



FONDO DE PROFESORES Y EMPLEADOS
Universidad de los Andes

Manual Interno de Políticas de Seguridad para la Protección de Datos

MAN – PLN – 002

Contenido

Introducción.....	4
Objetivo	4
Alcance.....	4
Nivel de cumplimiento	4
Sanciones por incumplimiento.....	4
Revisión de la política	4
Compromiso de la dirección	5
Capítulo I	5
Políticas Generales de Seguridad de la Información.....	5
Capítulo II	6
Políticas de Gestión de Activos	6
Capítulo III	7
Políticas de estructura organizacional de seguridad de la información	7
Capítulo IV	8
Política relacionada con la vinculación de funcionarios.....	8
Capítulo V	8
Política aplicable durante la vinculación de funcionarios.....	8
Capítulo VI	9
Políticas de desvinculación, licencias, vacaciones o cambio de labores de los funcionarios	9
Capítulo VII	9
Políticas para uso de Tokens de seguridad.....	9
Capítulo VIII	10
Políticas de acceso a redes y recursos de red	10
Capítulo IX	10
Políticas de administración de acceso de usuarios	10
Capítulo X	11
Políticas de responsabilidad de acceso a los usuarios	11

Capítulo XI	11
Políticas de seguridad para los equipos institucionales	11
Capítulo XII	12
Políticas de copias de respaldo de la información.....	12
Capítulo XIII	12
Políticas de control al software operativo	12
Capítulo XIV	13
Políticas de gestión de vulnerabilidades	13
Capítulo XV	13
Políticas de uso de correo electrónico.....	13
Capítulo XVI	14
Políticas de uso adecuado de internet	14
Capítulo XVII	15
Políticas de intercambio de información	15
Capítulo XVIII	15
Políticas de gestión de incidentes	15
Capítulo IXX	16
Políticas de cumplimiento con requisitos legales y contractuales	16
Capítulo XX	16
Políticas de privacidad y protección de datos personales	16
Requisitos.....	17
Control de cambios	17

Introducción

El Fondo de Profesores y Empleados de la Universidad de los Andes – **Fondo UNIANDES** identifica la información de sus asociados, funcionarios y proveedores como un componente importante para el cumplimiento de su objeto social. Por esta razón, el **Fondo UNIANDES** establece políticas para garantizar que la información esté protegida, independientemente de su tratamiento. Este documento contiene las políticas y normas de seguridad que adopta el **Fondo UNIANDES**, acogiéndose a la normatividad relacionada con la protección de datos y seguridad de la información.

Objetivo

Establecer las políticas de seguridad de la información cuyo tratamiento está a cargo del **Fondo UNIANDES**. Estas políticas deben ser cumplidas por los funcionarios y demás personas que tengan acceso a ella, garantizando la protección de la misma.

Alcance

Las Políticas de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control, buscando conseguir un adecuado nivel de protección de la información. Estas políticas deben ser cumplidas por los asociados, funcionarios y proveedores que tengan relación con el **Fondo UNIANDES**.

Nivel de cumplimiento

Los asociados, funcionarios y proveedores del **Fondo UNIANDES** deben cumplir en su totalidad las políticas establecidas en el presente manual.

Sanciones por incumplimiento

Es necesario que el incumplimiento a las políticas de seguridad de la información sea identificado y analizado, con el objetivo de aplicar medidas correctivas y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden incluir desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias.

Revisión de la política

Las Políticas de Seguridad de la Información del presente manual serán revisadas anualmente o cuando se identifiquen cambios en la estructura, objetivos o alguna condición que afecte la política, con el fin de asegurar que se encuentren ajustadas a los requerimientos del **Fondo UNIANDES**.

Compromiso de la dirección

La Junta Directiva del **Fondo UNIANDES** aprueba esta Política de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la entidad. La Junta Directiva y la Gerencia demuestran su compromiso a través de:

- La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en este documento.
- La promoción activa de una cultura de seguridad.
- Facilitar la divulgación de este manual a todos los funcionarios de la entidad.
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.
- La verificación del cumplimiento de las políticas aquí mencionadas.

