El presente Acuerdo de Comunicaciones tendrá por objeto definir las reglas de validez jurídica de la información y las comunicaciones basadas en mensajes de datos y de la utilización de mecanismos tales como: firma electrónica, biométrica, notificaciones, entre otros, que requieran el uso de cualquier medio electrónico, vinculados con los servicios que EL PROVEEDOR transe con EL CLIENTE. El Acuerdo de Comunicaciones será ejecutado y resulta vinculante entre EL PROVEEDOR y EL CLIENTE.

Para la legalización de los documentos, LAS PARTES acuerdan que los documentos necesarios para ello serán firmados utilizando mecanismos de firma electrónica de conformidad con el decreto 2364 de 2012, mediante mecanismos que cumplen los requisitos allí contemplados y que LAS PARTES reconocen como confiables y apropiados.
LAS PARTES aceptan que los documentos serán firmados mediante alguno del método de firma electrónica de la PLATAFORMA DE FIRMA ELECTRÓNICA Tsign. Es importante para LAS PARTES que firman este documento que tengan en cuenta los siguientes aspectos:
1. La firma electrónica permite realizar acuerdos sin que se requiera para ello la presentación personal, para que todas las PARTES puedan celebrar acuerdos de forma más rápida y efectiva.
2. Para realizar el firmado electrónico de este documento, LAS PARTES aceptan que el TOKEN será el número del teléfono celular (Tarjeta SIM) de cada PARTE; siempre que se requiera firmar un acuerdo entre LAS PARTES, cada PARTE recibirá una llamada telefónica a su número celular, donde se le dará un CODIGO DE VALIDACION de cuatro (4) dígitos, que podrá ver en su navegador y adicional escuchará en su celular y seguidamente deberá recitar dígito a dígito los 4 dígitos, cuando el sistema se lo solicite. Este CODIGO DE VALIDACION (OTP), será diferente para cada una de LAS PARTES. Igualmente, éste será válido única y exclusivamente para el trámite que se está realizando y no podrá ser utilizada para trámites futuros. Esto garantiza a cada PARTE, que como poseedor de su teléfono celular y/o tarjeta SIM, (el cual deberá tener a la mano al momento del firmado), es la única persona que podrá conocer el CODIGO DE VALIDACION enviado y, por ende, será el CODIGO que usará para firmar.

¿Cómo hacer uso del servicio de firmado electrónico con Tsign?

1. Cuando cada PARTE requiera firmar, el sistema **Tsign** solicitará los siguientes datos: país, correo electrónico, número celular y nombre.
2. **Tsign,** después de ser digitados los datos informará en la llamada el CODIGO DE VALIDACION (OTP) de firmado al celular (Tarjeta SIM), el cual deberá ser recitado en la llamada para **confirmar el deseo de firmar el acuerdo que esté realizando**, en caso de no estar de acuerdo simplemente no recitar el CODIGO DE VALIDACION (OTP) y colgar la llamada.
3. Firmado el acuerdo, la información y documentos que se hayan diligenciado, con todos los documentos que se hubieren anexado, se generará el Hash al audio y se usará la llave privada del certificado digital de la “Sociedad Tsign Sas”., junto con la llave pública de ANDES SCD, y se agrega al documento teniendo en cuenta que **Tsign** es la operadora del método de firma electrónica que usan las partes.
4. Posteriormente será entregado, vía email, en forma íntegra a cada una de LAS PARTES el documento en formato PDF. Este mecanismo reemplaza la presentación física de los documentos que soporten el trámite. La información digitada y los documentos (imágenes) anexados, será inmodificables luego del firmado, garantizando así la integridad de la información diligenciada.

¿Qué hacer en caso de cambio de email o de número celular?

Por razones de seguridad, la verificación de identidad realizada queda directamente asociada con la identificación de cada una de LAS PARTES -con el email – tarjeta SIM, por lo tanto, en caso de cambio del correo electrónico (email) o de número celular será indispensable, si alguna de LAS PARTES lo requiere a la otra PARTE, realizar un nuevo proceso de firmado del documento. En caso de no hacer el requerimiento una parte a la otra de volver a firmar el documento seguirá vigente de acuerdo a las condiciones al momento del firmado. Se recomienda especialmente que, en caso de cambio de número o cambio del correo electrónico, se informe a las otras PARTES si se deben firmar nuevamente los documentos.

