos de niveles de servicio que estén explícitos en el marco del acuerdo, contrato u oferta que se haya establecido; en caso de no existir un acuerdo de nivel de servicio explícito, el proveedor o tercero deberá actuar con la máxima diligencia para que la información de la Universidad de los Andes esté disponible cuando la Universidad lo requiera, se debe tener en cuenta que la información debe ser devuelta a la Universidad una vez se culmine el vínculo contractual.

10. DIRECTRIZ SOBRE LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La Universidad de los Andes cuenta con una metodología institucional para la gestión de riesgos, enfocada en la identificación estratégica de eventos, riesgos y oportunidades que puedan afectar el logro de los objetivos de la institución. La gestión de riesgos de seguridad de la información se enmarca en esta metodología, y se enfoca específicamente en las amenazas concretas que pueden causar pérdidas o daños en los activos de información.

La metodología institucional es definida y administrada por la Auditoría interna y la Dirección de Planeación y los directores de cada unidad o dueños de cada proceso que son los responsables de la implementación de dicha metodología para la identificación y valoración de sus riesgos.

La DSIT y la Jefatura de Administración Documental, apoyarán a las unidades en la identificación, tratamiento y seguimiento de los riesgos tecnológicos y de seguridad de la información asociados con sus procesos, siempre que estas lo requieran.

Adicionalmente, la DSIT es responsable de realizar una gestión integral de riesgos tecnológicos y de seguridad de la información sobre los sistemas e infraestructura a su cargo, incluyendo la identificación, análisis, definición de planes de respuesta, implementación y seguimiento de los mismos.

11. DIRECTRIZ SOBRE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Para la Universidad de los Andes es importante evitar, detectar, responder y recuperar los 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 supervisar sistemas de monitoreo y detección temprana de incidentes y lineamientos de control, erradicación y comunicación de incidentes. Dichas tareas deben ser definidas por la DSIT y aprobadas por el Comité de Gobierno de Información o por quien este designe.

La DSIT debe definir el marco para la gestión de incidentes de seguridad de la información y contar con las áreas de GHDO, Dirección Jurídica y Dirección de Comunicaciones, el cual debe incluir los lineamientos y procedimientos para el reporte, registro, categorización, atención, investigación, seguimiento, medición, comunicación y control de los incidentes de seguridad sobre las diferentes tecnologías de la información existentes en el ecosistema tecnológico de la Universidad. Estos procedimientos podrían llegar a incluir el contacto con entidades gubernamentales o autoridades estatales para el apoyo en el tratamiento y gestión de los incidentes de TI.

La DSIT deberá implementar las medidas y los controles adecuados para minimizar el impacto y evitar la ocurrencia de los incidentes de seguridad identificados. Así mismo, la DSIT deberá escalar los incidentes de seguridad críticos al Comité de Gobierno de Información, con el fin de que se establezcan medidas de protección a nivel institucional.

Todos los miembros de la comunidad Uniandina son responsables de informar sobre cualquier comportamiento que pueda generar un incidente de seguridad de la información.

12. DIRECTRIZ SOBRE LA GESTIÓN DE LA CONTINUIDAD

La construcción del plan de continuidad de la Universidad de los Andes debe empezar con el análisis de riesgos e impactos, que identifica los servicios y procesos críticos y acuerda las metas de recuperación necesarias para definir las estrategias de continuidad. Esta construcción debe ser llevada a cabo por un comité institucional designado para este fin por la alta dirección, quien a su vez es responsable de su aprobación y debe seguir una metodología que considere por lo menos las siguientes fases:

- Análisis de riesgos e impactos, en dónde se identifican los riesgos y se estima el impacto.
- Definición de metas de recuperación.
- Definición e implementación de estrategias de recuperación de los procesos críticos de la Universidad.
- Definición e implementación de los planes de recuperación de desastres.
- Capacitación, pruebas y mantenimiento de los planes de continuidad.

Los directores y los dueños de los procesos institucionales son los responsables de definir, documentar, implementar y ejecutar los planes y estrategias de recuperación de los procesos que tienen a su cargo; estos planes de recuperación deben estar enfocados en el cumplimiento de las metas de recuperación identificadas en el análisis de impacto realizado.

La DSIT con las diferentes áreas de la Universidad son las responsables de definir, documentar, implementar y ejecutar las estrategias de disponibilidad y continuidad de los servicios tecnológicos en los cuales se apoyan los procesos críticos de la Universidad, de acuerdo con los requerimientos y con los tiempos de recuperación definidos en el análisis de riesgos e impactos, realizado a los servicios y procesos de la Universidad. Este plan de recuperación de desastres (DRP) es parte integral del plan de continuidad de la Universidad.

