POLITICA TRATAMIENTO DE DATOS

SSH S.A

BOGOTÁ, COLOMBIA

TABLA DE CONTENIDO

1. ALCANCE

En desarrollo de los Artículos 15 y 20 de la Constitución Política de Colombia se ha expedido la Ley 1581 de 2012 y el Decreto 1377 de 2013, en los cuales se regula expresamente la autorización del Titular de información para el Tratamiento de sus datos personales. Siguiendo los lineamientos propuestos en la Ley 1581 de 2012, SSH S.A identificándose como el responsable del tratamiento de datos define la siguiente política cobijando a sus proveedores, clientes, empleados, socios y demás partes interesadas.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Cumplir como empresa el derecho que poseen todas las personas a conocer, rectificar y actualizar la información perteneciente a ellos mismos en archivos, documentos y bases de datos, otorgando un trato adecuado a sus datos siguiendo lo dictado en los artículos 15 y 20 de la Constitución Política de Colombia a través de acciones de aseguramiento de la Información.

2.2 OBJETIVOS ESPECIFICOS

● Mantener la confianza de los clientes en general y el compromiso de todos los funcionarios, contratistas o practicantes de la compañía respecto al correcto manejo y protección de la información que es gestionada y resguardada en SSH S.A.

● Identificar e implementar las tecnologías necesarias para fortalecer la función de la seguridad de la información.

● Establecer y divulgar a todos los Grupos de Interés la Política de Tratamiento de la Información

● Informar las responsabilidades de los involucrados en el tratamiento de datos

● Cumplir con los principios de seguridad de la información: disponibilidad, integridad y confidencialidad.

● Dar cumplimiento a los lineamientos establecidos en la Estrategia de Gobierno en Línea respecto a la Seguridad de la Información.

3. RESPONSABILIDADES DEL TRATAMIENTO DE LA INFORMACIÓN

SSH S.A se identifica como parte responsable del tratamiento apropiado de los datos personales provenientes de sus partes interesadas según lo definido por la Ley 1581 de 2012, de igual forma específica a continuación la fragmentación de las responsabilidades pertenecientes a esta política y que parte de la organización está encargada de las mismas junto con unas breves responsabilidades de los clientes.

3.1 RESPONSABILIDADES ARÉA DIRECCIÓN DE INGENIERÍA

- Establecer, mantener y divulgar las políticas y procedimientos de servicios de tecnología, incluida esta política de seguridad de información y todos sus capítulos, el uso de los servicios tecnológicos en toda la compañía de acuerdo con las mejores prácticas y lineamientos de la Dirección General de la compañía y directrices del Gobierno.
- Mantener la custodia de la información que reposa en los diferentes sistemas de información, bases de datos y aplicativos de la compañía.
- Informar de los eventos que estén en contra de la seguridad de la información y de la infraestructura tecnológica de la compañía a la Dirección General, las diferentes Direcciones y Jefaturas de **SSH S.A.**, así como a los entes de control e investigación que tienen injerencia sobre la compañía.
- Proporcionar medidas de seguridad físicas, lógicas y procedimentales para la protección de la información digital de la compañía.
- Aplicar y hacer cumplir la Política de Tratamiento de datos y sus componentes.
- Administrar las reglas y atributos de acceso a los equipos de cómputo, sistemas de información, aplicativos y demás fuentes de información al servicio de **SSH S.A.**
- Analizar, aplicar y mantener los controles de seguridad implementados para asegurar los datos e información gestionados en la compañía.
- Resolver de común acuerdo con las áreas y los propietarios de la información los conflictos que se presenten por la propiedad de la información al interior de la compañía. Esto incluye los posibles medios de acceso a la información, los datos derivados del procesamiento de la información a través de cualquier aplicación o sistema, los datos de entrada a las aplicaciones y los datos que son parte integral del apoyo de la solicitud.