Capítulo I

Políticas Generales de Seguridad de la Información

En el **Fondo UNIANDES** la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones, razón por la cual existe un compromiso expreso de protección, orientado al fortalecimiento del Fondo, la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de las necesidades actuales, el **Fondo UNIANDES** implementará un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, estableciendo una cultura de seguridad y garantizando el cumplimiento de los requerimientos legales, contractuales y regulatorios. Para dar cumplimiento a lo anterior se establecen las siguientes directrices:

- La identificación, clasificación y valoración de los activos de información del **Fondo UNIANDES**, como base para la realización del análisis de los riesgos a los que están expuestos y así seleccionar e implementar los controles necesarios para reducir los riesgos a un nivel aceptable.
- El aseguramiento de las instalaciones físicas del **Fondo UNIANDES** y las áreas de procesamiento de información, con el fin de evitar el acceso físico no autorizado, la interferencia o daño de la información propia o de terceros resguardada por el Fondo.
- El aseguramiento, a través de una adecuada gestión, de los eventos de seguridad y las debilidades asociadas con los sistemas de información para una mejora efectiva de su modelo de seguridad.
- El establecimiento de roles y responsabilidades de los funcionarios con el fin de crear compromisos en la protección de la información a la cual acceden y procesan, para evitar su pérdida, alteración, destrucción o uso inadecuado.

- El cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas en materia de seguridad de la información.

Los asociados, funcionarios, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información del **Fondo UNIANDES**, deben adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

Capítulo II Políticas de Gestión de Activos

La información, archivos físicos, los sistemas, los servicios y los equipos se consideran activos propiedad del **Fondo UNIANDES**, los cuales son utilizados por funcionarios del Fondo con el propósito de cumplir con el objeto del negocio.

El **Fondo UNIANDES** como propietario de la información física, así como de la información generada, tratada, almacenada y transmitida, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma. Para dar cumplimiento a lo anterior se establecen las siguientes directrices:

- Toda la información sensible del **Fondo UNIANDES**, así como los activos donde ésta se almacena y se procesa, deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que se dicten.
- Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos.
- Los propietarios de los activos de información deberán identificar, clasificar y valorar los activos de información del **Fondo UNIANDES** para establecer los mecanismos de protección necesarios.
- Los recursos tecnológicos (computadores, portátiles, teléfonos móviles y tabletas) que no pertenezcan al **Fondo UNIANDES** no pueden conectarse a la red y al sistema sin previa autorización. Lo anterior, debido a que los dispositivos electrónicos que no pertenecen al Fondo representan un riesgo para la seguridad de la información y una carga adicional a la red.
- Los funcionarios y terceros que utilicen activos del **Fondo UNIANDES** deben seguir las políticas para el uso adecuado de la información y de los activos.
- Se deben emplear medidas de protección para el cableado de la red y dispositivos de comunicación de manera que no se exhiban ni sean de fácil acceso, generando el riesgo de conexiones no autorizadas.
- Se deben emplear herramientas de borrado seguro y demás mecanismos de seguridad pertinentes en los equipos que contengan medios de almacenamiento

y que serán reutilizados o eliminados, con el fin de garantizar que la información del **Fondo UNIANDÉS** contenida en estos medios no se pueda recuperar.

- Los activos del **Fondo UNIANDÉS** como computadores, portal web y LINUX no deben ser utilizados para el almacenamiento de información que no es para propósitos laborales, como por ejemplo: almacenamiento de música, videos, películas, fotos, etc.
- Los propietarios de los activos de información deben monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información.
- El profesional de soporte del **Fondo UNIANDÉS** debe establecer una adecuada configuración para el uso de activos del Fondo, con el fin de preservar la seguridad de la información.
- El profesional de soporte del **Fondo UNIANDÉS** es responsable de preparar las estaciones de trabajo fijas y/o portátiles y entregar los activos del Fondo a los funcionarios o terceros.
- El profesional de soporte es responsable de recibir los equipos de trabajo fijo y/o portátil para su reasignación o disposición final y generar copias de seguridad de la información de los funcionarios que se retiren o cambien de labores.
- El profesional de soporte debe realizar un análisis de riesgo de seguridad de manera periódica, sobre los procesos del **Fondo UNIANDÉS**.
- Se deben realizar revisiones periódicas de los recursos de la plataforma tecnológica y los sistemas de información del Fondo.
- Los funcionarios no deben utilizar sus equipos de cómputo y dispositivos móviles personales para desempeñar las actividades laborales.
- Los funcionarios no deben utilizar software no autorizados o de su propiedad en los activos del Fondo.
- En el momento de desvinculación o cambio de labores, los funcionarios deben realizar la entrega de su puesto de trabajo al jefe inmediato y al profesional de soporte entregando los activos del Fondo; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

