POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y CONTINUIDAD DE LA OPERACIÓN

ARTÍCULO PRIMERO. Objeto. La presente tiene como objeto adoptar la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de **ECOSERVICIOS DE OCCIDENTE SAS ESP** en adelante la **EMPRESA**, las Políticas Generales de Manejo, así como definir lineamientos frente a su uso y manejo.

ARTÍCULO SEGUNDO. Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación. La **EMPRESA** protege, preserva y administra la integridad, confidencialidad, disponibilidad y autenticidad de la información, así como la seguridad digital y la gestión de la continuidad de la operación, conforme al mapa de procesos, en cumplimiento de los requisitos legales y reglamentarios. La **EMPRESA** previene incidentes mediante la gestión de riesgos integrales en seguridad y privacidad de la información y seguridad digital, con la implementación de controles de seguridad físicos y digitales, orientados a la mejora continua en la gestión y el alto desempeño del Sistema de Gestión de Seguridad de la Información, con la finalidad de preservar la información de nuestros clientes, proveedores y colaboradores.

ARTÍCULO TERCERO. Ámbito de Aplicación. La Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación y las Políticas Generales de Manejo aplica donde la **EMPRESA** tenga presencia o preste sus servicios.

ARTÍCULO CUARTO. Objetivos. La Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, tendrá los siguientes objetivos:

1. Brindar mecanismos de aseguramiento para el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información de la **EMPRESA**.
2. Mitigar los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación en la **EMPRESA**.
3. Gestionar los riesgos de seguridad y privacidad de la información, Seguridad Digital y Continuidad de la operación de la **EMPRESA**.
4. Establecer los lineamientos necesarios para el manejo de la información y los recursos tecnológicos de la **EMPRESA**.

POLÍTICAS GENERALES DE MANEJO DE INFORMACIÓN.

ARTÍCULO QUINTO. Privacidad y Tratamiento de la Información. Para el tratamiento de la información de los Clientes, Proveedores y Colaboradores que participan en el desarrollo de la prestación de los servicios de la **EMPRESA**, la **EMPRESA** cuenta con la "Política de Protección de Datos Personales ", dando cumplimiento con lo dispuesto en la Ley 1581 de 2012, reglamentada por el Capítulo 25 del Título 2 de la Parte 2 del Libro 2 del Decreto 1074 de 2015, la Ley 1712 de 2014, reglamentada por el Capítulo 2 del Título 1 de la Parte 1 del Decreto 1081 de 2015, y las demás normas externas que los modifiquen, adicionen o complementen.

ARTÍCULO SEXTO. Política de Seguridad de los Recursos Humanos. La **EMPRESA**, a través de Talento Humano, debe propender para que los Colaboradores y contratistas entiendan sus responsabilidades frente a la seguridad de la información con el fin de reducir el riesgo de robo,

fraude, mal uso de las instalaciones y medios, asegurando la confidencialidad, disponibilidad e integridad de la información.

PARÁGRAFO. El área Jurídica deberá incluir en las minutas de los contratistas cualquiera que sea su modalidad, las cláusulas u obligaciones correspondientes a la Seguridad de la Información con el fin de reducir el riesgo de robo, fraude, mal uso de las instalaciones y medios, asegurando la confidencialidad, disponibilidad e integridad de la información.

ARTÍCULO SÉPTIMO. Política de Gestión de Activos. La **EMPRESA**, a través de la Dirección Administrativa, establecerá y divulgará los lineamientos específicos para la identificación, clasificación y buen uso de los activos de información, con el objetivo de garantizar su protección.

a. Inventario de Activos: Los activos de la **EMPRESA** deben ser identificados, clasificados y controlados para garantizar su uso adecuado, protección y la recuperación ante desastres. Por tal motivo, se debe llevar el inventario de los activos de información de propiedad de la **EMPRESA**, discriminado por sede y/o centros de operación.

