andes Servicio de Certificación Digital	**POLÍTICA INTEGRADA**	Fecha de vigencia:	27/08/2026
		Versión:	8
		Clasificación de la información:	Público
		Elaboró:	Oficial de Seguridad de la Información y Continuidad de Negocio
		Revisó:	Director de Estrategia
		Aprobó:	Comité de Políticas y Seguridad

1. Propósito

La presente política establece el compromiso de Andes Servicio de Certificación Digital S.A. con la prestación de servicios de calidad y con seguridad de la información, asegurando la satisfacción de los clientes y demás partes interesadas, la protección de los activos de información que soportan la operación de la organización y la mejora continua de sus procesos. Este compromiso se cumple conforme a los requisitos legales, reglamentarios, contractuales y organizacionales aplicables, incluyendo las disposiciones regulatorias aplicables emitidas por la Superintendencia Financiera de Colombia relacionadas con ciberseguridad, computación en la nube, tercerización tecnológica y resiliencia operacional. y a las normas ISO 9001, ISO/IEC 27001, ISO/IEC 22301 e ISO/IEC 42001en sus versiones vigentes, la seguridad y privacidad en servicios de computación en la nube, la gestión de la inteligencia artificial, las buenas prácticas en materia de ciberseguridad, continuidad del negocio y resiliencia operacional, y los criterios de acreditación establecidos por el Organismo Nacional de Acreditación de Colombia – ONAC, y los principios y criterios WebTrust aplicables a los servicios de certificación digital, firma electrónica y servicios de confianza.

Para efectos de esta política, la seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información, conforme a lo establecido en la norma ISO/IEC 27001, así como de otros atributos asociados tales como la autenticidad, trazabilidad y no repudio, garantizando su protección frente a accesos no autorizados, uso indebido, divulgación, alteración, pérdida o destrucción, durante todo el ciclo de vida de la información. Dichos principios se aplican de manera consistente con los controles, prácticas operativas y salvaguardas exigidas por los esquemas de acreditación de ONAC y los criterios WebTrust, asegurando la confiabilidad de los servicios de certificación y la confianza de los usuarios y terceros dependientes.

La información se gestiona como un activo clave: disponible, íntegra, exacta, confiable, actualizada y accesible, de modo que cumpla los requisitos del cliente,

legales y reglamentarios y los de competencia técnica, imparcialidad, transparencia, eficacia operativa y continuidad que exigen ONAC y WebTrust, y contribuya a la eficacia de los procesos del Sistema de Gestión de la Calidad.

Esta política constituye el marco de referencia para establecer los objetivos de calidad y de seguridad de la información, gestionar los riesgos, definir, implementar y evaluar los controles técnicos, administrativos y operativos, y mejorar continuamente el Sistema Integrado de Gestión, manteniendo la conformidad con las normas ISO, la acreditación ONAC y los principios WebTrust y fortaleciendo la confianza en los servicios de ANDES SCD S.A.

2. Alcance

Aplica a todos los Procesos, Servicios, Colaboradores, Proveedores y/o Consultores y Partes Interesadas que intervienen en la operación de ANDES SCD S.A, en el marco de la prestación de servicios de certificación digital, firma electrónica y servicios de confianza, así como de las soluciones de gestión documental inteligente, procesamiento inteligente de documentos (IDP), automatización robótica de procesos (RPA), hiperautomatización, agentes inteligentes y demás productos y servicios basados en inteligencia artificial, incluyendo el uso de IA en los procesos internos de desarrollo de software y demás actividades relacionadas. Incluye igualmente los servicios ofrecidos a los clientes bajo modelo de Software como Servicio (SaaS) que incorporen funcionalidades de inteligencia artificial y las disposiciones regulatorias aplicables emitidas por la Superintendencia Financiera de Colombia relacionadas con ciberseguridad **(Circular Externa 007 de 2018, incorporada a la Circular Básica Jurídica)**, computación en la nube.

Las no aplicabilidades o exenciones se encuentran dentro de la declaración de aplicabilidad.

3. Política

La entidad, como prestadora de servicios de certificación digital en Colombia, se compromete a garantizar la confidencialidad, integridad y disponibilidad de la información; a mejorar continuamente la prestación de servicios seguros y de calidad para satisfacer al cliente; y a cumplir los requisitos normativos aplicables y los asociados a la seguridad de la información.