- Habilitar/Deshabilitar el reconocimiento y operación de Dispositivos de Almacenamiento externo de acuerdo con las directrices emitidas de parte de la Dirección General y las diferentes direcciones.
- Implementar los mecanismos de controles necesarios y pertinentes para verificar el cumplimiento de la presente política.
- Aplicar el procedimiento y la herramienta de borrado de datos cuando sea necesario o a solicitud del usuario
- Implementar el procedimiento de respuesta a incidentes en caso de que se presente uno y dar resolución al caso.

3.2 RESPONSABILIDADES GRUPO DE SOPORTE TECNOLÓGICO

- Garantizar la disponibilidad de los servicios y así mismo programar o informar a todos los usuarios cualquier problema o mantenimiento que pueda afectar la normal prestación de los mismos; así como gestionar su acceso de acuerdo con las solicitudes recibidas de las diferentes Direcciones, Jefaturas o Coordinaciones siguiendo el procedimiento establecido.
- Establecer, mantener y divulgar las políticas y procedimientos de los servicios de tecnología, incluidos todos los capítulos que hacen parte de esta Política, en toda la compañía de acuerdo con las mejores prácticas y directrices de la Entidad y del Gobierno.
- Determinar las estrategias para el mejoramiento continuo del servicio tecnológico, la optimización de los recursos tecnológicos, las mejoras en los sistemas de información con miras a un gobierno de tecnologías consolidado.
- Brindar el soporte necesario a los usuarios a través de los canales de mesa de ayuda actualmente implementados en la compañía.

3.3 RESPONSABILIDADES DE LOS PROPIETARIOS DE LA INFORMACIÓN

Son propietarios de la información cada uno de los directores, así como los jefes de las oficinas donde se genera, procesa y mantiene información, en cualquier medio, propia del desarrollo de sus actividades sea esta generada de forma interna o proveniente de partes interesadas.

- Valorar y clasificar la información que está bajo su administración y/o generación.
- Autorizar, restringir y delimitar a los demás usuarios de la compañía el acceso a la información de acuerdo con los roles y responsabilidades de los diferentes funcionarios, contratistas o practicantes que por sus actividades requieran acceder a consultar, crear o modificar parte o la totalidad de la información.
- Determinar los tiempos de retención de la información en conjunto con él grupo de Gestión Documental y Correspondencia y las áreas que se encarguen de su protección y almacenamiento de acuerdo con las determinaciones y políticas de la entidad como de los entes externos y las normas o leyes vigentes.
- Determinar y evaluar de forma permanente los riesgos asociados a la información, así como los controles implementados para el acceso y gestión de la administración comunicando cualquier anomalía o mejora tanto a los usuarios como a los custodios de la misma.
- Acoger e informar los requisitos de esta política a todos los funcionarios, contratistas y practicantes en las diferentes dependencias de la compañía.
- Informar incidentes en caso de presentarse mediante el formato de reporte de incidentes de la empresa.

3.4 RESPONSABILIDADES DE LOS FUNCIONARIOS, PROVEEDORES Y CLIENTES

- Utilizar solamente la información necesaria para llevar a cabo las funciones que le fueron asignadas, de acuerdo con los permisos establecidos o aprobados en el Manual de Funciones, Código Disciplinario Único – Ley 734 de 2002 o Contrato.
- Manejar la Información de la compañía y rendir cuentas por el uso y protección de tal información, mientras que este bajo su custodia. Esta puede ser física o electrónica e igualmente almacenada en cualquier medio.
- Proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido
- Evitar la divulgación no autorizada o el uso indebido de la información.
- Cumplir con todos los controles establecidos por los propietarios de la información y los custodios de la misma.
- Informar a sus superiores sobre la violación de estas políticas o si conocen de alguna falta a alguna de ellas.

