


POLÍTICA INSTITUCIONAL DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES DEL CONSEJO COLOMBIANO DE SEGURIDAD – CCS			
Guía	Rev.5	2026.05.12	

1. Aviso de Privacidad.

En cumplimiento de la Ley 1581 de 2012, reglamentada por el Decreto 1377 de 2013 y por el Decreto 1081 de 2015, sobre la protección de datos en Colombia, el CCS, ha implementado una Política de tratamiento y Protección de Datos Personales, que garantiza la seguridad, transparencia y correcto uso de la información, el cual podrá ser verificado en cualquier momento por parte de los titulares de los datos que reposen en la compañía.

El tratamiento de los datos personales de colaboradores, clientes y afiliados, proveedores personas naturales y jurídicas, visitantes, y cualquier otro usado para el cumplimiento de su actividad, tiene por finalidad servir como medio para el desarrollo del objeto social, los contratos de trabajo y el mantenimiento de vínculos comerciales, el manejo de la información recolectada, entre otros pero sin limitarse a estos, a través de sitios web, de relaciones comerciales/contractuales y de la línea de Emergencias del Centro de Información de Seguridad sobre Productos Químicos - Cisproquim®, así como el uso de imágenes a través del Circuito Cerrado de Televisión – CCTV. En consecuencia y con ese objetivo, la información podrá ser procesada, recolectada, almacenada, usada, actualizada y transmitida conforme lo indica el manual y el procedimiento previsto por el CCS para este efecto.

2. Introducción y Fundamento Legal.


El CCS, en cumplimiento de la Constitución Política de Colombia, la Ley 1581 de 2012, “*Por la cual se dictan disposiciones generales para la protección de datos personales*”, y establece los derechos de los titulares y las obligaciones de responsables y encargados, sus decretos reglamentarios y las demás normas concordantes sobre la materia, en especial, las circulares y resoluciones expedidas por la Superintendencia de Industria y Comercio sobre la materia; adopta esta Política Institucional de Tratamiento de Datos Personales.

El tratamiento de datos personales en el Consejo Colombiano de Seguridad (CCS) se encuentra sometido al marco normativo colombiano y a los lineamientos expedidos por la Superintendencia de Industria y Comercio (SIC), autoridad nacional de protección de datos personales.

El CCS toma igualmente como referente de obligatorio cumplimiento, la normatividad dispuesta en:

a. Decretos reglamentarios y normas concordantes:

- Decreto 1377 de 2013: reglamenta parcialmente la Ley 1581 de 2012, en aspectos relacionados con autorizaciones, políticas de tratamiento, derechos de los titulares, transferencia y transmisión internacional, datos sensibles y responsabilidad demostrada.
- Decreto 1081 de 2015: compila y actualiza las normas reglamentarias, consolidando parte de lo dispuesto en el Decreto 1377 de 2013 y armonizándolo dentro del Decreto Único Reglamentario del Sector Presidencia de la República.

POLÍTICA INSTITUCIONAL DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES DEL CONSEJO COLOMBIANO DE SEGURIDAD – CCS			
Guía	Rev.5	2026.05.12	

- Decreto 1074 de 2015: Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, que recoge y unifica disposiciones relevantes sobre protección de datos, incluyendo el deber de responsabilidad demostrada.
- b. Lineamientos y Circulares de la SIC:
 - Circular Externa No. 003 de 2024: dirigida a administradores societarios, establece obligaciones de supervisión y control en el cumplimiento de la normativa de protección de datos, con énfasis en el principio de responsabilidad demostrada (accountability).
 - Circular Externa No. 002 de 2024: fija lineamientos sobre el tratamiento de datos personales en sistemas de inteligencia artificial (IA), estableciendo medidas de transparencia, evaluación de riesgos y garantías adicionales para los titulares frente a decisiones automatizadas.
 - Circular Externa No. 001 de 2025: establece reglas específicas para el sector fintech en el uso de datos personales, reforzando obligaciones de seguridad, consentimiento informado y trazabilidad.
 - Resoluciones y sanciones de la SIC: la autoridad ejerce facultades de vigilancia y control, imponiendo sanciones a las entidades que incumplan la Ley 1581 de 2012 y sus reglamentos, y ordenando medidas correctivas cuando corresponda.


El CCS mantendrá actualizada esta Política conforme a futuras disposiciones legales y regulatorias, así como a los lineamientos que en adelante expida la SIC u otras autoridades competentes.

