Universidad de los Andes

DIRECTRIZ INSTITUCIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. SOBRE LA DIRECTRIZ

1.1. DECLARACIÓN

La Universidad de los Andes, como institución autónoma, independiente e innovadora que propicia el pluralismo, la tolerancia y el respeto de las ideas, declara que la información constituye un activo crítico para el desarrollo de su misión y el logro de su visión y, por lo tanto, establece la presente Directriz Institucional de Seguridad y Privacidad de la Información como el marco que debe regir toda actuación de la comunidad Uniandina sobre la seguridad de la información institucional.

1.2. OBJETIVOS

1.2.1. OBJETIVO GENERAL

Establecer y comunicar las normas y medidas de control que contribuyan con el aseguramiento y la gestión de la información de la Universidad de los Andes, minimizando el impacto generado sobre sus activos de información, por los riesgos identificados asociados a las operaciones institucionales, teniendo en cuenta las responsabilidades de cada uno de los miembros de la comunidad Uniandina, el cumplimiento de la legislación vigente y las buenas prácticas internacionales de seguridad de la información.

1.2.2. OBJETIVOS ESPECÍFICOS

- ✓ Proteger la información de la Universidad, a través de la definición de normas y procedimientos, asignación de responsabilidades e implementación de controles con relación a la integridad, confidencialidad y disponibilidad de la misma.
- ✓ Dar cumplimiento a las normas establecidas en materia de protección de datos y transparencia de la información.
- ✓ Establecer las responsabilidades en relación con la protección y la gestión de la seguridad de la información en la Universidad.
- ✓ Minimizar la probabilidad de ocurrencia de incidentes de seguridad que afecten los procesos institucionales de la Universidad.
- ✓ Consolidar un lenguaje común en relación con la gestión de la seguridad de la información en la Universidad.

1.3. A QUIÉNES APLICA

A quienes tengan acceso o responsabilidad sobre el tratamiento de la información institucional o sobre la información entregada por terceros a la Universidad, a quienes hagan uso de los activos de información e infraestructura tecnológica de la Universidad de los Andes, incluyendo a estudiantes, egresados, profesores, administrativos, visitantes, invitados y terceros con las que la Universidad establezca relaciones, cada uno de estos actores deberán leer, aceptar y cumplir diligentemente con las responsabilidades manifiestas en esta Directriz y en las normas, lineamientos y procesos asociados a la misma.

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.

1.4. CUMPLIMIENTO

En caso de presentarse algún tipo de incumplimiento a lo establecido en la presente Directriz, este será considerada como un "incidente de seguridad", acarreando sanciones de tipo académico, laboral o de responsabilidad contractual o extracontractual según el caso, lo anterior, de acuerdo a lo establecido en la normatividad Institucional o de acuerdo a los lineamientos legales que competen a cada una de las anteriores tipologías.

2. ROLES Y RESPONSABILIDADES FRENTE A LA SEGURIDAD DE LA INFORMACIÓN

2.1. DE LA COMUNIDAD UNIANDINA

La Universidad se considera una comunidad compuesta por sus estudiantes, profesores, egresados, directivos, administrativos y terceros quienes pueden tener un vínculo académico o contractual con la institución, en adelante Comunidad Uniandina; no obstante, esta Directriz se limita a las actividades que estos desarrollan directamente con la Institución. Por ello, las actuaciones de los miembros de esta Comunidad deben ser consecuentes con los principios, valores, misión y las normas establecidas en sus estatutos, políticas, reglamentos, directrices y lineamientos de tal manera que se genere confianza en los diferentes grupos de interés. Adicionalmente, la Comunidad Uniandina es responsable de proteger la información e infraestructura tecnológica que use, tenga acceso o tenga a su cargo; en virtud de su relación con la Universidad, ejecutando las acciones, cumpliendo los controles y aplicando las buenas prácticas institucionales definidas y necesarias para evitar que se materialicen eventos que afecten la integridad, disponibilidad o confidencialidad de la información.

Así mismo, todas las personas que tengan acceso a la información institucional deben garantizar la reserva y confidencialidad de la información que por su naturaleza no sea catalogada de carácter público.

2.2. DE LA VICERRECTORÍA ADMINISTRATIVA Y FINANCIERA

La Vicerrectoría Administrativa y Financiera es responsable de:

- ✓ Aprobar las actualizaciones realizadas a la Directriz Institucional de Seguridad y Privacidad de la Información.
- ✓ Asignar los recursos requeridos para la gestión de la seguridad de la información en la Universidad de los Andes.
- ✓ Promover la concientización y la educación de la comunidad Uniandina en lo relacionado con la seguridad de la información.
- ✓ Aprobar el Plan de Seguridad de la Información, sus anexos y demás lineamientos que apoyen su cumplimiento.
- ✓ Conocer la evaluación anual de la efectividad del plan implementado y su nivel de cumplimiento.