Responsabilidad.

Teniendo en cuenta que el firmado electrónico de este acuerdo **SUSTITUYE LA PRESENTACION FÍSICA,** es necesario que cada PARTE lo haga sin delegarlo en ningún tercero; es decir, como al momento de firmar se llama al número celular, es importante que sea LA PARTE dueña quien se encargue de dar la información al sistema al momento de ser requerida; hay que tener en cuenta que la administración de la firma, que es efectuada con un CODIGO DE VALIDACION (OTP), recitada con la voz y el TOKEN (el celular), es responsabilidad exclusiva del firmante, pues es su obligación mantener el control y custodia sobre los datos de creación de la firma, de conformidad con el régimen legal como se indica a continuación:

Soporte Legal

Este procedimiento de firmado electrónico se soporta legalmente en el Decreto 2364 del 22 de noviembre de 2012, el cual reza:

Artículo 1: Firma Electrónica: Métodos tales como códigos, contraseñas, datos biométricos o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los cuales se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente.

Artículo 4: Confiabilidad de la firma electrónica: La firma electrónica se considera confiable para el propósito por el cual el mensaje de datos fue generado o comunicado si:

1. Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante.
2. Es posible detectar cualquier alteración no autorizada del mensaje de datos, hecha después del momento de la firma.

Artículo 6: Obligaciones del firmante. El firmante debe:

1. Mantener el control y custodia sobre los datos de creación de la firma.
2. Actuar con diligencia para evitar la utilización no autorizada de sus datos de creación de la firma.
3. Dar aviso oportuno a cualquier persona que posea, haya recibido o vaya a recibir documentos o mensajes de datos firmados electrónicamente por el firmante, si:

a. El firmante sabe que los datos de creación de la firma han quedado en entredicho; o

b. Las circunstancias que tenga conocimiento el firmante den lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho.

Parágrafo: Se entiende que los datos de creación del firmante han quedado en entredicho. cuando estos, entre otras, han sido conocidos ilegalmente por terceros, corren peligro de ser utilizados indebidamente, o el firmante ha perdido el control o custodia sobre los mismos y en general cualquier otra situación que ponga en duda la seguridad de la firma electrónica o que genere reparos sobre la calidad de la misma.

POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

CONTENIDO

1. OBJETIVO

El objetivo de la política general de seguridad de la información de **LA COOPERATIVA DE PROFESORES DE LA UNIVERSIDAD NACIONAL DE COLOMBIA** es salvaguardar la confidencialidad, integridad y disponibilidad de la información de la entidad y sus asociados. Esto se logra mediante la implementación de controles de seguridad apropiados, la sensibilización y capacitación del personal, así como una respuesta efectiva a los incidentes de seguridad de la información. La política tiene como propósito garantizar el cumplimiento de los requisitos legales y normativos vigentes, incluyendo la Circular Externa 036 de 2022 de la Superintendencia de la Economía Solidaria, que establece directrices sobre seguridad y calidad de la información para las cooperativas que prestan servicios financieros. Asimismo, se busca fomentar una cultura de seguridad de la información en toda la entidad.

Se buscará implementar un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con los objetivos estratégicos de **LA COOPERATIVA DE PROFESORES DE LA UNIVERSIDAD NACIONAL DE COLOMBIA** y con los lineamientos regulatorios exigidos por la Superintendencia de la Economía Solidaria, conforme a la Circular Externa 036 de 2022. Esta alineación garantizará que las medidas de seguridad no solo protejan la información, sino que también impulsen la mejora continua de productos, servicios, procesos y proyectos, asegurando el cumplimiento de los requisitos de los asociados, la organización y las regulaciones aplicables.

Además, el SGSI permitirá identificar y mitigar los riesgos más críticos en materia de seguridad de la información y ciberseguridad, al tiempo que facilitará la detección y respuesta ágil ante incidentes, asegurando una gestión efectiva de la seguridad.

El Consejo de Administración se compromete a seguir buenas prácticas para lograr los siguientes objetivos:

- Revisar y aprobar la política general del Sistema de Gestión de Seguridad de la Información.
- Apoyar y fortalecer los objetivos estratégicos de la organización en materia de seguridad de la información.
- Supervisar la identificación y gestión de los riesgos más críticos en seguridad de la información y ciberseguridad.
- Supervisar la respuesta y gestión de incidentes de seguridad de la información.
- Promover una cultura organizacional de seguridad de la información y ciberseguridad mediante lineamientos estratégicos.