Con el objetivo de establecer los controles de seguridad físicos y digitales, las dependencias que tienen la custodia de la información generada en el marco de su función se encargarán de proteger la información, de mantener y actualizar el inventario de activos de información relacionados con sus servicios (información, software, hardware y recurso humano).

b. Archivos de Gestión: a través de la Dirección Administrativa y Gerencia y con el acompañamiento del Ingeniero de Sistemas, deberá implementar los controles necesarios para que los archivos de la **EMPRESA** cuenten con los mecanismos de seguridad, con el fin de proteger y conservar la confidencialidad, integridad y disponibilidad de la información de la **EMPRESA**.

ARTÍCULO OCTAVO. Responsabilidades de los Colaboradores y Contratistas frente al uso de los Recursos Tecnológicos. Todos los Colaboradores y contratistas que hagan uso de los activos de información de la **EMPRESA** tienen la responsabilidad de cumplir las políticas establecidas para su uso aceptable, entendiendo que el uso no adecuado de los recursos pone en riesgo la continuidad de la operación y seguridad de la información.

a. Del Uso del Correo Electrónico: El servicio de correo electrónico empresarial es una herramienta de apoyo a las funciones y responsabilidades de los Colaboradores y contratistas de la **EMPRESA**, con los siguientes lineamientos:

- El servicio de correo electrónico empresarial debe ser empleado únicamente para enviar y recibir mensajes de carácter empresarial. En consecuencia, no puede ser utilizado con fines personales, económicos, comerciales y/o cualquier otro ajeno a los propósitos de la Entidad.
- En cumplimiento de la iniciativa del uso aceptable del papel y la eficiencia administrativa, se debe preferir el uso del correo electrónico al envio de documentos físicos, siempre que la Ley lo permita.
- Los mensajes de correo están respaldados por la Ley 527 de 1999 (por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos,

Autopista Medellín km 19+050 C/S Barrio Santander El Rosal – Cundinamarca
Cel. 3203944148 correo electrónico servicioalcliente@ecoserviciosdeoccidente.com

del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.), la cual establece la legalidad de los mensajes de datos y las implicaciones legales que conlleva el mal uso de estos.

- La Dirección Administrativa junto con Gerencia y el Ingeniero de Sistemas deberán implementar herramientas tecnológicas que prevengan la pérdida o fuga de información de carácter reservada o clasificada.
- Está prohibido el envío de correos masivos (más de 150 destinatarios) sin autorización de Gerencia General.
- Todo mensaje sospechoso respecto de su remitente o contenido debe ser inmediatamente reportado al Ingeniero de Sistemas a través y proceder de acuerdo a las indicaciones remitidas; lo anterior, debido a que puede ser contentivo de virus, en especial si contiene archivos adjuntos con extensiones .exe, bat.prg, .bak, .pif, o tenga explícitas referencias no relacionadas con la misión de la **EMPRESA** (como, por ejemplo: contenidos eróticos, alusiones a personajes famosos).
- La cuenta de correo institucional no debe ser revelada en páginas o sitios publicitarios, de comercio electrónico, deportivos, agencias matrimoniales, casinos, o cualquier otra ajena a los fines de la **EMPRESA**.
- Está expresamente prohibido el uso del correo para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.
- Está expresamente prohibido distribuir información Privada de la **EMPRESA**, a otras empresas o ciudadanos sin la debida autorización del Gerente y/o Director Administrativo.
- El cifrado de los mensajes de correo electrónico empresarial será necesario siempre que la información transmitida esté catalogada como clasificada o reservada en el inventario de activos de información o en el marco de la Ley Colombiana vigente.
- El correo electrónico empresarial en sus mensajes debe contener una sentencia de confidencialidad, que será diseñada por Gerencia, Jurídica y la Dirección Administrativa, y debe reflejarse en todos los buzones con dominio@ecoserviciosdeoccidente.com
- Está expresamente prohibido distribuir, copiar, reenviar información de la **EMPRESA** a través de correos personales o sitios web diferentes a los autorizados en el marco de sus funciones u obligaciones contractuales.
- El único servicio de correo electrónico autorizado para el manejo o transmisión de la información institucional en la **EMPRESA** y que cuenta con el dominio @ecoserviciosdeoccidente.com, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso.

