FUNCIÓN DE CUMPLIMIENTO

-POLÍTICA PROTECCIÓN DE DATOS PERSONALES-

S3 CACEIS COLOMBIA S.A. SOCIEDAD FIDUCIARIA

CONTENIDO

1. INTRODUCCIÓN

La presente Política desarrolla lo establecido en los artículos 21 y 28 del Código de Conducta en materia de control de la información y confidencialidad, así como las consecuencias en caso de incumplimiento descritas en el Código General de Conducta de la Entidad y, por consiguiente, enlaza con sus valores éticos y ratifica su firme compromiso de mantener una conducta respetuosa tanto con las normas como los estándares que los empleados y administradores (miembros de la junta directiva y representantes legales) de la Entidad deben tener en cuenta en su operativa diaria.

Santander Caceis Colombia Sociedad Fiduciaria S.A, en adelante S3CC, llevará a cabo medidas que garanticen y permitan demostrar el cumplimiento de las exigencias legales en materia de protección de datos. Esto significa que no solo han de existir las mismas, sino que han de estar adaptadas a las circunstancias de la organización, implementadas y que funcionen en la práctica.

Los empleados y administradores están obligados a respetar la intimidad de las personas, tanto de otros empleados como de clientes, o de cualesquiera otras personas físicas a cuyos datos tengan acceso como consecuencia de la propia actividad de la entidad o desempeño de sus funciones.

2. CONCEPTOS Y TIPOS DE DATOS PERSONALES

En adopción a los lineamientos corporativos, se entenderá por dato de carácter personal: cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo (por ejemplo, datos biométricos), concerniente a personas físicas identificadas o identificables.

- **Información de identificación directa:** datos que incluyen información que permita identificar o distinguir a una persona física directamente y por si mismos sin necesidad de combinarlos con otros datos, como por ejemplo: nombre, dirección, número de teléfono, número de fax, dirección de correo electrónico, perfiles identificadores únicos, como el número de la seguridad social, el número del pasaporte, etc.

- **Datos de carácter identificativo:** Documentos identificativos (DNI, ID number o pasaporte), dirección, imagen, voz, número de seguridad social, teléfono, marcas físicas, nombre y apellidos, firma, huella y firma electrónica.

- **Datos biométricos:** datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

- **Información de identificación indirecta:** datos personales que incluyen información que, aunque por sí misma no pueda identificar ni distinguir directamente a la persona, alguna empresa del Grupo ó un tercero puedan asociarla o vincularla con una persona física teniendo en cuenta todos los medios que probable y razonablemente se puedan usarse. Se trata por tanto de datos que por sí solos no permiten la identificación de las personas pero que combinados junto con otros factores pueden permitir la identificación. Por ejemplo:

  - Datos relativos a las características personales: estado civil, datos de familia, fecha de nacimiento, lugar de nacimiento, edad, sexo, nacionalidad, lengua materna y características físicas.

  - Datos relativos a la personalidad: evaluaciones de perfiles, comportamientos y actitudes.

  - Datos relativos a las circunstancias sociales: características de alojamiento, vivienda, situación familiar, posesiones, aficiones, estilos de vida, pertenencia a asociaciones o clubes, licencias, permisos y autorizaciones.

  - Datos académicos y profesionales: formación, titulaciones, expediente académico y experiencia profesional.

  - Datos relativos al empleo: profesión, puestos de trabajo, datos no económicos de nómina e historial del trabajador.

- Datos que aportan información comercial: actividades y negocios, licencias comerciales y publicaciones en medios de comunicación.

- Datos económicos, financieros y de seguros: ingresos, rentas, inversiones, bienes patrimoniales, créditos, préstamos, avales, hipotecas, datos bancarios, nóminas, tarjeta de crédito, deducciones económicas y subsidios.

- Datos relativos a transacciones de bienes y servicios: bienes y servicios subministrados y/o recibidos por el afectado, direcciones IP, compensaciones, e indemnizaciones.

- Datos especialmente protegidos o sensibles: aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación. A manera enunciativa: ideología, afiliación sindical religión, creencias, origen racial o étnico, salud, vida sexual, datos sobre condenas e infracciones penales.

Tendrán también la consideración de datos especialmente protegidos, los datos de carácter personal relativos a menores de edad, que se determinará según lo establecido en la normativa local aplicable.

- **Identificable:** toda persona cuya identidad pueda determinarse, directa o indirectamente, bien mediante un número de identificación o uno o varios elementos específicos y característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.