- Proteger los datos almacenados en los equipos de cómputo y sistemas de información a su disposición de la destrucción o alteración intencional o no justificada y de la divulgación no autorizada.
- Reportar los Incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.
- Proteger los equipos de cómputo, de comunicaciones y demás dispositivos tecnológicos o técnico- científicos designados para el desarrollo de sus funciones. No está permitida la conexión de equipos de cómputo y de comunicaciones ajenos a la compañía al a red corporativa ni el uso de dispositivos de acceso externo a Internet o de difusión de señales de red que no hayan sido previamente autorizadas por la Oficina de Tecnologías de la Información**.**
- Usar software autorizado que haya sido adquirido legalmente por la compañía. No está permitido la instalación ni uso de software diferente al corporativo sin el consentimiento de sus superiores y visto bueno de la Oficina de Tecnologías de la Información.
- Divulgar, aplicar y el cumplir con la presente Política.
- Aceptar y reconocer que en cualquier momento y sin previo aviso, la Dirección General de la compañía puede solicitar una inspección de la información a su cargo sin importar su ubicación o medio de almacenamiento. Esto incluye todos los datos y archivos de los correos electrónicos corporativos, sitios web corporativos y redes sociales propiedad de la compañía, al igual que las unidades de red corporativos, computadoras, servidores u otros medios de almacenamiento propios de la Compañía. Esta revisión puede ser requerida para asegurar el cumplimiento de las políticas internamente definidas, por actividades de auditoría y control interno o en el caso de requerimientos de entes fiscalizadores y de vigilancia externos, legales o gubernamentales.
- Proteger y resguardar su información personal que no esté relacionada con sus funciones en la Compañía. **SSH S.A.** no es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito.

4. DEFINICIONES

- **Autorización:** Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.
- **Aviso de privacidad:** Comunicación verbal o escrita generada por el responsable (SSH S.A.), dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.
- **Base de datos:** Conjunto organizado de datos personales que sea objeto de tratamiento.
- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Dato público:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- **Datos sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o

que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

- **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento.
- **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.
- **Titular:** Persona natural cuyos datos personales sean objeto de Tratamiento.
- **Transferencia:** 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.
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

5. MARCO LEGAL Y/O NORMATIVO

- LEY 23 DE 1982 sobre Derechos de Autor. Congreso de la República. Disponible en Línea http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3431 [Recuperado en enero de 2018]

- CONSTITUCIÓN POLÍTICA DE COLOMBIA 1991; Artículo 15. "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. Disponible en Línea: http://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15 [Recuperado en enero de 2018]

- LEY 527 DE 1999; por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276 [Recuperado en enero de 2018]

- LEY 1266 DE 2008, por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones**.** Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488 [Recuperado en enero de 2018]

- LEY 1273 DE 2009, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492 [Recuperado en enero de 2018]

- LEY 1474 DE 2011 Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=43292 [Recuperado en enero de 2018]

- DECRETO 4632 DE 2011 Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones. Disponible en Línea: http://wsp.presidencia.gov.co/Normativa/Decretos/2011/Documents/Diciembre/09/dec463209122011.pdf [Recuperado en enero de 2018]

- LEY ESTATUTARIA 1581 DE 2012, Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981. [Recuperado en enero de 2018]

- DECRETO 2609 DE 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones

en materia de Gestión Documental para todas las Entidades del Estado". Disponible en Línea: http://www.mintic.gov.co/portal/604/articles- 3528_documento.pdf [Recuperado en enero de 2018]

- DECRETO 2693 DE 2012 Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones. Disponible en Línea: http://www.mintic.gov.co/portal/604/articles-3586_documento.pdf [Recuperado en enero de 2018]

- DECRETO 1377 DE 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646 [Recuperado en enero de 2018]

- NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC Colombiana 27001:2013. 2013-12-11. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

- MANUAL GOBIERNO EN LÍNEA 3.1 Ver 2014-06-12. Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea; Formato Política SGSI - Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.

- LEY 1712 DE 2014; Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882 [Recuperado en enero de 2018]

- DECRETO 2573 DE 2014 Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones. Disponible en Línea: http://www.mintic.gov.co/portal/604/articles-14673_documento.pdf [Recuperado en enero de 2018]

- DECRETO 103 DE 2015, por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones. Disponible en Línea: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60556 [Recuperado en enero de 2018]

- DECRETO 1494 DE 2015, Por el cual se corrigen yerros en la Ley 1712 de 2014. Disponible en Línea: http://wp.presidencia.gov.co/sitios/normativa/decretos/2015/Decretos2015/DECRETO%201494%20DEL%2013%20DE%20JULIO%20DE%202015.pdf [Recuperado en enero de 2018]

6. POLITICA

SSH S.A. se identifica como responsable en el tratamiento de datos siguiendo los lineamientos de la Ley 1581 de 2012, cuando estos son entregados por parte de alguna parte interesada como parte de alguna actividad, negocio o proceso. SSH S.A decide definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados con la misión, visión y funciones de la compañía.