En consecuencia, ANDES SCD S.A se compromete a:

- Fortalecer la resiliencia operacional de los servicios de certificación digital mediante la integración de capacidades de continuidad del negocio, recuperación ante desastres, gestión de crisis, ciberseguridad y gestión de proveedores críticos.
- Garantizar el cumplimiento de todos los requisitos legales, normativos, contractuales y demás disposiciones aplicables al contexto de la organización.
- Asegurar el aumento de la satisfacción de los clientes mediante la prestación de servicios seguros, confiables y de alta calidad, que respondan a sus necesidades y expectativas.
- Proteger la información gestionada por la organización frente a accesos no autorizados, alteraciones, pérdidas o cualquier otro tipo de amenaza que comprometa su confidencialidad, integridad o disponibilidad.
- Identificar, evaluar y gestionar de manera oportuna los riesgos asociados a la calidad y a la seguridad de la información, implementando controles eficaces para su mitigación.
- Fomentar una cultura organizacional orientada a la mejora continua, la concienciación y la corresponsabilidad en todos los niveles de la organización.
- Proveer los recursos humanos, tecnológicos y financieros necesarios para el mantenimiento, fortalecimiento y mejora del sistema integrado de gestión.
- Gestionar la ciberseguridad bajo un enfoque de prevención, protección y detección, respuesta y comunicación, y recuperación y aprendizaje, fortaleciendo

la resiliencia frente a ciberamenazas e incidentes que puedan afectar los servicios de certificación digital.
- Gobernar de forma segura el uso de servicios de computación en la nube, exigiendo a los proveedores las certificaciones, niveles de servicio, cifrado, independencia de los datos y estrategias de continuidad y migración apropiados.
- Promover el uso seguro, ético, responsable y transparente de la inteligencia artificial, tanto en los productos y servicios ofrecidos a los clientes como en los procesos internos de la organización, garantizando la protección de la información y de los datos personales, la supervisión humana proporcional al riesgo, la trazabilidad de los resultados, la gestión de riesgos asociados y el cumplimiento de los principios definidos en el Sistema de Gestión de Inteligencia Artificial.

4. Objetivos

4.1. Objetivos de Calidad

- Impulsar la mejora continua de los procesos y servicios mediante la implementación de acciones de mejora documentadas, con base en los resultados de auditorías internas y retroalimentación de clientes, para fortalecer la eficiencia operativa y la calidad del servicio.
- Incrementar la satisfacción de los clientes y partes interesadas, mediante la atención oportuna de quejas, sugerencias y la mejora continua de los procesos.
- Evaluar el desempeño del sistema de gestión de calidad mediante la ejecución de auditorías internas y la Revisión por la Dirección, con el fin de garantizar su eficacia y alineación con los objetivos estratégicos de la organización.

4.2. Objetivos de Seguridad de la Información

- Proteger la confidencialidad, integridad y disponibilidad de la información, asegurando que no se presenten incidentes críticos de seguridad durante el año,

mediante la implementación de controles técnicos y administrativos actualizados y el monitoreo continuo de los activos de información.

- Gestionar los riesgos de seguridad de la información evaluando los activos críticos al menos una vez al año, e implementando planes de tratamiento que reduzcan la probabilidad e impacto de amenazas identificadas.
- Establecer y mantener mecanismos eficaces de monitoreo, respuesta a incidentes y continuidad del negocio, garantizando que los incidentes sean detectados y atendidos, con seguimiento de su efectividad.
- Fomentar la cultura de seguridad de la información mediante la ejecución de campañas de concientización y una capacitación a los colaboradores, con el fin de reducir errores humanos y fortalecer la protección de los activos de información.
- Fortalecer la ciberseguridad, la continuidad del negocio y la resiliencia operacional, asegurando la detección, respuesta y recuperación oportuna ante incidentes cibernéticos, interrupciones operativas y desastres, y verificando periódicamente la efectividad de los controles implementados.

4.3. Objetivos de Continuidad de Negocio

- Mantener y probar periódicamente los planes de continuidad de negocio y recuperación ante desastres para asegurar la disponibilidad de los procesos y servicios críticos.
- Verificar el cumplimiento de los tiempos objetivos de recuperación (RTO) y puntos objetivos de recuperación (RPO) definidos para los servicios críticos, mediante pruebas y ejercicios periódicos.
- Fortalecer la resiliencia organizacional mediante la identificación y tratamiento de riesgos que puedan afectar la continuidad de los procesos críticos y la prestación de servicios de confianza digital.