- **Datos seudo-anónimos:** aquellos que no pueden atribuirse a un interesado específico sin usar información adicional, siempre que dicha información adicional se guarde por separado y esté sujeta a medidas técnicas y organizativas que garanticen que no se atribuye a una persona física identificada o identificable. Estos datos seguirán considerándose datos de carácter personal en tanto en cuanto se pueda llegar a identificar a la persona física a la que corresponden. En cualquier caso, el procedimiento de seud-onimización de los datos será una de las medidas a aplicar para minimizar riesgos en materia de protección de datos.

- **Datos anónimos:** datos que no permiten identificar a una persona ni la hacen de forma alguna identificable y por tanto los excluyen del ámbito de aplicación de la normativa en materia de protección de datos. Los datos anonimizados nunca serán considerados datos de carácter personal.

- **Interesado:** persona física titular de los datos sometidos a tratamiento, esto es la persona física a los que los datos identifican o hacen identificable.

- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

- **Encargado de Tratamiento:** persona física o jurídica que trata datos personales por cuenta del responsable del tratamiento.

- **Responsable de Tratamiento:** persona física o jurídica, que determina los fines y medios del tratamiento.

- **Incidente de seguridad:** incidente que afecta a datos de carácter personal o Brecha de confidencialidad: Acceso, comunicación y/o uso no autorizado a los datos personales de una o varias personas físicas.

- **Brecha de integridad:** Modificación, destrucción, pérdida o alteración accidental o ilícita de los datos personales trasmitidos, almacenados o tratados de una o varias personas físicas sin autorización de las mismas.

- **Brecha de disponibilidad:** Imposibilidad de acceso a los datos personales.

- **Transferencia internacional de datos:** La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.

- **Transmisión internacional de datos:** Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable.

- **Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento

- **Cookies y tecnologías** similares de seguimiento (local shared objects, web beacons, web bugs, pixeles de tracking, etc.): ficheros que se descargan y almacenan en el equipo (ordenador/Smartphone/Tablet) del usuario que navega a través de Internet al acceder a determinadas páginas web y aplicaciones y que se utilizan para almacenar y recuperar información sobre la navegación que se realiza desde ese equipo.

S3CC deberá velar por la confidencialidad, seguridad e integridad de la información de carácter personal de la que cada entidad es responsable, así como procurar que todos los terceros con acceso a datos de la entidad, es decir, los encargados del tratamiento, cumplan con las garantías y obligaciones legales y contractuales respecto al tratamiento de los datos e información a los que acceden.

3. AMBITO DE APLICACIÓN

S3CC es responsable de elaborar y aprobar en sus correspondientes Órganos de Gobierno la normativa interna propia que permita la aplicación en su ámbito de las previsiones contenidas en las diferentes normas del Grupo, con las adaptaciones que, en su caso, resulten estrictamente imprescindibles para hacerlas compatibles y cumplir con los requerimientos normativos, regulatorios o a las expectativas de sus supervisores.

4. PRINCIPIOS DE RESPONSABILIDAD Y ACCOUNTABILITY

S3CC adopta políticas adecuadas e implementa medidas técnicas y organizativas apropiadas y verificables para asegurar y poder acreditar de forma transparente que el tratamiento de datos personales se lleva a cabo de conformidad con la normativa aplicable en materia de protección de datos.

Se tendrá en cuenta los riesgos en materia de protección de datos en todos sus procesos, de forma que se garantice una adecuada protección de los datos de carácter personal desde el diseño y por defecto.

En este sentido, la incorporación de una metodología de análisis de riesgos en materia de protección de datos será un elemento esencial previo al tratamiento de datos de carácter personal.

Para dicho tratamiento, S3CC, cumplirá con una serie de principios y medidas establecidas en los lineamientos corporativos. Los cuales se cumplirán en la operatividad diaria.

5. PRINCIPIOS Y FINALIDADES FUNDAMENTALES

La normativa aplicable en materia de protección de datos tiene una incidencia directa en la operativa de las entidades de Grupo Santander, por cuanto en la actividad diaria de éstas se tratan datos de carácter personal. Para dicho tratamiento S3CC adopta los principios y medidas establecidas en la normatividad corporativa. A continuación, detallaremos los principales a cumplir en la operativa diaria:

a. Licitud, proporcionalidad y transparencia.