2. ALCANCE

La política general de seguridad de la información de **LA COOPERATIVA DE PROFESORES DE LA UNIVERSIDAD NACIONAL DE COLOMBIA** abarca a todos los trabajadores, contratistas, proveedores y terceros que manejen o tengan acceso a la información de la organización y sus filiales. Además, se aplica a todos los sistemas, dispositivos y redes utilizados para procesar, almacenar o transmitir dicha información. La política engloba toda la información de la entidad, incluyendo la información financiera, personal, confidencial y de propiedad, así como los procesos y actividades relacionados con su gestión y protección. Asimismo, se implementa en todas las ubicaciones de la entidad y en todas las fases del ciclo de vida de la información, desde su creación hasta su eliminación, incluyendo el cumplimiento de los requisitos técnicos y organizativos establecidos por la Supersolidaria en materia de seguridad y calidad de la información para servicios financieros.

3. DECLARACIONES

Para lograr estos objetivos y alcance, **LA COOPERATIVA DE PROFESORES DE LA UNIVERSIDAD NACIONAL DE COLOMBIA** se compromete a:

- Adoptar la norma ISO/IEC 27001:2022 como marco de referencia para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI).
- Brindar apoyo estratégico y seguimiento desde el Consejo de Administración, asegurando la asignación de recursos necesarios para la implementación y mantenimiento del SGSI.
- Proteger la información de la organización contra accesos no autorizados, pérdidas, robos, daños o divulgaciones indebidas, garantizando la confidencialidad, integridad y disponibilidad de los activos de información.
- Cumplir con las leyes, regulaciones y normativas aplicables en materia de seguridad de la información y privacidad de datos, incluyendo la Circular Externa 036 de 2022 de la Superintendencia de la Economía Solidaria, garantizando la implementación de controles y prácticas de seguridad adecuados para los servicios financieros ofrecidos.
- Gestionar los riesgos de seguridad de la información mediante un proceso estructurado de identificación, evaluación, tratamiento y monitoreo continuo de amenazas y vulnerabilidades.
- Aplicar el principio de mínimo privilegio y necesidad de conocer en la concesión de accesos, asegurando que solo los usuarios autorizados accedan a la información y sistemas según sus funciones.
- Desarrollar y mantener políticas, procedimientos e instrucciones alineadas con los requisitos de seguridad, abarcando áreas clave como gestión de contraseñas, control de accesos, seguridad física y respuesta a incidentes.

- Fomentar una cultura de seguridad a través de programas de capacitación y concienciación dirigidos a trabajadores, usuarios y demás partes relacionadas con COOPROFESORESUN.
- Monitorear y auditar regularmente los sistemas y activos de información para detectar y prevenir incidentes de seguridad, aplicando mejoras según los hallazgos obtenidos.
- Presentar informes de seguridad de la información al Consejo de Administración de manera periódica para garantizar el seguimiento y mejora continua del SGSI.
- Designar un responsable de Seguridad de la Información, encargado de la implementación del SGSI y de la gestión de políticas aprobadas por el Consejo de Administración.

4. HISTÓRICO DE CAMBIOS Y/O REVISIÓN

VERSIÓN	CAUSA DE LA REVISIÓN	FECHA DE APROBACIÓN
0.0	Versión Inicial	02/11/2023
1	Modificación y alcance de la política general de seguridad de la información.	29/05/2025

TABLA REVISIÓN Y APROBACIÓN

ELABORÓ	REVISÓ	APROBÓ
Angela María Montero González Directora Tics	**Edilberto Forero Vivas** Coordinador de Riesgos	**Consejo de Administración Sesión Ordinaria 29 de mayo de 2025 Acta 953**
Fecha:29/05/20205	Fecha:29/05/20205	Fecha:29/05/20205

El presente documento fue aprobado por el Consejo de Administración a los veintinueve (29) días del mes de mayo del año dos mil veinticinco (2025) en la ciudad de Bogotá, según consta en el Acta No. 953, y empezará a regir a partir de su aprobación.

JUAN MANUEL ARTEAGA DIAZ
Presidente del Consejo de Administración

SONIA ISABEL DURANGO ROSERO
Secretaria del Consejo de Administración