3. Objetivo General.

- Garantizar el derecho fundamental al Habeas Data, asegurando un manejo transparente, seguro y responsable de la información personal, definiendo para el efecto lineamientos claros para la recolección, almacenamiento, uso, circulación, transferencia, transmisión y supresión de datos personales en el CCS.

4. Objetivos Específicos.

- Garantizar la confidencialidad, integridad y seguridad de la información personal de sus colaboradores, clientes y afiliados, visitantes, proveedores, usuarios del Centro de Información de Seguridad sobre Productos Químicos - Cisproquim® y visitantes a los sitios web y soluciones del CSS que proporcionan enlaces o hacen referencia a esta Política de Tratamiento y Protección de Datos Personales, en especial, a quienes visitan los sitios web <https://ccs.org.co>, <https://campus.ccs.org.co>, <https://www.congresoccs.org.co> y https://gcruc.force.com/Contratista/HBT_Login , https://gcruc.force.com/Contratante/HBT_LoginContratante, así como las soluciones del CCS que proporcionan enlaces o hacen referencia a esta Política de Tratamiento y Protección de Datos Personales y que este último haya recolectado en desarrollo de su objeto social.
- Velar porque el tratamiento de los datos personales de sus colaboradores, clientes y afiliados, visitantes, proveedores, usuarios del Cisproquim® y visitantes a los sitios

POLÍTICA INSTITUCIONAL DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES DEL CONSEJO COLOMBIANO DE SEGURIDAD – CCS			
Guía	Rev.5	2026.05.12	

web y soluciones del CSS que proporcionan enlaces o hacen referencia a esta Política de Tratamiento y Protección de Datos Personales o a cualquier otra base de datos usada para el cumplimiento de la actividad del CSS, a los sitios web <https://ccs.org.co>, <https://campus.ccs.org.co>, <https://www.congresoccs.org.co> y https://gcruc.force.com/Contratista/HBT_Login, https://gcruc.force.com/Contratante/HBT_LoginContratante; así como las soluciones del CCS que proporcionan enlaces o hacen referencia a esta Política de Tratamiento y Protección de Datos Personales o a cualquier otra base de datos usada para el cumplimiento de la actividad del CCS; se dé dentro de los parámetros establecidos por la ley y por la Constitución Política de Colombia.


5. Alcance.

Esta política aplica a: colaboradores, clientes, afiliados, proveedores, visitantes, usuarios del Cisproquim®, y personas que interactúen con portales web, aplicaciones y soluciones digitales del CCS. Lo anterior, siempre y cuando el CCS haya recolectado la información antes referida, en desarrollo de su objeto social.

6. Principios Rectores.

Los principios que orientan el tratamiento de datos personales en el CCS son: legalidad, finalidad, libertad, veracidad, transparencia, acceso restringido, seguridad, confidencialidad, proporcionalidad y responsabilidad demostrada, así:

- Legalidad: El tratamiento de datos se realizará conforme a la Constitución, la Ley 1581 de 2012 y demás normas vigentes.
- Finalidad: Los datos se recolectan con propósitos legítimos, específicos e informados al titular, sin que puedan usarse para fines distintos.
- Libertad: El tratamiento se realiza solo con el consentimiento libre, previo, expreso e informado del titular, salvo excepciones legales.
- Veracidad o calidad: La información personal debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. No se admiten datos parciales, incompletos o que induzcan a error.
- Transparencia: Se garantiza al titular el derecho a obtener información sobre sus datos en cualquier momento y sin restricciones indebidas.
- Acceso restringido: El acceso a los datos está limitado a personas autorizadas y únicamente para las finalidades previamente establecidas.
- Seguridad: Se adoptan medidas técnicas, humanas y administrativas necesarias para proteger la información contra uso no autorizado o fraudulento.
- Confidencialidad: Todas las personas que intervengan en el tratamiento están obligadas a guardar reserva sobre la información personal, incluso después de finalizada su relación con el CCS.
- Proporcionalidad: Solo se recolectarán los datos estrictamente necesarios para cumplir la finalidad informada, evitando excesos o información no pertinente.
- Responsabilidad demostrada (accountability): El CCS debe demostrar, mediante documentación y evidencias, que cumple con los principios y obligaciones legales en el tratamiento de datos.