S3CC, deberá tratar los datos considerados de carácter personal de manera:

Lícita: El tratamiento de datos es una actividad reglada. Se obtendrán los datos siguiendo los requerimientos que establezca la normativa aplicable.

Con carácter general, el tratamiento será lícito cuando se realice bajo cualquiera de los siguientes supuestos:

- ✓ Se dispone del consentimiento para dicho fin por parte del sujeto afectado.
- ✓ El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales.
- ✓ El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable y encargado del tratamiento.
- ✓ El tratamiento es necesario para proteger intereses vitales de la persona física titular de los derechos, o de otra persona física.
- ✓ El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
- ✓ El tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular, cuando el interesado sea un menor.

Proporcional: Se tratarán los datos únicamente acorde con las finalidades que sean necesarias, adecuadas y pertinentes.

Transparente: La información a proporcionar en materia de protección de datos debe ser clara, concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo sin ambigüedades, es decir, fácil de entender por el interesado. El interesado tendrá derecho a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

b. Finalidades compatibles con el origen de la recopilación de datos personales

El tratamiento debe obedecer a una finalidad legítima según la constitución y la ley. S3CC, asegura que el tratamiento de los datos personales se circunscribe para los fines determinados, explícitos y legítimos para aquellos que fueron recopilados en origen y que no serán tratados ulteriormente de manera incompatible con dichos fines.

Como regla general, será necesario que se solicite el consentimiento expreso de los interesados cuando el tratamiento de los datos vaya más allá de los fines para los que se recogieron inicialmente y no sean compatibles con los mismos.

Con objeto de determinar la compatibilidad de los distintos fines de tratamiento, S3CC tendrá en cuenta:

- ✓ cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento al que sea previsto;
- ✓ el contexto en que se hayan recogido los datos personales.
- ✓ la naturaleza de los datos personales, en concreto cuando se traten de datos especialmente protegidos.
- ✓ las posibles consecuencias para los interesados del tratamiento ulterior previsto;
- ✓ la existencia de garantías adecuadas, como podrán ser el cifrado o la seudonimización.

Así pues, siempre y cuando el tratamiento de datos no esté basado en el consentimiento, el tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente sólo debe permitirse cuando sea compatible con los fines de su recogida inicial. En todo caso habrá que cumplir con los requisitos de transparencia que imponga la normativa local aplicable.

Por regla general, no se realizará tratamiento de datos especialmente protegidos o sensibles, exceptuando las situaciones mencionadas en la normativa aplicable. La entrega por parte del Titular de este tipo de datos será siempre facultativa.

c. Minimización y exactitud de los datos personales

Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines específicos para los que son tratados. Asimismo, se deberán adoptar todas las medidas razonables para garantizar que la información sujeta a Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible. El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales y de la normativa aplicable. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular o la ley.

d. Integridad, Confidencialidad, Disponibilidad, Resiliencia

S3CC, deberá velar por que los datos serán tratados con el debido nivel de seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas, humanas, administrativas, u organizativas apropiadas, como por ejemplo la seudonimización o el cifrado de datos personales.

En este sentido, S3CC deberán crear un registro de actividades de tratamiento efectuadas bajo su responsabilidad, donde además se valorarán cuáles son las medidas apropiadas para dispensar un nivel de seguridad adecuado al riesgo de los distintos

tratamientos, así como la capacidad para cumplir con los requerimientos de confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y actividades de tratamiento.

Adicionalmente, procurarán que los empleados y administradores, los terceros que presten servicios, las empresas subcontratadas por los terceros y los empleados de dichos terceros y subcontratistas, que en el desempeño de sus funciones tengan acceso a datos personales, se comprometan a guardar secreto y a no comunicar, en ningún caso, a terceras personas dicha información personal, salvo autorización expresa u obligación legal.

Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas por la normativa aplicable. En este sentido todas las personas con acceso a datos de carácter personal deberán firmar un acuerdo de secreto y confidencialidad.

e. Conservación de los datos personales

S3CC mantendrá los datos personales que procesan de forma que se permita la identificación de los interesados únicamente para los fines legítimos del tratamiento y durante el tiempo estrictamente necesario. Una vez transcurrido este tiempo, para la determinación de los plazos de conservación más allá del mismo, las entidades deberán tener en consideración la normativa local que le sea de aplicación, en particular en materia de prevención de blanqueo de capitales y financiación del terrorismo, así como los plazos de prescripción de las acciones penales, mercantiles, civiles y laborales aplicables.