13. DIRECTRIZ SOBRE EL CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

Se prohíbe utilizar los activos de información de la Universidad para llevar a cabo actividades que se consideren ilegales o que vayan en contra del cumplimiento normativo de la Universidad; así mismo, se prohíben todos los usos contrarios a la presente Directriz Institucional de Seguridad y Privacidad de la Información o que afecten el buen nombre de la Universidad de los Andes. La normatividad institucional puede ser consultada en este enlace.

El uso ilegal de los servicios, la infraestructura o la conectividad a la red de la Universidad de los Andes incluye la difamación, la coacción, la extorsión, la obscenidad, la discriminación, el acoso, la injuria, la calumnia, la violación de derechos de autor, marcas comerciales o licencias, entre otros. Los usuarios deben ser conscientes de que las leyes de privacidad en otros países pueden diferir de las leyes colombianas, por lo que deben informarse acerca de la legislación y normatividad que les aplica al hacer uso de los activos en instalaciones extranjeras o conectados a las mismas para apoyar su trabajo o investigación.

La Universidad de los Andes está comprometida con la protección y el adecuado tratamiento de los datos personales de sus estudiantes, profesores, administrativos y terceros asociados; en este sentido, la Universidad se acoge a las disposiciones legales establecidas en Colombia implementando el Manual de Políticas de tratamiento de datos personales y a las disposiciones de la SIC establecidas en las Circulares externas 5 y 8 de 2017 y 2 de 2018, así como a las disposiciones adicionales que las regulen, modifiquen o deroguen, estas normativas debe ser tenidas en cuenta por todos los miembros de la comunidad Uniandina en la gestión de activos de información institucionales.

En cuanto al cumplimiento de la Ley de derechos de autor y a la protección de la propiedad intelectual, la Universidad de los Andes cuenta con un Reglamento de propiedad intelectual que debe ser respetado por todos los miembros de la comunidad. En relación con las tecnologías de la información, la Universidad de los Andes condena de forma explícita cualquier acción que atente contra los derechos de autor y de propiedad intelectual de terceros y, en particular, prohíbe la instalación o uso de software que no se encuentre debidamente licenciado.

En caso de detectarse alguna conducta en contra del cumplimiento legal o normativo haciendo uso de los servicios o activos propiedad de la Universidad de los Andes, la Universidad tomará las medidas legales, académicas o administrativas pertinentes, incluyendo la posibilidad de ingresar por intermedio de Auditoria

Interna al equipo tecnológico o servicio de propiedad de la Universidad, previa apertura de un proceso legal o disciplinario.

Ningún usuario puede usar los servicios, información, recursos informáticos o de comunicación propiedad de la Universidad de los Andes para actividades de campaña política, con fines comerciales o publicitarios, o buscar beneficio económico a través de ellos.

Los dueños de los procesos institucionales son los responsables de identificar los requerimientos legales o contractuales a los cuales pueda estar sujeta la información o la función desarrollada por el proceso institucional del cual son responsables, incluyendo entre otras la Ley de Transparencia y del derecho de acceso a la información (Ley 1712 de 2014) y la Ley por la cual se reglamenta el acceso y uso de los mensajes de datos, de comercio electrónico y las firmas digitales (Ley 527 de 1999) y la ley general del archivos 594 de 2000.

13. TÉRMINOS Y DEFINICIONES

El glosario de términos y definiciones asociado a este documento puede ser consultado en este enlace

14. VERSIÓN

Versión	Descripción	Actualizado por	Fecha
0.1	Creación del documento	David Marcel Mosquera	06/06/2019
0.2	Ajustes sobre documento	David Marcel Mosquera	06/08/2019
0.3	Actualización del documento	Luz Dary Millán	20/04/2023

15. APROBACIÓN

	Nombre	Cargo	Fecha
Actualizó	David Marcel Mosquera	Ingeniero de Seguridad de la Información	01/07/2022
Revisó	Luz Dary Millan	Coordinadora Gobierno de TI y Datos	11/07/2022
	Andrés Moreno Tatiana Gonzalez	Jefe Planeación y Gobierno de TI Directora Oficina Jurídica	25/07/2022
	Comité de Dirección DSIT	DSIT	05/08/2022
	Luz Millán Adrián Gómez Adriana Ruiz Marlen Torres	Coordinador Gobierno TI – DSIT Auditor Interno Gestora procesos Documentales Coordinadora Procesos Documentales	01/03/2023
	Henry Rengifo	Jefe Gestión Documental	10/04/2023

	Jorge Charry Alexander Estacio Moreno	Auditor Director DSIT	
Aprobó	Mauricio Olivera Gonzalez	Vicerrector Administrativo y Financiero	18/04/2023