POLÍTICA INSTITUCIONAL DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES DEL CONSEJO COLOMBIANO DE SEGURIDAD – CCS			
Guía	Rev.5	2026.05.12	

7. Finalidades y Uso del Tratamiento.

El CCS usará los datos personales para:

- Gestión laboral y contractual: Se refiere al tratamiento de datos personales necesarios para la administración del vínculo laboral o contractual con colaboradores, proveedores y contratistas. Incluye procesos como la afiliación a seguridad social, pago de salarios y honorarios, administración de beneficios, evaluaciones de desempeño, cumplimiento de obligaciones contractuales y gestión de nómina.
- Procesamiento de pedidos y transacciones: Implica el uso de datos personales para la gestión de operaciones comerciales, como la recepción, validación, facturación y despacho de pedidos, así como la ejecución de transacciones financieras, conciliación de pagos y gestión de cuentas por cobrar y por pagar.
- Atención al cliente/afiliado/usuario y comunicaciones institucionales: Engloba las actividades destinadas a brindar soporte, resolver inquietudes y mantener informados a clientes, afiliados y usuarios sobre productos, servicios, eventos o actividades del CCS. Incluye la gestión de peticiones, quejas y reclamos (PQR), envío de boletines informativos, y comunicaciones sobre cambios relevantes en las políticas o servicios.
- Administración de postulaciones laborales y certificaciones: Comprende el tratamiento de datos personales de candidatos a procesos de selección, así como de estudiantes, participantes o usuarios que busquen acceder a capacitaciones, evaluaciones o certificaciones ofrecidas por el CCS. Incluye la verificación de antecedentes, registro académico y expedición de certificados.
- Uso de CCTV y herramientas tecnológicas para seguridad: Hace referencia al tratamiento de imágenes y demás datos captados mediante circuito cerrado de televisión (CCTV), sistemas de control de accesos, biometría u otras herramientas tecnológicas utilizadas para garantizar la seguridad de instalaciones, personas y bienes del CCS. También comprende la prevención y detección de conductas ilícitas. El tratamiento de imágenes captadas mediante sistemas de videovigilancia se realizará conforme a la política institucional de tratamiento de imágenes y grabaciones prevista en este documento.
- Cumplimiento de obligaciones legales y regulatorias: Se refiere al uso de datos personales para dar cumplimiento a las exigencias de ley y a los requerimientos de autoridades administrativas, judiciales y de control, tanto en Colombia como en el exterior. Incluye reportes a entidades de vigilancia, verificación en listas restrictivas y obligaciones en materia de prevención de lavado de activos y financiación del terrorismo (LA/FT).

Así, es posible que el CCS recopile información, incluida aquella de carácter personal, sobre sus colaboradores, clientes y afiliados, visitantes, proveedores, usuarios del Cisproquim® y visitantes a los sitios web y soluciones del CSS que proporcionan enlaces o hacen referencia a esta Política de Tratamiento y Protección de Datos Personales o a cualquier otra base de datos usada para el cumplimiento de la actividad del CSS, en la medida en que dichos titulares utilizan los sitios web y soluciones del CCS e interactúa con este último. Asimismo, el CCS adquiere información personal de fuentes confiables de terceros y también recurre a terceros para que recopilen información personal en su nombre.


Esta información recopilada la usamos con fines comerciales tales como:

- Procesar pedidos, incluidas las transacciones de pago.
- Ofrecer suscripciones a boletines informativos.
- Enviar y administrar las comunicaciones y preferencias de marketing.
- Crear una cuenta.
- Aprovisionar sitios web y soluciones y habilitar el uso de ciertas características.
- Personalizar, mejorar y optimizar la experiencia y las soluciones del usuario.
- Ofrecer servicio de atención al cliente.
- Estudiar de las postulaciones laborales.
- Administrar la educación, las pruebas y las certificaciones en línea.
- Combinar la información que recopilamos en nuestros diferentes sitios web y soluciones, con información obtenida de otras fuentes. Esto nos ayuda a mejorar la exactitud y también personalizar nuestras interacciones con los titulares de la mejor manera.

Si se opta por proporcionarle al CCS información personal de terceros (como nombre, correo electrónico y número de teléfono), los titulares declaran tener el permiso del tercero para hacerlo. Entre ejemplos de esto, se encuentra el hecho de reenviar material de referencia o marketing a un contacto o enviar referencias laborales. Los terceros pueden cancelar la suscripción de cualquier comunicación futura. En ciertos casos, el CCS, y los terceros con los que trabajamos, pueden recopilar datos de manera automática a través de cookies, registros de acceso, balizas web o beacons y otras aplicaciones similares. Esta información se utiliza para comprender aún más y mejorar la capacidad de uso, el rendimiento y la eficacia del sitio web o la solución y para personalizar las características, el contenido o las ofertas que se le muestran al usuario.