5. Principios de Seguridad de la Información

- **Confidencialidad:** Garantizar que la información solo sea accesible por personas debidamente autorizadas, evitando su divulgación no intencionada o el acceso indebido.
- **Integridad:** Asegurar que la información se mantenga precisa, completa y libre de modificaciones no autorizadas durante todo su ciclo de vida.
- **Disponibilidad:** Velar porque la información y los sistemas que la soportan estén accesibles y operativos para los usuarios autorizados en el momento en que se requieran.

6. Lineamiento de Ciberseguridad

ANDES SCD S.A gestiona la ciberseguridad como parte integral de su Sistema Integrado de Gestión, desarrollando las capacidades necesarias para anticipar, prevenir, detectar, responder y recuperarse ante ciberamenazas e incidentes que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información y la confiabilidad de los servicios de certificación digital. Para ello adopta los siguientes lineamientos:

- Prevención: establecer y documentar controles de acceso y gestión de identidades bajo el principio de mínimo privilegio, prevenir la fuga de información, asegurar la plataforma tecnológica, identificar riesgos cibernéticos emergentes e incorporar la respuesta a ciberataques dentro de los planes de continuidad del negocio. Dichos controles incluirán autenticación multifactor, revisión periódica de privilegios y gestión del ciclo de vida de las identidades.
- Protección y detección: monitorear de forma continua la plataforma tecnológica, gestionar las vulnerabilidades y emplear mecanismos de correlación de eventos que permitan identificar oportunamente eventos e

incidentes de ciberseguridad. Adicionalmente, la organización integra fuentes de inteligencia de amenazas para detectar indicadores de compromiso (IoC) y anticipar riesgos cibernéticos emergentes.

- Respuesta y comunicación: contar con procedimientos de respuesta a incidentes, preservar las evidencias digitales, reportar los incidentes a las autoridades competentes —incluyendo al COLCERT o a los CSIRT sectoriales cuando corresponda— e informar a las partes interesadas afectadas.
- Recuperación y aprendizaje: restaurar los servicios afectados, ajustar el Sistema de Gestión de Seguridad de la Información con base en los incidentes presentados y socializar las lecciones aprendidas.
- La gestión de la ciberseguridad se apoya en estándares de referencia tales como ISO/IEC 27001, se mide mediante indicadores de eficacia y se fortalece con una cultura permanente de concientización, difusión y capacitación dirigida a colaboradores, contratistas y terceros relevantes. Estas capacidades se desarrollan, además, en las políticas específicas de seguridad de la información y ciberseguridad de la organización, que hacen parte de la documentación complementaria de esta política rectora.
- La gestión de la ciberseguridad se integra con los procesos de continuidad del negocio, gestión de crisis y recuperación ante desastres, con el propósito de garantizar la resiliencia operacional y la continuidad de los servicios críticos ante eventos de origen tecnológico o cibernético.

7. Lineamiento Computación en la Nube

Cuando ANDES SCD S.A. soporta sus procesos o servicios en la nube, gestiona los riesgos derivados dentro del Sistema Integrado de Gestión, alineados a los requisitos en Seguridad de la Información de la norma ISO/IEC 27001 en su versión vigente, niveles de servicio acordes con la criticidad, cifrado de la información en tránsito y en reposo, independencia y respaldo de los datos, autenticación multifactor, cláusulas contractuales de seguridad y una estrategia de continuidad y migración.

Estos controles se desarrollan en la Política Seguridad de Servicios en la Nube, que hace parte de la documentación complementaria de esta política rectora.

Los proveedores de servicios en la nube deberán demostrar capacidades adecuadas de continuidad, recuperación ante desastres, gestión de incidentes y resiliencia operacional acordes con la criticidad de los servicios soportados.