La **EMPRESA** se reserva el derecho de monitorear los accesos y el uso de los buzones de correo institucionales, de todos sus Colaboradores o contratistas, además podrá realizar copias de seguridad en cualquier momento sin previo aviso, así como limitar el acceso temporal o definitivo, por solicitud expresa del Gerente, Subgerente, Director Administrativo, así como a todos los servicios y accesos a sistemas de información de la Entidad o de terceros operados en la **EMPRESA**.

b. Del Uso de Internet: La Gerencia General, establecerá políticas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones, las cuales deberán ser implementadas por el Ingeniero de Sistemas, además, será responsabilidad de los Colaboradores y contratistas entre otras las siguientes: El uso del servicio de Internet está limitado exclusivamente para propósitos laborales y contractuales.

- Los servicios a los que un determinado usuario pueda acceder en internet dependerán del rol, obligaciones contractuales o funciones que desempeña en la **EMPRESA** y para las cuales esté formal y expresamente autorizado.
- Todo usuario es responsable de informar a la Dirección Administrativa, los contenidos o acceso a servicios que no le estén autorizados y/o no correspondan a sus funciones u obligaciones dentro de la **EMPRESA**.
- Está expresamente prohibido el envío, descarga y visualización de páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.
- Está expresamente prohibido el acceso a páginas web, portales, sitios web y aplicaciones web que no hayan sido autorizadas por la **EMPRESA** a través de la política de navegación.
- Está expresamente prohibido el envío y descarga de cualquier tipo de software o archivos de fuentes externas, y de procedencia desconocida.
- Está expresamente prohibida la propagación de virus o cualquier tipo de código malicioso.

La **EMPRESA** se reserva el derecho de monitorear los accesos, y el uso del servicio de internet de todos sus Colaboradores o contratistas, además de limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro ajeno a los fines de la Entidad.

c. Del Uso de los Recursos Tecnológicos: Los recursos tecnológicos de la **EMPRESA** son herramientas de apoyo a las labores, obligaciones y responsabilidades de los Colaboradores y contratistas. Por ello, su uso está sujeto a las siguientes directrices:

- Los bienes de cómputo se emplearán de manera exclusiva y bajo la completa responsabilidad por el Colaborador o contratista al cual han sido asignados, únicamente para el desempeño de las funciones del cargo o las obligaciones contractuales pactadas. Por tanto, no pueden ser utilizados con fines personales o por terceros no autorizados por la Dirección Administrativa.
- Sólo está permitido el uso de software licenciado por la **EMPRESA**.
- En caso de que el colaborador deba hacer uso de equipos ajenos a la **EMPRESA**, estos deberán cumplir con la legalidad del Software instalado, antivirus licenciado,

actualizado y solo podrá conectarse a la red de la EMPRESA una vez esté avalado por los ingenieros de la **EMPRESA**.