El CCS puede hacer uso de la información personal, con el fin de llevar a cabo actividades comerciales y contribuir a asegurar la seguridad de su negocio, ofrecer, mejorar y personalizar sus sitios web y soluciones, enviar comunicaciones de marketing y de otros tipos, y para otros fines legítimos, dentro de lo permitido por la ley. Algunas de las maneras en las que el CCS puede usar la información personal, incluyen:

- Ofrecer una solución que se haya solicitado.
- Analizar, admitir y mejorar sus sitios web y soluciones y la experiencia del usuario.
- Personalizar sus sitios web y soluciones, boletines informativos y otro tipo de comunicaciones.
- Administrar y procesar los exámenes de certificación y capacitación.
- Administrar la relación e interacciones de los titulares con el CCS.
- Enviarle comunicaciones a los titulares, incluidas aquellas relacionadas con marketing o para fines de satisfacción del cliente, ya sea directamente desde el CCS o a través de sus partners.
- Consultar listas vinculantes y restrictivas en Colombia y en el exterior, en especial pero sin limitarse a ellas, las bases de datos para prevenir de lavado de activos y la financiación del terrorismo.

POLÍTICA INSTITUCIONAL DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES DEL CONSEJO COLOMBIANO DE SEGURIDAD – CCS			
Guía	Rev.5	2026.05.12	


8. Deber de veracidad de la entrega de la información de los Titulares.

El Cliente/Proveedor/Afiliado/Usuario, acepta suministrar información verídica, exacta, actualizada y completa al entregársela al CCS por cualquier medio. Es responsabilidad del Cliente/Proveedor/Afiliado/Usuario mantener y actualizar la información suministrada al CCS por cualquier medio, de tal manera que la misma siga siendo verídica, exacta, actualizada y completa. En caso tal que el Cliente/Proveedor/Afiliado/Usuario suministre información que sea fraudulenta, no verídica, inexacta, incompleta o desactualizada o que el CCS tenga motivos razonables para presumir que dicha información es fraudulenta, no verídica, inexacta, incompleta o desactualizada, el CCS, no será responsable de aquella información que se presume fraudulenta, no verídica, inexacta, incompleta o desactualizada que suministre el Cliente/Proveedor/Afiliado/Usuario, por ende, el Cliente/Proveedor/Afiliado/Usuario asumirá su responsabilidad ante terceros por aquella información que en uso del servicio que se brinda. El Cliente/Proveedor/Afiliado/Usuario mantendrá indemne al CCS, para lo cual acepta defender, indemnizar y eximir de responsabilidad al CCS y sus colaboradores (empleados o contratistas de prestación de servicios personales), de cualquier acción administrativa o judicial que origine o se relacione con la información fraudulenta, no verídica, inexacta, incompleta o desactualizada que suministre al CCS.

9. Derechos de los Titulares.

Los titulares tienen derecho a:

- Conocer, actualizar y rectificar sus datos personales: Los titulares tienen derecho a acceder a la información personal que repose en las bases de datos del CCS y a exigir que sea actualizada, corregida o rectificadas cuando esté incompleta, inexacta o desactualizada.
- Solicitar prueba de la autorización otorgada: El titular puede solicitar al CCS evidencia de la autorización previa, expresa e informada que otorgó para el tratamiento de sus datos personales, salvo en los casos exceptuados por la ley.
- Ser informados sobre el uso dado a sus datos: El titular tiene derecho a recibir información clara y suficiente sobre el tratamiento, finalidad y uso específico que el CCS ha dado a sus datos personales, en cumplimiento de los principios de transparencia y finalidad.
- Revocar la autorización o solicitar la supresión de datos: En cualquier momento, el titular podrá revocar la autorización otorgada o solicitar la supresión de sus datos, cuando considere que no se están respetando los principios, derechos y garantías constitucionales y legales. La revocatoria o supresión no procederán cuando exista un deber legal o contractual que obligue a conservar la información.
- Presentar quejas ante la SIC y otras autoridades competentes: El titular podrá presentar quejas y reclamos ante la Superintendencia de Industria y Comercio (SIC) o las autoridades correspondientes, por presuntas infracciones a lo dispuesto en la Ley 1581 de 2012 y sus decretos reglamentarios, así como por incumplimiento de las obligaciones establecidas en esta Política.