2.3. SECRETARÍA GENERAL

De acuerdo con los estatutos de la Universidad, la responsabilidad de la Secretaria General es "Preservar la memoria institucional mediante la organización del archivo general", establecida en el capítulo VII, artículo 35 numeral 6, delegando a la Jefatura de Administración Documental la participación activa en la generación e implementación de los lineamientos necesarios para garantizar la planeación, gestión, organización, uso y preservación de la memoria documental de la Universidad, en apoyo a la gestión académica y administrativa de las diferentes unidades.

2.4. DE LOS COMITÉS DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Gobierno de Información es el primer nivel de definición y control de las directrices y normas sobre seguridad de la información y a su vez, es responsable velar la implementación, la divulgación, la evaluación, el cumplimiento y el mejoramiento continuo de la Directriz Institucional de Seguridad y Privacidad de la Información de la Universidad, de acuerdo con las responsabilidades allí descritas.

Por otro lado, la Dirección de Servicios de Información y Tecnología (DSIT) preside el Comité Operativo de Seguridad de la Información, el cual está conformado por expertos en seguridad informática y de la información y en gestión de riesgos de TI, quienes hacen parte de los diferentes equipos de la DSIT y las unidades que tienen a su cargo la administración de servicios informáticos o plataformas tecnológicas. Este comité en conjunto con los administradores de las aplicaciones son los responsables de la definición, implementación y monitoreo de los controles técnicos de seguridad de la información y seguridad informática asociados con las plataformas tecnológicas de la Universidad, este comité está alineado con el Comité de Gobierno de Información.

2.5. DE LA DIRECCIÓN DE SERVICIOS DE INFORMACIÓN Y TECNOLOGÍA

La DSIT, como unidad encargada de la gestión de las Tecnologías de la Información (TI) en la Universidad de los Andes, es responsable de construir, implementar y mantener actualizado el Plan de Seguridad de la Información, que establecerá las acciones necesarias para proteger los activos de información digital de la Universidad, teniendo en cuenta los avances tecnológicos, las nuevas tendencias en ciberseguridad y las necesidades de la Universidad; dicho plan debe ser revisado, evaluado y monitoreado por el Comité de Gobierno de Información.

La DSIT también es responsable de garantizar que se cuente con la estructura funcional requerida para liderar el diseño, la implementación, el mantenimiento y el seguimiento de los controles tecnológicos de seguridad requeridos para la implementación de las normas de seguridad definidas y, en este sentido, debe garantizar el funcionamiento del Comité Operativo de Seguridad de la Información.

2.6. DE LA DIRECCIÓN DE PLANEACIÓN Y EVALUACIÓN

La Dirección de Planeación y Evaluación es la encargada del diseño, construcción y mejoramiento de la arquitectura institucional, del modelo de operación y de los procesos de la cadena de valor de la Universidad. En este sentido y como parte de esta labor se deben tener en consideración todos los activos de información que soportan a cada uno de estos procesos y los riesgos de seguridad a los que están expuestos.

2.7. De la Dirección de Gestión Humana y Desarrollo Organizacional

La Dirección de Gestión Humana y Desarrollo Organizacional como responsable de realizar los procesos de selección y contratación de personal en la Universidad, debe garantizar que sean realizadas todas las verificaciones de seguridad requeridas, incluyendo la comprobación de antecedentes, validación de experiencia y de títulos académicos de toda persona que se vaya a vincular laboralmente con la Universidad, adicionalmente deberá garantizar que todos los empleados firmen la presente Directriz en señal de haberla recibido, leído, entendido y aceptado cumplir sus responsabilidades en relación con la seguridad de la información en el cargo que desempeña.

Así mismo, esta Dirección es responsable de informar oportunamente a los interesados sobre la desvinculación o cambios de rol de los empleados, con el fin de que se revoquen sus accesos y autorizaciones, garantizando la adecuada segregación de funciones y el aseguramiento de la información gestionada por los empleados.

2.8. De los proveedores y terceros

A partir de su vinculación con la Universidad de los Andes, todo proveedor o tercero se obliga a aceptar y cumplir la presente Directriz, así como todos los lineamientos, procesos, procedimientos y otros documentos derivados de ella. El proveedor o tercero está obligado a proteger la información institucional de la Universidad de los Andes y a garantizar su confidencialidad, de acuerdo con lo estipulado en los términos del acuerdo o contrato firmado con la Universidad.

2.9. De los visitantes e invitados

Toda persona que utilice los servicios ofrecidos por la Universidad de los Andes debe aceptar y cumplir la presente Directriz.

2.10. DE LOS CLIENTES Y FINANCIADORES

Todo cliente o financiador que tenga acceso o haga uso de activos de información, de acuerdo con lo estipulado en los términos de los diferentes acuerdos establecidos con la Universidad, se obliga a aceptar y cumplir los lineamientos definidos en la presente Directriz, de tal manera que se vele por el cumplimiento de adecuadas medidas frente a la identificación, uso, administración y responsabilidad sobre los activos de Información.