- Es responsabilidad de los Colaboradores y contratistas entregar la información contenida en sus estaciones de trabajo a la Dirección Administrativa.
- Los usuarios no deben mantener almacenados en los discos duros de computadores de escritorio, portátiles o discos virtuales de red, archivos de video, música y fotos que no sean de carácter institucional o que atenten con los derechos de autor o propiedad intelectual de los mismos.
- No está permitido fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren elementos tecnológicos o información física que pueda estar expuesta a su daño parcial o total y, por ende, a la pérdida de la integridad de esta.
- No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo los elementos tecnológicos por fallas en el suministro eléctrico a los equipos de cómputo, salvo en aquellos casos que sean autorizados por la Dirección Administrativa.
- Las únicas personas autorizadas para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar y/o reparar sus componentes, son los designados por la Dirección Administrativa para tal labor.
- La Dirección Administrativa realizará monitoreo sobre los dispositivos de almacenamientos externos como USB, CD-ROM, DVD, Discos Duros externos, entre otros, con el fin de prevenir o detectar fuga de información.
- La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro será la Dirección Administrativa o quien este indique.
- La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, deberá ser informada de inmediato a la Dirección Administrativa por el Colaborador o contratista a quien se le hubiere asignado.
- La pérdida de información deberá ser informada con detalle a la Dirección Administrativa y Gerencia General como incidente de seguridad.
- Todo incidente de seguridad que comprometa la disponibilidad, integridad o confidencialidad de la información física o digital deberá ser reportado a la mayor brevedad posible a la Dirección Administrativa y Gerencia General.
- La Dirección Administrativa es la única dependencia autorizada para la administración del software, el cual no deberá ser copiado, suministrado a terceros ni utilizado para fines personales. Todo acceso a la red de la **EMPRESA** mediante elementos o recursos tecnológicos no institucionales deberá ser informado, autorizado y controlado por la Dirección Administrativa.
- La conexión a la red wifi de la **EMPRESA** para Colaboradores deberá ser administrada desde la Dirección Administrativa a través del Ingeniero de Sistemas mediante un SSID (Service Set Identifier) único a nivel nacional, la autenticación deberá ser con una clave única.
- La conexión a la red Empresarial para visitantes deberá tener un SSID y contraseñas diferentes a la de los Colaboradores, administrada por la Dirección

Administrativa a través del Ingeniero de Sistemas; la contraseña deberá cambiar semestralmente y estará disponible las 24 horas diarias.

- No se podrá conectar dispositivos celulares personales a la red wifi de Colaboradores, salvo los aprobados por la Dirección Administrativa.
- Los equipos deben quedar apagados cada vez que el Colaborador o contratista no se encuentre en la oficina o durante la noche, esto, con el fin de proteger la seguridad y distribuir bien los recursos de la **EMPRESA**, siempre y cuando no vaya a realizar actividades vía remota.
- Todo dispositivo móvil empresarial, que transmita y/o almacene información sensible de la Entidad, debe ser monitoreado a través de la herramienta de gestión tecnológica definida por la Dirección de Información y Tecnología.
- Todo dispositivo móvil personal que requiera acceder a los servicios tecnológicos de la **EMPRESA**, y que trasmita y/o almacene información sensible, debe ser monitoreado a través de la herramienta tecnológica definida por la Dirección Administrativa y el Ingeniero de Sistemas.

d. Del Uso de los Sistemas o Herramientas de Información: Todos los Colaboradores y contratistas de la **EMPRESA** son responsables de la protección de la información que acceden y/o procesan, así como de evitar su pérdida, alteración, destrucción y uso indebido, para lo cual se dictan los siguientes lineamientos:

- Las credenciales de acceso a la red y a los recursos informáticos (Usuario y Clave) son de carácter estrictamente personal e intransferible; los Colaboradores y contratistas no deben revelarlas a terceros ni utilizar claves ajenas.
- Todo Colaborador y contratista es responsable del cambio de clave de acceso a los sistemas de información o recursos informáticos periódicamente.
- Todo Colaborador y contratista es responsable de los registros y modificaciones de información que se hagan a nombre de su cuenta de usuario.
- En ausencia del Colaborador o contratista, el acceso a la estación de trabajo le será bloqueada con una solicitud a la Dirección Administrativa, con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad. Talento Humano debe reportar cualquier tipo de novedad de los Colaboradores y el Supervisor del Contrato las novedades de los contratistas.
- Cuando un Colaborador o contratista cesa en sus funciones o culmina la ejecución de contrato con la **EMPRESA**, todos los privilegios sobre los recursos informáticos otorgados le serán suspendidos inmediatamente; la información del Colaborador y/o contratista serán almacenados en un repositorio de los servidores de la Entidad.
- Cuando un Colaborador o contratista cesa en sus funciones o culmina la ejecución de contrato con la **EMPRESA**, el supervisor o jefe inmediato es el encargado de la custodia de los recursos de información, incluyendo la cesión de derechos de propiedad intelectual de acuerdo con la normativa vigente.
- Todos los Colaboradores y contratistas de la **EMPRESA** deben dar estricto cumplimiento a lo estipulado en la Ley 23 de 1982 "Sobre derechos de autor", la

Decisión 351 de 1993 de la Comunidad Andina de Naciones, así como cualquier otra que adicione, modifique o reglamente la materia.