Capítulo III

Políticas de estructura organizacional de seguridad de la información

El **Fondo UNIANDÉS** establecerá un esquema de seguridad de la información donde se definirán roles y responsabilidades que consideren actividades de administración, operación y gestión de la seguridad de la información. Para dar cumplimiento a lo anterior se establecen las siguientes directrices:

- La Gerencia debe definir y establecer los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo.
- La Gerencia debe revisar y aprobar las Políticas de Seguridad de la Información contenidas en este documento.
- La Gerencia debe promover activamente una cultura de seguridad de la información en el instituto.

- La Gerencia debe facilitar la divulgación de las Políticas de Seguridad de la Información a todos los funcionarios del Fondo y al personal provisto por terceras partes.
- La Gerencia y el profesional de soporte, deben asignar los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad de la información del Fondo.
- El profesional de soporte debe actualizar y presentar ante la Gerencia, la metodología para el análisis de riesgos de seguridad y la metodología para la clasificación de la información, según lo considere pertinente.
- El profesional de soporte debe analizar los incidentes de seguridad y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.
- El profesional de soporte debe liderar la generación de lineamientos para gestionar la seguridad de la información del **Fondo UNIANDES** y el establecimiento de controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad.
- El profesional de soporte debe validar y monitorear de manera periódica la implantación de los controles de seguridad establecidos.
- Los funcionarios o terceros que realicen labores en o para el **Fondo UNIANDES**, tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.

Capítulo IV

Política relacionada con la vinculación de funcionarios

El **FONDO UNIANDES** reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos misionales y estratégicos, con el interés de contar con el personal mejor calificado, garantizará que la vinculación de nuevos funcionarios se realice siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual estará orientado a las funciones y roles que deben desempeñar los funcionarios en sus cargos. Para dar cumplimiento a lo anterior se establecen las siguientes directrices:

- Se deben realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo.
- Los funcionarios o terceros que realicen actividades para el Fondo deben firmar un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.

Capítulo V

Política aplicable durante la vinculación de funcionarios

El **Fondo UNIANDES** en su interés por proteger su información y los recursos de tratamiento de la misma demostrará su compromiso, promoviendo que el personal cuente con el nivel deseado de conciencia en seguridad de la información para la

correcta gestión de los activos de información y ejecutando el proceso disciplinario necesario cuando se incumplan las Políticas de Seguridad de la Información del Fondo. Para dar cumplimiento a lo anterior se establecen las siguientes directrices:

- Todos los funcionarios del **Fondo UNIANDES** deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgos la seguridad y el buen nombre de la entidad.
- La Gerencia debe promover la importancia de la seguridad de la información entre los funcionarios del **Fondo UNIANDES**, así como motivar el entendimiento, la toma de conciencia y el cumplimiento de las políticas, normas, procedimientos y estándares para la seguridad de la información establecidos.
- La Gerencia debe definir y establecer el proceso disciplinario en el tratamiento de las faltas de cumplimiento a las políticas de seguridad.

Capítulo VI

Políticas de desvinculación, licencias, vacaciones o cambio de labores de los funcionarios

El **Fondo UNIANDES** asegurará que sus funcionarios serán desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura. Para dar cumplimiento a lo anterior se establece las siguientes directrices:

- El profesional de soporte debe verificar los reportes de desvinculación o cambio de labores y posteriormente debe solicitar la modificación o inhabilitación de usuarios en el sistema.
- El profesional de soporte debe verificar la entrega de activos.

Capítulo VII

Políticas para uso de Tokens de seguridad

El **Fondo UNIANDES** proveerá las condiciones de manejo de los tokens de seguridad para los procesos que los utilizan y velará porque los funcionarios hagan un uso responsable de éstos. Para dar cumplimiento a lo anterior se establecen las siguientes directrices:

- Los funcionarios que administren tokens deben recibirlos y realizar la activación necesaria en los respectivos portales o sitios de uso para poder realizar operaciones por medio de ellos.
- Los funcionarios que administren tokens deben crear los usuarios y perfiles en cada portal o sitio de uso, según las actividades a realizar por cada funcionario creado.
- Los funcionarios que administren tokens deben dar aviso a la Gerencia y a las entidades emisoras en caso de robo o pérdida de estos, con el fin de efectuar el bloqueo respectivo y la reposición de los mismos.