6. FINALIDADES Y PRINCIPIOS EN LA PROTECCIÓN DE DATOS PERSONALES

Para cumplir los criterios anteriores, S3CC, considera los siguientes aspectos:

a. Deber de la información

Antes de obtener cualquier tipo de dato personal, S3CC comunicarán a los interesados, la siguiente información de manera sencilla y clara, de modo que sea fácil de entender:

- Datos de contacto del área responsable o delegada de la protección de datos personales.
- Finalidad del tratamiento
- Base jurídica del tratamiento a que se designan los datos personales
- Destinatarios o categorías de destinatarios de datos personales
- El plazo durante el cual se conservarán los datos personales o, cuando no sea posible
- La posibilidad de ejercitar sus derechos sobre sus datos personales.
- El derecho a presentar una reclamación ante la autoridad competente, en su caso.
- Si la recogida de datos personales es un requisito legal, contractual o precontractual.
- Cuando los datos personales se obtengan a través de terceros, la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público.

En el ámbito de la utilización de cookies u otros dispositivos de seguimiento, contar con el consentimiento informado del interesado, según la normativa aplicable.

b. Derechos de los interesados

S3CC, informarán a todas las personas que les faciliten datos personales los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de sus datos de carácter personal.

En este sentido, S3CC facilitarán al interesado el ejercicio de sus derechos de forma gratuita y sencilla como regla general.

De manera enunciativa, los interesados gozarán de los siguientes derechos:

- ✓ Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento.
- ✓ Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, según la normativa vigente.
- ✓ Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales.
- ✓ Presentar ante la autoridad competente quejas por infracciones a la normativa aplicable sobre protección de datos.

- ✓ Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías presentes en la normativa aplicable.
- ✓ Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.
- ✓ Derecho de cancelación o supresión (derecho al olvido), únicamente en los casos en que sea procedente, según la normativa aplicable.
- ✓ Derecho a la portabilidad de los datos.
- ✓ Derecho a no ser objeto de una decisión basada únicamente en un tratamiento
- ✓ automatizado

7. Seguridad de la información y mecanismo de vigilancia

a. Políticas de seguridad de la información aplicables a Datos Personales:

Para el alcance de este documento la política de seguridad de la información se puede definir como el conjunto de medidas que aseguran la protección de la información de datos personales, manteniendo la confidencialidad, integridad y disponibilidad de la misma.

Todo el personal de la Entidad debe cumplir las normas de seguridad que se dicten en el ámbito del tratamiento de la información, respetando siempre las indicaciones contenidas en este documento. Igualmente, esta exigencia es de aplicación a terceras personas que tengan acceso a información propiedad de la Entidad debiendo cumplir los requisitos exigidos.

Esta política se aplica a todo el ciclo de vida de la información de datos personas en todas sus formas, ya sea electrónica o física (papel), y a los sistemas e infraestructuras que soportan la información en formato electrónico.

De manera general la política de seguridad de la información de S3CC se rige por los siguientes criterios generales:

- Confidencialidad: La información propiedad de la Entidad debe ser conocida y accesible exclusivamente por aquellas personas que la requieran para ejercer sus tareas, evitando la divulgación de la información a personas no autorizadas. Para ello se han de aplicar los siguientes mecanismos: cifrado, control de perfiles de usuarios, gestión de accesos, segregación funcional, entre otros.

- Integridad: Toda la información almacenada y procesada en la Entidad debe ser correcta y exacta. Por lo tanto, esta información no puede ser alterada sin autorización para ello.
  Para evitar cambios no autorizados en la información se aplican las siguientes medidas: control de usuarios, gestión de accesos o firmas digitales, entre otras.

- Disponibilidad: La disponibilidad hace referencia a que la información del sistema y los recursos para obtenerla deben permanecer accesibles cuando sea requerido, previniendo interrupciones no autorizadas/controladas de los recursos informáticos.
  Existen diversos mecanismos para cumplir con los niveles de servicio tales como: uso de backups, mecanismos de alta disponibilidad, redundancia a

distintos niveles como almacenamiento, infraestructura o diseño de aplicaciones, entre otros.

Para el cumplimiento de dichos criterios, se establecen una serie de medidas:

- Proporcionalidad: las medidas de seguridad deben ser proporcionales al nivel de riesgo que se pretenden mitigar.
- Perdurabilidad: ninguna medida de seguridad debe ser revocada sin autorización formal.