POLÍTICA INSTITUCIONAL DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES DEL CONSEJO COLOMBIANO DE SEGURIDAD – CCS			
Guía	Rev.5	2026.05.12	

10. Procedimiento para Ejercicio de Derechos.

Las solicitudes podrán realizarse vía correo electrónico a protecciondatos@ccs.org.co o de manera presencial en la sede principal en Bogotá, D. C., ubicada en la Carrera 20 No. 39-52. El CCS dará respuesta dentro de los plazos establecidos en la Ley 1581 de 2012.

11. Consulta de Centrales de Riesgos.

El Cliente/Proveedor/Afiliado/Usuario autoriza al CCS a consultar la información financiera en las distintas centrales de riesgos, el sistema financiero colombiano y en listas públicas tales como, en especial pero sin limitarse a ellas, la Procuraduría General de la Nación, la Contraloría General de la Nación, la Superintendencia de Sociedades, la Superintendencia de Industria y Comercio, las Cámaras de Comercio y demás entes de control nacional que tengan listas dispuestas para tal fin, así como consultar listas vinculantes y restrictivas en Colombia y en el exterior, en especial pero sin limitarse a ellas, las bases de datos para prevenir de lavado de activos y la financiación del terrorismo.

12. Tratamiento de Datos Sensibles.

El CCS sólo tratará datos sensibles con autorización previa, salvo excepciones legales. En estos casos, adoptará medidas reforzadas de seguridad y confidencialidad.

13. Tratamiento de Imágenes, Grabaciones y Datos Biométricos.

El Consejo Colombiano de Seguridad – CCS podrá realizar el tratamiento de imágenes, grabaciones audiovisuales y, cuando corresponda, datos biométricos, captados mediante sistemas de videovigilancia (CCTV), dispositivos móviles, plataformas virtuales, registros fotográficos institucionales, herramientas de control de acceso o tecnologías similares.

Estas imágenes constituyen datos personales cuando permiten identificar o hacer identificable a una persona natural, razón por la cual su tratamiento se realizará conforme a la Ley 1581 de 2012, el Decreto 1074 de 2015, las directrices de la Superintendencia de Industria y Comercio y las demás normas aplicables.

Las imágenes podrán ser utilizadas para:

- Garantizar la seguridad de personas, bienes e instalaciones del CCS.
- Controlar accesos físicos o lógicos a instalaciones o sistemas.
- Prevenir, detectar o investigar incidentes de seguridad.
- Soportar investigaciones internas o requerimientos de autoridades.
- Documentar actividades institucionales, académicas o eventos.
- Elaborar material institucional, informativo o educativo.

Cuando el CCS utilice sistemas de videovigilancia, informará previamente a los titulares mediante avisos visibles que indiquen al menos:

- la existencia del sistema de videovigilancia,
- la finalidad de la captura de imágenes,
- la identificación del responsable del tratamiento,
- el medio para ejercer derechos de habeas data.

Las grabaciones obtenidas mediante sistemas de videovigilancia serán conservadas únicamente por el tiempo estrictamente necesario para cumplir las finalidades del tratamiento o atender requerimientos legales o de autoridades competentes.

Transcurrido dicho término, las grabaciones serán eliminadas o anonimizadas conforme a los procedimientos internos de seguridad de la información.

El acceso a las grabaciones estará limitado exclusivamente a personal autorizado y se adoptarán medidas técnicas, administrativas y organizativas para evitar:

- accesos no autorizados,
- alteraciones,
- reproducciones indebidas,
- divulgación no autorizada.

En caso de utilizar tecnologías biométricas (reconocimiento facial, huella dactilar u otros), el CCS aplicará medidas reforzadas de protección por tratarse de datos sensibles, incluyendo:

- autorización explícita del titular cuando sea requerida,
- minimización de datos,
- controles de acceso estrictos,
- evaluación previa de riesgos de privacidad.

14. Tratamiento de Datos de Menores.

El tratamiento de datos de niños, niñas y adolescentes se realizará en protección de sus derechos fundamentales y con autorización expresa de sus padres o representantes legales.