- Los funcionarios que administren tokens deben realizar el cambio de estos, cuando se presente mal funcionamiento, caducidad, cambio de funciones o cambio de titular, reportando a la entidad emisora y devolviendo los dispositivos asignados.
- Los usuarios no deben usar los tokens fuera de las instalaciones del **Fondo UNIANDES** para evitar pérdida o robo de estos.

Capítulo VIII Políticas de acceso a redes y recursos de red

El profesional de soporte es responsable de las redes de datos y los recursos de red del Fondo. Debe garantizar que dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico. Para dar cumplimiento a lo anterior se establecen las siguientes directrices:

- El profesional de soporte debe establecer un procedimiento de autorización y control para proteger el acceso a la red y recursos tecnológicos del **Fondo UNIANDES**.
- El profesional de soporte debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en la red o recursos tecnológicos del **Fondo UNIANDES**, así como velar por la aceptación de las responsabilidades de dichos terceros. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de terceros.
- El profesional de soporte debe autorizar la creación o modificación de las cuentas de acceso a la red o recursos tecnológicos del Fondo.
- El profesional de soporte debe verificar periódicamente los controles de acceso para los usuarios en los recursos de red o software LINUX, con el fin de revisar que dichos usuarios tengan acceso permitido únicamente a aquellos recursos para los que fueron autorizados.
- Los equipos de cómputo que se conecten o deseen conectarse a las redes de datos del Fondo deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

Capítulo IX Políticas de administración de acceso de usuarios

El **Fondo UNIANDES** establece privilegios para el control de acceso lógico de cada usuario en la red, recursos tecnológicos y sistema de información. Así mismo, debe velar porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulado por normas y procedimientos establecidos para tal fin. Para dar cumplimiento a lo anterior se establecen las siguientes directrices:

- El profesional de soporte debe establecer un procedimiento formal para la administración de los usuarios en los recursos tecnológicos y el sistema de información del Fondo.
- El profesional de soporte debe asegurarse que los usuarios que tienen asignados los diferentes recursos de la plataforma tecnológica sean inhabilitados o eliminados en el momento de su desvinculación.
- Los propietarios de activos de información deben verificar y rectificar periódicamente todas las autorizaciones sobre sus recursos tecnológicos y sistema de información.

Capítulo X

Políticas de responsabilidad de acceso a los usuarios

Los responsables de los recursos tecnológicos y el sistema de información del **Fondo UNIANDES** realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual tienen acceso. Para dar cumplimiento a lo anterior se establecen las siguientes directrices:

- Los funcionarios no deben compartir sus cuentas de usuario y contraseñas con otros funcionarios o con personal provisto por terceras partes.
- Los funcionarios provistos por terceras partes que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información del Fondo deben acogerse a lineamientos para la configuración de contraseñas y demás normas del **FONDO UNIANDES**.

Capítulo XI

Políticas de seguridad para los equipos institucionales

El **Fondo UNIANDES** para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica que se encuentren dentro o fuera de las instalaciones, proveerá los recursos que garanticen la mitigación de riesgos. Para dar cumplimiento a lo anterior se establecen las siguientes directrices:

- El **Fondo UNIANDES** debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones.
- El **Fondo UNIANDES**, liderado por el profesional de soporte, debe realizar mantenimiento preventivo y correctivo de los recursos de la plataforma tecnológica del Fondo.
- El profesional de soporte debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios del **Fondo UNIANDES**, ya sea cuando son dados de baja o cambian de usuario.
- El profesional de soporte es la única persona autorizada para realizar movimientos y asignaciones de recursos tecnológicos, por consiguiente, se encuentra

prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos del Fondo.

- Los funcionarios del **Fondo UNIANDES** no deben dejar encendidas las estaciones de trabajo u otros recursos tecnológicos en horas no laborales. En caso de ser requerida la conexión remota debe estar autorizada previamente por el profesional de soporte.
- Los equipos de cómputo, bajo ninguna circunstancia deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.
- Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.