Adicionalmente, los activos de información tecnológicos donde reposan los datos personales deben estar protegidos ante pérdidas accidentales o malintencionadas y falsificaciones, de acuerdo con los adecuados requisitos legales, regulatorios, contractuales y de negocio. Para mitigar estos riesgos se dispone de los siguientes mecanismos:

- Backups o copias de respaldo.
- Mecanismos de alta disponibilidad, entendiendo como tal, aquellas medidas de índole principalmente tecnológica que se dotan a los sistemas para minimizar las probabilidades de interrupción del servicio prestado por los mismos.
- Incorporación de medidas para prevenir la fuga de información.

b. Uso seguro de la información asociada a datos personales

El uso de la información dentro de la Entidad por parte de sus empleados, administradores o terceros relacionados, tiene que cumplir con unos mínimos requerimientos de seguridad en función de su sensibilidad, criticidad o de los requerimientos legales que apliquen.

Para ello, los empleados y administradores deben ser informados y deben asumir su responsabilidad en relación con la seguridad de la información tanto de los datos personales que administren y gestionen como de la información que sea catalogada sensible.

Se considera propietario de la información o propietario del dato a la unidad, o función de la unidad que la ha recabado o generado en el desempeño de su actividad y que la emplea para el desarrollo de su negocio, independientemente de quien procese o custodie los datos.

Se implantan medidas para garantizar el uso seguro de la información, las cuales pueden agruparse de la siguiente manera:

- Accesos a la información

Todos los sistemas que almacenan o procesan información deben tener su acceso estrictamente controlado. El nivel de control de acceso requerido viene determinado por el grado de accesibilidad que se le pueda otorgar a los usuarios según la clasificación de los datos personales almacenados.

Debe existir un proceso formal para otorgar acceso a los activos, que requiera una aprobación por parte del nivel adecuado. Dicho proceso incluye desde el registro inicial de nuevos usuarios hasta la cancelación del registro de los usuarios cuando ya no necesiten tener acceso.

Los accesos otorgados a los usuarios de los sistemas donde se almacenan datos personales, están determinados por las necesidades óptimas de información de dichos usuarios en el desempeño de sus tareas, y por tanto los privilegios otorgados serán los mínimos y necesarios para desempeñar sus tareas. En la definición de los perfiles o roles de usuarios debe involucrarse tanto al responsable de tecnología como al dueño de la aplicación.

Debe definirse un procedimiento para añadir, modificar o eliminar las cuentas de usuarios de los sistemas de información. En el caso de que alguien abandone la empresa o cambie su función dentro de la Compañía, se deben tener los protocolos requeridos para garantizar que se elimina o actualizar debidamente sus permisos de acceso en tiempo y forma.

Adicionalmente, la segregación funcional es un tipo de control que se basa en que los usuarios no tengan permisos excesivos y que se requieran dos o más perfiles para la autorización y ejecución de acciones sensibles. La asignación de permisos de acceso a los usuarios se debe realizar teniendo en cuenta el principio de segregación de funciones, evitando que un mismo usuario disponga de permisos de ejecución y autorización de forma simultánea. Debe existir registro y trazabilidad de los accesos de los usuarios a los sistemas y aplicaciones donde reposa información de datos personales.

- Distribución segura

Se debe prestar especial atención a la distribución de información relacionada a datos personales cuya clasificación como activo de información se considera confidencial e interna, que esta almacenada en formato electrónico como en formato físico. Una buena práctica previa a la distribución es la verificación de los destinatarios.

- Acceso de terceros (Dentro del Grupo empresarial)

Antes de permitir el acceso de terceros a cualquier tipo de activo propiedad de la Entidad, se deben evaluar los riesgos asociados y se deben evaluar los controles establecidos para mitigar dichos riesgos, hasta un nivel aceptable.

Por lo tanto, se tiene que asegurar que se mantiene la seguridad de los activos de la información accedidos o procesados por terceros y que éstos conocen y aceptan sus responsabilidades relativas a la seguridad a través de un contrato y el correspondiente acuerdo de nivel de servicio cuando aplique. Además, cuando la información se procese en un tercero, los controles de seguridad tienen que ser al menos iguales que si fuera procesada por una empresa del Grupo.