ARTÍCULO NOVENO. Política de Control de Acceso. Los propietarios de los activos de información deben establecer medidas de control de acceso a nivel de red, sistema operativo, sistemas de información, servicios de tecnologías de la información e infraestructura física, con el fin de mitigar riesgos asociados al acceso a la información y servicios de infraestructura tecnológica de personal no autorizado, salvaguardando la integridad, disponibilidad y confidencialidad de la información de la **EMPRESA**.

ARTÍCULO DÉCIMO. Política de Seguridad Física y del Entorno. La **EMPRESA** debe contar con controles para la protección del perímetro de seguridad de las instalaciones físicas, controlar el acceso del personal y la permanencia en las oficinas e instalaciones, así como controlar el acceso a áreas restringidas (áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones), además mitigar los riesgos y amenazas externas y ambientales, con el fin de evitar afectación a la confidencialidad, disponibilidad e integridad de la información de la **EMPRESA**.

PARÁGRAFO 1. Todos los Colaboradores, contratistas y visitantes que se encuentren en las instalaciones físicas de la **EMPRESA** deben estar debidamente identificados, con un documento que acredite su tipo de vinculación, el cual deberá portarse en un lugar visible.

PARÁGRAFO 2. Los visitantes en la **EMPRESA** siempre deben permanecer acompañados por un Colaborador o contratista debidamente identificado

PARÁGRAFO 3. El personal de empresas contratistas que desempeñen funciones de forma permanente en las instalaciones de la **EMPRESA**, debe estar identificado con carné y chalecos o distintivos del Contratista y portar el carné de la ARL.

ARTÍCULO DÉCIMO PRIMERO. Política de Seguridad de las Operaciones. La Dirección Administrativa, a través del Ingeniero de Sistemas, será la encargada de la operación y administración de los recursos tecnológicos que soportan la operación de la **EMPRESA**. Así mismo, velará por la eficiencia de los controles asociados a los recursos tecnológicos protegiendo la confidencialidad, integridad y disponibilidad de la información, así como la de asegurar que los cambios efectuados sobre los recursos tecnológicos, serán controlados y debidamente autorizados. De igual manera, deberá proveer la capacidad de procesamiento requerida en los recursos tecnológicos y los sistemas de información de la **EMPRESA**, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica de acuerdo con el crecimiento de la **EMPRESA**.

La Dirección Administrativa a través del Ingeniero de Sistemas, deberá realizar y mantener copias de seguridad de la información de la **EMPRESA** en medio digital, siempre que ésta sea reportada por el responsable de la misma, con el objetivo de recuperarla en caso de cualquier tipo de falla, ya sea de hardware, software, o de procedimientos operativos al interior de la **EMPRESA**.

ARTÍCULO DÉCIMO SEGUNDO. Política de Seguridad de las Comunicaciones. La Dirección Administrativa a través del Ingeniero de Sistemas, establecerá los mecanismos necesarios para

proveer la disponibilidad de las redes y de los servicios que dependen de ellas, así mismo, dispondrá y monitoreará los mecanismos necesarios de seguridad para proteger la integridad y la confidencialidad de la información de la **EMPRESA**.