Capítulo XII

Políticas de copias de respaldo de la información

El **Fondo UNIANDES** certificará la generación de copias de respaldo y almacenamiento de su información, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades. Las áreas propietarias de la información, con el apoyo del profesional de soporte, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información. Para dar cumplimiento a lo anterior se establecen las siguientes directrices:

- El **Fondo UNIANDES** a través del profesional de soporte, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.
- El **Fondo UNIANDES** debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen información resguardada.
- Los responsables de recursos tecnológicos y el profesional de soporte deben definir estrategias para la generación, retención y rotación de las copias de respaldo de los activos de información.
- Es responsabilidad del profesional de soporte identificar la información que debe ser respaldada y almacenada de acuerdo con su nivel de clasificación.

Capítulo XIII

Políticas de control al software operativo

El **Fondo UNIANDES** a través del profesional de soporte establecerá procedimientos para controlar la instalación de software operativo, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma

tecnológica cuando el software operativo es actualizado. Para dar cumplimiento a lo anterior se establecen las siguientes directrices:

- El profesional de soporte debe asegurarse que el software operativo instalado en la plataforma tecnológica del Fondo cuenta con soporte de los proveedores.
- El profesional de soporte debe conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.
- El profesional de soporte debe validar los riesgos que genera la migración hacia nuevas versiones del software operativo. Se debe asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.
- El profesional de soporte debe establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo del Fondo.

Capítulo XIV

Políticas de gestión de vulnerabilidades

El **Fondo UNIANDES** a través del profesional de soporte revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización periódica de pruebas de vulnerabilidad, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas. Para dar cumplimiento a lo anterior se establecen las siguientes directrices:

- El profesional de soporte debe generar los lineamientos y recomendaciones para la mitigación de vulnerabilidad.
- El profesional de soporte debe revisar periódicamente la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores del software, con el fin de prevenir la exposición al riesgo de estos.

Capítulo XV

Políticas de uso de correo electrónico

El **Fondo UNIANDES**, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre asociados, funcionarios y proveedores; proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio. Para dar cumplimiento a lo anterior se establecen las siguientes directrices:

- El **Fondo UNIANDES** debe generar y divulgar un procedimiento para la administración de cuentas de correo electrónico. Dado que el correo utilizado por

el **Fondo UNIANDES** es el institucional de la Universidad de los Andes, su utilización se rige por los lineamientos definidos para ello.

- La utilización del correo electrónico se rige también por las normas establecidas para ello por la Universidad de los Andes, dado que el correo utilizado por el Fondo es el servicio institucional.
- El **Fondo UNIANDES** debe garantizar la divulgación de directrices técnicas para el uso de los servicios de correo electrónico.
- El profesional de soporte con el apoyo de la Gerencia, debe generar campañas para la concientización de los funcionarios, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio de correo electrónico.
- La cuenta de correo electrónico asignada es de carácter individual, por consiguiente ningún funcionario del Fondo debe utilizar una cuenta de correo que no sea la suya.
- Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objeto misional del Fondo. El correo electrónico institucional no debe ser utilizado para actividades personales.
- Los mensajes y la información contenida en los buzones de correo son propiedad del Fondo y cada funcionario es responsable de su correo. Dichos mensajes deben relacionarse únicamente con el desarrollo de sus funciones.
- Los usuarios de correo electrónico institucional tienen prohibido el envío de cadenas de mensajes de cualquier tipo (comercial, político, religioso, material audiovisual, contenido discriminatorio, etc.)
- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa del Fondo y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

Capítulo XVI

Políticas de uso adecuado de internet

El **Fondo UNIANDES**, consiente de la importancia de internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias. Para dar cumplimiento a lo anterior se establecen las siguientes directrices:

- El profesional de soporte debe monitorear continuamente el canal de Internet.
- El profesional de soporte debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.
- El profesional de soporte con el apoyo de la Gerencia debe promover campañas para concientizar a los funcionarios respecto a las precauciones que deben tener en cuenta cuando utilicen el servicio de internet.

- Los funcionarios del Fondo que tengan acceso a servicio de Internet, deben evitar la descarga de software sin previa autorización.
- Está prohibido el intercambio no autorizado de información propiedad del Fondo, respecto a sus asociados, funcionarios y proveedores.