15. Transferencia y Transmisión Internacional.

Se permitirá únicamente con autorización expresa del titular y cuando el país receptor cuente con estándares adecuados de protección de datos, conforme a la regulación colombiana.

16. Seguridad de la Información.

El CCS implementa medidas técnicas, humanas y administrativas para proteger los datos contra pérdida, adulteración, acceso no autorizado o uso indebido.

El CCS implementará un Programa Integral de Gestión de Datos Personales, basado en el principio de responsabilidad demostrada (accountability), que incluirá políticas, procedimientos, auditorías internas, capacitación del personal y mecanismos de mejora continua.

17. Gestión de Incidentes de Seguridad de la Información.

El Consejo Colombiano de Seguridad – CCS reconoce la importancia de garantizar la integridad, disponibilidad y confidencialidad de los datos personales bajo su responsabilidad. En ese sentido, ha adoptado procedimientos internos para la identificación, gestión y mitigación de incidentes de seguridad que puedan comprometer la información personal tratada en sus sistemas, bases de datos o infraestructuras tecnológicas.

Se entenderá por incidente de seguridad cualquier evento real o potencial que implique la pérdida, alteración, acceso no autorizado, divulgación indebida, destrucción o uso irregular de datos personales, así como cualquier vulneración de los controles de seguridad implementados para proteger dicha información.

Ante la ocurrencia de un incidente de seguridad que involucre datos personales, el CCS adoptará las siguientes medidas:

a. Detección y registro del incidente:

Una vez detectado el incidente, el CCS implementará las acciones necesarias para contener sus efectos, evitar su propagación y mitigar los posibles impactos sobre los titulares de los datos.

b. Evaluación del impacto:

El CCS evaluará la naturaleza del incidente, el tipo de datos comprometidos, el número de titulares potencialmente afectados y los riesgos asociados a la vulneración de la información.

c. Notificación a las autoridades competentes:

Cuando el incidente implique riesgos significativos para los titulares o constituya una vulneración de las medidas de seguridad, el CCS informará a la autoridad competente, en particular a la Superintendencia de Industria y Comercio (SIC), de conformidad con la normativa aplicable y los procedimientos establecidos por dicha entidad.

d. Comunicación a los titulares cuando sea necesario:

En aquellos casos en que el incidente pueda afectar de manera relevante los derechos o intereses de los titulares de los datos, el CCS podrá informar a los titulares afectados sobre la ocurrencia del incidente, las posibles consecuencias y las medidas adoptadas para su mitigación.

e. Implementación de medidas correctivas y preventivas:

Posteriormente al incidente, el CCS adoptará las acciones necesarias para corregir las causas que lo originaron, fortalecer sus controles de seguridad y prevenir la ocurrencia de situaciones similares en el futuro.

f. Registro y seguimiento:

El CCS mantendrá un registro interno de los incidentes de seguridad relacionados con datos personales, incluyendo las acciones adoptadas, con el fin de garantizar la trazabilidad, el aprendizaje organizacional y el cumplimiento del principio de responsabilidad demostrada (accountability).

El CCS podrá integrar este procedimiento dentro de su Sistema de Gestión de Seguridad de la Información, cuando corresponda, y realizar revisiones periódicas de su eficacia.

18. Uso de Inteligencia Artificial y Procesamiento Automatizado de Datos.

El CCS podrá utilizar herramientas tecnológicas basadas en inteligencia artificial, aprendizaje automático u otros sistemas automatizados para apoyar procesos operativos, analíticos, académicos o administrativos.

En todo caso, el uso de estas tecnologías se regirá por los principios de:

- legalidad
- transparencia
- responsabilidad demostrada
- proporcionalidad
- seguridad de la información
- protección de los derechos de los titulares

Previo a la implementación de soluciones de inteligencia artificial que impliquen tratamiento de datos personales, el CCS realizará evaluaciones de riesgo que permitan identificar:

- posibles impactos sobre los derechos de los titulares,
- riesgos de discriminación algorítmica,
- riesgos de tratamiento indebido o excesivo de datos.

Cuando el tratamiento de datos personales se realice mediante sistemas automatizados, el CCS garantizará que los titulares puedan conocer:

- la existencia de procesos automatizados,
- las finalidades del tratamiento,
- los criterios generales utilizados por dichos sistemas.

El CCS evitará adoptar decisiones que produzcan efectos jurídicos o afecten significativamente a los titulares basadas exclusivamente en procesos automatizados, salvo cuando:

- exista autorización expresa del titular,

- sea necesario para la ejecución de un contrato,
- exista habilitación legal.