PARÁGRAFO 1. Como parte de sus términos y condiciones iniciales de trabajo, los Colaboradores o contratistas, cualquiera sea su nivel jerárquico dentro de la entidad, firmarán un Compromiso de Confidencialidad y no divulgación, en lo que respecta al tratamiento de la información de la **EMPRESA**, y de igual manera la Autorización de tratamiento de datos personales, en los términos de la Ley 1581 de 2012, así como el capítulo 25 del Decreto 1074 de 2015 y la Ley 1712 de 2014 reglamentada por el capítulo 2 del Decreto 1081 de 2015 y las demás normas que las adicionen, modifiquen, reglamenten o complementen. Dicho compromiso y autorización (documento original) deberá ser retenido en forma segura por Talento Humano (Colaboradores), y/o Jurídica, según el caso. Así mismo, mediante el Compromiso de Confidencialidad el Colaborador o el contratista declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad ni los derechos del Colaborador o contratista.

ARTÍCULO DÉCIMO TERCERO. Política de Seguridad para la Adquisición, Desarrollo y Mantenimiento de Sistemas. La Dirección Administrativa a través del Ingeniero de Sistemas, velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad adecuados para la protección de la información de la **EMPRESA**.

La Dirección Administrativa a través del Ingeniero de Sistemas será la única dependencia de la Entidad con la capacidad de adquirir, desarrollar o avalar la adquisición y recepción de software de cualquier tipo, conforme a los requerimientos de las diferentes dependencias, con el fin de garantizar la conveniencia, soporte, mantenimiento y seguridad de la información de los sistemas que operan en la **EMPRESA**.

En consecuencia, cualquier software que opere en la **EMPRESA** y no haya sido entregado a la Dirección Administrativa, no serán responsabilidad de la misma, no se le brindará soporte y no se le salvaguardará la información.

ARTÍCULO DÉCIMO CUARTO. Política de Seguridad para Relación con Proveedores. La **EMPRESA** establecerá mecanismos de control en relaciones con sus proveedores, teniendo en cuenta que se debe asegurar la información a la que tengan acceso, supervisando el cumplimiento de lo establecido en el Eje de seguridad de la información. Los Supervisores de los contratos en conjunto con la Dirección Administrativa, tendrán la responsabilidad de la divulgación y revisión del cumplimiento de las políticas y procedimientos de la seguridad de la información.

ARTÍCULO DÉCIMO QUINTO. Política de Gestión de Incidentes de Seguridad de la Información. La **EMPRESA** promoverá entre los Colaboradores y contratistas el reporte de incidentes relacionados con la seguridad de la información y sus medios, reporte y seguimiento. Así mismo, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, de acuerdo con su criticidad. La Gerencia General o a quien éste delegue, son los únicos autorizados

Autopista Medellín km 19+050 C/S Barrio Santander El Rosal – Cundinamarca
Cel. 3203944148 correo electrónico servicioalcliente@ecoserviciosdeoccidente.com

para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

ARTÍCULO DÉCIMO SEXTO. Política de la Continuidad de la Operación. La **EMPRESA** dispondrá los planes necesarios para la implementación del proceso de continuidad de la operación de los servicios, los cuales serán operados por los líderes de procesos. La Dirección Administrativa liderará la elaboración del Análisis de Impacto al Negocio (BIA) y del Plan de Continuidad de los Servicios, así como la activación de este cuando sea necesario.

ARTÍCULO DÉCIMO SÉPTIMO. Política de Cumplimiento. La **EMPRESA** velará por la identificación, documentación y cumplimiento de los requisitos legales enmarcados en la seguridad de la información del Estado colombiano, entre ella la referente a derechos de autor y propiedad intelectual, protección de datos personales y ley de transparencia.

VIGENCIA DEL MANUAL.

El presente manual rige a partir de su publicación en la página web de Ecoservicios de Occidente.

ACEPTACIÓN DE ESTA POLÍTICA DE PRIVACIDAD

El titular de la información acepta el tratamiento de sus datos personales conforme los términos de esta Política de Tratamiento de Datos Personales, cuando proporciona los datos a través de nuestros canales o puntos de atención o cuando hace uso de cualquiera de estos servicios.

SARA VIVIANA ESPITIA PARRA
Gerente General
ECOSERVICIOS DE OCCIDENTE SAS ESP