Capítulo XVII Políticas de intercambio de información

El **Fondo UNIANDES** asegurará la protección de la información en el momento de ser transferida y establecerá los procedimientos y controles necesarios para el intercambio de información; así mismo, se establecerán acuerdos de confidencialidad e intercambio de información. Para dar cumplimiento a lo anterior se establecen las siguientes directrices:

- Los propietarios de los activos de información deben velar porque la información del Fondo o de sus asociados sea protegida de divulgación no autorizada, verificar el cumplimiento de las cláusulas relacionadas en los contratos, acuerdos de confidencialidad o acuerdos de intercambio establecidos.
- Los propietarios de los activos de información, o a quien ellos deleguen, deben verificar que el intercambio de información con terceros deje registro del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.
- No se debe utilizar el correo electrónico como medio para enviar o recibir información sensible del Fondo o de sus asociados.
- No está permitido el intercambio de información sensible del Fondo por vía telefónica.

Capítulo XVIII Políticas de gestión de incidentes

El **Fondo UNIANDES** promoverá entre los funcionarios el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información. De igual manera asignará al profesional de soporte como el responsable para el tratamiento de los incidentes de seguridad de la información, quien investigará y solucionará los incidentes reportados, tomando las medidas para evitar su reincidencia. Para dar cumplimiento a lo anterior se establecen las siguientes directrices:

- Los funcionarios del Fondo deben informar de cualquier evento que afecte la confidencialidad, integridad o disponibilidad de los recursos tecnológicos y de la información.
- Se deben definir y seguir procedimientos para la gestión de los incidentes de seguridad de la información que permitan ejecutar de manera organizada las actividades de planificación, atención de incidentes y mejora continua para enfrentar nuevos incidentes.

Capítulo IXX

Políticas de cumplimiento con requisitos legales y contractuales

El **Fondo UNIANDES** velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ella la referente a derechos de autor y propiedad intelectual. Para dar cumplimiento a lo anterior se establecen las siguientes directrices:

- El profesional de soporte debe identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables al Fondo y relacionados con la seguridad de la información.
- El profesional de soporte debe certificar que todo software que se ejecuta en el Fondo esté protegido por derechos de autor y requiera licencia de uso o en su lugar, sea un software de libre distribución y uso.
- Los usuarios no deben instalar software o sistemas de información en sus estaciones de trabajo.
- Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y su reproducción no autorizada es una violación de ley, no obstante, pueden distribuirse un número de copias bajo una licencia otorgada.

Capítulo XX

Políticas de privacidad y protección de datos personales

En cumplimiento de la Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales, el **FONDO UNIANDES** velará por la protección de los datos personales de sus asociados, funcionarios y proveedores, de los cuales recibe y administra información.

Se establecerán los términos, condiciones y finalidades para los cuales el Fondo, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personal que en algún momento, por razones de la actividad que desarrolla el Fondo, hayan suministrado datos personales.

El **Fondo UNIANDES** buscará proteger la privacidad de la información, estableciendo los controles necesarios para preservar aquella información que el Fondo conozca y almacene, velando que dicha información sea utilizada únicamente para funciones propias del Fondo y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización del titular. Para dar cumplimiento a lo anterior se establecen las siguientes directrices:

- Los funcionarios que procesan datos personales de asociados, funcionarios y proveedores, deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir,

actualizar y transmitir dichos datos personales en el desarrollo de las actividades del Fondo.

- Los funcionarios que procesan datos personales de asociados, funcionarios y proveedores deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.
- El profesional de soporte debe establecer los controles para el tratamiento y protección de los datos personales de los asociados, funcionarios y proveedores de los cuales se recibe y administra información.
- El profesional de soporte debe implantar los controles necesarios para proteger la información personal de los asociados, funcionarios y proveedores almacenada en la base de datos del Fondo.
- Los funcionarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información del Fondo.
- Es deber de los funcionarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información personalmente, por teléfono, por correo electrónico, por correo certificado, entre otros.
- Los funcionarios del Fondo que tengan acceso al sistema de información deben asumir la responsabilidad individual sobre la clave de acceso, así mismo dicha clave debe ser cambiada de manera periódica.

Requisitos

Documento	Descripción
Constitución política de Colombia	
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales
Decreto 1377	Por el cual se reglamenta parcialmente la Ley 1581 de 2012
	Aviso de privacidad
FMT – GT – 001	FMT – Autorización de tratamiento de datos personales

Control de cambios

Versión	Fecha	Control de cambio
000	08-07-2016	Elaboración del documento
001	07-02-2017	Se realizan modificación de forma al documento y finalmente se codifica de acuerdo con la estructura del SGC