3. Directrices específicas

Esta Directriz se compone de trece (13) directrices específicas que se encuentran a continuación y se explican de forma detallada en el archivo de anexos de la Directriz el cual se encuentra aquí.

3.1. Sobre la gestión de activos de información

Define los aspectos que deben ser tenidos en cuenta en la construcción, clasificación, etiquetado y administración del inventario de activos de información, así como las consideraciones en relación con la propiedad y la responsabilidad sobre los mismos.

3.2. SOBRE LA SEGURIDAD FÍSICA

Expone las normas básicas de seguridad física que garantizarán la protección de las ubicaciones físicas en las que se encuentra la información de la Universidad.

3.3. SOBRE EL CONTROL DE ACCESOS Y LA AUTORIZACIÓN

Describe las normas y responsabilidades para el correcto uso de la cuenta y contraseña institucional como método de acceso a los sistemas de información y aplicaciones institucionales, junto con los procedimientos que deben ser tenidos en cuenta para la protección y control de accesos de los usuarios a las herramientas y sistemas e información de la Universidad.

De igual forma se definen las medidas de control que deben ser implementadas a nivel técnico y funcional para garantizar la correcta asignación de roles y permisos, de tal manera que se vele por la adecuada segregación de funciones y el aseguramiento y control del acceso de la información gestionada por las herramientas y sistemas de la Universidad.

3.4. SOBRE LOS SISTEMAS DE COLABORACIÓN Y MENSAJERÍA

Precisa las normas en relación con el adecuado uso de los sistemas de colaboración y mensajería puestos a disposición de los usuarios.

3.5. SOBRE LA SEGURIDAD EN DISPOSITIVOS MÓVILES Y COMPUTADORES

Explica las disposiciones para garantizar la seguridad de los equipos propiedad y administrados por la Universidad, incluyendo las medidas para la protección contra códigos maliciosos o virus y las normas de seguridad relacionadas con medios removibles.

3.6. SOBRE LA SEGURIDAD DE LA INFRAESTRUCTURA DE TI

Define las normas relacionadas con la gestión de la seguridad de la infraestructura de TI de la Universidad, especificando los aspectos a tener en cuenta en relación con la seguridad de la red, la seguridad en los servidores y el almacenamiento, la seguridad en los ambientes virtualizados y la gestión de la vulnerabilidad técnica.

3.7. SOBRE LA SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

Establece los principios y buenas prácticas de seguridad que deben ser tenidas en cuenta durante todo el ciclo de vida de los sistemas de información, adquiridos o desarrollados por o para la Universidad de los Andes.

3.8. SOBRE LA SEGURIDAD EN LOS SERVICIOS EN LA NUBE

Describe las normas de seguridad de la información relacionadas con todo el ciclo de vida de los servicios en la nube.

3.9. SOBRE LA SEGURIDAD CON PROVEEDORES Y TERCEROS

Expone las normas que deben ser cumplidas para garantizar la seguridad de la información en las relaciones con proveedores y terceros, estableciendo pautas para el acceso a la red, a las aplicaciones y en general a todos los activos de información a los que se tenga acceso dentro del marco de cumplimiento de los acuerdos contractuales establecidos.

3.10. SOBRE LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Establece la metodología para la gestión de riesgos de seguridad de la información, definiendo los controles y las responsabilidades en relación con su identificación, análisis, monitoreo y atención.

3.11. SOBRE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Precisa los procedimientos y responsabilidades que permiten realizar una gestión adecuada de incidentes, vulnerabilidades y eventos de seguridad de la información.

3.12. SOBRE LA GESTIÓN DE LA CONTINUIDAD

Describe las responsabilidades en relación con el aseguramiento de la disponibilidad de los procesos institucionales críticos y con su recuperación en caso de interrupciones no deseadas o desastres.

3.13. SOBRE EL CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

Define las responsabilidades y las disposiciones para el cumplimiento de requisitos legales y contractuales relacionados con la seguridad de la información, como son los derechos de propiedad intelectual y la Ley de protección de datos personales.

4. VIGENCIA

La presente Directriz tiene vigencia a partir del momento de su aprobación y publicación. Debe ser revisada y actualizada por el Comité de Gobierno de Información anualmente o cuando se presenten cambios o eventualidades que así lo exijan.

Las Unidades deberán ajustar sus procedimientos a la presente Directriz, a las normas y lineamientos complementarios que serán expedidos y publicados.

5. TÉRMINOS Y DEFINICIONES

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

6. 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

7. 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 Jorge Charry Alexander Estacio Moreno	Jefe Gestión Documental Auditor Director DSIT	10/04/2023
Aprobó	Mauricio Olivera Gonzalez	Vicerrector Administrativo y Financiero	18/04/2023

Nota: Esta directriz deroga la Política de Seguridad de la Información aprobada en la sesión 135-15 del Consejo Académico, del 4 de junio de 2015