En estos casos, el titular tendrá derecho a:

- solicitar intervención humana,
- expresar su punto de vista,
- controvertir la decisión.

El CCS implementará medidas de gobernanza de datos para asegurar que los sistemas de inteligencia artificial:

- utilicen datos adecuados, pertinentes y no excesivos,
- cuenten con controles de calidad de datos,
- eviten sesgos indebidos,
- mantengan trazabilidad en los procesos de tratamiento.

19. Política en Página Web y RUC®.


El Cliente/Proveedor/Afiliado/Usuario acepta esta política al registrarse o interactuar en los portales web y software del CCS.

El Cliente/Proveedor/Afiliado/Usuario está obligado a suministrar información veraz y actualizada. En caso de información fraudulenta, asumirá la responsabilidad y mantendrá indemne al CCS.

20. Deberes del CCS.

El CCS, como Responsable del tratamiento, se compromete a:

- Informar oportunamente las finalidades del tratamiento: El CCS debe garantizar que todo titular conozca, de manera clara, previa y expresa, la finalidad específica para la cual se recolectan y utilizan sus datos personales, asegurando así el principio de transparencia y finalidad establecido por la Ley 1581 de 2012.
- Garantizar la veracidad, actualización y seguridad de la información: El CCS tiene la obligación de velar porque los datos personales bajo su custodia sean veraces, completos, exactos y actualizados, adoptando medidas técnicas, administrativas y humanas que garanticen su integridad, confidencialidad y seguridad, evitando adulteración, pérdida o acceso no autorizado.
- Tramitar consultas y reclamos en los términos legales: El CCS debe atender todas las consultas, solicitudes y reclamos de los titulares dentro de los plazos y condiciones señalados en la Ley 1581 de 2012 y sus decretos reglamentarios, garantizando un procedimiento ágil, transparente y gratuito para el ejercicio del derecho de Habeas Data.
- Cumplir estrictamente las disposiciones normativas vigentes: El CCS, como responsable del tratamiento, debe acatar de manera rigurosa las normas aplicables en materia de protección de datos personales, incluyendo la Ley 1581 de 2012, sus decretos reglamentarios, las circulares e instrucciones de la Superintendencia de

POLÍTICA INSTITUCIONAL DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES DEL CONSEJO COLOMBIANO DE SEGURIDAD – CCS			
Guía	Rev.5	2026.05.12	

Industria y Comercio, y cualquier regulación futura que modifique o complemente el régimen vigente.

21. Casos en los que no se requiere autorización.

La autorización de los titulares no será necesaria cuando se trate de:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial: Cuando una autoridad estatal, administrativa o judicial solicita datos personales en el marco de sus competencias legales, el CCS está facultado para entregarlos sin necesidad de contar con autorización previa del titular, siempre que exista un fundamento jurídico válido.
- Datos de naturaleza pública: La autorización no es necesaria cuando se trate de información considerada pública por la Constitución, la ley o actos administrativos, como por ejemplo datos contenidos en registros públicos, gacetas oficiales o documentos accesibles sin restricción.
- Casos de urgencia médica o sanitaria: Cuando la protección de la vida, salud o integridad del titular u otra persona lo requiera, el CCS puede tratar datos personales sin autorización previa. Esto aplica en situaciones de urgencia médica, sanitaria o de emergencia en las que obtener el consentimiento sea imposible o implique un riesgo mayor.
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos: La autorización tampoco es necesaria cuando los datos se traten con fines históricos, estadísticos o científicos, siempre que se apliquen medidas de anonimización y se respeten los principios de proporcionalidad y finalidad definidos en la ley.
- Datos relacionados con el Registro Civil de las personas: Los datos incluidos en el Registro Civil (nacimiento, matrimonio, defunción, etc.) son de carácter público y, por tanto, no requieren autorización del titular para su tratamiento.

22. Formatos.

El Cliente/Proveedor/Afiliado/Usuario acepta la totalidad de la política de tratamiento de datos personales del CCS, la cual se encuentra publicada en: <https://ccs.org.co/politica-de-privacidad/>

23. Vigencia.

La presente política entra en vigor el 12 de mayo del 2026 y permanecerá vigente mientras exista el CCS. Será revisada y actualizada periódicamente conforme a cambios normativos.

ADRIANA SOLANO LUQUE

Presidenta Ejecutiva