SSH S.A. se compromete a salvaguardar la información que genera en la ejecución de sus funciones o la que le es entregada en custodia por usuarios dentro de la ejecución de los trámites de la compañía, identificando y mitigando los riesgos asociados mediante la definición de lineamientos y directrices a las dependencias, funcionarios, contratistas, practicantes y todo aquel que tenga interacción con esta información y la utilización físicamente o a través de equipos, plataformas o sistemas de información dispuestos para su gestión y resguardo.

Toda la información que es generada por los funcionarios, contratistas y practicantes de SSH S.A. en beneficio y desarrollo de las actividades propias de la compañía es propiedad de SSH S.A., a menos que se acuerde lo contrario en los contratos escritos y autorizados. Esto también incluye la

información que pueda ser adquirida o cedida a la compañía de parte de entidades o fuentes externas de información que sean contratadas o que tengan alguna relación con la compañía.

SSH S.A. protege la información creada, procesada, transmitida o resguardada por los procesos de su competencia, su infraestructura tecnológica y activos, del riesgo que se genera con los accesos otorgados a terceros (ej.: contratistas, proveedores o clientes), o como resultado de servicios internos en outsourcing.

Las responsabilidades frente a la seguridad de la información de la compañía son definidas, compartidas, publicadas y deberán ser aceptadas por cada uno de los funcionarios, contratistas o practicantes de la compañía.

Como parte de esta política SSH S.A, establece las siguientes directrices frente al tratamiento de los datos personales:

• Cumplir con toda la normatividad legal vigente colombiana que dicte disposiciones para la protección de datos personales.

• A través de los colaboradores que hacen parte de la Gerencia General, Gerencia de Proyectos, Gerencia Comercial, Gerencia de Talento Humano, o a través de contratistas o mandatarios encargados, realizar el tratamiento apropiado de datos personales de: empleados, clientes, contratistas y subcontratistas, empleados de sus contratistas y subcontratistas, proveedores entre otros.

• SSH S.A, en calidad de responsable del tratamiento de datos personales, según el caso, adoptará las medidas de seguridad físicas, tecnológicas y/o administrativas que sean necesarias para garantizar los atributos de integridad, autenticidad y confiabilidad de los datos personales.

- SSH S.A cumplirá con el principio de minimización de datos, por tanto:
  - Solo se pueden recabar los datos personales que se vayan a tratar, es decir, los que sean estrictamente necesarios para el tratamiento.
  - Los datos solo podrán ser recogidos cuando vayan a ser tratados, por tanto, no se podrá recabar datos para usarlos tiempo después.
  - La información personal de los usuarios solo podrá ser utilizada para la finalidad con la que fue recogida, pero no con ningún otro objetivo.

7. DERECHOS DE LOS TITULARES DE DATOS PERSONALES

La Ley 1581 de 2012 establece que los Titulares de los datos personales tendrán los siguientes derechos:

- Conocer, actualizar y rectificar sus datos personales frente a los responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.
- Solicitar prueba de la autorización otorgada al responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la citada ley.
- Ser informado por el responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que se les ha dado a sus datos personales.
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la citada ley y las demás normas que la modifiquen, adicionen o complementen.
- Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el responsable o Encargado han incurrido en conductas contrarias a la ley y a la Constitución.
- Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.
- Adicionalmente, el Decreto reglamentario 1377 de 2013 define que los responsables deberán conservar prueba de la autorización otorgada por los Titulares de datos personales para el Tratamiento de los mismos.

8. DOCUMENTOS RELACIONADOS

- Política de la seguridad de la información
- Política de calidad

9. VIGENCIA

Esta política de protección de datos personales está vigente desde febrero de 2018.