- Uso de redes de comunicación:

Debe haber medidas de control debidamente implantadas para proteger la autenticidad, integridad y confidencialidad de información enviada a través de redes públicas o privadas de comunicación. Esto aplica a los siguientes aspectos:

- Protección de la red contra accesos no autorizados, pérdida de integridad y disponibilidad.
- Protección, tanto de los envíos como de la recepción de información
- información desde redes del Grupo a redes externas y viceversa.
- Protección de los accesos remotos.

- Seguridad en el uso de dispositivos corporativos.

El uso de cualquier dispositivo presenta riesgos adicionales de seguridad para el acceso a la información, por lo que se deben tomar medidas de seguridad basadas en los siguientes principios:

- Sólo deben utilizarse los dispositivos autorizados por la entidad para las actividades de negocio.
- Se deben implantar los controles físicos necesarios, controles de acceso, técnicas de cifrado y protección de software malicioso, cuando aplique.

De manera complementaria a las directrices descritas en este documento respecto a la gestión oportuna de la seguridad de la información, se considera necesario ampliar la información a través del modelo de ciberseguridad implementado por la entidad con el fin de dar un alcance mayor a la seguridad de la información de manera integral y teniendo en cuenta el alcance de clasificación de los datos personales recolectados.

c. Incidentes de seguridad de los datos personales

S3CC dispone de herramientas y procedimientos de respuesta necesarios frente a cualquier violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados, o la comunicación o acceso no autorizados a dichos datos, así como con los medios necesarios para demostrar que se ha aplicado toda la protección tecnológica adecuada y se han tomado las medidas organizativas oportunas que permitan determinar, a la mayor brevedad:

(i) si se ha producido una violación de la seguridad de los datos personales;
(ii) si constituye un riesgo para la intimidad de las personas físicas, y
(iii) si resulta necesario informar a la autoridad de control y al interesado.

Se cuenta con procedimientos claros y accesibles para todos los empleados y administradores que permitan una diligencia debida de los incidentes de seguridad que afecten a datos de carácter personal y faciliten la rápida coordinación de todas las áreas implicadas.

Se entiende por incidente de seguridad que afecta a datos de carácter personal:

- ✓ Acceso, comunicación y/o uso no autorizado a los datos personales de una o varias personas físicas.

- ✓ Modificación, destrucción, pérdida o alteración accidental o ilícita de los datos personales trasmitidos, almacenados o tratados de una o varias personas físicas sin autorización de las mismas.

- ✓ Imposibilidad de acceso a los datos personales.

8. Funciones y responsabilidades

S3CC, con carácter general, podrá actuar en calidad de responsable o como encargado para cada tratamiento de datos de carácter personal, derivándose las siguientes responsabilidades:

a. Responsables del tratamiento

S3CC, decidirá sobre la finalidad, el contenido y el uso del tratamiento de los datos personales de los clientes, potenciales clientes, ex clientes, accionistas, proveedores y empleados y de todos aquellos interesados con los que mantenga un vínculo.

Los empleados y administradores de S3CC que traten o quieran tratar datos de carácter personal, respetarán en todo momento la normativa y políticas internas en materia de protección de datos.

Respecto a los terceros proveedores de servicios con acceso a datos personales (encargados de tratamiento), S3CC trasladará las obligaciones como si el tratamiento fuera realizado por ellos mismos.

Según la normativa aplicable, el Responsable del Tratamiento tendrá los siguientes deberes:

- ✓ Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

- ✓ Solicitar y conservar, en las condiciones previstas en la ley, copia de la respectiva autorización otorgada por el Titular.

- ✓ Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

- ✓ Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- ✓ Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.

- ✓ Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.

- ✓ Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.

- ✓ Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la normativa aplicable.

- ✓ Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.

- ✓ Tramitar las consultas y reclamos formulados en los términos señalados en la normativa aplicable.

- ✓ Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la normativa aplicable y en especial, para la atención de consultas y reclamos.

- ✓ Informar al Encargado del Tratamiento cuando una determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.

- ✓ Informar a solicitud del Titular sobre el uso dado a sus datos.

- ✓ Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

- ✓ Cumplir las instrucciones y requerimientos que imparta la autoridad competente.

b. Encargado del tratamiento

S3CC, será el responsable de cumplir con las exigencias de la normativa y de quien actúe como responsable de Tratamiento.

Pondrán a disposición del responsable de tratamiento toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como ofrecer garantías suficientes, de manera que el tratamiento sea conforme con los requisitos de la normativa y garantice la protección de los derechos de los afectados por esa relación entre el responsable del tratamiento y el tercero.