8. Lineamiento de Uso Seguro y Responsable de la Inteligencia Artificial

ANDES SCD S.A usa la inteligencia artificial (IA) de forma segura, ética, responsable y transparente, asegurando la supervisión humana proporcional al riesgo, la protección de la información y de los datos personales, y la confiabilidad de los servicios de certificación digital, firma electrónica y servicios de confianza. La clasificación por nivel de riesgo, la gobernanza, el ciclo de vida, la protección de la información, la protección de datos personales, la seguridad, la continuidad de los servicios soportados por IA, la trazabilidad, la supervisión humana, la gestión de riesgos y el uso de IA en el desarrollo de software se desarrollan en la Política de Uso Seguro y Responsable de la Inteligencia Artificial alineada con la norma ISO/IEC 42001. Dicha política desarrolla, además, las condiciones específicas aplicables a los servicios SaaS con componentes de IA ofrecidos a los clientes, incluidas la transparencia contractual, la limitación de responsabilidad, los niveles de servicio, la segregación de datos entre clientes y la prohibición de utilizar información de clientes para entrenar modelos de terceros sin autorización expresa.

9. Responsabilidades

- La Alta Dirección lidera, respalda y promueve el Sistema Integrado de Gestión, asegura su alineación con la estrategia organizacional y provee los recursos necesarios para su implementación y mejora continua.
- El Oficial de Seguridad de la Información y Continuidad de Negocio y el Coordinador del Sistema de Gestión Integrado (SGI) coordinan la

implementación, el seguimiento, la evaluación y la mejora del sistema, y garantizan el cumplimiento de los requisitos normativos y organizacionales.

- Los propietarios de procesos, activos de información y servicios tecnológicos son responsables de identificar riesgos asociados a continuidad, ciberseguridad e inteligencia artificial, así como de implementar y mantener los controles definidos por la organización.
- Todos los colaboradores conocen, cumplen y aplican esta política en sus funciones, y participan activamente en el fortalecimiento del sistema integrado y en una cultura de calidad y seguridad de la información.
- Las áreas Comercial y Jurídica de Contratos son responsables de incorporar en los contratos y términos de servicio de las soluciones SaaS con componentes de IA las cláusulas de transparencia, limitación de responsabilidad, niveles de servicio y condiciones de uso de datos exigidas por la Política de Uso Seguro y Responsable de la Inteligencia Artificial.

10. Revisión, Vigencia y Documentación Complementaria

Esta política será revisada anualmente o cuando se presenten cambios significativos en el entorno legal, normativo o estratégico de la organización.

Asimismo, la Política Integrada constituye el marco rector para la calidad, la seguridad de la información, la continuidad del negocio, la ciberseguridad y el uso responsable de la inteligencia artificial dentro del Sistema Integrado de Gestión y es desarrollada mediante políticas, procedimientos, manuales y formatos específicos que incorporan los requisitos normativos y legales en materia de Calidad, Seguridad de la Información, Ciberseguridad, Computación en la Nube, Inteligencia Artificial, Protección de Datos Personales y Continuidad del Negocio, los cuales desarrollan los controles necesarios para su implementación y deben alinearse con los principios aquí establecidos. Entre dichos documentos específicos se encuentran, entre otros:

- Política de Uso Seguro y Responsable de la Inteligencia Artificial.
- Política Seguridad de Servicios en la Nube.

- Política de Tratamiento de Datos Personales.
- Lineamiento de Desarrollo Seguro de Aplicaciones.
- Política de Control de Acceso.
- Política de Uso de Controles Criptográficos.
- Política de Seguridad de la Información para la Relación con Proveedores.

En consecuencia, la Política Integrada define los principios, compromisos y lineamientos generales que rigen todo el Sistema Integrado de Gestión, mientras que el desarrollo detallado de cada materia se establece en las políticas específicas antes referenciadas.

Firmado por:
Sandra Cecilia Restrepo Martinez
2026/08/28 10:50:45:596

SANDRA CECILIA RESTREPO MARTINEZ
Presidente del Comité de Políticas y Seguridad

11. Control de Cambios

Versión	Fecha	Detalle	Responsable
1.0	12/02/2016	Original	Coordinador Sistemas de Gestión
1.1	16/05/2017	Se adiciona compromiso con a la identificación, valoración y determinación de controles. ajustes en redacción en cuanto a la normatividad y mejora continua.	Coordinador Sistemas de Gestión
1.2	02/10/2018	Se realiza revisión de la Política integral.	Coordinador Sistemas de Gestión