S3CC, cuenta con mecanismos de control que aseguran que las terceras empresas proveedoras de servicios que acceden a datos personales de la entidad en virtud de dicha prestación de servicios, cumplan con la normativa en vigor en la materia.

Según la normativa aplicable, el Encargado del Tratamiento tendrá los siguientes deberes:

- ✓ Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- ✓ Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- ✓ Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la normativa aplicable.
- ✓ Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.
- ✓ Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la normativa aplicable.

- ✓ Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la normativa aplicable y, en especial, para la atención de consultas y reclamos por parte de los Titulares.
- ✓ Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la normativa aplicable.
- ✓ Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
- ✓ Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la autoridad competente.
- ✓ Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
- ✓ Informar a la autoridad competente cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
- ✓ Cumplir las instrucciones y requerimientos que imparta la autoridad competente.

c. Transferencias Internacionales de Datos

Cada Responsable o Encargado de tratamiento deberá aplicar las garantías adecuadas para mantener dentro de un nivel de seguridad apropiado todas las transferencias internacionales de datos personales que se efectúan bajo su responsabilidad.

Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios. Esta prohibición no regirá cuando:

- ✓ Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia.
- ✓ Transferencias bancarias o bursátiles, conforme a la normativa aplicable.
- ✓ ransferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.
- ✓ Las demás previstas en la normativa aplicable.

d. Procedimiento para Consultas y Reclamos

Consultas

El Titular podrá consultar su información personal que repose en cualquier base de datos. S3CC deberá suministrar la información contenida en el registro individual o que esté vinculada con la identificación del Titular, según sea solicitado. El Titular podrá radicar su solicitud por cualquiera de los canales establecidos por S3CC. La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha del recibo de ella. Cuando no fuere posible atender la consulta dentro de dicho término, S3 Colombia informará al interesado, expresando los motivos de la demora y señalando la fecha en que

se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

Reclamos

El Titular que considere que la información contenida en la base de datos debe ser objeto de corrección, actualización o supresión, o cuando advierta el presunto incumplimiento de cualquiera de los deberes asignados a S3 Colombia sobre el tratamiento de datos personales, podrán presentar un reclamo ante S3 Colombia el cual será tramitado bajo las siguientes reglas:

- ✓ El reclamo se formulará directamente a S3 Colombia por cualquiera de los canales establecidos por S3 Colombia. El reclamo deberá establecer la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer.
- ✓ Si el reclamo resulta incompleto, se requerirá al Titular dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.
- ✓ Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo del reclamo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.
- ✓ El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

Queja ante autoridades.

El Titular sólo podrá elevar queja ante la autoridad competente una vez haya agotado el trámite de consulta o reclamo ante S3CC Colombia.

e. La Autoridad de Control

S3CC, responderá ante la Autoridad de Control Local que en su caso corresponda a través de la figura del Responsable de Protección de Datos designado.

9. GOBIERNO

S3CC deberá contar con un Modelo de Gobierno en el que se describan las funciones, responsabilidades y competencias en materia de protección de datos.

a. Área Responsable de Protección de Datos

En este sentido, S3CC deberá contar con un área Responsable de Protección de Datos, cuyas principales funciones serán:

- ✓ Ser el punto de contacto con la Autoridad de Control Local.
- ✓ En coordinación con las áreas de negocio, ser el punto de contacto con las personas físicas titulares de los derechos.
- ✓ Controlar y supervisar, junto con la Función de Cumplimiento, que todos los empleados y administradores de la entidad cumplen con la normativa en materia de protección de datos, con sus políticas internas en dicha materia y colaborar con las auditorías correspondientes.
- ✓ Promover la concienciación y garantizar la formación de los empleados y administradores de la entidad que tratan datos de carácter personal con el fin de informarles de los derechos y las obligaciones que les incumben como consecuencia de su puesto de trabajo.
- ✓ Asesorar a las áreas y responsables de la entidad en materia de protección de datos y en particular en relación a los análisis de riesgo que se lleven a cabo.
- ✓ Cooperar en los programas de selección de proveedores, para delimitar las obligaciones en materia de protección de datos que dichos terceros deben cumplir.

b. Comité de Riesgos Estatutario

Se le asignaron funciones al comité de Riesgos Estatutario de la Junta Directiva, como el foro encargado a salvaguardar el correcto funcionamiento de las directrices y políticas de protección de datos de la Entidad y un seguimiento al mismo. Sus funciones son:

- Aprobación, seguimiento y/o tramitación de situaciones de excepción planteadas, posibles incumplimientos normativos y/o corporativos relacionados a las políticas de protección de datos de la Entidad.
- Por lo menos cada 6 meses se debe presentar un estatus de la situación actual de la Entidad en materia de protección de datos personales desde el punto de vista regulatorio, así como las novedades relevantes.

c. Junta Directiva

Corresponderá a la Junta Directiva aprobar la Política de Protección de Datos Personales, una vez la revise y apruebe el Comité de Riesgos y Cumplimiento de la Junta Directiva.