		se registra el cambio de la nueva representación legal y Gerencia general de la organización.	
1.3	29/04/2020	Se separó un objetivo del SST quedando 6 objetivos.	Coordinador Sistemas de Gestión – Líder SST
1.4	4/08/2021	Se incluyen los objetivos del SGC. Se actualiza "requisitos legales" a "requisitos". Se elimina la descripción inicial de la organización. Se integran objetivos de SST con los objetivos de calidad.	Director SGI / Líder SST / Analista Senior SGI
2	23/09/2022	Se actualiza la firma por la de la nueva Gerente General, Sandra Cecilia Restrepo Martínez.	Director SGI/ Analista Senior SGI
3	14/04/2023	Se actualiza logo, encabezado y tipo de letra del documento de acuerdo con la nueva identidad corporativa. Se actualiza cargo "Director SGI" a "Director Administrativo y Financiero" Se incluye lineamiento de desarrollo sostenible	Director Administrativo y Financiero / Analista Junior SGI
4	20/02/2024	Se realiza la Inclusión nuevo objetivo de SST: "Evaluar el grado de efectividad y cumplimiento de las acciones del Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST), que se han definido para la mejora continua" Se actualiza el cargo responsable de la elaboración de Analista Senior SGI a Profesional SGI	Consultor SST Profesional SGI

		Se actualiza el cargo Director Administrativo y Financiero por Director de Estrategia y Procesos.	
5	11/06/2024	Se incluye objetivo asociado a Incorporación de las consideraciones sobre el cambio climático de acuerdo con la NTE-3.3-62	Analista SGI / Profesional SGI
6	19/08/2025	Se realiza la unifican la política integral y la política de seguridad de la información, asegurando que exprese de forma clara las intenciones de la organización. Se establece la política integral dando cumplimiento a los requerimientos de la norma ISO9001 e ISO27001 en sus versiones actuales. Se sintetizan los objetivos establecidos, garantizando que sean medibles, relevantes y útiles para la toma de decisiones estratégicas, de acuerdo con la norma ISO9001 e ISO27001 en sus versiones actuales. Se detallan las responsabilidades frente a los sistemas de gestión y política integral.	Oficial de Seguridad de la Información y Continuidad de Negocio / Coordinador SGI
7	25/06/2026	- Se incorporan los elementos de ciberseguridad de la Circular Externa 007 de 2018, estableciendo el ciclo de prevención, protección y detección, respuesta y comunicación, y	Oficial de Seguridad de la Información y Continuidad de Negocio / Analista

		recuperación y aprendizaje, mediante la creación de la sección de Ciberseguridad y un objetivo de seguridad asociado. - Se realiza la actualización del documento, cambiando la denominación de Política Integral a Política Integrada- Se incorporan los elementos de computación en la nube de la Circular Externa 005 de 2019 (selección y certificación de proveedores, cifrado de la información, independencia y respaldo de datos, autenticación de múltiple factor, cláusulas contractuales y continuidad/estrategia de migración), mediante la creación de la sección de Computación en la Nube. - Se incluye la sección de Uso Seguro y Responsable de la Inteligencia Artificial, alineada con la norma ISO/IEC 42001 y la normatividad de protección de datos personales. - Se amplía el marco normativo del numeral 1. Propósito con las normas ISO/IEC 27017, ISO/IEC 27018 e ISO/IEC 42001, y se incorporan los compromisos de ciberseguridad, nube e inteligencia artificial en la Política. - Se renombra la sección duplicada "Responsabilidades" a "Revisión,	de seguridad de la información

		Vigencia y Documentación Complementaria".	
8	27/08/2026	-Se ajusta el numeral 2 (Alcance) y el numeral 8 (Lineamiento de Uso Seguro y Responsable de la Inteligencia Artificial) para dejar explícito que el marco rector cubre los servicios ofrecidos a los clientes bajo modelo de Software como Servicio (SaaS) con componentes de IA, incluyendo la transparencia contractual, la limitación de responsabilidad, los niveles de servicio, la segregación de datos entre clientes y la restricción al uso de datos de clientes para entrenar modelos de terceros. -Se incluyen el item 4.3 Objetivos de Continuidad de Negocio -Se incorpora en el numeral 9 (Responsabilidades) el rol de las áreas Comercial y Jurídica de Contratos frente a las cláusulas contractuales de IA en los servicios SaaS. -Se incorporan los lineamientos de Ciberseguridad	Oficial de Seguridad de la Información y Continuidad de Negocio