10. REGIMEN SANCIONATORIO

a. Régimen sancionatorio Interna

Se aplicarán las medidas sancionatorias a que haya lugar, en el evento de que los administradores o empleados a S3CC incumplan con la normativa, políticas, y procedimientos en materia de Protección de Datos Personales. Para tales efectos, se tendrán en cuenta las siguientes directrices:

- Todos los funcionarios de la Entidad, deben acatar y cumplir con las diferentes disposiciones implementadas en materia de Protección de Datos Personales.
- Se reportará cualquier situación irregular o evento potencial de incumplimiento a las políticas de Protección de Datos Personales, al comité de Riesgos de la Junta Directiva, quien tomara una decisión de las actuaciones disciplinarias a lugar.
- El área de recursos humanos será la encargada de adelantar las actuaciones administrativas a que haya lugar cuando se falte a la anterior política.
- Se realizarán programas de sensibilización y capacitación a todos los empleados y administradores cuando se identifiquen conductas por incumplimiento a las políticas y directrices de Protección de Datos Personales.

b. Régimen sancionatorio ante autoridades competentes

La Superintendencia de Industria y Comercio (SIC) en Colombia ejerce la vigilancia para garantizar el tratamiento de datos personales en donde se deben respetar los principios, derechos, garantías, y procedimientos previstos en la ley 1581 de 2012, cuyas funciones se encuentran descritas en el Artículo 21 y las medidas sancionatorias establecidas al incumplimiento de la citada ley en los Artículos 23 y 24 respectivos.

Dentro de los principales motivos de sanción interpuesta por el organismo de vigilancia a las Entidades, se resumen los siguientes:

- ✓ Envío de correos electrónicos con fines comerciales, sin copia oculta, quedando en evidencia cientos de correos electrónicos personales. (el correo electrónico personal, es considerado un dato personal semiprivado).
- ✓ Envío de correos electrónicos con fines comerciales, sin contar con autorización expresa por parte del titular para el envío de información.
- ✓ Llamadas telefónicas ofreciendo servicios y/o productos, sin contar con la autorización expresa por parte del titular para el contacto telefónico.
- ✓ No dar trámite a las solicitudes de supresión de correo electrónico por envío de información comercial.
- ✓ Recolectar información personal que se encuentra en redes sociales o publicadas en Internet, para posteriormente contactarse con el titular, para ofrecerle producto o servicios. (El hecho que la información personal esté publicada en internet, no la hace pública).
- ✓ No reportar incidentes de manera oportuna al órgano de vigilancia
- ✓ No comunicar incumplimiento y las respectivas medidas a los interesados.

Las entidades deben notificar a la autoridad competente sobre cualquier incumplimiento que presente algún riesgo, se deberán desarrollar planes de respuesta y mitigación ante los mismos.

11. CAPACITACION

S3CC asegura que la totalidad de los empleados, directivos y miembros de la Junta Directiva este familiarizada con las políticas y directrices en materia de protección de datos personales y con las herramientas de gestión y control utilizadas. Con dicho fin, se llevan a cabo planes de formación introductorios y recurrentes para todos los empleados, directivos y miembros de la Junta Directiva; por lo menos una vez al año.

Los planes de capacitación serán permanentemente revisados y actualizados, así como también contarán con mecanismos de evaluación de los resultados obtenidos, para medir la efectividad y alcance de los objetivos definidos.

Control de cambios

Versión	Responsable documento	Responsable mantenimiento	Fecha Cambio	Responsable de validación	Comité Aprobado	Fecha Aprobación	Fecha revisión programada
1	Alexander Ruiz		05/05/2023	**ARC**	**CER/JD**	**21-06-2023**	**01-03-2025**
2							
3							
4							
5							
6							

Versión	Descripción del Cambio
1	Política Protección de Datos Personales
2	
3	
4	
5	
6	